概念と用例
ScreenOS リファレンス ガイド

第 1 部 :
概要

リリース 6.0.0、改訂 02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

品番 : 530-017767-01-JP, 改訂 02

Copyright Notice

Copyright © 2007 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

目次

第 1 部 : 概要

概念と用例 ScreenOS リファレンス ガイドについて xlvii

各部の構成 xlix
ドキュメントの規則 lvi
Web ユーザーインターフェースの規則 lvi
コマンドラインインターフェースの規則 lvi
ネーミング規則および文字タイプ lvii
説明図の規則 lviii
技術ドキュメントおよびテクニカルサポート lix

索引 ..... IX-I

第 2 部 : 基本

本編について ix

ドキュメントの規則 x
Web ユーザーインターフェースの規則 x
コマンドラインインターフェースの規則 x
ネーミング規則および文字タイプ xi
説明図の規則 xii
技術ドキュメントおよびテクニカルサポート xiii
..... xiii

第 1 章 ScreenOS アーキテクチャ 1

セキュリティゾーン 2
セキュリティゾーンのインターフェース 3
物理インターフェース 3
サブインターフェース 3
仮想ルーター 4
ポリシー 5
VPN (仮想プライベートネットワーク) 8
仮想システム 10
パケットフローシーケンス 11
ジャンボフレーム 14
ScreenOS アーキテクチャの例 14
例 : (第 1 部) 6 つのゾーンを持つ企業 14
例 : (第 2 部) 6 つのゾーンを持つインターフェース 16
例 : (第 3 部) 2 つのルーティングドメイン 19
例 : (第 4 部) ポリシー 20

第 2 章　ゾーン　25

構成済みゾーンの表示 26
セキュリティゾーン 28
　Global ゾーン 28
　SCREEN オプション 28
トンネルゾーンにトンネルインターフェースをバインドする 29
セキュリティゾーンとトンネルゾーンの構成 30
　ゾーンの作成 30
　ゾーンの変更 31
　ゾーンの削除 32
機能ゾーン 33

第 3 章　インターフェース　35

インターフェースタイプ 35
　論理インターフェース 35
　　物理インターフェース 36
　　ワイヤレスインターフェース 36
　　ブリッジグループインターフェース 36
　　サブインターフェース 37
　　統合インターフェース 37
　　冗長インターフェース 37
　　仮想セキュリティインターフェース 38
　機能ゾーンインターフェース 38
　　管理インターフェース 38
　　高可用性インターフェース 38
　トンネルインターフェース 39
　　トンネルインターフェースの削除 42
インターフェースの表示 43
セキュリティゾーンインターフェースを構成する 45
　インターフェースをセキュリティゾーンにバインドする 45
　インターフェースをセキュリティゾーンからアンバインドする 46
　L3 セキュリティゾーンインターフェースのアドレス設定 47
　　公開 IP アドレス 47
　　非公開 IP アドレス 48
　　インターフェースのアドレスを設定する 48
　インターフェース設定を変更する 49
　ルートシステムにサブインターフェースを作成する 50
　サブインターフェースの削除 51
2 次 IP アドレスを作成する 51
ループバックシステムインターフェース 52
　バックアップインターフェースの構成 53
　　IP トラッキングバックアップインターフェースの構成 53
　　tunnel-if バックアップインターフェースの構成 54
　　ルート監視バックアップインターフェースの構成 57
ループバックインターフェース 58
　ループバックインターフェースを作成する 60
　管理用ループバックインターフェースの設定 60
　ループバックインターフェースでの BGP の設定 60
　ループバックインターフェースでの VSI の設定 61
　ループバックインターフェースをソースインターフェースに設定 61

インターフェース状態の変化 62
物理的接続の監視 64
IP アドレスのトラッキング 64
インターフェース監視 69
2 つのインターフェースの監視 71
インターフェースループの監視 72
セキュリティゾーンの監視 75
ダウン状態のインターフェースとトラフィックフロー 76
出口インターフェースでの障害 77
出口インターフェースでの障害 78

第 4 章 インターフェースモード 81

透過モード 82
ゾーンの設定 83
VLAN ゾーン 83
定義済みのレイヤー 2 ゾーン 83
トラフィックの転送 83
宛先不明のユニキャストの処理方式 84
フラッド方式 85
ARP/Trace-Route 方式 87
管理用の VLAN1 インターフェースの構成 89
透過モードの構成 91
NAT モード 94
インバウンドおよびアウトバウンドの NAT トラフィック 96
インターフェース設定 97
NAT モードの構成 97
Route モード 100
インターフェース設定 101
Route モードの構成 101

第 5 章 ポリシー用ビルディングブロック 105

アドレス 105
アドレスエントリ 106
アドレスの追加 106
アドレスの変更 107
アドレスの削除 107
アドレスグループ 108
アドレスグループを作成する 109
アドレスグループエントリの編集 110
メンバおよびグループの削除 110
サービス 110
定義済みサービス 111
インターネット制御メッセージプロトコル 112
ICMP 不明エラーの処理 114
インターネット関連の定義済みサービス 115
Microsoft リモートプロシージャコールサービス 116
動的ルーティングプロトコル 118
ストリーミングビデオ 118

Sun リモートプロシージャコールサービス 119
セキュリティおよびトンネルサービス 120
IP 関連サービス 120
インスタントメッセージサービス 120
管理サービス 121
メールサービス 122
UNIX サービス 122
その他のサービス 122
顧客サービス 123
顧客サービスの追加 124
顧客サービスの変更 124
顧客サービスの削除 125
サービスタイムアウトの設定 125
サービスタイムアウトの構成とルックアップ 125
考慮事項 126
例 127
ICMP（インターネット制御メッセージプロトコル）
カスタムサービスの削除 128
リモートシェル ALG 129
Sun リモートプロシージャコール (RPC) アプリケーションレイヤー
ゲートウェイ 129
一般的な RPC 呼び出し手順 129
Sun RPC サービスのカスタマイズ 130
Microsoft リモートプロシージャコール ALG のカスタマイズ 130
リアルタイムストリーミングプロトコル（RTSP）アプリケーション
レイヤーゲートウェイ 132
RTSP 要求メソッド 133
RTSP ステータスコード 135
プライベートドメイン内でのメディアサーバーの構成 137
パブリックドメイン内でのメディアサーバーの構成 139
サービスグループ 140
サービスグループを変更する 142
サービスグループを削除する 142
動的 IP プール 143
ポートアドレス変換 144
PAT の DIP Pool を作成する 144
DIP プールの変更 145
スティッキー DIP アドレス 145
異なるサブネットでの DIP の使用 146
ループバックインターフェースでの DIP の使用 151
DIP グループを作成する 155
反復スケジュールの設定 158

第 6 章 ポリシー 161

基本要素 162
3 種類のポリシー 163
地域間ポリシー 163
ゾーン内ポリシー 164
グローバルポリシー 164
ポリシーセットリスト 165

定義済みポリシー 166
ポリシーとルール 166
ポリシーの構成 167
ID 168
ゾーン 168
アドレス 168
サービス 168
アクション 169
アプリケーション 169
名前 170
VPN トンネル 170
L2TP トンネリング 170
徹底監視 (Deep Inspection) 171
ポリシーリストの最上位の配置 171
ソースアドレス変換 171
宛先アドレス変換 172
ユーザー認証 172
HA セッションバックアップ 174
Web フィルタリング 174
ロギング 174
カウンティング 174
トラフィックアラームしきい値 174
スケジュール 175
ウィルス対策スキャン 175
トラフィックシェーピング 175
適用されるポリシー 177
ポリシーの閲覧 177
ポリシーの作成 177
ゾーン間ポリシーメールサービスの作成 177
ゾーン間ポリシー群の作成 180
ゾーン内ポリシーの作成 185
グローバルポリシーの作成 186
ポリシーの内容の入力 187
ポリシーコンポーネントごとの複数の項目 187
アドレス否定の設定 188
ポリシーの変更と使用不可 191
ポリシーの検証 192
ポリシーの再順序付け 193
ポリシーの削除 194

第 7 章　トラフィックシェーピング　195

ポリシーレベルでの帯域幅管理 196
トラフィックシェーピングの設定 197
サービス優先順位の設定 200
優先順位キューの設定 201
ingress ポリシング 205
仮想インターフェースのトラフィックシェーピング 206
インターフェースレベルのトラフィックシェーピング 206
ポリシーレベルのトラフィックシェーピング 208
パケットフロー 208
例 : ingress ポリシングのあるルートベースの VPN 209
例 : ingress ポリシングのあるルートベースの VPN 212
ループバックインターフェースを使用したトラフィックシェーピング 216
DSCP マーキングとシェーピング 216

第 8 章 システムパラメータ 219

ドメイン名システムサポート 219
DNS ルックアップ 220
DNS 状況テーブル 221
DNS サーバーとリフレッシュスケジュールの設定 222
DNS リフレッシュ間隔の設定 222
動的ドメイン名システム 223
DynDNS サーバー用の DDNS の設定 223
Setting Up DDNS for a DDO Server 224
プロキシ DNS アドレスの分割 225
動的ホスト構成プロトコル 227
DHCP サーバーの構成 228
DHCP サーバーオプションのカスタマイズ 232
NSRP クラスタの DHCP サーバーの配置 233
DHCP サーバー検出 233
DHCP サーバー検出の有効化 234
DHCP サーバー検出の無効化 234
DHCP リレーエージェントとしてのセキュリティデバイスの割り当て....235
すべての DHCP パケットの転送 239
Next-Server-IP の構成 240
セキュリティデバイスを DHCP クライアントとして使用 241
TCP/IP 設定の伝播 243
仮想システムの DHCP の構成 245
仮想システムの DHCP メッセージリレーの設定 246
Point-to-Point Protocol over Ethernet 246
PPPoE の設定 247
1 次およびバックアップ Untrust インターフェースに PPPoE を構成する....250
単一インターフェースでの複数の PPPoE セッションの構成....250
PPPoE と高可用性....253
ライセンスキー 254
ライセンスサービスの登録およびアクティブ化....255
トライアルサービス 255
サブスクリプションキーの更新 256
既存または新しいデバイスへのアンチウィルス、Web フィルタリング、アンチスパム、徹底監視の追加....256
システムクロック 257
日付および時刻....257
夏時間 257
タイムゾーン 258
ネットワークタイムプロトコル 258
複数の NTP サーバーの構成....258
バックアップ NTP サーバーの構成 258
最大時間調整....259
NTP および NSRP 260
NTP サーバーへの最大時間調整値の設定 260
セキュア NTP サーバー 260

索引 ....IX-I

第 3 部 : 管理

本編について vii

ドキュメントの規則 ... vii
Web ユーザーインターフェースの規則 ... vii
コマンドラインインターフェースの規則 ... viii
ネーミング規則および文字タイプ ... viii
説明図の規則 ... ix
技術ドキュメンおよびテクニカルサポート ... x

第 1 章 管理 1

Web ユーザーインターフェースからの管理 ... 1
WebUI ヘルプ ... 2
ローカルドライブにヘルプファイルをコピーする ... 2
WebUI を新しいヘルプ位置にポイントさせる ... 3
HTTP（ハイパーテキスト転送プロトコル） ... 3
セッション ID ... 4
セキュアソケットレイヤー ... 5
SSL の構成 ... 6
HTTP を SSL に転送する ... 8
コマンドラインインターフェースからの管理 ... 9
Telnet ... 9
Telnet 接続を保護する ... 10
セキュアシェル ... 11
クライアント要件 ... 12
デバイス上の基本的な SSH 構成 ... 13
認証 ... 14
SSH と Vsys ... 16
ホスト鍵 ... 16
例 : SSHv1 で PKA を使用して自動ログインする ... 17
セキュアコピー ... 18
Serial Console ... 19
リモートコンソール ... 20
V.92 モデムポートを使用するリモートコンソール ... 20
AUX ポートを使用するリモートコンソール ... 21
モデムポート ... 22
NetScreen-Security Manager からの管理 ... 22
NSM エージェントと MGT システムの接続の開始 ... 23
NSM エージェントを使用可能、使用不可、設定解除する ... 24
管理システムのプライマリ サーバーの IP アドレスの設定 ... 25
アラームおよび統計データ レポートの設定 ... 25
構成同期化 ... 26
例 : 構成状態を表示する ... 26
例 : 構成ハッシュを取得する ... 27
構成タイムスタンプを取得する ... 27
管理トラフィックのコントロール ... 28
MGT および VLAN1 インターフェース ... 29
例 : MGT インターフェースによる管理 ... 29
例 : VLAN1 インターフェースを介した管理 ... 29
管理インターフェースオプションの設定 ... 30
複数のインターフェースに対して管理 IP を設定する ... 31

管理レベル 33
ルート管理者 33
読取 / 書込管理者 34
読取専用管理者 34
仮想システム管理者 34
仮想システム読取専用管理者 35
管理ユーザーの定義 35
例 : 読取専用管理者を追加する 35
例 : 管理者を変更する 35
例 : 管理者を削除する 36
例 : ダイアルアップ接続用の管理者アカウントを構成する 36
例 : 管理者のセッションを消去する 37
セキュアな管理トラフィック 37
ポート番号を変更する 38
管理者ログイン名およびパスワードを変更する 39
例 : 管理ユーザーのログイン名およびパスワードを変更する 40
例 : ユーザー自身のパスワードを変更する 40
ルート管理者パスワードの最小文字数を設定する 41
デバイスのデフォルト設定へのリセット 41
管理者アクセスを制限する 42
例 : 管理を 1 つのワークステーションに制限する 42
例 : 管理を特定のサブネットに制限する 42
ルート管理者をコンソールアクセスに制限する 42
管理トラフィックの VPN トンネル 43
ルートベース手動鍵 VPN トンネルを介した管理 44
ポリシーベース手動鍵 VPN トンネルを介した管理 47
パスワードポリシー 51
パスワードポリシーを設定する 51
パスワードポリシーを削除する 52
パスワードポリシーを表示する 52
拒否されたデフォルトの管理者パスワードからの回復 52
ログインバナーの作成 53

第 2 章 セキュリティ デバイスの監視 55

ログ情報の保存 55
イベントログ 57
重大度とキーワードでイベントログを参照する 58
イベントログのソーティングとフィルタリング 59
イベントログのダウンロード 60
例 : イベント ログ全体をダウンロードする 60
例 : クリティカルイベントのイベントログをダウンロードする 60
トラフィックログ 61
トラフィックログの参照 62
例 : トラフィックログのエントリを参照する 62
トラフィックログのソーティングとフィルタリング 63
例 : 時刻でトラフィックログをソーティングする 63
トラフィックログのダウンロード 64
終了の理由フィールドを削除する 64
自己ログ 66
自己ログの参照 67
自己ログのソーティングとフィルタリング 67
例 : 自己ログを時刻でフィルタリングする 67
自己ログのダウンロード 68
リカバリ ログのダウンロード 68

トラフィック警告 69
例 : ポリシーベースの侵入試行を検出する 69
例 : システム妥協通知をする 70
例 : E メール警報を送信する 71
Syslog 72
例 : 複数の Syslog サーバーを使用可能にする 72
WebTrends を通知イベントで有効にする 73
簡易ネットワーク管理プロトコル 74
インプリメンテーションの概要 76
読取 / 書込 SNMP コミュニティを定義する 77
自己開始トラフィックの VPN トンネル 78
例 : ルートベースのトンネルを経由する自己生成のトラフィック 79
例 : ポリシーベースのトンネルを経由する自己生成のトラフィック 86
Screen カウンタを参照する 93

索引 ..... IX-I

第 4 部 : 攻撃の検出と防衛機能

本編について ix

ドキュメントの規則 x
Web ユーザーインターフェースの規則 x
コマンドラインインターフェースの規則 xi
ネーミング規則および文字タイプ xi
説明図の規則 xii
技術ドキュメントおよびテクニカルサポート xiii

第 1 章 ネットワークの保護 1

攻撃の段階 2
検出と防衛機能 2
攻略の監視 5
例 : Untrust ゾーンからの攻撃を監視する 5

第 2 章 偵察阻止 7

IP アドレススイープ 7
ポートスキャン 9
IP オプションを使用したネットワーク偵察 10
オペレーティングシステム探査 12
SYN および FIN フラグセット 12
ACK フラグのない FIN フラグ 13
フラグが設定されていない TCP ヘッダー 14
回避技法 15
FIN スキャン 15
非 SYN フラグ 16
IP スプーフィング 19
例 : L3 IP スプーフィング保護 21
例 : L2 IP スプーフィング保護 23
IP スプーフィング保護 24

第 3 章　サービス拒否 (DoS) 攻撃の防御　29

ファイアウォール DoS 攻撃 30
セッションテーブルフラッド 30
ソースベースおよび宛先ベースセッション制限 30
例 : ソースベースのセッション制限 32
例 : 宛先ベースのセッション制限 32
アグレッシブエージング 33
例 : アグレッシブにエージアウトするセッション 34
SYN-ACK-ACK プロキシフラッド 34
ネットワーク DoS 攻撃 36
SYN フラッド 36
例 : SYN フラッド保護 42
SYN クッキー 47
ICMP フラッド 49
UDP フラッド 50
ランド攻撃 51
OS 指定 DoS 攻撃 52
Ping of Death 52
ティアドロップ攻撃 53
WinNuke 54

第 4 章　コンテンツの監視とフィルタリング　57

フラグメントの再アセンブリ 58
不正な URL からの保護 58
アプリケーションレイヤーゲートウェイ 59
例 : パケットフラグメント内の不正な URL をブロックする 60
ウィルス対策スキャン 62
外部 AV スキャン 62
スキャンモード 63
ロードバランスを行う ICAP サーバー 64
内部 AV スキャン 64
IM トラフィックの AV スキャン 66
IM クライアント 66
IM サーバー 66
IM プロトコル 67
インスタントメッセージのセキュリティの問題 67
IM のセキュリティ上の問題 68
チャットメッセージのスキャン 68
ファイル転送のスキャン 68
AV スキャンの結果 69
ポリシーベースの AV スキャン 70
アプリケーションプロトコルのスキャン 71
FTP トラフィックのスキャン 72
HTTP トラフィックのスキャン 73
IMAP/POP3 トラフィックのスキャン 75
SMTP トラフィックのスキャン 77
トラフィックを ICAP AV スキャンサーバーに転送 79
内蔵スキャナの AV パターンファイルの更新 80
AV 署名サービスの利用契約 80

AV パターンファイルの更新 81
AV スキャナのグローバル設定 83
AV リソースの配分 83
故障モードの動作 83
最大コンテンツ容量と最大メッセージ数（内部 AV スキャンのみ） 84
HTTP キープアライブ 85
HTTP トリックリング（内部 AV スキャンのみ） 85
AV プロファイル 87
AV プロファイルを既存のファイアウォールポリシーに割り当て 88
内部 AV 用の AV プロファイルの起動 88
例 : (内部 AV) あらゆる種類のトラフィックのスキャンの設定 89
例 : SMTP および HTTP トラフィックのみの AV スキャン 89
AV プロファイル設定 90
スパム対策フィルタリング 94
ブラックリストとホワイトリスト 95
基本構成 95
スパムトラフィックのフィルタリング 95
スパムメッセージのドロップ 96
ブラックリストの定義 96
ホワイトリストの定義 96
デフォルトアクションの定義 97
スパムブロッキングリストサーバーを使用可能に設定 97
スパム対策のテスト 98
Web フィルタリング 98
CLI で Web フィルタリングモードを開始 99
統合型 Web フィルタリング 99
SurfControl サーバー 100
Web フィルタリングキャッシュ 101
統合型 Web フィルタリングの構成 101
例 : 統合型 Web フィルタリング 107
Web フィルタリングの転送 108
仮想システムサポート 110
転送型 Web フィルタリングの構成 111
例 : Web フィルタリングの転送 114

第 5 章　徹底監視 (Deep Inspection)　117

概要 118
攻撃オブジェクトデータベースサーバー 122
定義済みのシグネチャパッケージ 122
シグネチャパッケージの更新 123
攻撃オブジェクトの更新を始める前に 124
即時更新 124
自動更新 125
自動通知と即時更新 126
手動更新 128
攻撃オブジェクトとグループ 130
サポートされているプロトコル 131
ステートフル署名 135
TCP ストリームシグネチャ 136
プロトコルアノーマリ (プロトコル異常) 136
攻撃オブジェクトグループ 137
重大度レベルの変更 137
例 : P2P の徹底監視 138
攻撃オブジェクトの無効化 140

攻撃アクション 141
例 : 攻撃アクション ー Close Server、Close、Close Client 142
ブルートフォース攻撃アクション 149
ブルートフォース攻撃オブジェクト 149
ブルートフォース攻撃ターゲット 150
ブルートフォース攻撃のタイムアウト 150
例 1 151
例 2 151
例 3 151
攻撃のログ出力 152
例 : 攻撃グループごとにログ出力を無効化 152
顧客サービスとアプリケーションのマッピング 154
例 : アプリケーションと顧客サービスのマッピング 155
例 : HTTP を悪用する攻撃に関するアプリケーションとサービスの対応づけ 157
カスタマイズした攻撃オブジェクトとグループ 158
ユーザー定義のステートフルシグネチャ攻撃オブジェクト 158
正規表現 159
例 : ユーザー定義のステートフル署名攻撃オブジェクト 160
TCP ストリームシグネチャ攻撃オブジェクト 162
例 : ユーザー定義のストリームシグネチャ攻撃オブジェクト 163
プロトコルアノーマリパラメータの構成 164
例 : パラメータの変更 165
否定 165
例 : 攻撃オブジェクトの否定 166
HTTP コンポーネントの細分ブロッキング 170
ActiveX コントロール 170
Java アプレット 171
EXE ファイル 171
ZIP ファイル 171
例 : Java アプレットと .exe ファイルのブロッキング 171

第 6 章 侵入探知と阻止 173

IDP 対応のセキュリティデバイス 174
IDP 対応デバイスでのトラフィックフロー 175
侵入探知と阻止の構成 176
構成の前に 176
例 1: IDP の基本構成 177
例 2: アクティブ / パッシブフェールオーバー向けの IDP の構成 180
例 3: アクティブ / アクティブフェールオーバー向けの IDP の構成 182
セキュリティポリシーの構成 184
セキュリティポリシーについて 184
セキュリティポリシーの管理 184
セキュリティポリシーのインストール 185
IDP ルールベースの使用 185
IDP ルールベースの役割ベースの管理 186
オブジェクトの IDP ルール向け構成 186
セキュリティポリシーテンプレートの使用 187
ファイアウォールルールで IDP を使用可能にする 187
IDP を使用可能にする 188
インラインモードまたはインラインタップモードの指定 188

IDP ルールの構成 189
IDP ルールベースの追加 190
トラフィックとのマッチング 191
ソースゾーンおよび宛先ゾーン 191
ソースおよび宛先アドレスオブジェクト 192
例 : ソースと宛先の設定 192
例 : 複数のソースおよび宛先の設定 192
Services 193
例 : デフォルトサービスの設定 193
例 : 特定のサービスの設定 194
例 : 非標準サービスの設定 194
ターミナルルール 195
例 : ターミナルルールの設定 196
アクションの定義 197
攻撃オブジェクトの設定 198
攻撃オブジェクトを個別に追加する 198
攻撃オブジェクトのカテゴリ別の追加 198
例 : 攻撃オブジェクトのサービス別の追加 198
攻撃オブジェクトのオペレーティングシステム別の追加 199
重大度別攻撃オブジェクトの追加 199
IP アクションの設定 200
IP アクションの選択 200
ブロッキングオプションの選択 200
ロギングオプションの設定 201
タイムアウトオプションの設定 201
通知の設定 201
ロギングの設定 201
警報の設定 201
パケットのロギング 201
重大度の構成 202
ターゲットの設定 202
コメントの入力 202
免除ルールの構成 202
免除ルールベースの追加 203
一致の定義 204
ソースゾーンおよび宛先ゾーン 204
ソースおよび宛先アドレスオブジェクト 205
例 : ソース / 宛先ペアの免除 205
攻撃オブジェクトの設定 205
例 : 特定の攻撃オブジェクトの免除 205
ターゲットの設定 206
コメントの入力 206
ログビューアから免除ルールを作成 206
バックドアルールの構成 207
バックドアルールベースの追加 208
一致の定義 209
ソースゾーンおよび宛先ゾーン 209
ソースおよび宛先アドレスオブジェクト 209
Services 210
操作の設定 210
アクションの設定 210

バックドアルールの構成（続き）
通知の設定 210
ロギングの設定 210
警報の設定 211
パケットのロギング 211
重大度の構成 211
ターゲットの設定 211
コメントの入力 212
IDP 攻撃オブジェクトの構成 212
IDP 攻撃オブジェクトのタイプ 212
シグネチャ攻撃オブジェクト 212
プロトコルアノーマリ攻撃オブジェクト 213
複合攻撃オブジェクト 213
定義済み IDP 攻撃オブジェクトおよびグループの表示 213
定義済み攻撃の表示 213
定義済みグループの表示 214
カスタム IDP 攻撃オブジェクトの作成 215
シグネチャ攻撃オブジェクトの作成 217
プロトコルアノーマリ攻撃の作成 222
複合攻撃の作成 223
カスタム攻撃オブジェクトの編集 225
カスタム攻撃オブジェクトの削除 226
カスタム IDP 攻撃グループの作成 226
静的グループの構成 226
動的グループの構成 227
例 : 動的グループの作成 228
動的グループの更新 230
カスタム攻撃グループの編集 230
カスタム攻撃グループの削除 230
デバイスをスタンドアロンの IDP デバイスとして構成する 230
IDP を使用可能にする 231
例 : スタンドアロンの IDP 用のファイアウォールルールの構成 ... 231
役割ベースの管理の構成 232
例 : IDP 専用管理者の構成 232
IDP の管理 234
攻撃データベース更新 234
攻撃データベース更新のダウンロード 234
更新された攻撃オブジェクトの使用 234
IDP エンジンの更新 235
IDP ログの表示 237

第 7 章　不審なパケット属性　239

ICMP フラグメント 240
ラージ ICMP パケット 241
不良 IP オプション 242
不明のプロトコル 243
IP パケットフラグメント 244
SYN (周期) フラグメント 245

付録 A　ユーザー定義シグネチャのコンテキスト　A-I

索引 ..... IX-I

第 5 部 :
仮想プライベート ネットワーク

本編について vii

ドキュメントの規則 ... viii
Web ユーザーインターフェースの規則 ... viii
コマンドラインインターフェースの規則 ... viii
ネーミング規則および文字タイプ ... ix
説明図の規則 ... x
技術ドキュメントおよびテクニカルサポート ... xi

第 1 章 インターネットプロトコルセキュリティ 1

VPN (仮想プライベートネットワーク) の紹介 ... 2
IPSec の概念 ... 3
モード ... 4
トランスポートモード ... 4
トンネルモード ... 4
プロトコル ... 6
認証ヘッダー ... 6
セキュリティペイロードのカプセル化 ... 6
鍵管理 ... 7
手動鍵 ... 7
AutoKey IKE ... 7
セキュリティアソシエーション ... 8
トンネルネゴシエーション ... 8
フェーズ 1 ... 9
メインモードとアグレッシブモード ... 9
Diffie-Hellman の鍵交換 ... 10
フェーズ 2 ... 11
完全転送機密保持 ... 11
再生保護 ... 12
IKE および IPSec パケット ... 12
IKE パケット ... 12
IPSec パケット ... 15

第 2 章 公開鍵暗号化 19

公開鍵暗号化序論 ... 20
証明書を署名する ... 20
デジタル署名を確認する ... 20
公開鍵基盤 ... 22
証明書および CRL ... 24
証明書を手動で要求する ... 25
証明書と CRL をロードする ... 28
CRL 設定を構成する ... 29
ローカル証明を自動で取得する ... 30
証明書の自動更新 ... 33
鍵ペアの生成 ... 33
OCSP (オンライン証明書ステータスプロトコル) ... 34
証明書取り消しチェック方法を指定する ... 35
ステータスチェック属性を表示する ... 35
オンライン証明書ステータスプロトコルレスポンダ URL を指定する ... 35
ステータスチェック属性を削除する ... 35

自己署名証明書 36
証明書の検証 37
自己署名証明書の手動作成 38
管理者定義の自己署名証明書を設定する 39
証明書の自動生成 42
自己署名証明書の削除 43

第 3 章 VPN (仮想プライベートネットワーク) のガイドライン 45

暗号オプション 46
サイトツーサイトの暗号オプション 46
ダイヤルアップ VPN オプション 53
ルートベーストンネルおよびポリシーベーストンネル 59
パケットフロー : サイトツーサイト VPN 61
トンネル構成のガイド 66
ルートベース VPN (仮想プライベートネットワーク) のセキュリティ検討事項 68
Null ルート 69
ダイヤルアップまたはリース回線 70
リース回線または Null ルートへの VPN フェールオーバー 71
おとりトンネルインターフェース 74
トンネルインターフェースの仮想ルーター 74
別のトンネルへの再ルーティング 75

第 4 章 サイト間 VPN (仮想プライベートネットワーク) 77

サイト間 VPN 構成 78
ルートベースのサイト間 VPN、AutoKey IKE 84
ポリシーベースのサイト間 VPN、AutoKey IKE 93
ルートベースのサイト間 VPN、動的ピア 99
ポリシーベースのサイト間 VPN、動的ピア 107
ルートベースのサイト間 VPN、手動鍵 116
ポリシーベースのサイト間 VPN、手動鍵 122
FQDN を使用した動的 IKE ゲートウェイ 127
エイリアス 128
FQDN を使用した AutoKey IKE ピアを設定する 129
アドレスがオーバーラップする VPN サイト 137
透過モード VPN 148

第 5 章 ダイヤルアップ仮想プライベートネットワーク 157

ダイヤルアップ 158
ポリシーベース ダイヤルアップ VPN、AutoKey IKE 159
ルートベース ダイヤルアップ VPN、動的ピア 164
ポリシーベース ダイヤルアップ VPN、動的ピア 171
ダイヤルアップ VPN ユーザー用の双方向性ポリシー 177
グループ IKE ID 182
証明書付きグループ IKE ID 182
ワイルドカードおよびコンテナ ASN1-DN IKE ID タイプ 184
グループ IKE ID（証明書）の作成 187
事前共有鍵を使用するグループ IKE ID の設定 191
共有 IKE ID 197

第 6 章　レイヤー 2 トンネリングプロトコル　205

L2TP について 205
パケットのカプセル化と脱カプセル化 208
　カプセル化 208
　脱カプセル化 209
L2TP パラメータの設定 211
L2TP と L2TP-Over-IPSec 213
　L2TP 構成 213
　L2TP-over-IPSec を構成する 218
　双方向の L2TP-over-IPSec 226

第 7 章　高度な仮想プライベート ネットワーク機能　233

NAT-Traversal 234
　NAT の精査 235
　NAT デバイスのトラバース 237
　UDP チェックサム 239
　キープアライブパケット 240
　イニシエータ / 受信側シンメトリー 240
　NAT-Traversal を使用可能にする 241
　NAT-Traversal との IKE ID の使用 242
VPN の監視 243
　再入力および最適化オプション 244
　ソースインターフェースおよび宛先アドレス 245
　ポリシー考慮事項 246
　VPN 監視機能の構成 247
　SNMP VPN 監視オブジェクトおよびトラップ 255
1 つのトンネルインターフェースに対する複数のトンネル 256
　ルートからトンネルへのマッピング 257
　リモートピアのアドレス 259
　手動および自動テーブルエントリ 260
　　手動テーブル入力 260
　　自動テーブル入力 261
　　オーバーラップするサブネットに対応する 1 つのトンネル インターフェースでの VPN の設定 262
　　自動ルートおよび NHTB テーブル エントリのバインディング 281
　　自動ルー テーブル エントリでの OSPF の使用方法 292
冗長 VPN ゲートウェイ 294
　VPN グループ 295
　監視機構 296
　　IKE ハートビート 296
　　DPD（デッド ピア検出） 297
　　IKE 復旧手順 298
　TCP SYN-Flag チェック 300
　　冗長 VPN ゲートウェイの作成 300
VPN 対向の作成 306
ハブアンドスポーク方式 VPN の作成 313

第 8 章　AutoConnect 仮想プライベートネットワーク　323

概要 323

機能 324
NHRP メッセージ 324
ACVPN トンネルの開始 326
AC-VPN の構成 327
ネットワークアドレス変換 327
ハブでの構成 327
各スポークでの構成 328
例 328

索引 ..... IX-I

第 6 部 : 音声 IP 化

本編について vii

ドキュメントの規則 vii
Web ユーザーインターフェースの規則 viii
コマンドラインインターフェースの規則 viii
ネーミング規則および文字タイプ ix
説明図の規則 x
技術ドキュメントおよびテクニカルサポート xi

第 1 章 H.323 アプリケーションレイヤー ゲートウェイ 1

概要 1
例 2
例 : Trust ゾーンのゲートキーパー 2
例 : Untrust ゾーンのゲートキーパー 3
例 : NAT での発信コール 5
例 : NAT での受信コール 8
例 : NAT での Untrust ゾーン内のゲートキーパー 10

第 2 章 セッション起動プロトコル アプリケーション レイヤーゲートウェイ 13

概要 13
SIP 要求方法 14
SIP 応答のクラス 16
SIP アプリケーションレイヤーゲートウェイ 17
セッション記述プロトコルのセッション 18
ピンホールの作成 19
セッション無活動タイムアウト 21
SIP 攻撃保護 21
例 : SIP 保護拒否 22
例 : シグナリングおよびメディア無活動タイムアウト 22
例 : UDP フラッディング保護 22
例 : SIP 接続の最大数 23

ネットワークアドレス変換での SIP 23
出力コール 24
受信コール 24
転送されたコール 25
コールの終了 25
コールの Re-INVITE メッセージ 25
コールセッションタイマー 26
コールのキャンセル 26
フォーク 26
SIP メッセージ 26
SIP ヘッダー 27
SIP ボディ 28
SIP NAT の手順 29
例 31
SIP Registrar を使用する受信 SIP コールのサポート 32
例 : 受信コール (インターフェース DIP) 33
例 : 受信コール (DIP プール) 36
例 : MIP での受信コール 38
例 : プライベートゾーン内のプロキシ 40
例 : パブリックゾーン内のプロキシ 43
例 : 3 つのゾーン、DMZ 内のプロキシ 45
例 : Untrust ゾーン内 48
例 : Trust ゾーン内 52
例 : フルメッシュ VPN での SIP 54
VoIP サービスの帯域幅管理 63

第 3 章 メディアゲートウェイ制御プロトコルのアプリケーションレイヤーゲートウェイ 67

概要 67
MGCP セキュリティ 68
MGCP について 69
MGCP 内のエンティティ 69
端点 69
接続 69
コール 69
コールエージェント 70
コマンド 70
応答コード 73
例 74
加入者の自宅におけるメディアゲートウェイ - ISP でのコールエージェント 74
ISP ホストサービス 76

第 4 章 スキニィクライアント制御プロトコルのアプリケーションレイヤーゲートウェイ 81

概要 81
SCCP セキュリティ 82

SCCP について 82
SCCP のコンポーネント 83
SCCP クライアント 83
コールマネージャ 83
クラスタ 83
SCCP トランザクション 84
クライアントの初期化 84
クライアント登録 84
コールの設定 85
メディアの設定 85
SCCP 制御メッセージと RTP フロー 86
SCCP メッセージ 87
例 88
例 : Trust ゾーンのコールマネージャ /TFTP サーバー 88
例 : Untrust ゾーン内のコールマネージャ /TFTP サーバー 90
例 : 3 ゾーン、DMZ 内のコールマネージャ /TFTP サーバー 92
例 : ゾーン内、Trust ゾーンのコールマネージャ /TFTP サーバー 96
例 : ゾーン内、Untrust ゾーンのコールマネージャ /TFTP サーバー 99
例 : フルメッシュ VPN での SCCP 102

索引 ..... IX-I

第 7 部 : ルーティング

本編について **ix**

ドキュメントの規則 x
Web ユーザーインターフェースの規則 x
コマンドラインインターフェースの規則 x
ネーミング規則および文字タイプ xi
説明図の規則 xii
技術ドキュメントおよびテクニカルサポート xiii

第 1 章 静的ルーティング **1**

概要 1
静的ルートのしくみ 2
静的ルートを構成するとき 3
静的ルートの構成 5
静的ルートの設定 5
トンネルインターフェースに静的ルートを設定する 9
ゲートウェイトラッキングを使用可能にする 10
Null インターフェースへトラフィックを転送する 11
他のルーティングテーブルのルートルックアップを防ぐ 11
トンネルトラフィックが非トンネルインターフェース上に送信されることを防ぐ 11
ルートの要約により生じたループを防ぐ 12
永続アクティブルート 12
等価コストマルチパスのルーティング優先度の変更 13

第 2 章 ルーティング 15

概要 16
仮想ルータールーティングテーブル 17
宛先ベースのルーティングテーブル 18
ソースベースのルーティングテーブル 19
ソースのインターフェースベースのルーティングテーブル 22
仮想ルーターの作成と変更 24
仮想ルーターの設定変更 24
仮想ルーター ID を割り当てる 25
仮想ルーター間でトラフィックを転送する 26
2 つの仮想ルーターの設定 26
仮想ルーターの作成と削除 28
カスタム仮想ルーターを作成する 28
カスタム仮想ルーターを削除する 29
仮想ルーターと仮想システム 29
Vsys 上に仮想ルーターを作成する 30
仮想ルーター間の共有ルート 31
ルーティングテーブルの最大ルート情報数 32
ルーティング機能および例 32
ルートの選択 32
ルートの優先度値を設定する 33
ルートのメトリック 34
デフォルトのルートルックアップ順序の変更 34
複数の仮想ルーターにおけるルートルックアップ 36
等価コストマルチパスルーティングの構成 38
ルート情報の再配布 40
ルートマップの設定 40
ルートのフィルタリング 42
アクセスリストの構成 43
ルート情報を OSPF に再配布 43
仮想ルーター間でルート情報をエクスポート / インポート 45
エクスポート規則を設定する 45
自動エクスポートを設定する 46

第 3 章 オープンショーテストパスファースト (OSPF) 49

概要 50
エリア 50
ルーターの分類 51
Hello プロトコル 51
ネットワークタイプ 52
ブロードキャストネットワーク 52
ポイントツーポイントネットワーク 52
ポイントツーマルチポイントネットワーク 52
接続状態の通知 53
OSPF の基本設定 53
OSPF ルーティングインスタンスの作成と削除 54
OSPF インスタンスを作成する 54
OSPF インスタンスを削除する 55
OSPF エリアの作成および削除 55
OSPF エリアを作成する 56
OSPF エリアの削除 56

OSPF の基本設定（続き）
OSPF エリアにインターフェースを割り当て 57
エリアにインターフェースを割り当てる 57
エリア範囲の設定 57
インターフェース上で OSPF を稼動 58
インターフェース上で OSPF を稼動 58
インターフェース上の OSPF を停止する 58
設定内容の確認 59
ルーティングプロトコルへのルート情報の再配布 60
再配布されたルート情報の要約 61
再配布されたルート情報の要約 61
OSPF に関する大域パラメータ 62
デフォルトルートの通知 63
仮想リンク 63
仮想リンクの作成 64
仮想リンクの自動作成 65
インターフェースごとの OSPF パラメータ 66
セキュリティ構成 68
接続デバイスを認証する 68
クリアテキストパスワードを設定する 68
MD5 パスワードを設定する 68
OSPF 隣接ノードリストの設定 69
デフォルトルートを拒否する 70
フラッディングの回避 70
Hello しきい値を構成する 70
LSA しきい値を構成する 71
フラッディングを省略する設定 71
トンネルインターフェースについて、要求回路を作成する 71
ポイントツーマルチポイントトンネルインターフェース 72
OSPF リンクタイプの設定 73
Route-deny 機能の無効化 73
ポイントツーマルチポイントネットワークの作成 73

第 4 章　ルーティング情報プロトコル (RIP)　77

概要 78
RIP の基本設定 79
RIP インスタンスの作成と削除 80
RIP インスタンスの作成 80
RIP インスタンスの削除 80
RIP をインターフェースで使用可能・不可にする 81
インターフェース上の RIP を有効にする 81
インターフェース上の RIP を停止する 81
ルートの再配布 81
RIP 情報の表示 83
RIP データベースの表示 83
RIP 詳細の表示 84
RIP 隣接情報の表示 85
特定のインターフェースの RIP 詳細の表示 86
RIP に関する大域パラメータ 87
デフォルトルートの通知 88
RIP インターフェースパラメータの構成 89

セキュリティ構成 90
パスワードを設定して隣接ノードを認証する 90
Trusted 隣接ノードを構成する 91
デフォルトルートを拒否する 92
フラッディングの回避 92
アップデートしきい値を構成する 93
トンネルインターフェース上で RIP を稼動させる 93
オプションの RIP 構成 94
RIP バージョンの構成 94
プレフィックスサマリを使用不可・可能にする 96
プレフィックスサマリを有効にする 96
プレフィックスサマリを使用不可にする 97
代替ルートを設定する 97
トンネルインターフェースの要求回路 99
静的隣接ノードの構成 100
ポイントツーマルチポイントトンネルインターフェースの構成 100

第 5 章 境界ゲートウェイプロトコル 107

概要 108
BGP メッセージのタイプ 108
パス属性 109
外部および内部 BGP 109
基本的な BGP 構成 110
BGP インスタンスを作成して使用可能にする 111
BGP ルーティングインスタンスを作成する 111
BGP インスタンスを削除する 112
BGP をインターフェースで使用可能・不可にする 112
BGP をインターフェースで使用可能にする 112
BGP をインターフェースで使用不可にする 112
BGP ピアおよびピアグループの構成 113
BGP ピアを構成する 114
IBGP ピアグループを構成する 114
BGP 構成を確認する 116
セキュリティ構成 117
BGP 近隣ノードを認証する 117
デフォルトルートを拒否する 118
オプションの BGP 構成 118
ルートを BGP へ再配布する 120
AS-Path アクセスリストの構成 120
BGP にルートを追加 121
条件付きルートアドバタイズメント 122
ルートの重みの設定 122
ルート属性の設定 123
Route-Refresh 機能 123
インバウンドルーティングテーブルアップデートの要求 124
アウトバウンドルーティングテーブルアップデートの要求 124
ルートリフレクションを構成する 125
コンフェデレーションの構成 127
BGP コミュニティ 128
ルートの集約 129
異なる AS-Path のルートを集約 129
更新の際、より限定的なルートを除外 130
パス属性を割り当てるルートの選択 131
集約ルートの属性変更 132

第 6 章 ポリシーベースのルーティング 133

ポリシーベースのルーティングの概要 134
拡張アクセスリスト 134
適合グループ 134
アクショングループ 135
ポリシーベースのルーティングを使用するルートルックアップ 136
ポリシーベースのルーティングの構成 136
拡張アクセスリストの構成 137
適合グループの構成 138
アクショングループの構成 139
PBR ポリシーの構成 140
ポリシーベースのルーティングポリシーのバインディング 140
ポリシーベースのルーティングポリシーのインターフェースへのバインディング 140
ポリシーベースのルーティングポリシーのゾーンへのバインディング 140
ポリシーベースのルーティングポリシーの仮想ルーターへのバインディング 141
ポリシーベースのルーティングの出力の表示 141
拡張アクセスリストの表示 141
適合グループの表示 142
アクショングループの表示 142
ポリシーベースのルーティングポリシー構成の表示 143
完全なポリシーベースのルーティング構成の表示 143
高度な PBR の例 144
ルーティング 145
PBR 要素 146
拡張アクセスリスト 147
適合グループ 147
アクショングループ 147
PBR ポリシー 148
インターフェースのバインディング 148
可用性およびスケーラビリティが高い、高度な PBR 148
回復力のある PBR ソリューション 148
スケーラブルな PBR ソリューション 149

第 7 章 マルチキャストルーティング 151

概要 151
マルチキャストアドレス 152
逆方向パス転送 152
セキュリティデバイスによるマルチキャストルーティング 153
マルチキャストルーティングテーブル 153
静的マルチキャストルートの設定 154
アクセスリスト 155
トンネルインターフェース上に一般ルーティングのカプセル化を構成する 155
マルチキャストポリシー 157

第 8 章 IGMP (Internet Group Management Protocol) 159

概要 160
ホスト 161
マルチキャストルーター 161
セキュリティデバイスで稼動する IGMP 162
BGP をインターフェースで使用可能・不可にする 162

あるインターフェース上で IGMP を稼動させる 162
インターフェース上の IGMP を停止する 163
ホストの参加を許可するグループを列挙したアクセスリストの設定 .. 163
IGMP の構成 164
IGMP に関する設定事項の確認 166
IGMP 運用パラメータ 167
IGMP プロキシ 168
メンバーシップレポートをソースに転送する手順 169
マルチキャストデータを受信者に送る手順 169
IGMP プロキシの設定 170
インターフェース上で IGMP プロキシを設定する 171
IGMP および IGMP プロキシ設定のマルチキャストポリシー 173
IGMP 用のマルチキャストグループポリシーの作成 173
IGMP プロキシ設定の作成 173
IGMP 送信元プロキシの設定 180

第 9 章 プロトコル独立マルチキャスト 187

概要 188
PIM-SM 190
マルチキャスト配布ツリー 190
代表ルーター 191
集合地点のグループへのマッピング 191
配布ツリーでのトラフィックの転送 192
PIM-SM 194
セキュリティデバイスで PIM-SM を構成する方法 195
VR 上に PIM-SM インスタンスを有効にし、削除します。 195
PIM-SM インスタンスを有効にする 195
PIM-SM インスタンスの削除 196
PIM-SM をインターフェースで使用可能・不可にする 196
インターフェース上の PIM-SM を有効にする 196
インターフェース上の PIM-SM を無効にする 197
マルチキャストグループポリシー 197
Static-RP-BSR メッセージ 197
Join-Prune メッセージ 197
PIM-SM のマルチキャストグループポリシーの定義 198
PIM-SM の基本設定 198
設定内容の確認 203
集合地点の設定 205
静的集合地点の設定 205
Candidate 集合地点の設定 206
セキュリティ検討事項 207
マルチキャストグループの制限 207
マルチキャストソースの制限 208
集合地点の制限 209
PIM-SM インターフェースパラメータ 210
Neighbor Policy を定義する 210
Bootstrap Border を定義する 211
プロキシ集合地点の設定 212
PIM-SM および IGMPv3 221

第 10 章 ICMP ルーター検出プロトコル 223

概要 223
ICMP ルーター検出プロトコルの構成 224
ICMP ルーター検出プロトコルを使用可能にする 224
WebUI からの ICMP ルーター検出プロトコルの構成 224
CLI からの ICMP ルーター検出プロトコルの構成 225
インターフェースの通知 225
アドレスのブロードキャスト 225
最大通知間隔の設定 225
最小通知間隔の設定 225
通知寿命値の設定 226
応答遅延の設定 226
初期通知間隔の設定 226
初期通知パケット数の設定 226
IRDP を使用不可にする 227
IRDP 設定の表示 227

索引 ..... IX-I

第 8 部 : アドレス変換

本編について v

ドキュメントの規則 v
Web ユーザーインターフェースの規則 vi
コマンドラインインターフェースの規則 vi
ネーミング規則および文字タイプ vii
説明図の規則 viii
技術ドキュメントおよびテクニカルサポート ix

第 1 章 アドレス変換 1

アドレス変換の概要 1
ソースネットワークアドレス変換 1
宛先ネットワークアドレス変換 3
ポリシーベースの NAT-Dst 4
マップ IP: 6
仮想 IP 6
ポリシーベースの変換のさまざまな形態 7
例 : NAT-Src - DIP プールからアドレス取得、PAT 機能あり 7
例 : NAT-Src - DIP プールからアドレス取得、PAT 機能あり 8
例 : NAT-Src - DIP プールからアドレスシフティングによりアドレス取得 ... 8
例 : NAT-Src - Egress インターフェース IP アドレスに変換 9
例 : NAT-Dst を特定の IP アドレスに変換、ポートマッピングあり 9
例 : NAT-Dst を特定の IP アドレスに変換、ポートマッピングなし 9
例 : 所定の IP アドレス範囲を特定の IP アドレスに変換した NAT-Dst .. 10
例 : IP アドレス範囲間の NAT-Dst 10
NAT-Src と NAT-Dst の適用方向 10

第 2 章 ソースネットワークアドレス変換 13

NAT-Src の概要 13
NAT-Src - DIP プールからアドレス取得、PAT 機能あり 14
例 : PAT を有効にした NAT-Src の設定 15

NAT-Src - DIP プールからアドレス取得、PAT 機能なし 18
例 : PAT を無効にした NAT-Src の設定 18
NAT-Src - DIP プールからアドレスシフティングによりアドレス取得 19
例 : アドレスシフティングによる NAT-Src の設定 20
NAT-Src - Egress インターフェース IP アドレスに変換 23
例 : DIP プールを使わない NAT-Src の設定 23

第 3 章 宛先ネットワークアドレス変換 27

NAT-Dst の概要 28
NAT-Dst のパケットフロー 29
NAT-Dst のルーティング 32
例 : 同じインターフェースに接続されたアドレス 33
例 : 同じインターフェースに接続されているが、ルーターにより分離されたアドレス 33
例 : 別々のインターフェースに接続されたアドレス 34
NAT-Dst-1 対 1 のマッピング 35
例 : 1 対 1 の宛先アドレス変換 35
単一のアドレスから複数のアドレスへの変換 38
例 : 1 対多の宛先アドレス変換 38
NAT-Dst- 多対 1 のマッピング 40
例 : 多対 1 の宛先アドレス変換 40
NAT-Dst- 多対多のマッピング 43
例 : 多対多の宛先アドレス変換 44
ポートマッピングを伴う NAT-Dst 46
例 : ポートマッピングを伴う NAT-Dst 46
１つのポリシーで NAT-Src と NAT-Dst を適用 49
例 : NAT-Src と NAT-Dst の組み合わせ 49

第 4 章 マップアドレスと仮想アドレス 61

マップ IP アドレス 61
MIP と Global ゾーン 62
例 : Untrust ゾーンインターフェース上の MIP 63
例 : 別のゾーンから MIP に到達するトラフィック 65
例 : MIP をトンネルインターフェースに追加 68
MIP を Untrust ゾーンとして扱うインターフェース 69
例 : Untrust ゾーンインターフェース上の MIP 69
MIP とループバックインターフェース 71
例 : 2 つのトンネルインターフェースに対する MIP 72
MIP グルーピング 78
例 : マルチセルポリシーにおける MIP グルーピング 78
仮想 IP アドレス 79
VIP と Global ゾーン 81
例 : 仮想 IP サーバーの設定 81
例 : VIP 設定の編集 83
例 : VIP 設定の削除 83
例 : カスタムサービス、複数のポートを使うサービスに対応した VIP 83

索引 ..... IX-I

第 9 部 : ユーザー認証

本編について vii

ドキュメントの規則 viii
Web ユーザーインターフェースの規則 viii
コマンドラインインターフェースの規則 viii
ネーミング規則および文字タイプ ix
説明図の規則 x
技術ドキュメントおよびテクニカルサポート xi

第 1 章 認証 1

ユーザー認証タイプ 1
管理ユーザー 2
複数タイプユーザー 3
グループ式 4
例 : グループ式 (AND) 5
例 : グループ式 (OR) 7
例 : グループ式 (NOT) 8
バナーのカスタマイズ 9
例 : WebAuth バナーのカスタマイズ 9
ログインバナー 10
例 : ログインバナーの作成 10

第 2 章 認証サーバー 11

認証サーバータイプ 12
ローカルデータベース 13
例 : ローカルデータベースタイムアウト 14
外部認証サーバー 15
認証サーバーオブジェクトプロパティ 16
認証サーバータイプ 17
リモート認証ダイヤルインユーザーサービス 17
RADIUS 認証サーバーオブジェクトプロパティ 18
サポートされるユーザータイプと機能 18
RADIUS ディクショナリーファイル 19
RADIUS アクセスチャレンジ 21
認証および XAuth ユーザーにサポートされている RADIUS 拡張機能 22
SecurID 25
SecurID 認証サーバーオブジェクトプロパティ 26
サポートされるユーザータイプと機能 26
軽量ディレクトリアクセスプロトコル 27
LDAP 認証サーバーオブジェクトプロパティ 28
サポートされるユーザータイプと機能 28
TACACS+ (Terminal Access Control Access Control System Plus) 28
TACACS+ サーバーオブジェクトプロパティ 30
管理認証の優先 30
認証サーバーオブジェクトの定義 31
例 : RADIUS 認証サーバー 31
例 : SecurID 認証サーバー 33
例 : LDAP 認証サーバー 35
例 : TACACS+ 認証サーバー 36

デフォルト認証サーバーの定義 37
例 : デフォルト認証サーバーの変更 37

第 3 章 インフラネットの認証 39

統合型アクセス管理ソリューション 40
ファイアウォールとインフラネットコントローラの連携 41
インフラネット認証用の構成 42

第 4 章 認証ユーザー 43

ポリシーで認証ユーザーを参照する 44
ランタイム認証 44
事前ポリシーチェック認証 (WebAuth) 45
ポリシーでの認証ユーザーグループの参照 46
例 : ランタイム認証 (ローカルユーザー) 47
例 : ランタイム認証 (ローカルユーザーグループ) 48
例 : ランタイム認証 (外部ユーザー) 49
例 : ランタイム認証 (外部ユーザーグループ) 51
例 : 複数グループのローカル認証ユーザー 53
例 : WebAuth (ローカルユーザーグループ) 55
例 : WebAuth (外部ユーザーグループ) 57
例 : WebAuth + SSL のみ (外部ユーザーグループ) 59

第 5 章 IKE、XAuth、および L2TP ユーザー 63

IKE ユーザーとユーザーグループ 63
例 : IKE ユーザーの定義 64
例 : IKE ユーザーグループの作成 65
ゲートウェイの IKE ユーザーを参照 66
XAuth ユーザーとユーザーグループ 66
IKE モードのイベントロギング 67
IKE ネゴシエーションの XAuth ユーザー 68
例 : XAuth 認証 (ローカルユーザー) 70
例 : XAuth 認証 (ローカルユーザーグループ) 71
例 : XAuth 認証 (外部ユーザー) 72
例 : XAuth 認証 (外部ユーザーグループ) 74
例 : XAuth 認証およびアドレス割り当て (ローカルユーザーグループ) 77
XAuth クライアント 81
例 : XAuth クライアントとしてのセキュリティデバイス 81
L2TP ユーザーとユーザーグループ 82
例 : ローカルおよび外部 L2TP 認証サーバー 82

第 6 章 ワイヤレスおよびイーサネットインターフェース用の拡張認証 87

概要 88
サポートされている EAP のタイプ 88
802.1X 認証を使用可能または使用不可能にする 89
イーサネットインターフェース 89
ワイヤレスインターフェース 89

802.1X 設定の構成 90
802.1X ポート制御の構成 90
802.1X 制御モードの構成 91
同時ユーザーの最大数の設定 91
再認証期間の設定 92
EAP 再送信を使用可能にする 92
EAP 再送信回数の構成 93
EAP 再送信期間の構成 93
サイレント（沈黙）期間の構成 93
認証サーバーオプションの構成 94
認証サーバーの指定 94
イーサネットインターフェース 94
ワイヤレスインターフェース 94
アカウントタイプの設定 95
ゾーン確認を使用可能にする 95
802.1X 情報の表示 96
802.1X グローバル構成情報の表示 96
インターフェースの 802.1X 情報の表示 96
802.1X 統計の表示 97
802.1X セッション統計の表示 97
802.1X セッション詳細の表示 98
設定例 98
直接接続しているクライアントと RADIUS サーバーを持ったセキュリティデバイスの構成 98
クライアントとセキュリティデバイスの間にハブを持ったセキュリティデバイスの構成 99
ワイヤレスインターフェースを持った認証サーバーの構成 101

索引 ..... IX-I

第 10 部 : 仮想 システム

本編について v

ドキュメントの規則 v
Web ユーザーインターフェースの規則 v
コマンドラインインターフェースの規則 vi
ネーミング規則および文字タイプ vi
説明図の規則 viii
技術ドキュメンおよびテクニカルサポート ix

第 1 章 仮想システム 1

概要 2
Vsys オブジェクト 4
Vsys オブジェクトと管理者の作成 4
Vsys にデフォルト仮想ルーターを設定する 6
ゾーンを共有仮想ルーターにバインドする 6
Vsys 管理者としてログイン 7

仮想システムプロファイル 9
Vsys セッションカウンタ 10
Vsys セッション情報 10
高可用性ペアにおける動作 10
Vsys プロファイルの作成 10
リソース限度の設定 11
Vsys プロファイル割り当てによるセッション限度の追加 12
セッションの変更設定 13
セッション限度到達アラームの変更設定 13
Vsys プロファイルの削除 14
Vsys 設定値の表示 14
変更設定の表示 14
プロファイルの表示 15
セッションの統計情報の表示 17
CPU リソースの共有と分割 17
CPU ウェイトの構成 18
公平モードのパケットフロー 19
公平モードから共有モードへの移行 20
CPU 限度機能を使用可能にする 20
CPU 使用率の測定 20
共有から公平モードへ移行 CPU 使用率しきい値の設定 23
共有モードに戻る方法を構成 25
ルート Vsys 固定 CPU ウェイトの設定 26
Vsys と仮想プライベートネットワーク 27
セキュリティアソシエーションの表示 27
IKE クッキーの表示 28
ポリシー スケジューリング 29
ポリシースケジューラの作成 29
ポリシースケジュールをポリシーにバインド 30
ポリシースケジュールの表示 30
ポリシースケジュールの削除 30

第 2 章 VLAN ベースのトラフィック分類 31

概要 31
VLAN 32
VLANs with Vsys 33
レイヤー 2 仮想システムの構成 34
例 1: 1 ポートを構成 35
例 2: それぞれが個別の Untrust ゾーンを持つ 2 つの 4 ポート統合の構成 39
例 3: 1 つの Untrusted ゾーンを共有する 2 つの 4 ポート統合の構成 45
サブインターフェースと VLAN タグの定義 51
仮想システム間の通信 54
VLAN の再タグ付け 57
例 : 58

第 3 章 トラフィックの振り分け 61

概要 61
トラフィックの振り分け 61
通過トラフィックの振り分け 62
専用および共有インターフェース 67
専用インターフェース 67
共有インターフェース 67
物理インターフェースのインポートとエクスポート 69
物理インターフェースを仮想システムにインポートする 69
物理インターフェースを仮想システムからエクスポートする 70

第 4 章 IP ベースのトラフィック分類 71

概要 71
ルートシステムに IP 範囲を指定する 72
IP ベースのトラフィック分類を設定する 73

索引 ..... IX-I

第 11 部 :
高可用性

本編について v

ドキュメントの規則 v
Web ユーザーインターフェースの規則 vi
コマンドラインインターフェースの規則 vi
ネーミング規則および文字タイプ vii
説明図の規則 viii
技術ドキュメンおよびテクニカルサポート ix

第 1 章 NetScreen 冗長プロトコル 1

高可用性の概要 1
NSRP の概要 2
NSRP デフォルト設定 4
NSRP-Lite 4
NSRP-Lite の デフォルト設定 6
NSRP の基本設定 6
コントロールリンクメッセージ 6
データリンクメッセージ 7
動的ルーティング勧告 8
2 重リンク精査 9
NSRP クラスタ 10
クラスタ名 11
アクティブ / パッシブ構成 11
アクティブ / アクティブ構成 12
アクティブ / アクティブ ー フルメッシュ構成 14
NSRP クラスタの認証および暗号化 15
ランタイムオブジェクト 15
RTO ミラー動作状態 16

NSRP クラスタ（続き）
NSRP クラスタの同期 18
ファイルの同期 18
構成同期化 18
ルートの同期化 19
ランタイムオブジェクトの同期化 19
システムクロックの同期化 20
VSD グループ 20
プリエンプトオプション 21
メンバー状態 22
ハートビートメッセージ 23
VSI と静的ルート 24
設定例 25
アクティブ / アクティブ、フルメッシュ NSRP のためのデバイスの配線 . 25
NSRP クラスタの作成 28
アクティブ / パッシブ NSRP クラスタの構成 30
アクティブ / アクティブ NSRP クラスタの構成 34
手作業での RTO の同期化 40
手動リンク精査の設定 40
自動リンク精査の設定 41

第 2 章 インターフェースの冗長性およびフェールオーバー 43

冗長インターフェースとゾーン 43
ホールドダウンタイム設定 44
統合インターフェース 45
インターフェースフェールオーバー 46
バックアップインターフェーストラフィック 46
1 次インターフェース トラフィック 47
トラフィックの自動フェールオーバー 47
シリアルインターフェース 48
デフォルトルートの削除 48
デフォルトルートの追加 49
ポリシーの無効化 49
フェールオーバーの監視 49
IP トラッキングによるインターフェースフォールオーバー 50
アクティブトンネルからバックアップトンネルへのフェールオーバー 51
VPN トンネル監視を使用したインターフェースフェールオーバー 51
フェールオーバーのトリガーを監視する NSRP オブジェクト 52
セキュリティモジュール 53
物理インターフェース 54
ゾーンオブジェクト 54
トラック IP オブジェクト 55
デバイスフェールオーバー用のトラック IP 57
仮想セキュリティデバイスグループのフェールオーバー 57
仮想システムのフェールオーバー 58
デバイスフェールオーバー 59

構成例 60
デバイスフェールオーバー用のトラック IP の構成 60
冗長 VPN トンネルの構成 63
仮想セキュリティインターフェースの構成 67
2 系統のアクティブなトンネルの構成 70
トラック IP を使用したインターフェースフォールオーバーの構成 74
トンネルのフェールオーバーウェイトの構成 77
仮想システムのフェールオーバーの構成 83

索引 ..... IX-I

第 12 部 : WAN、DSL、ダイアル、およびワイヤレス

本編について ix

ドキュメントの規則 ix
Web ユーザーインターフェースの規則 x
コマンドラインインターフェースの規則 x
ネーミング規則および文字タイプ xi
説明図の規則 xii
技術ドキュメンおよびテクニカルサポート xiii

第 1 章 ワイドエリアネットワーク 1

WAN の概要 1
シリアル 2
T1 3
E1 3
T3 4
E3 4
ISDN 5
WAN インターフェースのオプション 7
Hold Time (保持時間) 8
フレームチェックサム 9
アイドルサイクルフラグ 9
開始 / 終了フラグ 10
ラインエンコーディング 10
Alternate Mark Inversion エンコーディング 10
B8ZS および HDB3 ラインエンコーディング 11
バイトエンコーディング 11
ラインビルドアウト 12
フレーミングモード 12
T1 用のスーパーフレーム 13
T1 用の拡張スーパーフレーム 13
T3 用の C ビットパリティフレーミング 13
クロッキング 13
クロッキングモード 14

クロッキングソース 15
内部クロック速度 15
送信クロックの反転 16
信号処理 17
ループバック信号 18
リモートループバックとローカルループバック 18
ループバックモード 18
CSU 互換モード 20
リモートループバック応答 21
FEAC 応答 22
タイムスロット 22
フラクショナル T1 22
フラクショナル E1 23
ビット誤り率テスト 23
ISDN オプション 25
スイッチタイプ 25
SPID 25
TEI ネゴシエーション 26
発呼者番号 26
T310 値 26
送信完了 27
BRI モード 27
専用回線モード 27
Dialer Enable 27
ダイヤラーオプション 28
WAN インターフェースの使用不可 29
WAN インターフェースのカプセル化 29
ポイントツーポイントプロトコル 30
フレームリレー 30
Cisco ハイレベルデータリンク伝送制御手順（Cisco-HDLC） 31
基本的なカプセル化オプション 32
番号なしインターフェース 32
プロトコル最大送信単位の構成 32
静的 IP アドレスの構成 33
キープアライブ 33
PPP カプセル化オプション 34
PPP アクセスプロファイル 34
PPP 認証方法 35
パスワード 36
PPP 認証プロトコル 36
チャレンジハンドシェイク認証プロトコル（CHAP） 36
パスワード認証プロトコル 37
ローカルデータベースユーザー 37
フレームリレーカプセル化オプション 38
キープアライブメッセージ 38
フレームリレー LMI タイプ 38
PVC の作成と構成 39
逆アドレス解決プロトコル 40

マルチリンクカプセル化 41
概要 41
基本的なマルチリンクバンドルの設定 42
バンドル識別子 42
ドロップタイムアウト 43
フラグメントしきい値 43
最小リンク 44
基本的な設定手順 45
最大受信再構築単位 45
シーケンスヘッダーの形式 46
マルチリンクフレームリレー構成オプション 46
基本的な設定手順 46
MLFR のリンク割り当て 47
確認リトライ 47
肯定応答タイマー 48
ハロータイマー 48
WAN インターフェース構成例 48
シリアルインターフェースの構成 49
T1 インターフェースの構成 49
E1 インターフェースの構成 50
T3 インターフェースの構成 51
E3 インターフェースの構成 51
ISDN 接続用のデバイスの構成 52
手順 1: ISDN スイッチタイプの選択 52
手順 2: PPP プロファイルの構成 52
手順 3: ISDN BRI インターフェースのセットアップ 53
1 つの宛先のみのダイヤルアウト 53
ダイヤラーインターフェースを使用したダイヤルアウト 54
専用回線モードの使用 57
手順 4: 宛先へのトラフィックのルーティング 58
カプセル化設定例 59
PPP カプセル化の構成 59
MLPPP カプセル化の構成 60
フレームリレーカプセル化の構成 62
MLFR カプセル化の構成 62
Cisco HDLC カプセル化の構成 64

第 2 章 デジタル加入者線 65

デジタル加入者線の概要 65
非同期転送モード 66
ATM 通信品質 67
Point-to-Point Protocol over ATM 68
マルチリンクポイントツーポイントプロトコル 69
DSL インターフェースの Discrete Multitone 69
アネックスモード 70
仮想回路 71
VPI/VCI および複合方式 71
PPPoE または PPPoA 72
静的 IP アドレスおよびネットマスク 73
ADSL インターフェース 74
G.SHDSL インターフェース 75
ループバックモード 75
操作、管理、および保守 76
信号対雑音比 77

ADSL 設定例 77
例 1:（小規模なビジネス / 自宅）ADSL インターフェース上の PPPoA .. 78
例 2:（小規模なビジネス / 自宅）ADSL インターフェース上の 1483 ブリッジング 81
例 3:（小規模なビジネス）ADSL インターフェース上の 1483 ブリッジング 83
例 4:（小規模なビジネス / 自宅）ダイヤルアップバックアップ 85
例 5:（小規模なビジネス / 自宅）Ethernet バックアップ 88
例 6:（小規模なビジネス / 自宅）ADSL バックアップ 91
例 7:（小規模なビジネス）MLPPP ADSL 94
例 8:（小規模なビジネス）ローカルサーバーへのアクセスを許可 96
例 9:（支店）ADSL を通した VPN トンネル 99
例 10:（支社）2 次 VPN トンネル 103

第 3 章 ISP フェールオーバーとダイヤル回復 109

フェールオーバーの ISP 優先順位の設定 109
ISP フェールオーバーの条件の定義 110
ダイヤルアップ回復ソリューションの構成 111

第 4 章 ワイヤレス ローカル エリア ネットワーク 115

概要 116
ワイヤレス製品によるインターフェース名指定の違い 117
基本的なワイヤレスネットワーク機能の構成 118
サービスセット識別子の作成 118
SSID ブロードキャストの抑制 118
クライアントの分離 119
2.4 GHz トランシーバへの操作モードの設定 119
5GHz トランシーバへの操作モードの設定 120
データ送信最低速度の構成 120
送信パワーの設定 121
WLAN 構成の再起動 122
SSID への認証と暗号化の設定 122
WEP（有線と同等のプライバシー）の構成 123
複数の WEP 鍵 123
オープン認証の設定 125
WEP 共有鍵認証の設定 127
Wi-Fi 保護アクセスの構成 128
WPA と WPA2 の 802.1X 認証の構成 129
WPA と WPA2 のため事前共有鍵認証の構成 130
アンテナ使用の指定 131
国コード、チャネルおよび周波数の設定 131
拡張チャネルの使用 132
サイト調査の実行 132
利用可能なチャネルの発見 133
アクセス制御リストエントリの設定 133
Super G の構成 134
Atheros XR（拡張範囲）の構成 135
Wi-Fi マルチメディアサービス品質の構成 136
WMM を有効にする 136
WMM サービス品質の構成 136
アクセスのカテゴリ 136
デフォルトの WMM 設定 137
例 139

詳細なワイヤレスパラメーターの設定 140
エージング間隔の構成 140
ビーコン間隔の設定 141
DTIM（Delivery Traffic Indication Message）期間の構成 142
バーストしきい値の構成 142
フラグメントしきい値の構成 143
送信要求しきい値の構成 143
送信可モードの構成 144
送信可速度の構成 144
送信可タイプの構成 144
スロット時間の設定 145
プリアンブル長の構成 145
ワイヤレスインターフェースでの作業 146
SSID のワイヤレスインターフェースへのバインド 146
ワイヤレスインターフェースのトランシーバへのバインド 146
ワイヤレスブリッジグループの作成 147
ワイヤレスインターフェースの使用不可 148
ワイヤレス構成情報の表示 148
設定例 149
例 1: オープン認証および WEP 暗号化 149
例 2: パスフレーズおよび自動暗号化を持っている WPA-PSK 認証 150
例 3: 透過モードの WLAN 150
例 4: 複数および差別化されたプロファイル 154

索引 ..... IX-I

第 13 部 : ジェネラルパケットラジオサービス

本編について v

ドキュメントの規則 v
Web ユーザーインターフェースの規則 v
コマンドラインインターフェースの規則 vi
ネーミング規則および文字タイプ vi
説明図の規則 vii
技術ドキュメンおよびテクニカルサポート viii

第 1 章 GPRS 1

GPRS トンネリングプロトコルファイアウォールとしてのセキュリティデバイス 2
Gp と Gn インターフェース 3
Gi インターフェース 3
動作モード 4
仮想システムサポート 5
ポリシーベースの GPRS トンネリングプロトコル 5
例 : GTP 検査を使用可能にするポリシーの構成 6
GPRS トンネリングプロトコル検査オブジェクト 7
例 : GTP 検査オブジェクトの作成 8

GTP メッセージフィルタリング 8
パケットサニティチェック 9
メッセージ長のフィルタリング 9
例 : GTP メッセージ長の設定 9
メッセージタイプのフィルタリング 10
例 : メッセージタイプの許可および拒否 10
サポートされているメッセージタイプ 11
メッセージレートの制限 12
例 : レート制限の設定 13
シーケンス番号検証 13
例 : シーケンス番号検証を使用可能にする 13
IP フラグメント化 14
GTP-in-GTP パケットフィルタリング 14
例 : GTP-in-GTP パケットフィルタリングを使用可能にする 14
徹底監視 (Deep Inspection) 14
例 : 徹底監視を TEID で使用可能にする 14
GTP 情報要素 15
アクセスポイント名のフィルタリング 15
例 : APN と選択モードの設定 16
IMSI プレフィックスフィルタリング 17
例 : IMSI プレフィックスとフ APN フィルタを組み合わせて設定する 17
無線アクセス技術 18
例 : RAT および APN フィルタの設定 18
ルーティングエリアアイデンティティとユーザーロケーション情報 18
例 : RAI および APN フィルタの設定 19
例 : ULI および APN フィルタの設定 19
APN Restriction 19
IMEI-SV 19
例 : IMEI-SV および APN フィルタの設定 20
プロトコルおよびシグナリング要件 20
IE フィルタリングの組み合わせのサポート 21
サポートされる R6 情報要素 22
3GPP R6 IE の排除 24
例 : R6 の排除 24
GTP トンネル 24
GTP トンネル制限 24
例 : GTP トンネル制限の設定 24
パケット状態監視 25
GTP トンネル確立および終了 25
SGSN 間ルーティングエリアの更新 25
高可用性のためのトンネルフェールオーバー 26
放置された GTP トンネルのクリーンアップ 26
例 : GTP トンネルのタイムアウトの設定 26
SGSN と GGSN 転送 27
過大請求攻撃の回避 27
過大請求攻撃の説明 27
過大請求攻撃の防御 29
例 : 過大請求攻撃を回避するための設定 30

GTP トラフィック監視 32
トラフィックロギング 32
例 : GTP パケットロギングを使用可能にする 33
トラフックカウンティング 34
例 : GTP トラリフィックカウンティングを使用可能にする 34
法に順守した傍受 35
例 : 法に順守した傍受を使用可能にする 35

索引 ..... IX-I

第 14 部 : IPv6 によるデュアルスタックアーキテクチャ

本編について vii

ドキュメントの対象 viii
ドキュメントの規則 viii
Web ユーザーインターフェースの規則 viii
コマンドラインインターフェースの規則 ix
ネーミング規則および文字タイプ ix
説明図の規則 x
技術ドキュメンおよびテクニカルサポート xi

第 1 章 インターネットプロトコルバージョン 6 の紹介 1

概要 2
IPv6 アドレス指定 2
表記 2
プレフィックス 3
アドレスのタイプ 3
ユニキャストアドレス 3
エニーキャストアドレス 4
マルチキャストアドレス 4
IPv6 ヘッダー 4
基本ヘッダー 4
拡張ヘッダー 5
IPv6 パケットの処理 6
IPv6 ルーターおよびホストのモード 7
IPv6 トンネリングのガイドライン 8

第 2 章 IPv6 の構成 9

概要 10
アドレスの自動構成 11
EUI（Extended Unique Identifier） 11
ルーターの通知メッセージ 12
ルーター要請メッセージ 12
プレフィックス一覧 12
隣接ノード発見 13
隣接ノードキャッシュテーブル 13
隣接ノード到達不能検出 14
隣接ノードエントリのカテゴリ 14
隣接ノード到達可能性状態 14
到達可能性状態の移行 15

IPv6 環境の有効化 18
デバイスレベルでの IPv6 の有効化 18
デバイスレベルでの IPv6 の無効化 19
IPv6 ホストの構成 19
IPv6 インターフェースのゾーンへのバインディング 20
IPv6 ホストモードの有効化 20
インターフェース ID の設定 20
アドレス自動構成の構成 21
隣接ノード発見の構成 21
IPv6 ルーターの構成 22
IPv6 インターフェースのゾーンへのバインディング 22
IPv6 ルーターモードの有効化 22
インターフェース ID の設定 23
アドレス自動構成の設定 23
Outgoing Router Advertisements フラグ 23
Managed Configuration フラグ 24
Other Parameters Configuration フラグ 24
アドレス自動構成の無効化 24
アドバタイジング時間間隔の設定 25
通知された到着可能時間間隔 25
通知された再送信時間間隔 26
最大通知間隔 26
最小通知間隔 26
通知されたデフォルトのルーター寿命 27
アドバタイジングパケットの性質 27
リンク MTU 値 27
現在のホップ制限 28
通知ルーターの性質 28
リンクレイヤーアドレスの設定 28
通知されたルーターの優先度 28
隣接ノード発見パラメータの構成 29
隣接ノード到達不能検出 29
MAC セッション ー キャッシング 29
静的隣接ノードキャッシュエントリ 30
ベース到着可能時間 30
プローブ時間 31
再送信時間 31
重複アドレス検出再試行カウント 31
IPv6 インターフェースパラメータの表示 32
隣接ノード発見構成の表示 32
現在の RA 構成の表示 32
設定例 32
IPv6 ルーター 32
IPv6 ホスト 33

第 3 章　接続およびネットワークサービス　35

概要 36

動的ホスト構成プロトコルバージョン 6 36
デバイスユニーク ID 37
ID アソシエーションプレフィックス委譲 ID 37
プレフィックスの特徴 37
サーバーの優先度 38
DHCPv6 サーバーの構成 38
DHCPv6 クライアントの構成 40
DHCPv6 設定の表示 41
ドメイン名システムサーバーの構成 42
DNS および DNS 検索リスト情報の要求 43
プロキシ DNS アドレス分割の設定 44
PPPoE の構成 46
フラグメント化の設定 47

第 4 章 静的および動的ルーティング 49

概要 50
デュアルルーティングテーブル 50
静的および動的ルーティング 51
上流および下流プレフィックスの委譲 51
静的ルーティング 52
RIPng の構成 53
RIPng インスタンスの作成と削除 54
RIPng インスタンスの作成 54
RIPng インスタンスの削除 54
RIPng をインターフェースで使用可能・不可にする 55
インターフェース上の RIPng を有効にする 55
インターフェース上の RIPng を停止する 55
RIPng に関する大域パラメータ 55
デフォルトルートの通知 56
デフォルトルートを拒否する 57
Trusted 隣接ノードを構成する 57
ルートの再配布 58
更新しきい値を設定してフラッディングを防止 59
インターフェースごとの RIPng パラメータ 60
ルート、インターフェース、およびオフセットメトリック 60
アクセスリストおよびルートマップ 61
静的ルートの再配布 61
ポイズンリバース付きスプリットホライズンの構成 63
ルーティングおよび RIPng 情報の表示 64
ルーティングテーブルの表示 64
RIPng データベースの表示 64
仮想ルーター別 RIPng の詳細の表示 65
インターフェース別 RIPng の詳細の表示 66
RIPng 隣接情報の表示 66
設定例 67
トンネルインターフェース上で RIPng を稼動させる 67
ISP ルーターへのトラフィックループの回避 69
顧客構内装置の構成 69
ゲートウェイの構成 73
ISP ルーターの構成 75
OSPF への Null インターフェース再配布の設定 76
発見したルートの OSPF への再配布 77
OSPF サマリーのインポートのセットアップ 77

第 5 章　アドレス変換　79

概要 80
ソース IP アドレスの変換 81
IPv6 から IPv4 への DIP 81
IPv4 から IPv6 への DIP 81
宛先 IP アドレスの変換 82
IPv6 から IPv4 への MIP 82
IPv4 から IPv6 への MIP 83
設定例 83
IPv6 ホストから複数 IPv4 ホストへの送信 84
IPv6 ホストから単一 IPv4 ホストへの送信 86
IPv4 ホストから複数 IPv6 ホストへの送信 87
IPv4 ホストから単一 IPv6 ホストへの送信 89
ドメイン名システムサーバーアドレスの変換 91

第 6 章　IPv4 環境での IPv6　95

概要 95
手動トンネリングの構成 96
6to4 トンネリングの構成 99
6to4 ルーター 99
6to4 リレールーター 100
リモートネイティブホストへのトンネル 101
リモート 6to4 ホストへのトンネル 104

第 7 章　IPSec トンネリング　107

概要 107
IPSec 6in6 トンネリング 108
IPSec 4in6 トンネリング 111
IPSec 6in4 トンネリング 115
フラグメント化を有効にした手動トンネリング 119
IPv6 to IPv6 ルートベースの VPN トンネル 120
IPv4 to IPv6 ルートベースの VPN トンネル 122

第 8 章　IPv6 XAuth ユーザー認証　125

概要 126
RADIUSv6 126
単一クライアント、単一サーバー 126
複数クライアント、単一サーバー 126
単一クライアント、複数サーバー 127
複数ホスト、単一サーバー 127
IPSec アクセスセッション管理 128
IPSec アクセスセッション 128
IAS 機能を使用可能にまたは使用不可能にする 130
IAS セッションの解除 130
IAS 制限設定 130
デッドピア検出 131

設定例 132
XAuth と RADIUS 132
RADIUS と XAuth ルートベース VPN 133
RADIUS と XAuth、およびドメイン名ストリッピング 136
IP プール範囲の割り当て 140
RADIUS リトライ 146
Calling-Station-Id 146
IPSec アクセスセッション 147
デッドピア検出 155

付録 A スイッチング A-I

索引 ..... IX-I

概念と用例 ScreenOS リファレンス ガイド について

Juniper Networks セキュリティデバイスは、インターネットに接続しているとき、セキュリティゾーンを柔軟に保護するため、次のファイアウォール、仮想プライベートネットワーク（VPN）およびトラフィックシェーピング機能を統合しています。

- **ファイアウォール :** ファイアウォールは、プライベート LAN と公開ネットワーク (インターネットなど) との境界を通過するトラフィックをスクリーニングします。

- **レイヤード（多層化）セキュリティ :** レイヤードセキュリティソリューションは、攻撃を防御することを目的として異なる複数の箇所に配備されます。1 つのレイヤーでの防御が失敗した場合、次のレイヤーが攻撃を捕捉します。サイトツーサイト VPN のリモート位置を保護します。周辺に配備されたデバイスは、ネットワークベースの攻撃を防御します。侵入検出予防（IDP）および徹底監視を使用して、別のレイヤーが、自動的に攻撃を検出し、損害の発生を防ぎます。

  ネットワークセグメンテーションは、最後のセキュリティレイヤであり（仮想化とも呼ばれる）、ネットワークをいくつかのセキュアドメインに分割することによって、非認証のローミングユーザーやネットワーク攻撃から重大なリソースを保護します。

- **コンテンツの保全 :** 不正な URL からユーザーを保護し、内蔵のウィルス対策スキャン機能と Web フィルタ機能も提供します。さらに、サードパーティ製品と連動することによって、外部のウィルス対応スキャン、スパム対応、および Web フィルタ機能を提供します。

- **VPN:** VPN は、複数のリモートネットワークアプライアンスの間でセキュア通信チャネルを実現します。

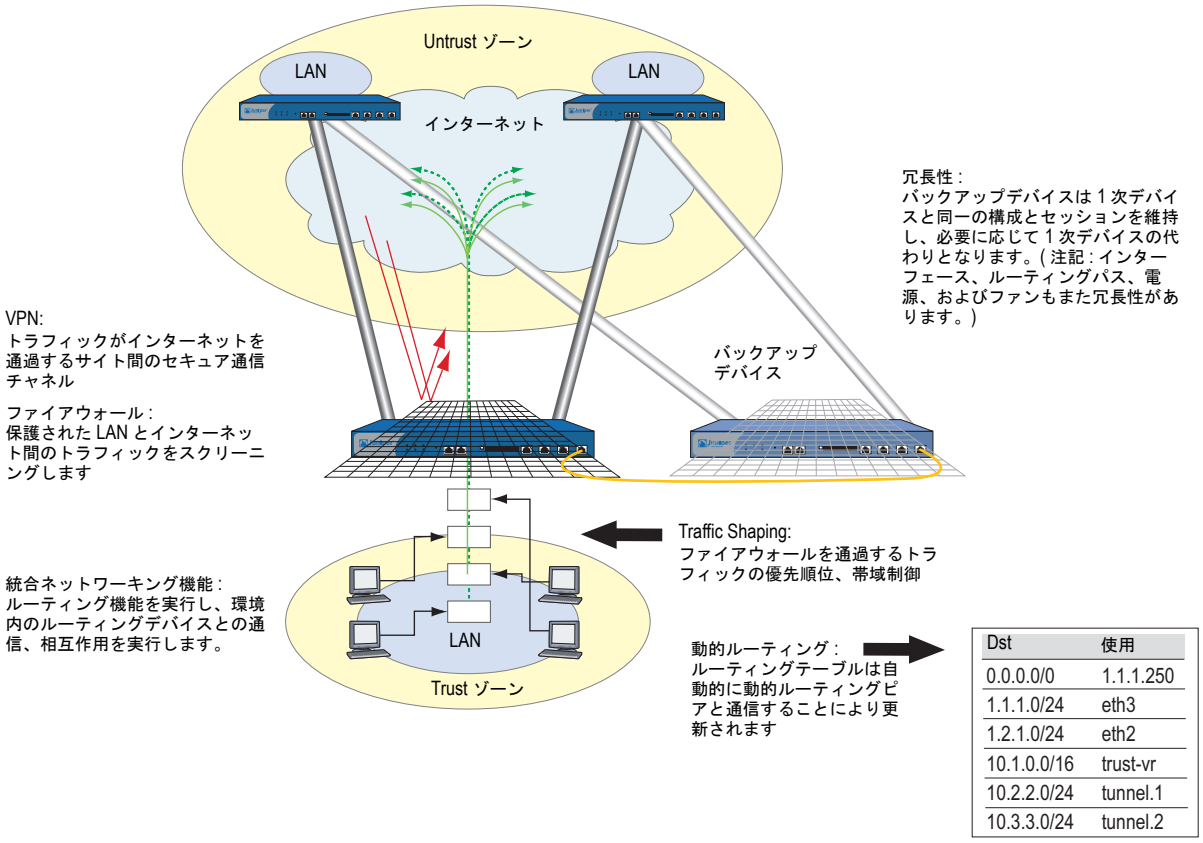
- **統合ネットワーキング機能 :** 動的ルーティングプロトコルによって到達可能性がわかり、動的に変化するネットワークトポロジが通知されます。さらに、トラフィックシェーピング機能により、ネットワークのサービスの品質 (QoS) レベルを維持するために、Juniper Networks ファイアウォールを通過するトラフィックを管理者が監視したり、制御したりすることができます。

- **中央集中管理 :** Netscreen-Security Manager ツールによって、セキュリティデバイスの構成、配備、管理が簡単に行えます。

- **冗長性 :** インターフェース、ルーティングパス、セキュリティデバイスの高可用性、またハイエンドの Juniper Networks デバイスでは電源やファンの高可用性によって、以上のエリアのポイントでの障害を予防することができます。

注： FIPS（米連邦政府情報処理規格）に準拠する Juniper Networks についての情報や、FIPS 準拠のセキュリティデバイスを FIPS モードで設定する方法については、ドキュメンテーション CD のプラットフォーム固有の Cryptographic Module Security Policy に関する資料を参照してください。

図 1: ScreenOS における重要な機能



ScreenOS システムは、任意のセキュリティアプライアンスまたはシステムのセットアップと管理にに必要なすべての機能を備えています。本書は、ScreenOS を介して Juniper Networks セキュリティデバイスを構成し、管理するためのリファレンスガイドです。

各部の構成

*概念と用例 ScreenOS リファレンスガイド*は、複数の部から成るマニュアルです。以下は、各部を概説し、まとめたものです。

第 1 部 : 概要

- 「目次」には、このマニュアルに集録されている各部の基本目次が記載されています。
- 「索引」は、このマニュアルの各部の索引です。

第 2 部 : 基本

- 第 1 章「ScreenOS アーキテクチャ」は、ScreeOS アーキテクチャの基本要素を示し、これらの要素を組み込む企業ベースの構成を説明する 4 つの例で締めくくっています。本章とその後のすべての章では、各概念に図解された例が添付されています。
- 第 2 章「ゾーン」では、セキュリティゾーン、トンネルゾーン、機能ゾーンを説明します。
- 第 3 章「インターフェース」では、セキュリティデバイスにあるさまざまな物理インターフェース、論理インターフェース、および仮想インターフェースについて説明します。
- 第 4 章「インターフェースモード」は、透過モード、NAT (ネットワークアドレス変換) モード、ルートインターフェース操作モードについて説明します。
- 第 5 章「ポリシー用ビルディングブロック」は、ポリシーと VPN(Virtual Private Netwark) の作成に使用する要素について説明します。アドレス（および VIP アドレス）、サービス、および DIP プールについて説明します。また、H.323 プロトコルをサポートするいくつかの構成例も示します。
- 第 6 章「ポリシー」では、ポリシーのコンポーネントと機能について説明し、その作成と応用に関する指針を示します。
- 第 7 章「トラフィックシェーピング」では、インターフェースとポリシーレベルの帯域を管理し、サービスの優先順位を決める方法を説明します。
- 第 8 章「システムパラメータ」では、ドメイン名システム（DNS）アドレス指定の背後にある概念、TCP/IP 設定を割り振ったり、リレーするためのダイナミックホスト設定プロトコル（DHCP）の使用法、システム設定やソフトウェアをダウンロードしたりアップロードする方法、システムクロックの設定方法を示します。

第3 部 : 管理

- 第 1 章「管理」は、ローカルおよびリモートの両方で、セキュリティデバイスの管理に利用できる様々な方法について説明します。本章はまた、定義可能な 4 段階のネットワーク管理者のそれぞれに与えられる権限についても説明します。

- 第 2 章「セキュリティ デバイスの監視」は、様々な監視方法について説明すると共に、監視出力を理解する手引きを提供しています。

第4 部 : 攻撃の検出と防衛機能

- 第 1 章「ネットワークの保護」では攻撃の基本的な段階と、各段階でアタッカーと闘うために使用できるファイアウォールのオプションの概略を説明します。

- 第 2 章「偵察阻止」では、IP アドレススイープ、ポートスキャン、およびターゲットとなったシステムのオペレーティングシステム (OS) の種類を検出しようとする試みをブロックするために使用できるオプションについて説明します。

- 第 3 章「サービス拒否 (DoS) 攻撃の防御」では、ファイアウォールアタック、ネットワークアタック、および OS 別の DoS アタックと、ScreenOS がそれらのアタックを防ぐ方法について説明します。

- 第 4 章「コンテンツの監視とフィルタリング」では、不正な URL (ユニフォームリソースロケータ) から HTTP (ハイパーテキスト転送プロトコル) ユーザーを保護する方法や、サードパーティ製品と連携してウィルス対策や Web フィルタリングを行うためにセキュリティデバイスを構成する方法について説明します。

- 第 5 章「徹底監視 (Deep Inspection)」では、DI (徹底監視) 攻撃オブジェクトの更新を取得するためにセキュリティデバイスを構成する方法、ユーザー定義の攻撃オブジェクトおよび攻撃オブジェクトグループを作成する方法、およびポリシーレベルで IDP を適用する方法について説明します。

- 第 6 章「侵入探知と阻止」では、ネット - ワーク内へ進入しようとする企みを検出し攻撃を未然に阻止する Juniper Networks IDP（進入検出と阻止）テクノロジについて説明します。IDP をポリシーレベルで適用し、攻撃者がネットワークに入る前に不正なパケットや接続をドロップする方法について示します。

- 第 7 章「不審なパケット属性」は、潜在的に危険なパケットをブロックする多くの SCREEN オプションについて説明します。

- 付録 A「ユーザー定義シグネチャのコンテキスト」では、ステートフルなシグニチャ攻撃オブジェクトを定義する際に指定できるコンテキストを一覧にして説明しています。

第 5 部 : 仮想プライベート ネットワーク

- 第 1 章「インターネットプロトコルセキュリティ」は、IPSec に関する背景情報を示し、Aggressive モードと Main モードの IKE ネゴシエーションのフェーズ 1 のフローシーケンスを示し、最後に、IKE と IPSec パケットのカプセル化に関する情報を示します。
- 第 2 章「公開鍵暗号化」は、デジタル証明書および CRL（証明書取り消しリスト）の取得と読み込み方法に関する情報を示します。
- 第 3 章「VPN (仮想プライベートネットワーク) の ガイドライン」は、使用可能な VPN オプションの選択に役立つ情報を示します。また、VPN パケットの処理を解読するためのパケットフローチャートも示します。
- 第 4 章「サイト間 VPN (仮想プライベートネットワーク)」は、2 つのプライベートネットワークを接続する広範な VPN 構成例を示します。
- 第 5 章「ダイヤルアップ仮想プライベート ネットワーク」は、AutoKey IKE を使用したクライアントから LAN への通信例を示します。また、グループ IKE ID および共有 IKE ID 構成についても詳細に示します。
- 第 6 章「レイヤー 2 トンネリングプロトコル」では、レイヤー 2 トンネリングプロトコルについて、またその単独使用および IPSec (L2TP-over-IPSec) との連携について説明します。
- 第 7 章「高度な仮想プライベート ネットワーク機能」は、NAT-Traversal、VPN 監視、複数のトンネルの単独トンネルインターフェースへのバインディング、およびハブアンドスポーク方式の対向トンネル設計など、さらに高度な VPN 構成について説明し、その例を示します。
- 第 8 章「AutoConnect 仮想プライベートネットワーク」では、セキュリティデバイスが必要に応じて AutoConnect VPN をセットアップできるように、ScreenOS が NHRP（ネクストホップレゾリューションプロトコル）メッセージをどのように使用するかを説明します。本章では、AC-VPN が使用される場合の典型的なシナリオの例を提供します。

第6 部 : 音声 IP 化

- 第 1 章「H.323 アプリケーションレイヤー ゲートウェイ」では、H.323 プロトコルについて解説し、一般的なシナリオを例示します。
- 第 2 章「セッション起動プロトコル アプリケーション レイヤーゲートウェイ」では、SIP（セッション起動プロトコル）について解説し、SIP ALG がルートモードおよび NAT（ネットワークアドレス変換）モードのコールを処理する方法について説明します。SIP のアーキテクチャの要約に続いて、一般的なシナリオを例示します。
- 第 3 章「メディアゲートウェイ制御プロトコルの アプリケーションレイヤーゲートウェイ」では、MGCP (メディアゲートウェイ制御プロトコル) ALG の概要を説明し、実装できるファイアウォールセキュリティ機能のリストを示します。MGCP のアーキテクチャの要約に続いて、一般的なシナリオを例示します。
- 第 4 章「スキニィクライアント制御プロトコルの アプリケーションレイヤーゲートウェイ」では、SCCP（スキニィクライアント制御プロトコル）ALG の概要を説明し、実装できるファイアウォールセキュリティ機能のリストを示します。SCCP のアーキテクチャの要約に続いて、一般的なシナリオを例示します。

第 7 部 : ルーティング

- 第 1 章「静的ルーティング」では、ScreenOS ルーティングテーブル、セキュリティデバイスの基本ルーティングプロセス、およびセキュリティデバイスでの静的ルートの構成方法について説明します。
- 第 2 章「ルーティング」、はセキュリティデバイス上の仮想ルーターの構成方法およびプロトコル間または仮想ルーター間のルーティングテーブルエントリの再配布の方法を説明します。
- 第 3 章「オープンショーテストパスファースト (OSPF)」、では、セキュリティデバイスの OSPF 動的ルーティングプロトコルの構成方法について説明します。
- 第 4 章「ルーティング情報プロトコル (RIP)」、では、セキュリティデバイスの RIP 動的ルーティングプロトコルの構成方法について説明します。
- 第 5 章「境界ゲートウェイプロトコル」、では、セキュリティデバイスの BGP 動的ルーティングプロトコルの構成方法について説明します。
- 第 6 章「ポリシーベースのルーティング」では、トラフィックをネットワークの特定のパスを通過させる方法について説明します。
- 第 7 章「マルチキャストルーティング」、では、マルチキャストルーティングの基本的な概念を紹介します。
- 第 8 章「IGMP (Internet Group Management Protocol)」、では、セキュリティデバイスの IGMP (インターネットグループ管理プロトコル) の構成方法について説明します。
- 第 9 章「プロトコル独立マルチキャスト」、では、セキュリティデバイスの PIM (プロトコル独立マルチキャスト) ルーティングプロトコルの構成方法について説明します。
- 第 10 章「ICMP ルーター検出プロトコル」では、ホストとルーターの間の ICMP（インターネット制御メッセージプロトコル）メッセージ交換をセットアップする方法について説明します。

第8 部 : アドレス変換

- 第 1 章、「アドレス変換」、はさまざまな変換オプションの概要。詳細は、これ以降の各章で説明します。
- 第 2 章 、「ソースネットワークアドレス変換」、はソース IP アドレスのパケットのヘッダーの変換 (NAT-src) を説明しています。ポートアドレス変換 (PAT) の有無についても説明ていします。
- 第 3 章 、「宛先ネットワークアドレス変換」、は宛先 IP アドレスのパケットのヘッダーの変換 (NAT-dst) について説明しています。宛先ポートアドレスのマッピングの有無についても説明しています。さらに、NAT-src を実行する場合のパケットフロー情報、ルーティングの留意点、アドレスシフティングについても説明しています。
- 第 4 章 、「マップアドレスと仮想アドレス」、はある宛先 IP アドレスから別のアドレスへの、IP アドレス単体 (マップ IP) に基づくマッピング、または宛先 IP アドレスと宛先ポート番号に基づくマッピング (仮想 IP) について説明しています。

第9 部: ユーザー認証

- 第 1 章「認証」では、ScreenOS がサポートする様々な認証方法とその用途について説明します。
- 第 2 章「認証サーバー」では、外部認証サーバーとなる可能性のある RADIUS、SecurID、LDAP の 3 種類のうちのいずれか 1 つあるいは内部データベースを使用するオプションについて説明し、さらにそれぞれと連動させるためのセキュリティデバイスの構成方法について説明します。
- 第 3 章「インフラネットの認証」では、統合型アクセス制御（UAC）ソリューションで、セキュリティデバイスが配備される方法を詳説します。Juniper Networks 統合型アクセス管理 ソリューション（UAC）は、企業インフラネットを横断したアプリケーションおよびサービスの配布を、安全かつ確実に行います。
- 第 4 章「認証ユーザー」では、認証ユーザーのプロファイルを定義する方法と、ローカルまたは RADIUS 認証サーバーのどちらかに格納されているユーザーグループに認証ユーザーを追加する方法を説明しています。
- 第 5 章「IKE、XAuth、および L2TP ユーザー」では、IKE ユーザー、XAuth ユーザー、および L2TP ユーザーを定義する方法について説明しています。XAuth セクションではセキュリティデバイスを XAuth サーバーとして使用する方法を中心に説明していますが、サブセクションで高性能なセキュリティデバイスを XAuth クライアントとして動作させるための構成方法についても説明します。
- 第 6 章「ワイヤレスおよびイーサネットインターフェース用の拡張認証」、では、イーサネットおよびワイヤレスインターフェースの認証を行う、拡張認証プロトコル（EAP）で利用可能なオプションとプロトコルの使用例を説明します。

第 10 部: 仮想 システム

- 第 1 章「仮想システム」では、仮想システム、オブジェクト、管理タスクについて解説します。
- 第 2 章「VLAN ベースのトラフィック分類」、は仮想システムの VLAN ベーストラフィック分類および VLAN タギングについて説明します。
- 第 3 章「トラフィックの振り分け」、は ScreenOS がトラフィックを振り分ける方法を説明します。
- 第 4 章、「IP ベースのトラフィック分類」、は仮想システムの IP ベーストラフィック分類を説明します。

第 11 部 : 高可用性

- 第 1 章 、「NetScreen 冗長プロトコル」、は、NetScreen 冗長性プロトコル (NSRP) を使用した高い可用性 (HA) を提供するために冗長グループで Juniper Networks セキュリティデバイスを配線、構成、および管理する方法を説明します。
- 第 2 章 、「インターフェースの冗長性および フェールオーバー」、は、Juniper Networks セキュリティデバイスがインターフェースの冗長性を提供する種々の方法を説明します。

第 12 部 : WAN、DSL、ダイアル、およびワイヤレス

- 第 1 章、「ワイドエリアネットワーク」では、ワイドエリアネットワーク（WAN）を構成する方法を説明します。
- 第 2 章「デジタル加入者線」、では、セキュリティデバイスの ADSL (非対称デジタル加入者線) インターフェースについて説明します。ADSL は、既存の電話回線を使って音声電話サービスと高速デジタル伝送を可能にする DSL (デジタル加入者線) テクノロジです。
- 第 3 章、「ISP フェールオーバーとダイヤル回復」では、ISP フォールオーバーの際の優先順位の設定方法および条件の定義方法、そしてダイヤルアップリカバリソリューションの設定方法について説明します。
- 第 4 章、「ワイヤレス ローカル エリア ネットワーク」では、Juniper Networks ワイヤレスデバイス上のワイヤレスインターフェースについて説明し、その構成例を示します。

第 13 部 : ジェネラルパケットラジオサービス

- 第 1 章「GPRS」、では ScreenOS の GPRS トンネリングプロトコル (GTP) 機能を説明し、GTP 機能性を Juniper Networks セキュリティデバイスで構成する方法を示します。

第 14 部 : IPv6 によるデュアルスタックアーキテクチャ

- 第 1 章、「インターネットプロトコルバージョン 6 の紹介」は、IPv6 のヘッダー、概念、およびトンネリングのガイドラインを説明しています。
- 第 2 章、「IPv6 の構成」は、IPv6 ルーターまたはホストとして動作するためのインターフェースの構成方法を説明しています。
- 第 3 章「接続およびネットワークサービス」は、動的ホスト構成プロトコルバージョン 6（DHCPv6）、ドメイン名サービス（DNS）、PPPoE（Point-to-Point Protocol over Ethernet）、およびフラグメント化を構成する方法を説明しています。
- 第 4 章「静的および動的ルーティング」は、静的および動的ルーティングをセットアップする方法を説明しています。この章では、RIPng（Routing Information Protocol-Next Generation）の ScreenOS によるサポートについて説明します。
- 第 5 章、「アドレス変換」は、IPv4/IPv6 境界を通過するため、ネットワークアドレス変換（NAT）を動的 IP（DIP）およびマップ IP（MIP）アドレスと使用する方法を説明しています。

- 第 6 章「IPv4 環境での IPv6」、では、手動による、または動的なトンネリング方法を説明します。
- 第 7 章、「IPSec トンネリング」では、異種ホストを接続するため IPSec トンネリングを構成する方法を説明しています。
- 第 8 章「IPv6 XAuth ユーザー認証」、では、RADIUS（Remote Authentication Dial In User Service）および IPSec アクセスセッション（IAS）管理を構成する方法を説明しています。
- 付録 A、「スイッチング」では、IPv6 トラフィックを通過させるためスイッチとしてセキュリティデバイスを使用するオプションを示します。

ドキュメントの規則

このドキュメントは、次のセクションで説明されている規則を使用しています。

- lvi ページの「Web ユーザーインターフェースの規則」
- lvi ページの「コマンドラインインターフェースの規則」
- lvii ページの「ネーミング規則および文字タイプ」
- lviii ページの「説明図の規則」

Web ユーザーインターフェースの規則

WebUI（Web ユーザーインターフェース）では、各作業の操作指示は、操作手順と構成設定値に分かれています。構成設定を入力できる WebUI ページを開くには、画面の左側にあるナビゲーション ツリーのメニュー項目をクリックして、そのページに移動します。先へ進むと、ナビゲーション パスが画面の上部に表示されます。各ページは角括弧で分離されています。

WebUI のパスおよびアドレスを定義するためのパラメータは、以下のとおりです。

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask :(**選択**), 10.2.2.5/32
Zone: Untrust

構成設定のオンラインヘルプを開くには、画面の左上にある疑問符（?）をクリックします。

ナビゲーションツリーにも、Help > Config Guide 構成ページがあり、セキュリティポリシーおよび IPSec （インターネットプロトコルセキュリティ）の構成に役立ちます。ドロップダウンメニューからオプションを選択して、そのページの指示に従います。構成設定のオンラインヘルプを開くには、左上にある **?** 文字をクリックします。

コマンドラインインターフェースの規則

次の規則は、例とテキストにおいて、コマンドラインインターフェース（CLI）コマンドの構文を示すために使用されます。

例においては、次のように使用されます。

- 角括弧 [ ] 内にあるものはすべてオプションです。
- 中括弧 { } 内にあるものはすべて必須です。
- 選択肢が複数ある場合、各選択肢はパイプ (|) で区切られています。例えば、次のように表示されます。

```
set interface { ethernet1 | ethernet2 | ethernet3 } manage
```

- 変数は*斜体*で表示されます。

  set admin user *name1* password *xyz*

テキストにおいては、コマンドは**太字**で、変数は*斜体*で表示されます。

注 : キーワード入力時には、単語を間違いなく識別できる数の文字を入力すれば十分です。**set admin user wheezer j12fmt54** というコマンドを入力する際には、**set adm u whee j12fmt54** と入力するだけで十分です。ただし、本編に記載されたコマンドはすべて本来の形式で記載されています。

ネーミング規則および文字タイプ

ScreenOS はオブジェクトの名前 (アドレス、管理ユーザー、認証サーバー、IKE ゲートウェイ、仮想システム、VPN トンネルおよびゾーンなど、ScreenOS 構成に定義されているもの) に関して、次の規則に従います。

- 名前文字列に 1 つまたは複数のスペースが含まれる場合、文字列全体を二重引用符で囲む必要があります。例 :

  set address trust “local LAN” 10.1.1.0/24

- 二重引用符で囲まれた文字列の先頭または末尾のスペースを取り除きます。たとえば、**「 local LAN 」**は**「local LAN」**となります。

- 連続した複数のスペースは、一つのスペースとして扱われます。

- CLI キーワードの多くはケースセンシティブではありませんが、名前文字列はケースセンシティブです。たとえば、**「local LAN」**は**「local lan」**とは異なります。

ScreenOS は、次の文字タイプをサポートします。

- 1 バイト文字セット (SBCS) およびマルチバイト文字セット (MBCS)。SBCS の例に、ASCII、欧州言語、およびヘブライ語があります。2 バイト文字セット (DBCS) とも呼ばれる MBCS の例に、中国語、韓国語、および日本語があります。

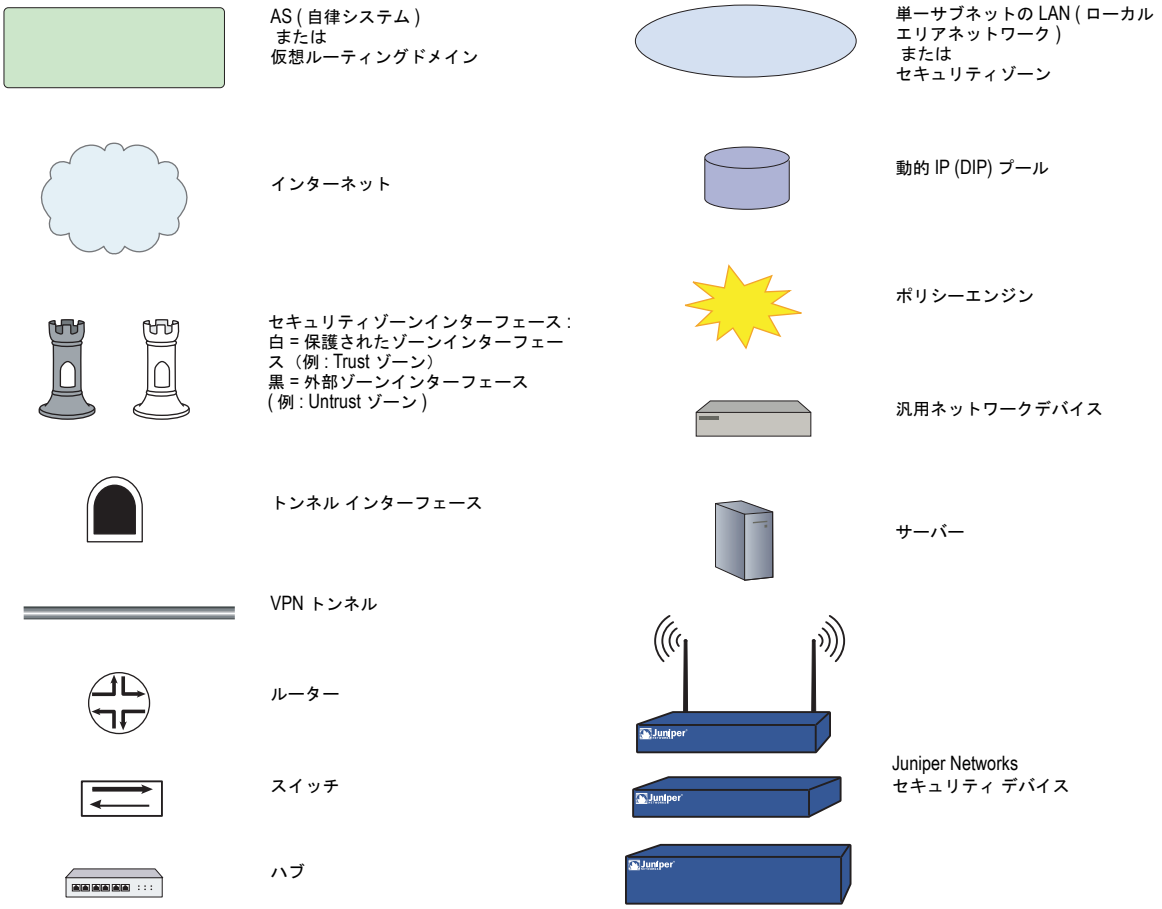
- ASCII 文字の 32（16 進数の 0x20）から 255（0xff)。ただし二重引用符 (“) は、スペースを含む名前文字列の先頭と末尾を示す特殊な意味をもつため、例外とします。

注 : コンソール接続では、SBCS のみがサポートされます。ご利用のブラウザがサポートする文字セットに応じて、WebUI は SBCS および MBCS の両方をサポートします。

説明図の規則

次の図は、本編を通して説明図に使用されている画像の基本的なものです。

図 2: 説明図の画像



技術ドキュメントおよびテクニカルサポート

Juniper Networks 製品のいずれかの技術ドキュメントを入手するには、www.juniper.net/techpubs/ をご覧になってください。

テクニカルサポートについては、http://www.juniper.net/customers/support/ にある Case Manager を使って事例サポートを開くか、1-888-314-JTAC (米国内) か 1-408-745-9500 (その他の国) までお問い合わせください。

本書に間違いや欠落があった場合は、techpubs-comments@juniper.net までお知らせください。

索引

数字

2 次 IP アドレス 51
3 方向ハンドシェイク 36
3DES 6
3DES 暗号化 117
4in6 トンネリング
　基本セットアップ 111
　定義 111
6in4 トンネリング 107
　IPv4 WAN 上 115
　基本セットアップ 116
6over4 トンネリング
　アドレス、処理 96
　手動トンネリング 96
　種類 95
　使用する時 95
　定義 95
6to4
　アドレス 8, 99, 104
　トンネリング 95, 99
　トンネリング、説明 99
　ホスト 104
　リレールーター 99, 100
　ルーター 99

A

AAL5 カプセル化 66
AAL5 複合 74
ACL 133
ActiveX コントロール、ブロッキング 170
administrative traffic 29
admins 2
　種類 4
　パスワードの変更 4, 7
ADSL
　VPN トンネル 99
　インターフェースの構成 74
　概要 74
AES 6
AES (次世代標準暗号)AES 6
AES128 暗号化 116
AH 3, 6
ALG 59, 17
　SIP 13
　SIP NAT 23
ALGALG
　MS RPC 130
　RTSP 132
　Sun RPC 129
　カスタムサービス 169
APN
　選択モード 16
　フィルタリング 15–16
ARP 84, 55
　ブロードキャスト 29
　ルックアップ 39
ARP、入口 IP アドレス 87
ATM 67
ATM Adaptation Layer 5 74
AV オブジェクト
　タイムアウト 89
AV スキャン 62–87
　FTP 72
　HTTP 73
　HTTP キープアライブ 85
　HTTP トリックリング 85
　IMAP 75
　MIME 75
　POP3 75
　SMTP 77
　解凍 90
　クライアントあたりの AV リソース 83
　購読 80
　故障モード 83
　ファイル拡張子 91

B

BGP
　AS-path アクセスリスト 120
　external 109
　仮想ルーター、インスタンスの作成 111
　近隣ノード、認証 117
　構成、確認 116
　コミュニティ 128
　コンフェデレーション 127
　正規表現 120
　設定、セキュリティ 117
　内部 109

BGP（続き）
パス属性 109
パラメータ 118
プロトコルの概要 108
メッセージタイプ 108
ロードバランス 39
BGP 使用可能
VR での 111
インターフェース上 112
BGP ルート
おもみ、設定 122
再配布 120
条件付きアドバタイズメント 122
除外 130
属性、設定 123
追加 121
デフォルト、拒否 118
リフレクション 125
BGP ルート、集約
AS-Path の 131
AS-Set の 129
の属性 132
BGP 、構成
peers 113
ステップ 110
ピアグループ 113
BGP ルート
集約 129
bypass-auth 67

C

C ビットパリティモード 13
CA 証明書 22, 25
CHAP 207, 211, 77
Chargen 131
CLI 9, 30, 32
CLI 、vip マルチポートを設定 80
CLI、set arp always-on-dest 76, 79
CompactFlash 56
CRL
CRL (証明書の取り消しリスト) を参照
CSU 互換性、T3 インターフェース 20

D

DC コードポイントマーキング 196, 202, 216
DDoS 29
DES 6
DHCP 98, 102, 247, 131
client 227
HA 233
PXE など 239
サーバー 227
リレーエージェント 227
DHCPv6
TLA と SLA 37
委譲されたプレフィックス 38
クライアントとサーバー 36
目的 35
DI (徹底監視) 138–162
カスタムシグネチャ 159–162
攻撃アクション 141–148
攻撃オブジェクトデータベース 122–129
顧客サービス 154–158
正規表現 159–160
Diffie-Hellman 10
Diffie-Hellman グループ 116
DiffServ 176, 202, 216
DC コードポイントマーキングも参照
DIP 101, 143–146, 96
PAT 144
グループ ..... 155, ??–157
固定ポート 145
プール 171
プール、変更 145
DIP プール
NAT-Src 1
VPN の NAT 137
アドレスに関する留意点 14
拡張インターフェース 137
サイズ 14
Discrete multitone
DMT を参照
DMT 69, 70
DN 182
DNS 219, 131
アドレス、分割 226
サーバー 248
サーバー、トンネリング 225
状況テーブル 221
ルックアップ 220
ルックアップ、ドメイン 225
DNS (ドメイン名システム) アドレス
変換 91
DNS、L2TP 設定 211
Domain Name System (DNS) addresses
分割 44, 45
DoS
OS 指定 52–55
セッションテーブルフラッ 18, 30
ネットワーク 36–51
ファイアウォール 30–35
DoS 攻撃 29–55
drop-no-rpf-route 20
DSL 242, 247
dynamic IP 80
dynamic IP, from IPv6 to IPv4 81

E

ECMPECMP 39, 62
ESP 3, 6
　暗号化と認証 52, 58
　暗号化のみ 52
　認証のみ 52
exe ファイル、ブロッキング 171
E メール警報通知 71, 73

F

filter source route 97
FIN スキャン 15
Finger 132

G

Gi インターフェース 2
Gn インターフェース 2
Gopher 132
Gp インターフェース 2
GPRS トンネリングプロトコル (GTP)
　GTP を参照
GTP
　GTP-in-GTP パケットフィルタリング 14
　IMSI プレフィックスフィルタリング 17
　IP フラグメント化 14
　アクセスポイント名 (APN) のフィルタリング ..15
　基準 9
　検査オブジェクト 5–7
　トンネルタイムアウト 26
　パケットサニティチェック 9
　パケット状態監視 25
　プロトコル 2
　ポリシーベース 5
GTP トラフィック 34, 32
GTP トンネル
　制限 24
　タイムアウト 26
　フェールオーバー 26
GTP メッセージ 10, 11, 12
　種類 10–11
　長さ、フィルタリング 9

H

HA
　NSRP も参照
　DHCP 233
　インターフェース、仮想 HA 39
　高可用性を参照
HA (high availability、高可用性) 4, 26
HMAC 6
HMAC (ハッシュベースメッセージ認証コード) 6
Host モード 46, 112
HTTP
　キープアライブ 85
　コンポーネントのブロッキング 170–171
　セッションタイムアウト 33
　トリックリング 85
HTTP、セッション ID 4
HTTP（ハイパーテキスト転送プロトコル）、セッション ID 4

I

ICMP 132
　フラグメント 240
　ラージパケット 241
ICMP サービス 128
　メッセージコード 128
　メッセージタイプ 128
ID アソシエーションプレフィックス委譲 ID（IAPD-ID） 37, 39
IDENT 132
Ident-ResetIdent-Reset 28
IDP
　インラインモードまたはインラインタップモードの指定 188
　基本設定 176
　デバイスのスタンドアロン IDP 用の構成 230
　ファイアウォールルールで使用可能にする 187
IDP エンジン
　更新 235
IDP エンジンの更新 235
IDP 攻撃オブジェクト 186
IDP 対応システム 174
IDP モード 188
IDP ルール 189
　IDP 攻撃オブジェクトの構成 186
　IP アクションの構成 200
　Match 列の構成 191
　アクションの構成 197
　アドレスオブジェクトの構成 186
　攻撃の構成 198
　攻撃の重大度の構成 202
　構成 191
　コメントの入力 202, 206, 212
　サービスオブジェクトの構成 186
　サービスの構成 193
　ソースおよび宛先の構成 192
　ターゲットの構成 202
　ターミナルルールの構成 195
　通知の構成 201
IDP ルールベース
　概要 189
　種類 185
　セキュリティポリシーへの追加 190
　役割ベースの管理 186
IEEE 802.1Q VLAN 規格 31

IGMP
アクセスリスト、利用 ... 163
インターフェース、稼動 ... 162
クエリア ... 161
構成、確認 ... 166
設定、基本 ... 164
パラメータ ... 166, 167
ホストメッセージ ... 161
ポリシー、マルチキャスト ... 173
IGMP (Internet Group Management Protocol)
IGMP を参照
IGMP プロキシ ... 168
インターフェース上 ... 170
送信側 ... 180
IKE ... 7, 84, 93, 159
IKE ID ... 49, 50, 55, 56
IKE ID に関するアドバイス ... 68
IKE ID、Windows 2000 ... 220, 227
共有 IKE ID ユーザー ... 197–203
グループ IKE ID ユーザー ... 182–197
グループ IKE ID、コンテナ ... 185
グループ IKE ID、ワイルドカード ... 185
冗長ゲートウェイ ... 294, 306
第 1 段階提案、定義済み ... 9
第 2 段階提案、定義済み ... 11
ハートビート ... 296
ハローメッセージ ... 296
プロキシ ID ... 11
リモート ID、ASN1-DN ... 185
IKE ユーザー ... 63–66
IKE ID ... 63, 77
グループ ... 63, 64
グループ、定義グループ、定義 ... 65
サーバーサポート ... 12
定義 ... 64
他のユーザータイプ ... 4
IMSI プレフィックスフィルタリング ... 17
in-short エラー ... 94
Interior Gateway Protocol (IGP) ... 51
IP
パケットフラグメント ... 244
IP (インターネットプロトコル) アドレス
IP アドレスを参照
IP アドレス
2 次、ルーティング ... 52
2 次 ... 51
NetScreen-Security Manager サーバー ... 25
インターフェース、トラッキング ... 64
拡張 ... 137
管理 ... 97
管理 IP ... 31
公開 ... 47
ネットワーク ID ... 48
非公開 ... 47
IP アドレス（続き）
非公開アドレス範囲 ... 48
ポート、定義 ... 106
ホスト ID ... 48
IP アドレス、仮想 ... 79
IP オプション ... 10–11
record route ... 11
stream ID ... 11
timestamp ... 11
ストリクトソースルート ... 11, 24–26
セキュリティ ... 10, 11
ソースルート ... 24
属性 ... 10–11
不正なフォーマットの ... 242
ルーズソースルート ... 10, 24–26
IP スプーフィング ... 19–24
Layer 2 ... 20, 23
Layer 3 ... 19, 21
drop-no-rpf-route ... 20
IP セキュリティ
IPSec を参照
IP トラッキング ... 55, 111
vsys ... 65
ping と ARP ... 55
インターフェース、共有 ... 65
インターフェース、サポートされる ... 64
ウェイト ... 66
オブジェクトの障害しきい値 ... 66
動的オプション ... 65
トラフィックの再ルーティング ... 64–80
IP トラッキング、障害
入口インターフェース、オン ... 78–80
出口インターフェース、オン ... 77–78
トラックされる IP のしきい値 ... 66
IP プール
DIP プールを参照
IP ベースのトラフィック分類 ... 71
IPSec
AH ... 2, 51, 57
ESP ... 2, 51, 57
L2TP-over-IPSec ... 4
SA ... 2, 8, 11
SPI ... 2
デジタル署名 ... 20
トランスポートモード ... 4, 207, 213, 218
トンネル ... 2
トンネルネゴシエーション ... 8
トンネルモード ... 4
セキュリティアソシエーション
SA を参照
IPSec Access Session (IAS) ... 128
IPv4
addresses, mapped ... 80, 84
WAN ... 108

IPv4 to IPv6
host mapping....89
network mapping....87
IPv4/IPv6 boundaries....87
IPv4/IPv6 境界....79–84
IPv6
addresses, SLA....37
backbone....83, 111
networks, island....108
アドレス、TLA....37
IPv6 to IPv4 host mapping....86
IPv6/IPv4 boundaries....80–86
IP アドレス
L3 セキュリティゾーン....47–48
IP を管理する....97
ISP....225
Priority....109
フェールオーバーホールドダウンタイマー....110
ISP IP アドレスとネットマスク....73

J

Java アプレット、ブロッキング....171

K

keys
事前共有....159
手動....116, 122

L

L2TP....205–231, 3
Hello 信号....216, 222
RADIUS サーバー....211
ScreenOS サポート....207
SecurID サーバー....211
Windows 2000 で L2TP のみを使用....207
Windows 2000 トンネル認証....216, 221
アクセスコネクター
アドレス割り当て....82
外部認証サーバー....82
カプセル化 L2TP....208
キープアライブ....216, 222
強制構成....205
双方向....207
脱カプセル化....209
デフォルトパラメータ....211
動作モード....208
トンネル....213
任意構成....205
ネットワークサーバー
ユーザー認証....82
ローカルデータベース....82
L2TP ユーザー....82
XAuth と共に....4
サーバーサポート....12
L2TP-over-IPSec....4, 213, 218
双方向....207
トンネル....213
L2TP ポリシー....170
LAC....205
LAC を参照
NetScreen-Remote 5.0....205
Windows 2000....205
LDAP....132, 27–28
構造....27
サーバーポート....28
識別名....28
通称名識別子....28
ユーザータイプサポート....28
LNS
LNS を参照
LPR スプーラ....132

M

MAC アドレス....13, 21, 29
mapped IP (MIP)
IPv4 ホストから単一 IPv6 ホストへの送信....89
IPv4 ホストから複数 IPv6 ホストへの送信....87
IPv6 から IPv4 への MIP....82
IPv6 ホストから単一 IPv4 ホストへの送信....86
IPv6 ホストから複数 IPv4 ホストへの送信....84
IPv6-to-IPv4 ネットワークマッピング....84
MD5....6
America Online Instant MessagingAmerica Online Instant Messaging
AIM を参照
MGT インターフェース、管理オプション....29
MGT インターフェース....38
MIB II....28, 74
MIB ファイル、インポート....255
Microsoft Network Instant MessengerMicrosoft Network Instant Messenger
MSN Instant Messenger を参照
Microsoft-Remote Procedure CallMicrosoft-Remote Procedure Call
MS-RPC を参照
MIME、AV スキャン....75
MIP....12, 61, 80
Global ゾーン....62
Untrust ゾーンとして扱うインターフェース....69–71
アドレス範囲....64
グルーピング、マルチセルポリシー....78
他のゾーンから到達可能....65
定義....6
両方向の変換....6

MIP 作成
アドレス 63
ゾーンインターフェース上に 63
トンネルインターフェース上に 68
MIP 、デフォルト MIP
仮想ルーター 64
MIP、VPN 138
MIP、インターフェースベースの NAT を使ったゾーン向け 96
MIP 、デフォルト MIP
ネットマスク 64
mode config 67
MS RPC ALG、定義済み 130
MS-RPCMS-RPC 134

N

NAT
IPSec および NAT 234
NAT サーバー 234
NAT-src と NAT-dst 49–60
定義 1
NAT ベクタエラー 96
NAT モード 94–100, 2, 4
Untrust ゾーンに向かうトラフィック 81, 96
インターフェース設定 97
NAT-dst 28–60
MIP や VIP との同時使用 4
VPN 138
アドレスシフティング 5
一方向の変換 7, 10
パケットフロー 29–31
ポートマッピング 4, 28, 46
ルートに関する留意点 29, 32–34
NAT-dst, 、アドレス
1 対多の変換 38
シフティング 28, 43
所定の範囲の IP アドレスを特定の IP アドレスに変換 10, 40
範囲 4
範囲から範囲 10, 43
NAT-dst 、単一 IP
ポートマッピング 9
ポートマッピングなし 9
NAT-dst, 、アドレス
1 対 1 の変換 35
NAT-PT 79
NAT-PT, IPSec, when to use 108
NAT-Src 1, 13–25
egress インターフェース 23–25
VPN 140
インターフェースベース 2
固定ポートナンバー 14
NAT-src 、DIP プール 1
PAT あり 7, 14–17
アドレスシフトで変換 8
固定ポートナンバー 8
NAT-src 、アドレス
シフティング 19–23
シフティング、範囲に関する留意点 20
NAT-src 、変換
一方向 7, 10
ポートアドレス 2
NAT-src、Route モード 100
NAT-T 234–242
IKE パケット 237
IPSec パケット 238
NAT の精査 235–236
VPN の障 Q 物 237
イニシエータとレスポンダ 240
キープアライブの周期 240
使用可能 241
NAT-Traversal
NAT-T を参照
Neighbor Solicitation (NS)
設定 30
NetBIOSNetBIOS 134
NetInfo 228
NetScreen Reliable Transport Protocol
NSTP を参照
NetScreen 冗長プロトコル
NSRP を参照
NetScreen-Remote
NAT-T オプション 234
VPN AutoKey IKE 159
動的ピア 164, 171
NetScreen-Security Manager
NSM エージェント 22, 25
NSM エージェントを使用可能にする 24
UI 22
イベントのレポート 25
管理オプション 28
管理システム 22, 23, 25
接続の初期設定 23
定義 22
ロギング 25
Network Address Translation-Port Translation (NAT-PT) 79
NFS 132
NHTB テーブル 256–261
アドレス計画 259
自動入力 261
手動入力 260
ルートをトンネルにマッピングする 257
NNTP 132
NRTP 19

NSM エージェント 22, 23
イベントのレポート 25
使用可能 24
NSRP 1
ARP ブロードキャスト 29
ARP ルックアップ 39
clear cluster コマンド 10
debug cluster コマンド 10
DHCP 233
DIP グループ 155, 157
HA セッションバックアップ 174
hold-down 時間 36, 38
NAT モードとルートモード 2
NTP 同期化 260, 20
RTO 34
VSD グループ 183, 20, 34
VSI 38, 2
VSI、静的ルート 24, 69, 70
インターフェース監視 29
仮想システム 58–87
管理 IP 55
冗長インターフェース 37
冗長ポート 2
制御メッセージ 7, 13
セカンダリパス 29
セキュア通信 29
デフォルトの設定 6
同期設定 19
配線 25–28
パケット転送と動的ルーティング 8
バックアップ 11
負荷分散 83
プリエンプトモード 21
フルメッシュ構成 25, 58
マスタ 11
優先順位番号 21
NSRP HA
インターフェース 6
セッションバックアップ 15
配線、ネットワークインターフェース 27
ポート、冗長インターフェース 43
NSRP-Lite 19
クラスタ 11
セキュア通信 15
NSRP-Lite 同期化
使用不可 18
NSRP RTO 15–16
状態 16
同期 19
NSRP クラスタ 30, 34
名前 11, 28
NSRP データ 8
メッセージ 7
NSRP 同期化
NTP, NSRPNTP, NSRP 20
RTO 19
NSRP ポート
フェールオーバー 43
NTP 258–261, 132
NSRP 同期化 260
サーバー 258
最大時間調整 259
セキュアサーバー 260
認証タイプ 261
複数のサーバー 258
NTP 、NSRP 同期化 NTP 、NSRP 同期化 20
Null ルート 83

O

OCSP (オンライン証明書ステータスプロトコル) .. 34
client 34
レスポンダ 34
OSPF
ECMP への対応 62
Hello プロトコル 51
LSA の省略 71
LSA フラッディングの省略 L 71
Tunnel インターフェース 72
インターフェースパラメータ 66
インターフェース、エリアに割り当て 57
仮想リンク 63
近隣ノード、認証 68
近隣ノード、フィルタリング 69
準スタブエリア 51
スタブエリア 51
セキュリティ設定 68
接続状態の通知 50
設定の手順 53
大域パラメータ 62
フラッディングの回避 70
ブロードキャストネットワーク 52
ポイントツーポイントネットワーク 52
ポイントツーマルチポイント 72
リンクタイプ、設定 73
ロードバランス 39
OSPF エリア 50
インターフェース、エリアに割り当て 57
定義 55
OSPF ルーター
VR 上にインスタンス作成 54
種類 51
代表 51
バックアップ代表 51
隣接関係 51

OSPF ルート
route-deny 機能、無効化 ... 73
再配布 ... 60
再配布、要約 ... 61
デフォルト、拒否 ... 70

P

P2PP2P ... 134
BitTorrentBitTorrent ... 134
DC ... 134
eDonkeyeDonkey ... 134
FastTrackFastTrack ... 134
Gnutella ... 134
KaZaa ... 134
MLdonkeyMLdonkey ... 134
SkypeSkype ... 134
SMB ... 134
WinMXWinMX ... 134
PAP ... 207, 211
PAT ... 144, 14
PCMCIA ... 56
PFS ... 11, 51, 57
PIM-SM ... 190, 194
IGMPv3 ... 221
インスタンス、作成 ... 195
インターフェースパラメータ ... 210
集合地点 ... 191
集合地点の設定 ... 205
セキュリティ設定 ... 207
設定の手順 ... 195
代表ルーター ... 191
トラフィック、転送 ... 192
プロキシ RP ... 212
ping
管理オプション ... 28
Ping of Death ... 52
PKI (公開鍵基盤) ... 22
PKI 鍵 ... 6
Point-to-Point Protocol (PPP) ... 46
Point-to-Point Protocol over ATM
PPPoA を参照
Point-to-Point Protocol over Ethernet
PPPoE を参照
PPP ... 206, 66
PPPoA ... 66, 68, 74
PPPoE ... 66, 74
PPPoE - Point-to-Point Protocol over Ethernet ... 46
protocol distribution、NetScreen-Security Manager へのレポート ... 25
PXE ... 239
PXE サーバー ... 240

Q

QoS ... 195

R

RA
ルーター通知 ... 12
RADIUS ... 39, 132, 17–20
L2TP ... 211
オブジェクトのプロパティ ... 18
共有秘密値 ... 18
再試行タイムアウト ... 18
ディクショナリーファイル ... 2, 19
認証サーバーオブジェクト ... 31
ポート ... 18
RADIUSv6 ... 126
record route IP option ... 11
request packets, outgoing from IPv6 to IPv4 ... 82
rexec ... 132
RFC
0792, *インターネット制御メッセージプロトコル* 128
1918, *Address Allocation for Private Internets* ... 48
2326, *Real Time Streaming Protocol (RTSP)* ... 132, 137
1349, *1349、インターネットプロトコルスイートのサービスのタイプ* ... 176
2474, *2474、IPv4、IPv6 ヘッダーの差別化フィールド（DS フィールド）の定義* ... 176
793, *793、Transmission Control Protocol* ... 13
2132, *DHCP Options and BOOTP Vendor Extensions* 232
791, *Internet Protocol* ... 10
1038, *Revised IP Security Option* ... 10
RFC 1777、*Lightweight Directory Access Protocol* ... 27
RIP
インスタンス、VR で作成 ... 80, 54
インターフェースパラメータ ... 89, 60
インターフェース、稼動 ... 81, 55
近隣ノードの認証 ... 90
近隣ノード、フィルタリング ... 57
構成 ... 53
大域パラメータ ... 87, 55
データベース ... 97
バージョン ... 94
バージョン、プロトコル ... 94
フラッディングの回避 ... 92, 59
プレフィックスサマリ ... 96
ポイントツーマルチポイント ... 100
要求回路の設定 ... 99
隣接ノードのフィルタリング ... 91
ロードバランス ... 39
RIP ルート
再配布 ... 81, 58
代替 ... 97
デフォルトを拒否 ... 92
デフォルト、拒否 ... 57
要約、設定 ... 96

RIP 、設定
ステップ....79
デマンド回線....99
セキュリティ....90
RIP 、表示
インターフェース詳細....86
近隣ノード情報....85, 66
データベース....84, 65
プロトコル詳細....84, 65
RIPng....49, 51
インターフェースコストメトリック 60, 61
オフセットメトリック....60, 61
メトリックの計算....61
ルート情報の再配布....51
ルートのメトリック....60, 61
rlogin....132
route tracking....111
Route モード....100–103
RSA 認証....116
rsh....132
RSH ALG 129
RTO....15–16
同期....19
動作状態....16
ピア....22
RTSP 132
RTSP ALG
ステータスコード....135
定義....132
パブリックドメイン内のメディアサーバー 139
プライベートドメイン内のメディアサーバー 137
要求メソッド....133

S

SA 8, 11
パケットフローのチェック....63
SA ポリシー 96
SCEP (簡易認証送受信プロトコル) 30
SCP
CLI コマンドの例....18
使用可能....18
SCREEN
IP スプーフィング 19–24
SYN フラッド 36–42
ScreenOS
Global ゾーン....28
RADIUS ベンダー ID....20
VR....6
概要....1
仮想システム....10
機能ゾーン....33
セキュリティゾーン....2, 28
セキュリティゾーン、Global....2
セキュリティゾーン、定義済み 2
ScreenOS（続き）
ゾーン....25, ??–33, 6
トンネルゾーン....29
パケットフロー....11, ??–13
ポリシー....3
ScreenOS インターフェース
サブインターフェース....3
セキュリティゾーン....3
SCREEN、MGT ゾーン....28
SDP....17–19
SecurID 25
ACE サーバー 26
Authentication Port....26
authenticator....25
L2TP....211
Use Duress オプション 26
暗号化のタイプ....26
トークンコード....25
認証サーバーオブジェクト....33
ユーザータイプサポート....26
SecurID クライアント
リトライ....26
SecurID クライアント SecurID
タイムアウト....26
Server Message BlockServer Message Block
SMB を参照
service requests, outgoing 84, 86
SHA-1 6
SIP
ALG....17, 20
RTCP 19
RTP....19
SDP 17–19
応答コード....16
シグナリング....17
接続情報....18
定義....13
ピンホール....17
マルチメディアセッション....13
メッセージ....14
メディア通知....18
要求メソッド....14
SIP NAT
DIP プールを使用 36
DMZ 内のプロキシ 45
Trust ゾーン内....52
Untrust ゾーン内....48, 96
VPN、フルメッシュの使用 54, 102
インターフェース DIP を使用 33
コール設定....23, 29
受信 DIP を使用 32
受信、MIP で....36, 38

SIP NAT（続き）
定義 23
パブリックゾーン内のプロキシ 43
プライベートゾーン内のプロキシ 40, 88
SIP タイムアウト
シグナリング無活動 21, 22
セッション無活動 21
無活動 21
メディア無活動 21, 22
Site-Local Aggregator (SLA) 37, 39
SMB
NetBIOSNetBIOS 134
SMTP サーバー IP 71
SNMP 28, 74
MIB ファイル、インポート 255
VPN 監視 255
暗号化 77, 78
管理オプション 28
構成 77
コールドスタートトラップ 74
SNMP トラップ
100, ハードウェア問題 75
200, ファイアウォール問題 75
300, ソフトウェア問題 75
400, トラフィック問題 75
500, VPN 問題 75
許可もしくは拒否 76
システム アラーム 75
種類 75
トラフィック アラーム 75
SNMPTRAP 133
SNMP コミュニティ
公開 77
非公開 77
SSH 11–16, 133
PKA 15
PKA 認証 14
PKA 認証のみを強制 16
管理オプション 28
公開鍵をロードする、CLI 15
公開鍵をロードする、TFTP 15, 17
公開鍵をロードする、WebUI 15
自動ログイン 17
接続手続き 12
認証方法優先度 16
パスワード認証 14
SSID
ワイヤレスインターフェースへのバインド 146
SSL 5, 133
WebAuth + SSL 59
SSL ハンドシェイクプロトコル
SSLHP を参照
SSLHP 5
stream ID IP オプション 11
Sun RPC ALG
定義 129
呼び出し手順 129
Super G 134
SurfControl 99, 108
SYN および FIN フラグセット 12
SYN クッキー 47
SYN チェック 16, 16–19
セッションテーブルフラッ 18
セッションの中断 17
調査ホール 18
非対称ルーティング 17
SYN フラグメント 245
SYN フラッド 36–42
SYN クッキー 47
宛先しきい値 41
アラームしきい値 40
キューサイズ 42
攻撃 36
攻撃しきい値 40
しきい値 37
ソースしきい値 41
タイムアウト 42
未知の MAC アドレスをドロップする 42
SYN-ACK-ACK プロキシフラッド 34
SYSLOG 56, 133
暗号化 78
機能 72, 81, 89
セキュリティ機能 73, 81, 89
ポート 72, 81, 89
ホスト 72
ホスト名 72, 73, 81, 88
メッセージ 72

T

T3 インターフェース
C ビットパリティモード 13
CSU 互換性 20
TACACS+
Client Retries 30
Client Timeout 30
オブジェクトのプロパティ 30
共有秘密値 30
再試行タイムアウト 30
認証サーバーオブジェクト 36
ポート 30
TCP
SYN フラグチェック 300
ストリームシグネチャ 162
セッションタイムアウト 33
フラグのないパケット 14
TCP proxy 97
Telnet 9, 133
Telnet 管理オプション 28

Telnet、によるログイン 10
TFTP 133
timestamp IP オプション 11
Top-Level Aggregator (TLA) 37
trace-route 87
Transparent モード、管理オプション 29
tunnel tracking 111
Tunnel インターフェース 39
  定義 39
  ポリシーベース NAT 39

U

UDP
  NAT-T のカプセル化 234
  セッションタイムアウト 34
  チェックサム 239
upstream routers 38
URL フィルタリング
  Web フィルタリングを参照
USB 56

V

VC 66
VCI 66
Verisign 34
VIP 12
  グローバルゾーン 81
  構成 81
  削除 83
  他のゾーンから到達可能 81
  定義 6
  必要な情報 79
  編集 83
VIP サービス
  カスタムおよび複数のポート 83–87
  カスタム、低いポートナンバー 80
VIP、インターフェースベースの NAT を使ったゾーン向け 96
virtual routers, RIP 53–68
VLAN
  VLAN ベースのトラフィック分類 31–57, 70
  作成 33–54
  サブインターフェース 51
  タグ 33, 51
  透過モード 32, 33
  トランク処理 32
  別の VLAN との通信 54–57, 69
VLAN ゾーン 83
VLAN ベースのトラフィック分類 31–57, 70
VLAN1
  インターフェースをチェックします 83, 89
  ゾーン 83
VLAN1、管理オプション 29
VLAN、タグ 3
VNC 133
VPI 66
VPI/VCI
  値 74
  構成 71
VPN
  AutoKey IKE 79, 43, 7
  Diffie-Hellman グループ 10
  Diffie-Hellman の鍵交換 10
  FQDN エイリアス 128
  MIP 138
  NAT-dst 138
  NAT-Src 140
  SA 8
  VPN 監視および再入力 244
  VPN グループ 294
  アグレッシブモード 10
  暗号オプション 46, 59
  インターフェースベースの NAT で保護されたゾーン向け 96
  オーバーラップしているアドレスの NAT 137, 148
  管理トラフィック用 78
  ゲートウェイの FQDN 127–137
  構成のヒント 66–68
  再生保護 12
  手動鍵 43, 79
  冗長グループ、復旧手順 298
  冗長ゲートウェイ 294–306
  トランスポートモード 4
  トンネルインターフェース 1 つあたりに複数のトンネル 256–292
  トンネルゾーン 29
  トンネルの常時作動 244
  パケットフロー 61–66
  フェーズ 1 9
  フェーズ 2 11
  プロキシ ID、一致 67
  ポリシー 170
  メインモード 9
  両方向のポリシー 123
  ルートベースとポリシーベース 59
VPN AutoKey IKE 43, 79, 7
  管理 7
VPN 監視 112
  ICMP エコー要求 255
  SNMP 255
  宛先アドレス 245–248
  宛先アドレス、XAuth 246
  再入力オプション 244, 261
  出力インターフェース 245–248
  状態変化 243, 247
  ポリシー 246
  ルーティング設計 68
VPN 待機時間 69

VR 40–45, 6
2 つを使用 26
BGP 110–117
ECMPECMP 39
OSPF 53–71
RIP 79–94
SBR 19
SIBR 22
VR 間のトラフィック転送 5
vsys 上の 29
アクセスリスト 43
共有 67
共有、作成 68
設定変更 24
はじめに 4
ルーター ID 25
ルートのメトリック 34
VR 、ルーティングテーブル
最大エントリ 32
VR 、ルーティングテーブル VR 、
複数の仮想ルーターにおけるルックアップ 36
VR 、ルート VR
選択 32
マップ 41
インポート 45
エキスポート中 45
フィルタリング 42
優先度 33
VRRP 55
VR 、ルート VR
再配布 40
VSA 19
VSA 属性タイプ 20
VSD グループ 183, 20
hold-down 時間 36, 38
ハートビート 23, 29
フェールオーバー 57
メンバー状態 22
優先順位番号 21
VSI 2, 20
VSD ごとの複数の VSI 58
静的ルーティング 24
vsys
admin 7
オブジェクト、作成 4

W

Web フィルタリング
SurfControl CPA サーバー 99
SurfControl SCFP 111
SurfControl サーバー 100
SurfControl サーバーポート 111
SurfControl サーバー名 111
Web フィルタリング（続き）
URL カテゴリ 102
vsys ごとのサーバー 110
Websense サーバーポート 111
Websense サーバー名 111
キャッシュ 101
組み込み型 99
サーバー状態 114
通信タイムアウト 111
ブロックされた URL メッセージ 113
ブロック済み URL メッセージタイプ 113
プロファイル 104
プロファイルをポリシーに適用 106
リダイレクト型 108
ルーティング 114
..... 174
Web ユーザーインターフェース
WebUI を参照
WebAuth 12, 45
SSL 59
外部ユーザーグループ 57
事前ポリシー認証 45
ユーザーグループ、ローカル 55
WebAuth、事前ポリシー認証手続き 173
WebTrends 56, 73
暗号化 73, 78
メッセージ 73
WebUI 1, 32
管理オプション 28
ヘルプファイル 2
WebUI、サンプルクライアント上、下流ルーター .40
Web ブラウザ要件 2
WEP 123
Whois 133
WinNuke 攻撃 54
WINS
L2TP 設定 211
WINS サーバー 126
Wired Equivalent Privacy （有線と同等のプライバシー）
WEP を参照
WLAN
DTIM 142
Super G の構成 134
WMM 136
XR 135
アクセス制御リスト 133
暗号化と認証 122
エージング間隔 140
拡張チャネル 132
国コードおよびチャネル 131
構成、再起動 134

WLAN（続き）
サイトの調査 132
詳細なパラメーター 140
スロット時間 145
送信可速度 144
送信可タイプ 144
送信可モード 144
送信要求しきい値 143
バーストしきい値 142
ビーコン間隔 141
フラグメントしきい値 143
プリアンブル長 145
ブリッジグループ 147
利用可能なチャネルの発見 133
ワイヤレス構成情報の表示 148
WLAN WAP 動作モード
802.11b クライアント、構成 119, 120
802.11g クライアント、構成 119
WLAN、ワイヤレスインターフェース
バインド 146
WMM
アクセスのカテゴリ 136
サービス品質の構成 136
使用可能 136
デフォルトの設定 137

X

XAuth
bypass-auth 67
TCP/IP 割り当て 68
VPN 監視 246
VPN 待機時間 69
外部 72
外部 XAuth 72
仮想アダプタ 66
クエリーリモート設定 67
クライアントとしての ScreenOS 81
クライアント認証 81
使用する時 126
定義 66
認証 132
ユーザー認証 72
XAuth アドレス
IP アドレス寿命 68–69
タイムアウト 68
認証 77
割り当て 66
XAuth ユーザー ??–80
L2TP と共に 4
サーバーサポート 12
認証 66
ローカルグループ 71
ローカル認証 70
66–??
XAuth、外部
ユーザーグループ認証 74
認証サーバー
XAuth クエリー 67
XR、構成 135

Y

Yahoo! Messenger 133

Z

zip ファイル、ブロッキング 171

あ

アイドルセッションタイムアウト 17
アクセスコンセントレータ（AC） 46
アクセス制御リスト
ACL を参照
アクセスポイント名
APN を参照
アクセスポリシー
ポリシーを参照
アクセスリスト
IGMP 163
PIM-SM 207
マルチキャストルーティング 155
ルートの 43
アグレッシブエージング 33–34
アグレッシブモード 10
宛先ゲートウェイ 96
宛先不明のユニキャストの処理方式 84–89
ARP 87–89
trace-route 87
フラッド 85–86
アドレス
MAC 13, 21, 29
IP、ホストおよびネットワーク ID 48
L2TP 割り当て 82
XAuth ユーザーの IP 寿命 68
公開 47
自動構成 11
定義 168
非公開 48
分割 44
ポリシー内 168
リンクローカル 12
アドレス帳エントリ 106–110
アドレスグループ 108, 168
エントリ、削除 110
オプション 108
作成 109
編集 110

アドレス帳
アドレス
削除 ... 110
設定変更 ... 107
追加 ... 106
アドレスも参照
エントリ ... 106
グループ ... 108
グループエントリ、編集 ... 110
アドレス否定 ... 188
アドレス変換
NAT, NAT-dst および NAT-src を参照
アドレス、XAuth
割り当て ... 66
アドレス、XAuth アドレス、XAuth
タイムアウト ... 68
アドレス、処理
4in6 トンネリング ... 111
6to4 トンネリング ... 101
IPv4 から IPv6 への DIP ... 82
IPv4 ホストから単一 IPv6 ホストへの送信 ... 108
IPv6 から IPv4 への DIP ... 81
IPv6 ホストから複数 IPv4 ホストへの送信 ... 84
宛先アドレス変換 ... 82
手動トンネリング ... 96
アドレス、重複範囲 ... 52, 72
アプリケーションオプション、ポリシーで ... 169
アプリケーションレイヤーゲートウェイ
ALG を参照
アラーム
トラフィック ... 69–71
アラーム、しきい値 ... 174
暗号オプション ... 46–59
ESP ... 52, 58
トンネルモード ... 58
IKE ID ... 49, 50, 55, 56
IPSec プロトコル ... 51, 57
PFS ... 51, 57
暗号化アルゴリズム ... 49–55, 58
鍵方式 ... 47
再生防止チェック ... 50, 57
サイトツーサイト ... 46–53
サイトツーサイト VPN の推奨オプション ... 53
証明書のビット長 ... 48, 54
ダイヤルアップ ... 53–59
ダイヤルアップ VPN の推奨オプション ... 59
トランスポートモード ... 58
認証アルゴリズム ... 49, 52, 55, 59
認証タイプ ... 48, 54
フェーズ 1 モード ... 47, 54
暗号化 ... 107, 111
3DES ... 117
AES128 ... 116
NSRP ... 29
暗号化（続き）
NSRP-Lite ... 15
アルゴリズム ... 6, 49, 52–58
暗号化と認証
Wi-Fi Protected Access （Wi-Fi 保護アクセス）
WPA を参照
Wired Equivalent Privacy （有線と同等のプライバシー）
WEP を参照
複数の WEP 鍵 ... 123
暗号化、SecurID ... 26

い

委託管理者 ... 109
移動端末 (MS) モード ... 16
イベントログ ... 57
インスタントメッセージ ... 133
AIM ... 133
IRC ... 133
MSN Messenger ... 133
Yahoo! Messenger ... 133
インターネット鍵交換
IKE を参照
インターネットサービスプロバイダ（ISP） ... 225, 36, 44, 96
インターフェース
DIP ... 143
Gi ... 2
Gn ... 2
Gp ... 2
MIP ... 62
null ... 83
VIP ... 79
VLAN1 ... 83
VSI ... 38
デフォルト ... 49
物理、vsys からのエクスポート ... 70
物理、vsys へのインポート ... 69
2 次 IP アドレス ... 51
DHCPv6 ... 35
HA 機能ゾーン ... 38
HA、二重 ... 8
IP トラッキング (IP トラッキングを参照)
L3 セキュリティゾーン ... 47
Manageable ... 31
MGT ... 38
ND ... 29
NDP ... 30
NUD ... 29
PPPoE ... 46
VSI ... 24
アップ、物理的 ... 62

インターフェース（続き）
アドレス設定....47
インターフェース表を表示する....43
インターフェース表、表示....43
拡張....137
仮想 HA....39, 27
監視....29
管理オプション....28
期限ゾーン....38
共有....67, 71
状態の変化....62
冗長....37, 43
セキュリティゾーンの物理....36
接続、監視....64
設定変更....49
専用....67, 71
ゾーンにバインドする....45
ゾーン、アンバインド....46
ダウン、物理的....62
デュアルルーティングテーブル....50
統合....37, 45
トンネル....39, 39–43
ポリシーベース NAT トンネル....39
ループバック....59
インターフェース、IGMP 上で稼動....162
インターフェース、監視....69–75
セキュリティーゾーン....75
ループ....70
インフラネットエンフォーサ
概要....40
接続ポリシー、構成....40
インフラネットエンフォーサの接続ポリシー、構成....40
インフラネットコントローラ
アクション....41
概要....40
リソースポリシー....41
インフラネット認証....42
インラインタップモード....188
インラインモード....188

え

エージェント、ゾンビ....29, 31
エコー....132

お

オープンショーテストパスファースト (OPSF)
OSPF を参照
オブジェクト
攻撃オブジェクト....212
攻撃オブジェクト、カスタム....215
攻撃オブジェクト、シグネチャ....212
攻撃オブジェクト、プロトコルアノーマリ....213
オブジェクト、監視....52
オペレーティングシステム、ホストの探査....12–15
親接続....96
音声 IP 化
帯域幅管理....63

か

解凍、AV スキャン....90
回避....15–26
拡張チャネル、WLAN 用の設定....132
カスタムサービス、ルート、vsys....123
仮想 HA インターフェース....39, 27
仮想 IP
VIP を参照
仮想アダプタ....66
仮想回路
VC を参照
MIP、仮想システム MIP....61
仮想システム....10
admins....34
read-only admins....34
NSRP....58
VIP....61
管理性とセキュリティ....73
フェールオーバー....58
負荷分散....83
仮想システムサポート....5
仮想セキュリティインターフェース
VSI を参照
仮想セキュリティデバイスグループ
VSD グループを参照
仮想チャンネル識別子
VCI を参照
VPI を参照
仮想パス識別子 / 仮想チャネル識別子
VPI/VCI を参照
仮想プライベート ネットワーク
VPN を参照
仮想ルーター
VR を参照
....50, 99
過大請求攻撃
説明....27
防御策....29
予防....27–32
予防、設定....30
カプセル化....100, 107, 112
監視....3
完全転送機密保持
PFS を参照
管理
CLI....9
WebUI....1
制限....42
管理 IP....31

管理 IP, VSD グループ 0 2
管理オプション
Manageable 31
MGT インターフェース 29
NetScreen-Security Manager 28
ping 28
SNMP 28
SSH 28
SSL 28
Telnet 28
VLAN1 29
WebUI 28
インターフェース 28
透過モード 29
管理クライアント IP アドレス 42
管理情報ベース II
MIB II を参照
管理方法
CLI 9
SSL 5
Telnet 9
WebUI 1
コンソール 19
管理ユーザー 2
RADIUS の権限 3
サーバーサポート 12
タイムアウト 16
認証の優先 30
管理、vsys 7

き

キープアライブ
L2TP 216
周期、NAT-T 240
キー、ライセンス 254
機能ゾーンインターフェース 38
HA 38
管理 38
共有ゾーン 67

く

攻撃オブジェクト
シグネチャ 212
クッキー、SYN 47
国コードおよびチャネル 131
国コードとチャネル、規制されているドメインの 131
クラスタ 11, 34
クラスタ名、NSRP 11, 28
グラフ、履歴 174
グループ
アドレス 108
サービス 140
グループ IKE ID
事前共有鍵 197
証明書 191
事前共有鍵 191
証明書 182
グループ式 4–8
オペレータ 5
サーバーサポート 12
ユーザー 5
グローバルゾーン 81
グローバルユニキャストアドレス 99, 116
クロック、システム
システムクロックも参照

け

警告
E メール警報 69
NetScreen-Security Manager へのレポート 25
しきい値 69
軽量ディレクトリアクセスプロトコル
LDAP を参照
ゲートキーパーデバイス 1
ケーブル、シリアル 19
検証済みモード 16

こ

公開アドレス 47
公開鍵基盤
PKI を参照
公開鍵 / 秘密鍵ペア 23
高可用性
IP トラッキング 55
仮想インターフェース 27
データリンク 8
配線 25–28
メッセージ 7
リンク精査 9
高可用性インターフェース
HA リンクとしてネットワークを配線 27
冗長 43
統合 45
高可用性フェールオーバー
アクティブ / パッシブ 11
アクティブ / アクティブ 12
攻撃
SYN フラッド 36–42
検出と防衛のオプション 2–4
攻撃 130
DoS 29–55
IP パケットフラグメント 244
Ping of Death 52
SYN フラグメント 245
UDP フラッド 50
WinNuke 54

攻撃（続き）
一般的な目的....1
再生....12
セッションテーブルフラッ....18, 30
段階....2
ティアドロップ....53
未知のプロトコル....243
ラージ ICMP パケット....241
ランド....51
攻撃アクション....141–148
close client....141
close server....141
drop....141
drop packet....141
ignore....141
なし....142
閉鎖....141
攻撃オブジェクト....119
TCP ストリームシグネチャ....162
概要....212
再有効化....140
使用不可....140
ステートフルシグネチャ....135
ストリームシグネチャ....136
否定....165
ブルートフォース....149
プロトコルアノーマリ....136
攻撃オブジェクトグループ
重大度の変更....137
ヘルプ....134
攻撃オブジェクト
IDP....186
プロトコルアノーマリ....213
カスタム....215
攻撃オブジェクトグループ....137
重大度レベル....137
ロギング....152
ポリシーで適用....130
攻撃オブジェクトデータベース....122–129
自動更新....125
自動通知と手動更新....126
手動更新....128
即時更新....124, 125
デフォルト URL の変更....128
攻撃データベース更新
概要....234
ダウンロード....234
攻撃オブジェクト
プロトコルアノーマリ....164
攻撃保護
セキュリティゾーンレベル....4
ポリシーレベル....4
攻撃、過大請求....27–29
高水準しきい値....33
構成
ADSL 2/2 + PIM....74
VPI/VCI ペア....71
仮想回路....71
フルメッシュ....58
構成の設定、ブラウザ要件....2
構成例
6to4 ホスト、へのトンネリング....105
DNS サーバー情報、要求....43
IPv4 上で IPv6 から IPv4 ネットワークへ....108
Ipv6 上の Ipv4 トンネリング（autokey IKE）..112, 116
IPv6 要求の複数 IPv4 ホストへの送信....85
native host, tunneling to....101
PPPoE instance, configuring....46
prefixes, delegating....38, 40
アクセスリストおよびルートマップ....61
手動トンネリング....97
静的ルートの再配布....61
攻略
攻撃を参照
互換性モードのオプション
T3 インターフェース....20
顧客構内装置（CPE）....39, 128
顧客サービス....123
故障モード....83
異なる IP スタック....82, 83
コマンドラインインターフェース
CLI を参照
コンソール....56
コンテナ....185
コンテンツフィルタリング....57–116

さ

サーバー、認証
認証サーバーを参照
サービス....110
ICMP....128
カスタム....154
タイムアウトしきい値....125
定義....168
ドロップダウンリスト....110
ポリシー内....168
サービス拒否
DoS を参照
サービスグループ....140–142
削除....142
作成....141
設定変更....142
サービスグループ (WebUI)....140
サービス購入
一時サービス....255
登録およびアクティブ化....255–257

サービスブック
エントリ、削除（CLI）....125
エントリ、変更（CLI）....124
サービスブック、サービス
カスタム 110
カスタム（CLI）....124
追加 124
定義済み 110
サービスブック、サービスグループ (WebUI)....65
サービスプロバイダ、からの情報....65
サービス、カスタム....123
ALGALG 169
vsys....123
再生防止チェック....50, 57
再生保護....12
再送信時間....31
最大送信単位（MTU）....12
サイトの調査....132
再入力オプション、VPN 監視 244
サブインターフェース....3, 51
vsys ごとに複数....51
削除 51
作成 (vsys) 51
作成する (ルートシステム)....50
設定 (vsys) 51
サブネット、重複....52
サブレートオプション....20

し

シーケンス番号検証....13
しきい値
高水準 33
低水準 33
識別名....28
識別名（DN）....182
シグネチャパッケージ、DI....122
自己ログ....66
システムパラメータ 260
システムクロック 257–261
クライアントとの同期化 257
タイムゾーン 258
日付および時刻 257
事前共有鍵....7, 159
自動構成
アドレスの自動構成 11
ステートレス 11
ルーター通知メッセージ 12
手動 6over4 トンネリング....95
手動鍵....116, 122
管理 7
手動鍵、VPN 43, 79
手動トンネリング....96
状態の移行
静的なエントリ 18
端点ホスト 16
次ホップゲートウェイルーター 16
トンネルゲートウェイ 17
冗長ゲートウェイ 294–306
SYN フラグチェック 300
復旧手順 298
証明書....7
CA....22, 25
E メール経由 25
CRL のローディング 23
取り消し 24, 34
要求 25
ローカル 25
ローディング 28
証明書の取り消しリスト (CRL: Certificate Revocation List)....23, 34
ローディング 23
シリアルケーブル....19
自律システム (AS) 番号....111
侵入の検出と予防、定義済み....173

す

スクリーン
ACK フラグのない FIN、ドロップ....13
ACK をもたない FIN....16
ICMP 240
ICMP フラッド....49
IP オプション....10
IP パケットフラグメント、ブロック 244
Ping of Death....52
SYN および FIN フラグセット....12
SYN フラグメント、検出....245
SYN-ACK-ACK プロキシフラッド....34
UDP フラッド....50
VLAN ゾーンおよび MGT ゾーン 3
WinNuke 攻撃 54
アドレススイープ 7
ストリクトソースルート IP オプション、検出.26
ソースルート IP オプション、拒否する....26
ティアドロップ 53
フラグのない TCP パケット、検出 14
不良 IP オプション、ドロップ....242
ポートスキャン 9
未知の MAC アドレスをドロップする 42
未知のプロトコル、ドロップ 243
ラージ ICMP パケット、ブロック 241
ランド攻撃 51
ルーズソースルート IP オプション....26
スケジュール....158, 175
ステートレスアドレス自動構成....11
ストリームシグネチャ....136
ストリクトソースルート IP オプション 11, 24–26

せ

正規表現 159–160
制御メッセージ 13
　HA 7
　HA 物理リンクハートビート 7
　RTO ハートビート 7
精査 31
静的 IP アドレス 74
静的ルーティング 2–10, 1
　Null インターフェースで転送する 11
　構成 5
　使用 3
　マルチキャスト 154
セカンダリパス 29
セキュアコピー
　SCP を参照
セキュアシェル
　SSH を参照
セキュアソケットレイヤー
　SSL を参照
セキュアハッシュアルゴリズム -1
　SHA-1 を参照
セキュリティ IP オプション 10, 11
セキュリティアソシエーション (SA) 96
セキュリティゾーン 2
　グローバル 2
　決定、宛先ゾーン 13
　決定、ソースゾーン 11
　ゾーンを参照
　定義済み 2
セキュリティゾーン、インターフェース 3
　物理 36
セキュリティデバイス 9
セキュリティペイロードのカプセル化
　ESP を参照
セキュリティポリシー 184
　テンプレート 187
　ルール 184
　ルールベース 184
　ルールベースの実行 187
セッション ID 4
セッションアイドルタイムアウト 17
セッション制限 30–32
　宛先ベース 31, 32
　ソースベース 30, 32
セッションタイムアウト
　HTTP 33
　TCP 33
　UDP 34
セッションテーブルフラッ 18, 30
接続状態 (LSA) の通知抑止 71
選択モード
　APN 16
　移動端末 (MS) 16
　検証済み 16
　ネットワーク 16

そ

ソースアドレス変換 81
ソースのインターフェースベースのルーティング (SIBR) 22
ソースベースのルーティング (SBR) 19
ソースルート 97
ゾーン 25–33, 6
　Layer 2 83
　VLAN 33, 83
　Global セキュリティ 2
　Vsys 6
　機能 33
　機能、MGT インターフェース 38
　共有 67
　グローバル 28
　定義 30
　トンネル 29
　編集 31
ゾーン、ScreenOS ..... 25, ??–33
　セキュリティインターフェース 3
　定義済み 2
ゾーン、グローバル 81
ゾーン、セキュリティ 2, 28
　インターフェース、監視 75
　インターフェース、物理 36
　グローバル 2
　決定、宛先ゾーン 13
　決定、ソースゾーン 11
ソフトウェアキー 67
ゾンビエージェント 29, 31

た

帯域幅 176
　Priority
　　キュー 200
　　デフォルト 200
　　レベル 201
　管理 196
　最大 176, 196, 201
　最大、無限の 196
　保証 176, 196, 201
タイプ、フィルタリング 10
タイムアウト 26
　管理ユーザー 16
　認証ユーザー 16
タイムゾーン 258
タグ、VLAN 3

探査
オープンポート 9
オペレーティングシステム 12, 15
ネットワーク 7
端点ホスト状態
Probe Forever 状態....31
Stale モード....30
再送信時間 31
重複アドレス検出（DAD）....31
到達可能時間 30
プローブ時間 31
ベース到着可能時間 30

ち

チャネル、利用可能なものの発見....133
チャレンジハンドシェイク式認証プロトコル....36
CHAP を参照
調査
FIN スキャン 15
IP オプション....10
SYN および FIN フラグセット....12
アドレススイープ 7
フラグのない TCP パケット、検出....14
ポートスキャン 9
重複アドレス検出（DAD）
機能 31
再試行カウント 31

つ

通称名....28
次ホップゲートウェイ....31

て

ティアドロップ攻撃....53
提案
フェーズ 1 ....9, 66
フェーズ 2....11, 66
ディクショナリーファイル、RADIUS....2
偵察....7–26
低水準しきい値....33
データベース、ローカル....13–14
データメッセージ....7
データ暗号化規格 (DES)....6
デジタル署名....20
徹底監視 (DI)
概要 118
カスタム攻撃オブジェクト 158
攻撃オブジェクト 119
攻撃オブジェクトグループ 137, 152
攻撃オブジェクトの最有効化 140
攻撃オブジェクトの否定 165
攻撃オブジェクトの無効化 140
コンテキスト I
シグネチャパッケージ 122
徹底監視 (DI)（続き）
重大度の変更 137
ステートフルシグネチャ 135
ストリームシグネチャ 136
プロトコルアノーマリ 136
ライセンスキー 120
デバイスフェールオーバー....59
デバイスユニーク ID（DUID）....37
デバイス、工場出荷時のデフォルト設定にリセット. 41
デフォルト設定、デバイスをリセット....41
デュアルスタックアーキテクチャ....50
networks, dissimilar....50
WAN backbones, dissimilar....50
ルーティングテーブル 50
テンプレート
セキュリティポリシー 187

と

透過モード....32, 33, 4
ARP 以外のトラフィックを遮断....84
ARP/trace-route 85
IP 以外のトラフィックを遮断....84
フラッド 85
ブロードキャストトラフィック 84
未知の MAC アドレスをドロップする 42
ユニキャストオプション 85
ルート 84
....82–94
同期
RTO....19
構成 19
統計、NSM へのレポート....25
統合インターフェース....37, 45
統合型アクセス制御ソリューション
概要 .... liii, vii, 39
動作可能モード
NAT....4
ルート 4
透過 4
到達可能性状態....14
到達可能性状態、移行....16
動的 IP（DIP）プール....145, 171
動的 IP
DIP を参照
動的パケットフィルタリング....3
トークンコード....25
ドメイン名システム
DNS を参照
ドメイン名システム (DNS)....42, 43
DHCPv6 検索リスト....36
DHCP クライアントホスト....43
IPv4 または IPv4 アドレス....42
サーバー 126

ドメイン名システム (DNS)（続き）
サーバー、トンネリング....44
ドメイン名の一部....36
ドメインルックアップ....44
プロキシ....44
トラフィック
Priority....176
VLAN ベース....31–57, 70
カウンティング....174, 5
シェーピング....195
通過トラフィック、vsys への振り分け....62–65
ロギング....174, 5
トラフィック アラーム....69–71
トラフィックシェーピング....195
サービス優先順位....200
自動....196
トランクポート....33
トランクポート、透過モード....32
トランスポートモード....4, 207, 213, 218
トリプル DES
3DES を参照
トンネル終端ポイント....99
トンネルモード....4
トンネル
特定の....243

な

内部フラッシュストレージ....56

に

認証....107, 111, 132
Allow Any....173
NSRP....29
NSRP-Lite....15
アルゴリズム....6, 49, 52, 55, 59
ポリシー....172
ユーザー....172
優先....30
認証サーバー....11–38
external....15
ID 番号....16
LDAP....27–28
SecurID....25
SecurID、定義....33
アイドルタイムアウト....16
アドレス....16
最大数....12
種類....16
定義....31–38
デフォルト....37, 38
認証サーバーを参照
認証プロセス....15
バックアップ....16
認証サーバー、RADIUS....17–20
ユーザータイプサポート....18
認証サーバー、RADIUS 認証サーバー、RADIUS
定義....31
認証サーバー、TACACS +
定義....36
認証サーバー、オブジェクト
プロパティ....16
認証サーバー、オブジェクト認証、サーバー、オブジェクト
名前....16
認証テーブルエントリ....41
認証と暗号化、RADIUS サーバーを使用した....124
認証ヘッダー (AH)....6
認証ユーザー....43–62
admin....2
WebAuth....173
IKE....12, 63
L2TP....82
WebAuth....12
XAuth....66
グループ....43, 46
サーバーサポート....12
事前ポリシー認証....173
手動鍵....12
タイプおよびアプリケーション....1–4
タイムアウト....16
認証ユーザーを参照
複数タイプ....3
ポリシー内....44
ユーザータイプ....12
ランタイム認証....172
ランタイム認証プロセス....172
ローカルデータベース....13–14
ログイン、異なる....4
認証ユーザー、WebAuth....45
SSL....59
ユーザーグループ、外部....57
ユーザーグループ、ローカル....55
認証ユーザー、認証
事前ポリシー....45
認証サーバー....12
ポイント....1
認証ユーザー、ランタイム
認証....44
ユーザーグループ、外部....51
ユーザーグループ、ローカル....48
ユーザー、外部....49
ローカル、ユーザー....47
認証ユーザー、ランタイム認証ユーザー、ランタイム
認証プロセス....44

ね

ネイティブホスト 99, 101
ネットマスク 48, 168
ネットマスク、MIP デフォルト、MIP 64
ネットワークアドレス変換 - ポート変換
dynamic IP (DIP) 80
DIP アドレス、変換 82
IPv4 から IPv6 への MIP 83
IPv4 ホストから単一 IPv6 ホストへの送信 89
IPv4 ホストから複数 IPv6 ホストへの送信 87
IPv6 から IPv4 への DIP 81
IPv6 ホストから単一 IPv4 ホストへの送信 86
IPv6 ホストから複数 IPv4 ホストへの送信 84
サービス要求送信 80, 83
使用する時 80
ソースアドレス変換 81
ネットワークアドレス変換 (NAT) 96
ネットワークモード 16
ネットワーク、帯域幅 195

は

バージョン 0 および 1 11
ハートビート
HA 物理リンク 7
RTO 7
破棄 131
パケット 97
IPSec 95
アドレス spoofing 攻撃 95
インターネット制御メッセージプロトコル (ICMP) 93, 95
拒否 96
受信 94, 95, 96
受信不能 94, 95
衝突 94, 95
転送アンダーラン 94
ドロップ 96, 97
ネットワークアドレス変換 (NAT) 96
フラグメント化 97
ポイントツーポイントトネリングプロトコル (PPTP) 95
ランド攻撃 95
ルーティング不能 96
パケット状態 3
監視 3
シグネチャ 135
パケットフロー ..... 11, ??–13
アウトバウンド VPN 63
インバウンド VPN 63–65
ポリシーベース VPN 65–66
ルートベース VPN 61–65
パケットフロー、NAT-Dst 29–31
パスのコストによるロードバランス 39, 62
パスワード
ルート管理者 41
忘れたとき 39
パスワード認証プロトコル
PAP を参照
パスワード、管理者の変更 4, 7
パターンで 136
バックストア 94
バックドアルール 207–212
Match 列の構成 209
アクションの構成 210
サービスの構成 210
重大度の構成 211
操作の構成 210
ソースおよび宛先の構成 209
ゾーンの構成 209
ターゲットの構成 211
バックドアルールベース
概要 207
セキュリティポリシーへの追加 208
ハッシング、セキュアハッシュアルゴリズム（SHA） 116
バナー 9
汎用ルーティングのカプセル化 (GRE) 155

ひ

非アクティブ SA 96
ピアツーピア
P2P を参照
非公開アドレス 48
ビットストリーム 94
否定、DI (徹底監視) 165
否定、アドレス 188
非同期転送モード
ATM を参照
ピンホール 19

ふ

ファイル拡張子、AV スキャン 91
フェーズ 1 9
提案 9
定義済み 9
フェーズ 2 11
提案 11
定義済み 11
フェールオーバー
Dual Untrust インターフェース 46, 49
VSD グループ 57
オブジェクト監視 52
仮想システム 58
デバイス 59
フォールバック
プロパティの割り当て 30
負荷分散 83

複合、構成 71
不正な URL からの保護 58–61
物理インターフェース
C ビットパリティモード 13
CSU 互換性 20
vsys からのエクスポート 70
vsys へのインポート 69
論理インターフェース 36
プライベート 137
ブラウザ要件 2
フラグメントの再アセンブリ 58–61
フラッド
SYN 36–42, 47
UDP 50
セッションテーブル 30
プリエンプトモード 21
ブリッジグループ
アンバインド 46
論理インターフェース 36
ブルートフォース
攻撃アクション 149
ブルートフォース攻撃オブジェクト 149
フルメッシュ構成 58
プレフィックス一覧 12
プローブ時間 31
プロキシ ID 11
一致 60, 67
プロトコル
IGP 51
NRTP 19
NSRP 1
PPP 46
VRRP 55
CHAP 207
PAP 207
PPP 206
プロトコルアノーマリ 136
ALGALG 134
P2P アプリケーション 134
インスタントメッセージ 133
基本ネットワークプロトコル 131
サポートされているプロトコル 131–135
パラメータ設定 164
プロトコル独立マルチキャスト
PIM を参照
プロトコル、CHAP 77
プロパティの割り当て 30

へ

URL ヘルプ 134
ヘルプファイル 2
ベンダー ID、VSA ベンダー ID、VSA 20
ベンダー固有属性 19

ほ

ポイントツーポイントトネリングプロトコル (PPTP) 95
ポイントツーポイントプロトコル
PPP を参照
ポイントツーマルチポイント構成
OSPF 72
放置された GTP トンネル 26
法に順守した傍受 35
ポート
1 次トラステッドとアントラステッド 43
2 次トラステッドとアントラステッド 43
冗長 2
番号 86
フェールオーバー 43
マッピング 4, 28
ポートアドレス変換
PAT を参照
ポートスキャン 9
ポートマッパ 132
ポート、トランク 32, 33
ポート、モデム 20, 22
ポリシー 3, 5
ID 168
Deny 169
DIP グループ 155
HA セッションバックアップ 174
L2TP 170
L2TP トンネル 170
NAT-dst 172
NAT-Src 171
permit 169
Reject 169
VPN 170
VPN ダイアルアップユーザーグループ 168
アクション 169
アドレス 168
アドレスグループ 168
アドレス否定 188
アプリケーション、に明示的にリンク 169
カウンティング 174
仮想システム 166
管理 177
機能 161
グローバル 164, 177, 186
警告 174
検証 192
コアセクション 17, 120
コンポーネントごとの複数の項目 187
コンテキスト 122
サービス 110, 168
サービスグループ 140

ポリシー（続き）
サービスブック 110
再順序付け 193
最上位 171, 193
最大制限 109
削除 194
シャドウ 192
種類 163–164
順序 193
使用可能 191
使用不可 191
スケジュール 175
セキュリティゾーン 168
ゾーン内 164, 177, 185
帯域幅の管理 196
地域間 163, 177, 180
徹底監視 (DI) 171
トラフィックシェーピング 175
トラフィックロギング 174
トンネル 169
内部ルール 166
名前 170
認証 172
必要な要素 162
変更 191
編集 191
ポリシーセットリスト 165
ポリシーの内容 187
マルチキャスト 157
両方向 VPN 170, 123
ルートシステム 166
ルックアップの順序 165
ポリシーベース NAT、トンネルインターフェース 39
ポリシーベース VPN 59
ポリシーベースの NAT
NAT-dst と NAT-src を参照
ポリシー、構成 6

ま

マッピング
host, IPv4 to IPv6 89
host, IPv6 to IPv4 86
network, IPv4 to IPv6 87
マップ 82
マップド IP
MIP を参照
マルチキャスト
IGMP のポリシー 173
アドレス 152
逆方向パス転送 152
静的ルーティング 154
配布ツリー 190
ポリシー 157
ルーティングテーブル 153
マルチキャストルーティング
IGMP 159
PIM 187
マルチメディアセッション、SIP 13

み

未知のプロトコル 243

め

メインモード 9
メッセージ
HA 7
WebTrends 73
エラー 57
緊急 57
クリティカル 57
警報 57
情報 57
制御 13
注意 57
通知 57
デバッグ 57
メッセージダイジェストバージョン 5 (MD5) 6
免除ルール 202–207
Match 列の構成 204
攻撃の構成 205
構成 204
ソースおよび宛先の構成 205
ゾーンの構成 204
ターゲットの構成 206
ログビューアからの構成 206
免除ルールベース
概要 202
セキュリティポリシーへの追加 203

も

モード
Stale 30
Tunnel 4, 58
ホスト 46, 112
ルーター 52
L2TP 動作 208
Main 9
NAT とルート 2
NAT、Untrust ゾーンに向かうトラフィック 81
アグレッシブ 10
透過 82
トランスポート 4, 58, 207, 213, 218
フェーズ 1 暗号 47, 54
優先使用 21

モード、選択
APN....16
移動端末 (MS)....16
検証済み....16
ネットワーク....16
モード、透過....32
モード、動作
NAT....4
ルート....4
透過....4
モジュラス....10
モデム ポート....20, 22

や

役割ベースの管理
IDP 専用管理者の構成....232
IDP ルールベース....186

ゆ

ユーザー
admin....2
IKE
IKE ユーザーを参照
L2TP....82–85
WebAuth....12
XAuth....66–80
共有 IKE ID....197–203
グループ IKE ID....182–197
管理、タイムアウト....16
グループ、サーバーサポート....12
複数タイプ....3
ユーザー、IKE
IKE ユーザーを参照
ユーザー、認証
認証ユーザーを参照
ユーザー、複数の管理ユーザー....33
優先順位キュー....200

よ

要求回路 、RIP....99
要件、基本機能....4

ら

ライセンスキー....254
アドバンスモード....120
攻撃パターンの更新....120
ランタイムオブジェクト
RTO を参照
ランタイム認証....172, 44
ランド攻撃....51

り

リカバリログ....68
リモート終端ポイント....101, 104
リモート認証ダイヤルインユーザーサービス
RADIUS を参照
履歴グラフ....174
リンクローカルアドレス....12, 14
隣接ノードキャッシュテーブル....13, 14, 16, 25, 30
隣接ノードキャッシュテーブル、隣接ノードエントリのカテゴリ....14
隣接ノード通知（NA）....30
隣接ノード到達不能検出（NUD）....14
隣接ノードキャッシュテーブル....25
隣接ノード到達不能検出（NUD）、隣接ノードキャッシュテーブル....14
隣接ノード発見（ND）....29
Accept Incoming RAs....21
使用可能....29
定義....13
到達可能性状態....29
バイパス MAC セッションキャッシング....29
パケット、送信のため現在キューにはいっている....13
隣接ノードエントリのエージ....13
隣接ノードキャッシュテーブル....13, 29
隣接ノード到達可能性状態....13, 30
隣接ノード発見（ND）、表示....32
隣接ノード発見パラメータ（NDP）....21, 30
隣接ノード要請（NS）....14, 31

る

ルーズソースルート IP オプション....10, 24–26
ルーター
upstream....38
仮想....50, 99
ルーターモード....52
ルーター要請（RS）....12
ルーティング情報プロトコル (RIP)
RIP を参照
ルーティングテーブル....17
種類....17
複数の仮想ルーターにおけるルックアップ....36
マルチキャスト....153
ルートの選択....32
ルーティング、マルチキャスト....151
ルート
null....83
インポート....45
エキスポート中....45
再配布....40
選択....32
フィルタリング....42
マップ....41
メトリック....34
優先度....33
ルート管理者、ログイン....42
ルートベース VPN....59–61

ルートモード 2, 4
NAT-Src 100
インターフェース設定 101
ルートルックアップ
順序 34
複数の仮想ルーター 36
ルートを定義する Null インターフェース 11
ループバックインターフェース 59
ルール、ポリシーから派生 166

れ

レイヤー 2 トンネリングプロトコル
L2TP を参照
レート制限、GTP-C メッセージ 12
レート、制限 12

ろ

ローカル証明書 25
ローカルデータベース
IKE ユーザー 64
タイムアウト 14
ユーザータイプサポート 14
ロギング 174, 55–68
CompactFlash (PCMCIA) 56
E メール 56
NetScreen-Security Manager 25
SNMP 56, 74
SYSLOG 56, 72
USB 56
WebTrends 56, 73
イベントログ 57
攻撃オブジェクトグループ 152
コンソール 56
自己ログ 66
内部 56
リカバリログ 68
ロギング、トラフィック 5
ログエントリ
IDP ルールで使用可能 237
ログビューア
免除ルールの作成 206

わ

ワイヤレスインターフェース
SSID のバインド 146
構成 146
使用不可 148
トランシーバへのバインド 146
論理インターフェース 36
ワイヤレスブリッジグループ 147
ワイヤレス ローカル エリア ネットワーク
WLAN を参照
ワイルドカード 185, 16



概念と用例
ScreenOS リファレンス ガイド

第 2 部 :
基本

リリース 6.0.0、改訂 02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

品番 : 530-017768-01-JP, 改訂 02

Copyright Notice

Copyright © 2007 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

目次

本編について ix

ドキュメントの規則 x
Web ユーザーインターフェースの規則 x
コマンドラインインターフェースの規則 x
ネーミング規則および文字タイプ xi
説明図の規則 xii
技術ドキュメントおよびテクニカルサポート xiii
xiii

第 1 章 ScreenOS アーキテクチャ 1

セキュリティゾーン 2
セキュリティゾーンのインターフェース 3
物理インターフェース 3
サブインターフェース 3
仮想ルーター 4
ポリシー 5
VPN (仮想プライベートネットワーク) 8
仮想システム 10
パケットフローシーケンス 11
ジャンボフレーム 14
ScreenOS アーキテクチャの例 14
例 : (第 1 部) 6 つのゾーンを持つ企業 14
例 : (第 2 部) 6 つのゾーンを持つインターフェース 16
例 : (第 3 部) 2 つのルーティングドメイン 19
例 : (第 4 部) ポリシー 20

第 2 章 ゾーン 25

構成済みゾーンの表示 26
セキュリティゾーン 28
Global ゾーン 28
SCREEN オプション 28
トンネルゾーンにトンネルインターフェースをバインドする 29
セキュリティゾーンとトンネルゾーンの構成 30
ゾーンの作成 30
ゾーンの変更 31
ゾーンの削除 32
機能ゾーン 33

第 3 章 インターフェース 35

インターフェースタイプ....35
論理インターフェース....35
物理インターフェース....36
ワイヤレスインターフェース....36
ブリッジグループインターフェース....36
サブインターフェース....37
統合インターフェース....37
冗長インターフェース....37
仮想セキュリティインターフェース....38
機能ゾーンインターフェース....38
管理インターフェース....38
高可用性インターフェース....38
トンネルインターフェース....39
トンネルインターフェースの削除....42
インターフェースの表示....43
セキュリティゾーンインターフェースを構成する....45
インターフェースをセキュリティゾーンにバインドする....45
インターフェースをセキュリティゾーンからアンバインドする....46
L3 セキュリティゾーンインターフェースのアドレス設定....47
公開 IP アドレス....47
非公開 IP アドレス....48
インターフェースのアドレスを設定する....48
インターフェース設定を変更する....49
ルートシステムにサブインターフェースを作成する....50
サブインターフェースの削除....51
2 次 IP アドレスを作成する....51
ループバックシステムインターフェース....52
バックアップインターフェースの構成....53
IP トラッキングバックアップインターフェースの構成....53
tunnel-if バックアップインターフェースの構成....54
ルート監視バックアップインターフェースの構成....57
ループバックインターフェース....58
ループバックインターフェースを作成する....60
管理用ループバックインターフェースの設定....60
ループバックインターフェースでの BGP の設定....60
ループバックインターフェースでの VSI の設定....61
ループバックインターフェースをソースインターフェースに設定....61
インターフェース状態の変化....62
物理的接続の監視....64
IP アドレスのトラッキング....64
インターフェース監視....69
2 つのインターフェースの監視....71
インターフェースループの監視....72
セキュリティゾーンの監視....75
ダウン状態のインターフェースとトラフィックフロー....76
出口インターフェースでの障害....77
出口インターフェースでの障害....78

第 4 章　インターフェースモード　81

透過モード 82
ゾーンの設定 83
VLAN ゾーン 83
定義済みのレイヤー 2 ゾーン 83
トラフィックの転送 83
宛先不明のユニキャストの処理方式 84
フラッド方式 85
ARP/Trace-Route 方式 87
管理用の VLAN1 インターフェースの構成 89
透過モードの構成 91
NAT モード 94
インバウンドおよびアウトバウンドの NAT トラフィック 96
インターフェース設定 97
NAT モードの構成 97
Route モード 100
インターフェース設定 101
Route モードの構成 101

第 5 章　ポリシー用ビルディングブロック　105

アドレス 105
アドレスエントリ 106
アドレスの追加 106
アドレスの変更 107
アドレスの削除 107
アドレスグループ 108
アドレスグループを作成する 109
アドレスグループエントリの編集 110
メンバおよびグループの削除 110
サービス 110
定義済みサービス 111
インターネット制御メッセージプロトコル 112
ICMP 不明エラーの処理 114
インターネット関連の定義済みサービス 115
Microsoft リモートプロシージャコールサービス 116
動的ルーティングプロトコル 118
ストリーミングビデオ 118
Sun リモートプロシージャコールサービス 119
セキュリティおよびトンネルサービス 120
IP 関連サービス 120
インスタントメッセージサービス 120
管理サービス 121
メールサービス 122
UNIX サービス 122
その他のサービス 122
顧客サービス 123
顧客サービスの追加 124
顧客サービスの変更 124
顧客サービスの削除 125
サービスタイムアウトの設定 125
サービスタイムアウトの構成とルックアップ 125
考慮事項 126
例 127

サービス（続き）
ICMP（インターネット制御メッセージプロトコル）カスタムサービスの削除.128
リモートシェル ALG.....129
Sun リモートプロシージャコール(RPC)アプリケーションレイヤーゲートウェイ.129
一般的な RPC 呼び出し手順.....129
Sun RPC サービスのカスタマイズ.....130
Microsoft リモートプロシージャコール ALG のカスタマイズ.....130
リアルタイムストリーミングプロトコル（RTSP）アプリケーション
レイヤーゲートウェイ.....132
RTSP 要求メソッド.....133
RTSP ステータスコード.....135
プライベートドメイン内でのメディアサーバーの構成.....137
パブリックドメイン内でのメディアサーバーの構成.....139
サービスグループ.....140
サービスグループを変更する.....142
サービスグループを削除する.....142
動的 IP プール.....143
ポートアドレス変換.....144
PAT の DIP Pool を作成する.....144
DIP プールの変更.....145
スティッキー DIP アドレス.....145
異なるサブネットでの DIP の使用.....146
ループバックインターフェースでの DIP の使用.....151
DIP グループを作成する.....155
反復スケジュールの設定.....158

第 6 章　ポリシー　161

基本要素.....162
3 種類のポリシー.....163
地域間ポリシー.....163
ゾーン内ポリシー.....164
グローバルポリシー.....164
ポリシーセットリスト.....165
定義済みポリシー.....166
ポリシーとルール.....166
ポリシーの構成.....167
ID.....168
ゾーン.....168
アドレス.....168
サービス.....168
アクション.....169
アプリケーション.....169
名前.....170
VPN トンネル.....170
L2TP トンネリング.....170
徹底監視 (Deep Inspection).....171
ポリシーリストの最上位の配置.....171
ソースアドレス変換.....171
宛先アドレス変換.....172
ユーザー認証.....172
HA セッションバックアップ.....174
Web フィルタリング.....174
ロギング.....174
カウンティング.....174

定義済みポリシー（続き）
トラフィックアラームしきい値 174
スケジュール 175
ウィルス対策スキャン 175
トラフィックシェーピング 175
適用されるポリシー 177
ポリシーの閲覧 177
ポリシーの作成 177
ゾーン間ポリシーメールサービスの作成 177
ゾーン間ポリシー群の作成 180
ゾーン内ポリシーの作成 185
グローバルポリシーの作成 186
ポリシーの内容の入力 187
ポリシーコンポーネントごとの複数の項目 187
アドレス否定の設定 188
ポリシーの変更と使用不可 191
ポリシーの検証 192
ポリシーの再順序付け 193
ポリシーの削除 194

第 7 章　トラフィックシェーピング　195

ポリシーレベルでの帯域幅管理 196
トラフィックシェーピングの設定 197
サービス優先順位の設定 200
優先順位キューの設定 201
ingress ポリシング 205
仮想インターフェースのトラフィックシェーピング 206
インターフェースレベルのトラフィックシェーピング 206
ポリシーレベルのトラフィックシェーピング 208
パケットフロー 208
例 : ingress ポリシングのあるルートベースの VPN 209
例 : ingress ポリシングのあるルートベースの VPN 212
ループバックインターフェースを使用したトラフィックシェーピング 216
DSCP マーキングとシェーピング 216

第 8 章　システムパラメータ　219

ドメイン名システムサポート 219
DNS ルックアップ 220
DNS 状況テーブル 221
DNS サーバーとリフレッシュスケジュールの設定 222
DNS リフレッシュ間隔の設定 222
動的ドメイン名システム 223
DynDNS サーバー用の DDNS の設定 223
Setting Up DDNS for a DDO Server 224
プロキシ DNS アドレスの分割 225
動的ホスト構成プロトコル 227
DHCP サーバーの構成 228
DHCP サーバーオプションのカスタマイズ 232
NSRP クラスタの DHCP サーバーの配置 233
DHCP サーバー検出 233
DHCP サーバー検出の有効化 234
DHCP サーバー検出の無効化 234

動的ホスト構成プロトコル（続き）
DHCP リレーエージェントとしてのセキュリティデバイスの割り当て.....235
すべての DHCP パケットの転送 239
Next-Server-IP の構成 240
セキュリティデバイスを DHCP クライアントとして使用 241
TCP/IP 設定の伝播 243
仮想システムの DHCP の構成 245
仮想システムの DHCP メッセージリレーの設定 246
Point-to-Point Protocol over Ethernet 246
PPPoE の設定 247
1 次およびバックアップ Untrust インターフェースに PPPoE を構成する....250
単一インターフェースでの複数の PPPoE セッションの構成.....250
PPPoE と高可用性.....253
ライセンスキー 254
ライセンスサービスの登録およびアクティブ化.....255
トライアルサービス 255
サブスクリプションキーの更新 256
既存または新しいデバイスへのアンチウィルス、Web フィルタリング、アンチスパム、徹底監視の追加 256
システムクロック 257
日付および時刻.....257
夏時間 257
タイムゾーン 258
ネットワークタイムプロトコル 258
複数の NTP サーバーの構成.....258
バックアップ NTP サーバーの構成 258
最大時間調整.....259
NTP および NSRP 260
NTP サーバーへの最大時間調整値の設定 260
セキュア NTP サーバー 260

索引 .....IX-I

本編について

*第 2 部 : 基本*では、さまざまな要素の構成例も含めて、ScreenOS アーキテクチャと要素について説明します。本編の章は、以下のようになります。

- 第 1 章、「ScreenOS アーキテクチャ」は、ScreeOS アーキテクチャの基本要素を示し、これらの要素を組み込む企業ベースの構成を説明する 4 つの例で締めくくっています。本章とその後のすべての章では、各概念に図解された例が添付されています。
- 第 2 章「ゾーン」は、セキュリティゾーン、トンネルゾーン、機能ゾーンについて説明します。
- 第 3 章、「インターフェース」では、さまざまな物理インターフェース、論理インターフェース、および仮想インターフェースについて説明しています。
- 第 4 章、「インターフェースモード」は、透過モード、NAT (ネットワークアドレス変換) モード、ルートインターフェース操作モードについて説明します。
- 第 5 章、「ポリシー用ビルディングブロック」は、ポリシーと VPN (Virtual Private Netwark) の作成に使用する要素について説明します。アドレス (および VIP アドレス) 、サービス、および DIP プールについて説明します。
- 第 6 章、「ポリシー」では、ポリシーのコンポーネントと機能について説明し、その作成と応用に関する指針を示します。
- 第 7 章、「トラフィックシェーピング」では、インターフェースとポリシーレベルの帯域を管理し、サービスの優先順位を決める方法を説明します。
- 第 8 章、「システムパラメータ」では、ドメイン名システム (DNS) アドレス指定の背後にある概念、TCP/IP 設定を割り振ったり、リレーするためのダイナミックホスト設定プロトコル (DHCP) の使用法、システム設定やソフトウェアをダウンロードしたりアップロードする方法、システムクロックの設定方法を示します。

ドキュメントの規則

このドキュメントは、次のセクションで説明されている規則を使用しています。

- x ページの「Web ユーザーインターフェースの規則」
- x ページの「コマンドラインインターフェースの規則」
- xi ページの「ネーミング規則および文字タイプ」
- xii ページの「説明図の規則」

Web ユーザーインターフェースの規則

WebUI (Web ユーザーインターフェース) では、各作業の操作指示は、操作手順と構成設定値に分かれています。構成設定を入力できる WebUI ページを開くには、画面の左側にあるナビゲーション ツリーのメニュー項目をクリックして、そのページに移動します。先へ進むと、ナビゲーション パスが画面の上部に表示されます。各ページは角括弧で分離されています。

WebUI のパスおよびアドレスを定義するためのパラメータは、以下のとおりです。

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.2.2.5/32
Zone: Untrust

構成設定のオンラインヘルプを開くには、画面の左上にある疑問符 (?) をクリックします。

ナビゲーションツリーにも、Help > Config Guide 構成ページがあり、セキュリティポリシーおよび IPSec (インターネットプロトコルセキュリティ) の構成に役立ちます。ドロップダウンメニューからオプションを選択して、そのページの指示に従います。構成設定のオンラインヘルプを開くには、左上にある **?** 文字をクリックします。

コマンドラインインターフェースの規則

次の規則は、例とテキストにおいて、コマンドラインインターフェース (CLI) コマンドの構文を示すために使用されます。

例においては、次のように使用されます。

- 角括弧 [ ] 内にあるものはすべてオプションです。
- 中括弧 { } 内にあるものはすべて必須です。
- 選択肢が複数ある場合、各選択肢はパイプ (|) で区切られています。例えば、次のように表示されます。

```
set interface { ethernet1 | ethernet2 | ethernet3 } manage
```

- 変数は*斜体*で表示されます。

  set admin user *name1* password *xyz*

テキストにおいては、コマンドは**太字**で、変数は*斜体*で表示されます。

注 : キーワード入力時には、単語を間違いなく識別できる数の文字を入力すれば十分です。**set admin user wheezer j12fmt54** というコマンドを入力する際には、**set adm u whee j12fmt54** と入力するだけで十分です。ただし、本編に記載されたコマンドはすべて本来の形式で記載されています。

ネーミング規則および文字タイプ

ScreenOS はオブジェクトの名前 (アドレス、管理ユーザー、認証サーバー、IKE ゲートウェイ、仮想システム、VPN トンネルおよびゾーンなど、ScreenOS 構成に定義されているもの) に関して、次の規則に従います。

- 名前文字列に 1 つまたは複数のスペースが含まれる場合、文字列全体を二重引用符で囲む必要があります。例 :

  set address trust “local LAN” 10.1.1.0/24

- 二重引用符で囲まれた文字列の先頭または末尾のスペースを取り除きます。たとえば、**「 local LAN 」**は**「local LAN」**となります。

- 連続した複数のスペースは、一つのスペースとして扱われます。

- CLI キーワードの多くはケースセンシティブではありませんが、名前文字列はケースセンシティブです。たとえば、**「local LAN」**は**「local lan」**とは異なります。

ScreenOS は、次の文字タイプをサポートします。

- 1 バイト文字セット (SBCS) およびマルチバイト文字セット (MBCS)。SBCS の例に、ASCII、欧州言語、およびヘブライ語があります。2 バイト文字セット (DBCS) とも呼ばれる MBCS の例に、中国語、韓国語、および日本語があります。

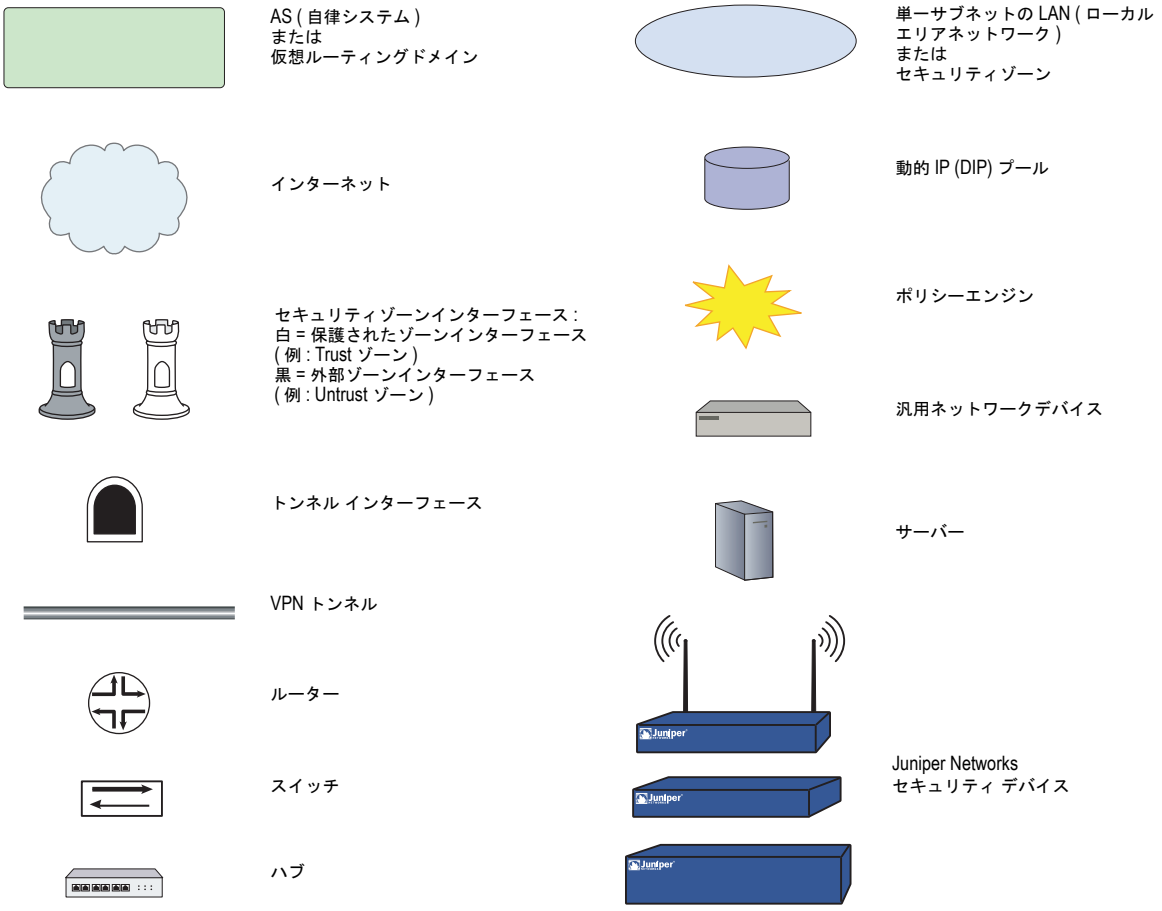
- ASCII 文字の 32 (16 進数の 0x20) から 255 (0xff)。ただし二重引用符 (“) は、スペースを含む名前文字列の先頭と末尾を示す特殊な意味をもつため、例外とします。

注 : コンソール接続では、SBCS のみがサポートされます。ご利用のブラウザがサポートする文字セットに応じて、WebUI は SBCS および MBCS の両方をサポートします。

説明図の規則

次の図は、本編を通して説明図に使用されている画像の基本的なものです。

図 1: 説明図の画像



技術ドキュメントおよびテクニカルサポート

Juniper Networks 製品のいずれかの技術ドキュメントを入手するには、www.juniper.net/techpubs/ をご覧になってください。

テクニカルサポートについては、http://www.juniper.net/customers/support/ にある Case Manager を使って事例サポートを開くか、1-888-314-JTAC (米国内) か 1-408-745-9500 (その他の国) までお問い合わせください。

本書に間違いや欠落があった場合は、techpubs-comments@juniper.net までお知らせください。

第 1 章

ScreenOS アーキテクチャ

Juniper Networks ScreenOS アーキテクチャは、ネットワークセキュリティのレイアウトを設計するときに大きな柔軟性を提供します。複数のインターフェースを持つ Juniper Networks セキュリティデバイス上で、多数のセキュリティゾーンを作成し、ゾーン間とゾーン内部でトラフィックを規制するポリシーを構成できます。各ゾーンに 1 以上のインターフェースをバインドし、各ゾーンに異なった管理およびファイアウォールのオプションを使用できます。ScreenOS では、ネットワーク環境で必要な数のゾーンを作成し、各ゾーンが必要とする数のインターフェースを割り当て、必要に応じて各インターフェースを設計できます。

本章では ScreenOS の概要を説明します。本章のセクションは、以下のようになります。

- 2 ページの「セキュリティゾーン」
- 3 ページの「セキュリティゾーンのインターフェース」
- 4 ページの「仮想ルーター」
- 5 ページの「ポリシー」
- 8 ページの「VPN (仮想プライベートネットワーク)」
- 10 ページの「仮想システム」
- 11 ページの「パケットフローシーケンス」
- 14 ページの「ジャンボフレーム」

本章の後半では、ScreenOS を使用する セキュリティデバイスの基本構成を説明する例が 4 部に分けて記載されています。

- 14 ページの「例 : (第 1 部) 6 つのゾーンを持つ企業」
- 16 ページの「例 : (第 2 部) 6 つのゾーンを持つインターフェース」
- 19 ページの「例 : (第 3 部) 2 つのルーティングドメイン」
- 20 ページの「例 : (第 4 部) ポリシー」

セキュリティゾーン

セキュリティゾーンとは、ポリシー経由のインバウンドトラフィックおよびアウトバウンドトラフィックの規制を必要とする 1 つ以上のネットワークセグメントの集まりです (5 ページの「ポリシー」を参照)。セキュリティゾーンとは、1 つか複数のインターフェースがバインドされた論理エンティティです。さまざまなタイプの Juniper Networks セキュリティデバイスを使用して、複数のセキュリティゾーンを定義できます。ユーザー定義のゾーンに加えて、定義済みのゾーンである Trust、Untrust、DMZ (レイヤー 3 での動作) 、あるいは V1-Trust、V1-Untrust、V1-DMZ (レイヤー 2 での動作) も使用できます。必要に応じて、定義済みゾーンだけを使用し続けることができます。定義済みゾーンを無視してユーザー定義ゾーンだけを使用することもできます。オプションとして、定義済みとユーザー定義の両方のゾーンを並行して使用することができます。ゾーンが柔軟に構成できるため、お客様のニーズに最も適したネットワークを設計できます。See 図 2.

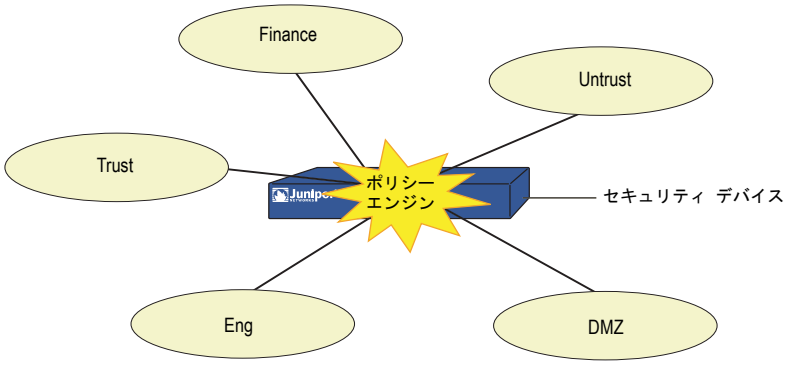
注 : Global ゾーンはネットワークセグメントを必要としないセキュリティゾーンです。(詳細については、28 ページの「Global ゾーン」を参照してください)。また、インターフェースがバインドされていないゾーンやアドレス帳入力にもネットワークセグメントが含まれていないと考えることができます。

以前のバージョンの ScreenOS からアップグレードした場合、これらのゾーンの構成は変更されません。

定義済みセキュリティゾーンを削除することはできません。ただし、ユーザー定義ゾーンを削除することはできます。セキュリティゾーンを削除すると、そのゾーン用に構成されたアドレスをすべて自動的に削除することになります。

図 2 は、3 つのデフォルトゾーン (Trust、Untrust、DMZ) と 2 つのユーザー定義ゾーン (Finance、Eng) の 5 つのセキュリティゾーンで構成されるネットワークを示します。トラフィックはポリシーが許可した場合に限り、1 つのセキュリティゾーンから他方のセキュリティゾーンに通過します。

図 2: 定義済みのセキュリティゾーン



セキュリティゾーンのインターフェース

セキュリティゾーンのインターフェースは、TCP/IP トラフィックが、そのゾーンと他のゾーンの間を通過する際の出入口といえます。

ポリシーを定義することによって、トラフィックが 1 方向に流れるかまたは双方向に流れるかを指定します。ルートを定義することによって、あるゾーンから別のゾーンへ送信されるトラフィックが使用するべきインターフェースを指定します。1 つのゾーンに複数のインターフェースをバインドできるため、ルートを計画しておくことは選択したインターフェースにトラフィックを導くために重要です。

注 : トラフィックが同じゾーンにバインドしたインターフェース間をフローするためには、両方のインターフェースがセキュリティ相当物を持っているため、ポリシーは必要とされません。ScreenOS は、ゾーン内でないゾーン間のトラフィックにポリシーを必要とします。ゾーン内のトラフィックにはポリシーは必要ありません。

ゾーンからゾーンへのトラフィックのフローを許可するには、ゾーンにインターフェースをバインドします。Route モードまたは NAT モードのインターフェースの場合は、(81 ページの「インターフェースモード」を参照) そのインターフェースに IP アドレスを割り当てます。一般的な 2 つのインターフェースタイプとして、物理インターフェース、および (仮想システムサポート付きのデバイスの場合) サブインターフェース (すなわち、物理インターフェースをレイヤー 2 で実体化したもの) があります。詳細については、35 ページの「インターフェース」を参照してください。

物理インターフェース

物理インターフェースとは、セキュリティデバイスに物理的に存在しているコンポーネントを指します。インターフェースの命名規則はデバイスごとに異なります。

注 : 具体的なセキュリティデバイスの命名規則については、そのデバイスのインストールおよび設定のガイドを参照してください。

サブインターフェース

VLAN (仮想 LAN) をサポートするデバイスでは、物理インターフェースをいくつかの仮想サブインターフェースに論理的に分けることができます。各サブインターフェースは、その由来となった物理インターフェースから必要とする帯域幅を借用します。サブインターフェースは、物理的インターフェースとまったく同様に機能する抽象物で、802.1Q VLAN タギングによって識別されます。セキュリティデバイスは IP アドレスと VLAN タグによって、サブインターフェースを使用してゾーンを行き来するようトラフィックに指示します。便宜上、管理者は通常サブインターフェース番号と同じ番号を VLAN タグに割り当てます。たとえば、VLAN タグ 3 を使用するインターフェース ethernet1/2 には *ethernet1/2.3* という名前が付けられます。これは、第 1 ベイにあるインターフェースモジュールの第 2 ポート、サブインターフェース番号 **3** (*ethernet1/2.3*) を意味します。

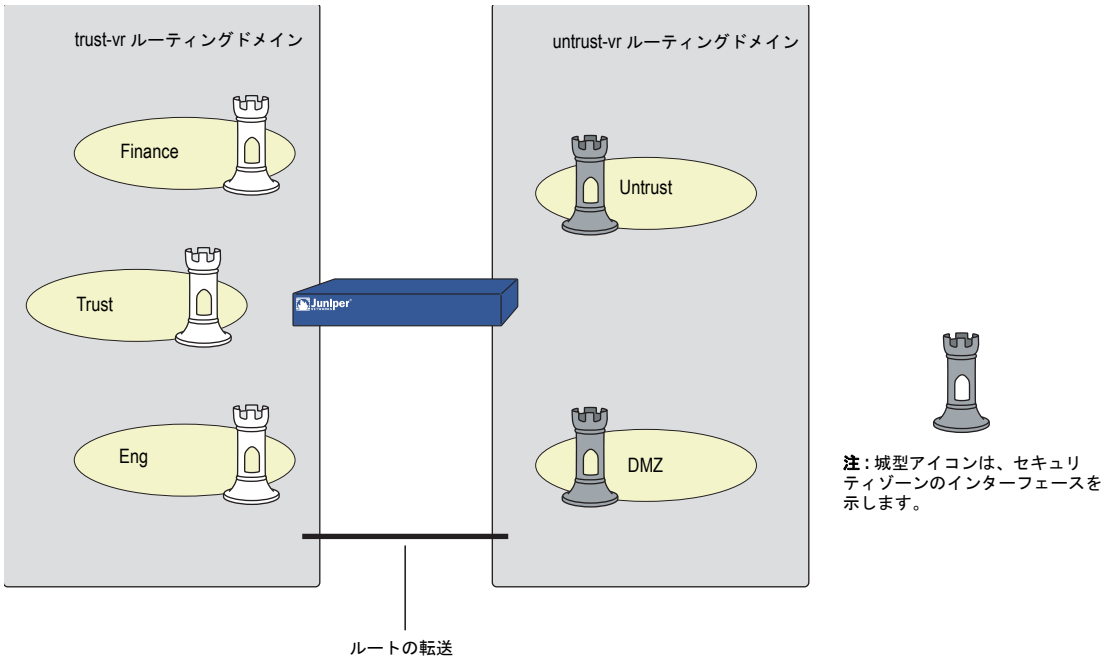
注： 802.1Q は、仮想ブリッジ LAN の実装と VLAN タギングによる VLAN メンバーシップを示すために使用されるイーサネットフレームフォーマットの機構を定義する IEEE 標準です。

サブインターフェースはその識別の一部を物理インターフェースと共有しますが、サブインターフェースをバインドするゾーンは、物理インターフェースをバインドするゾーンには依存しないということに注意してください。物理インターフェース *ethernet1/2* をバインドするゾーンや、*ethernet1/2.2* をバインドするゾーンとは異なるゾーンにサブインターフェース *ethernet1/2.3* をバインドすることができます。同様に、IP アドレスの割り当てについても制限はありません。*subinterface* という用語は、そのアドレスが物理インターフェースのアドレス空間のサブネット内にあるという意味ではありません。

仮想ルーター

VR (仮想ルーター) はルーターとして機能します。VR には固有のインターフェースや、ユニキャストおよびマルチキャストのルーティングテーブルがあります。ScreenOS では、セキュリティデバイスは、定義済みの仮想ルーターを 2 つサポートしています。これによって、セキュリティデバイスはユニキャストとマルチキャストの 2 つの別個のルーティングテーブルを維持し、1 つの仮想ルーターのルーティング情報をもう一方の仮想ルーターから隠すことができます。たとえば untrust-vr は通常、アントラステッドパーティとの通信に使用され、保護されたゾーンのルーティング情報は全く含まれていません。保護されたゾーンのルーティング情報は trust-vr によって維持されます。このため、untrust-vr から不正にルートを抽出して、内部ネットワークの情報が収集されることはありません。図 3 を参照してください。

図 3: 仮想ルーターのセキュリティゾーン



セキュリティデバイスに仮想ルーターが 2 つある場合、トラフィックを許可するポリシーがあるときでも、異なる仮想ルーターに存在するゾーンの間でトラフィックが自動的に転送されることは*ありません*。仮想ルーターの間をトラフィックが通過するには、VR 間のルートをエクスポートするか、一方の VR を次のホップとして定義する静的ルートをもう一方の VR で構成する必要があります。2 つの仮想ルーターを使用する場合の詳細については、*第 7 部 : ルーティング*を参照してください。

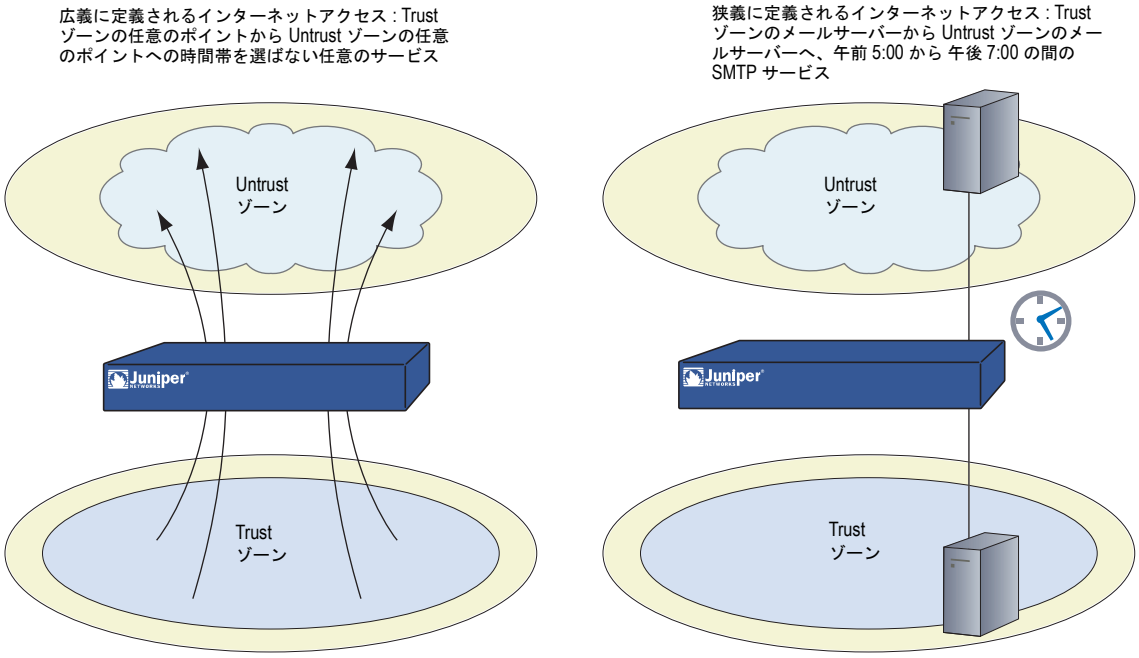
ポリシー

Juniper Networks セキュリティデバイスは、あるセキュリティゾーンから他のセキュリティゾーンへの通過を必要とする接続の試行をすべて検査し、許可または拒否することによってネットワークを保護します。

デフォルトでは、セキュリティデバイスは全方向のすべてのトラフィックを拒否します。ポリシーを作成し、指定したソースから指定した宛先までスケジュールした時間に通過を許可するトラフィック種類を定義することにより、ゾーンからゾーンへのトラフィックフローを制御できます。最も広範囲なレベルでは、1 つのゾーンの任意のソースから他のゾーンの任意の宛先へ通過するすべての種類のトラフィックをスケジュールの制約なく許可することができます。最も狭いレベルでは、あるゾーンの指定したホストと他のゾーンの指定したホストとの間で、1 種類のトラフィックだけをスケジュールした時間の間許可するポリシーを作成できます。図 4 を参照してください。

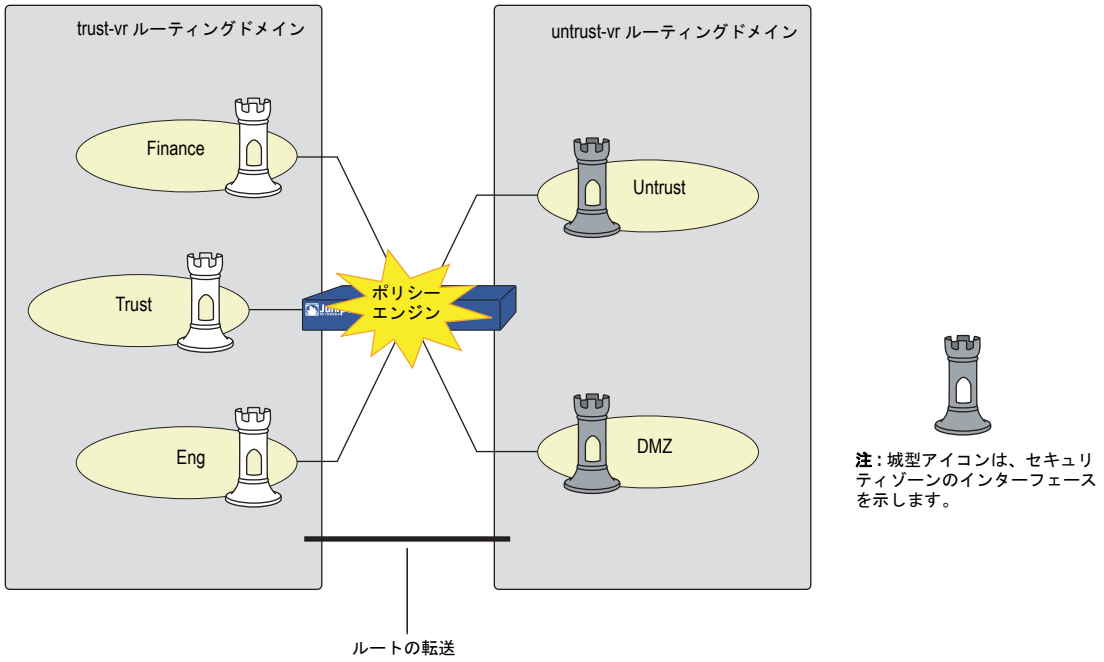
注 : 一部のセキュリティデバイスでは、Trust ゾーンから Untrust ゾーンへのアウトバウンドトラフィックすべてを許可し、Untrust ゾーンから Trust ゾーンへのインバウンドトラフィックすべてを拒否するデフォルトポリシーが付属しています。

図 4: デフォルトポリシー



パケットが 1 つのゾーンから別のゾーンへの通過を試みたり、同じゾーンにバインドされた 2 つのインターフェースの間を通過しようとする場合は必ず、セキュリティデバイスがポリシーセットリストを確認し、そうしたトラフィックを許可するポリシーがあるか確かめます (165 ページの「ポリシーセットリスト」を参照)。トラフィックが、1 つのセキュリティゾーンから別のセキュリティゾーン (たとえばゾーン A からゾーン B まで) を通過できるようにするには、ゾーン A がゾーン B へトラフィックを送信するのを許可するポリシーを構成する必要があります。トラフィックが反対方向に流れるようにするには、ゾーン B からゾーン A へのトラフィックを許可する別のポリシーを構成する必要があります。1 つのゾーンから別のゾーンへトラフィックが通過するには、それを許可するポリシーが必要です。また、イントラゾーンブロッキングが使用可能である場合、そのゾーン内で 1 つのインターフェースから別のインターフェースへのトラフィックの通過を許可するポリシーが必要です。7 ページの図 5 を参照してください。

図 5: ポリシーのアーキテクチャ



注 : 詳細については、161 ページの「ポリシー」を参照してください。

セキュリティデバイスのマルチキャストルーティングを構成する場合には、マルチキャストポリシーの構成が必要な場合があります。デフォルトでは、セキュリティデバイスではゾーン間のマルチキャスト制御トラフィックが許可されていません。マルチキャスト制御トラフィックは、PIM (プロトコル独立マルチキャスト) などのマルチキャストプロトコルによって伝送されるメッセージです。マルチキャストポリシーは、マルチキャスト制御トラフィックのみのフローを制御します。ゾーン間のデータトラフィック (ユニキャスト、マルチキャストとも) を許可するためには、これとは別にファイアウォールポリシーを設定する必要があります。(詳細は、**7**-157 ページの「マルチキャストポリシー」を参照してください。)

VPN (仮想プライベートネットワーク)

ScreenOS はいくつかの VPN (仮想プライベートネットワーク) 構成オプションをサポートしています。主なタイプには次の 2 つがあります。

- **ルートベース VPN** - ルートルックアップが、セキュリティデバイスによってカプセル化されるトラフィックを決定します。ポリシーはルートで指定された宛先へのトラフィックを許可または拒否します。ポリシーがトラフィックを許可しており、ルートが VPN トンネルにバインドされたトンネルインターフェースを参照している場合、セキュリティデバイスもそのトラフィックをカプセル化します。この構成では、ポリシーの適用と VPN トンネルの適用が区別されます。構成が行われると、VPN トンネルは 1 つのセキュリティゾーンから別のセキュリティゾーンまでトラフィックを保護するために使用できるリソースとして存在します。

- **ポリシーベース VPN** - ポリシーが特定の VPN トンネルを参照し、アクションとして“tunnel”を指定する場合、ポリシールックアップがセキュリティデバイスによってカプセル化されるトラフィックを決定します。

ルートベース VPN は単一の VPN トンネルを通過するトラフィックに複数のポリシーを適用できるため、サイトツーサイトの VPN 構成に適しています。ポリシーベース VPN はダイヤルアップの VPN 構成に適しています。これは、ダイヤルアップクライアントは内部 IP アドレスを持っていないことがあり、その場合はルートを設定することができないためです。図 6 を参照してください。

次の手順では、ルートベース VPN の構成に関係する主な要素を示しています。

1. VPN トンネル (例 : *vpn-to-SF*。*SF* は宛先またはエンドエンティティ) の構成時に、ローカルデバイスの物理インターフェースまたはサブインターフェースを出力インターフェースとして指定します。(このインターフェースの IP アドレスは、リモートピアがそのリモートゲートウェイの構成時に使用する必要があります。)

2. トンネルインターフェース (例 : *tunnel.1*) を作成し、セキュリティゾーンにバインドします。

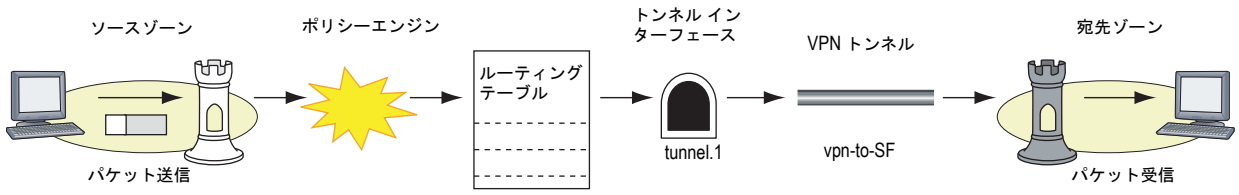
注 : VPN トラフィックの宛先と同じゾーンにトンネルインターフェースをバインドする必要はありません。ルートがそのインターフェースをポイントしている場合、どのゾーンへのトラフィックもトンネルインターフェースにアクセスできます。

---

3. トンネルインターフェース *tunnel.1* を VPN トンネル *vpn-to-SF* にバインドします。

4. このトンネルを経由してトラフィックを導くため、*SF* へのトラフィックは、*tunnel.1* を使用する必要があることを示したルートを設定します。

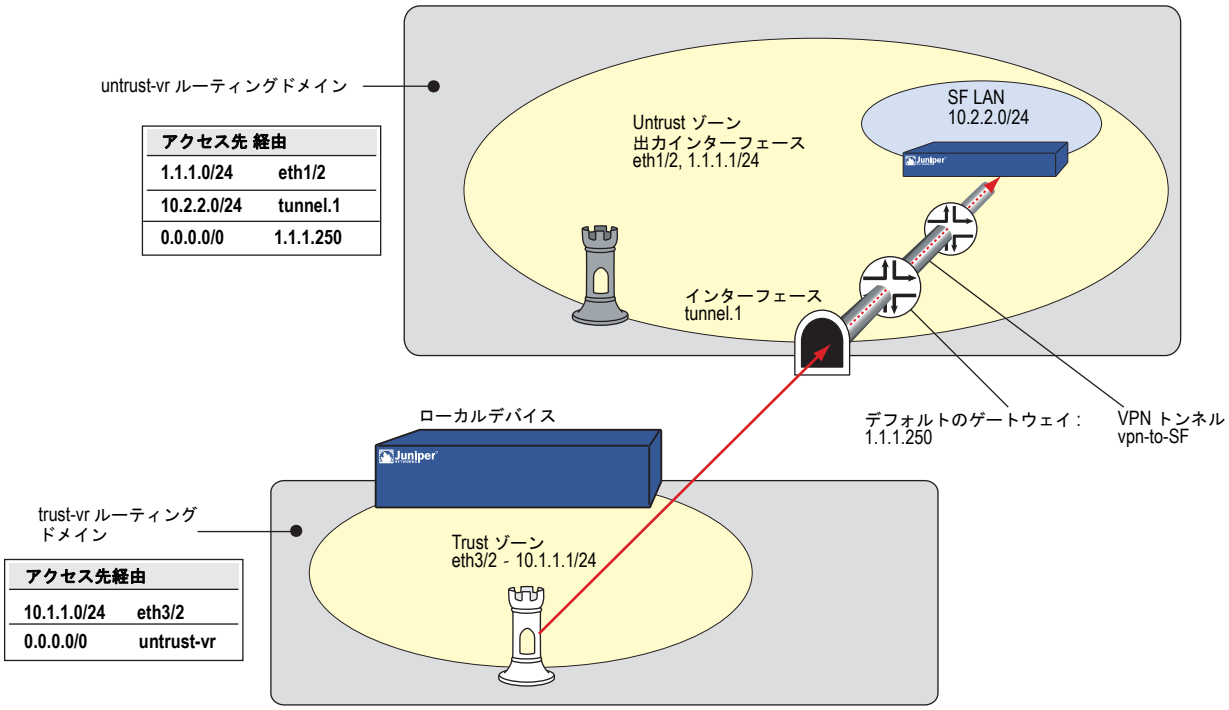
図 6: VPN トラフィック



この時点でトンネルは、*SF* を宛先としたトラフィックを受け入れる準備ができています。また、Trust LAN (10.1.1.0/24) や SF LAN (10.2.2.0/24) などアドレス帳入力を作成し、ポリシーを設定して、Trust LAN など指定したソースから SF LAN など指定した宛先へのさまざまなタイプのトラフィックを許可またはブロックできます。9 ページの図 7 を参照してください。

図 7: Untrust セキュリティゾーンからの VPN トラフィック

ローカルセキュリティデバイスは、Trust ゾーンからのトラフィックを tunnel.1 インターフェースを経由して Untrust ゾーンの SF LAN 宛に送ります。tunnel.1 は VPN トンネル vpn-to-SF にバインドされているため、デバイスはトラフィックを暗号化し、このトンネルを経由してリモートピアに送信します。

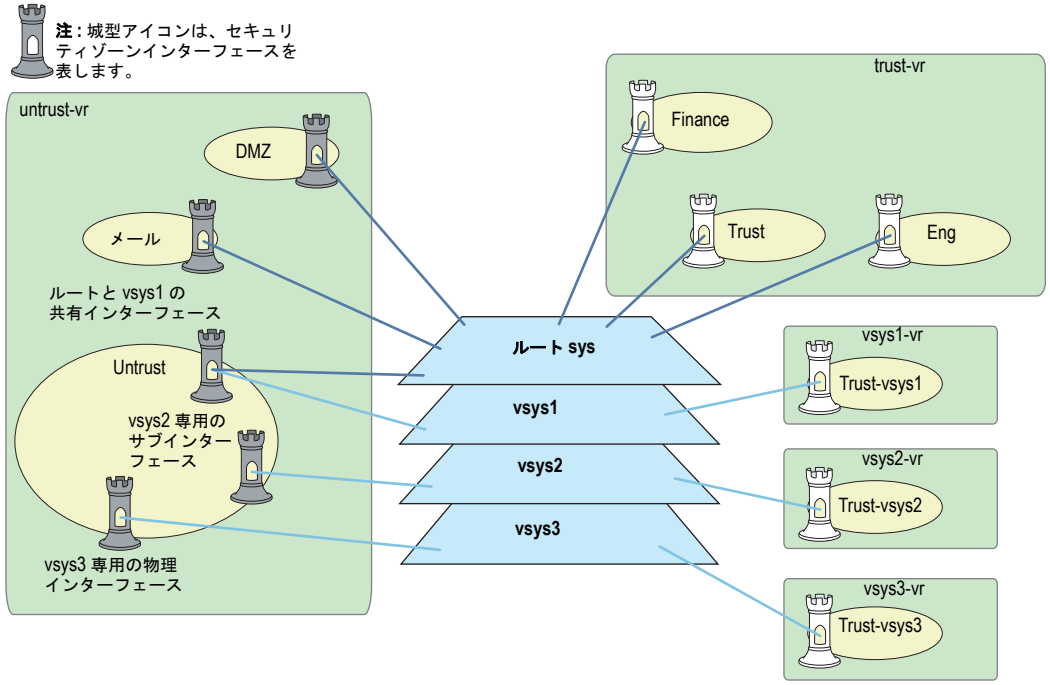


注 : VPN の詳細については、*第 5 部 : 仮想プライベート ネットワーク* を参照してください。

仮想システム

Juniper Networks セキュリティデバイスには、複数の仮想システム (vsys) をサポートするものがあります仮想システムは、メインシステムのサブディビジョンで、ユーザーからはスタンドアロンのエンティティに見えます。仮想システムは、それぞれ別個に存在し、同じセキュリティデバイス内のルートシステムからも別個に存在します。ScreenOS を仮想システムに適用するには、3 つの主要コンポーネントであるゾーン、インターフェース、および仮想ルーターの調整が必要です。図 8 では、ScreenOS がルートレベルおよび vsys レベルでこれらのコンポーネントを統合する方法の概念を説明しています。

図 8: vsys アーキテクチャ

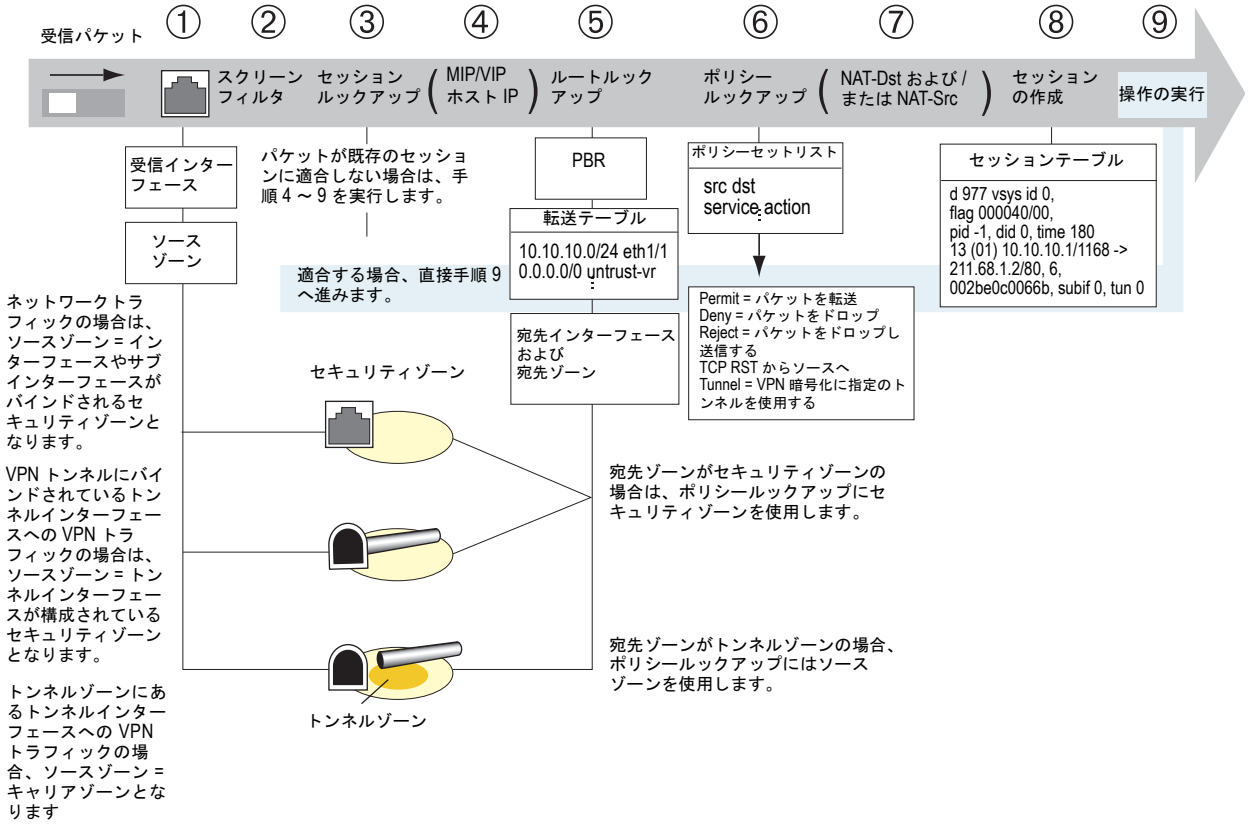


注 : 仮想システム、および仮想システムのコンテキストでのゾーン、インターフェース、仮想ルーターの適用の詳細については、*第 10 部 : 仮想 システム*を参照してください。

パケットフローシーケンス

ScreenOS では、受信パケットのフローシーケンスは、図 9 に示すように進みます。

図 9: セキュリティゾーンを通過するパケットフロー



1. インターフェースモジュールが受信インターフェースを確認し、その結果、インターフェースがバインドされるソースゾーンを確認します。

   インターフェースモジュールは、ソースゾーンの決定に次の基準を使用します。

   - パケットがカプセル化されていない場合、ソースゾーンは受信インターフェースや受信サブインターフェースがバインドされるセキュリティゾーンです。
   - パケットがカプセル化され、トンネルインターフェースが VPN トンネルにバインドされている場合、ソースゾーンはトンネルインターフェースが構成されているセキュリティゾーンです。
   - パケットがカプセル化され、トンネルインターフェースがトンネルゾーンに存在する場合、ソースゾーンは、そのトンネルゾーンに対応するキャリアゾーン (トンネルゾーンを *含む* セキュリティゾーン) です。

2. Untrust ゾーンに対して SCREEN オプションが有効になっていれば、セキュリティデバイスはこの時点で SCREEN モジュールをアクティブにします。SCREEN モジュールによるチェックの結果は、次の 3 つのうちいずれかになります。

   - SCREEN 機構が異常な動きを検出し、パケットを拒否する場合、NetScreen デバイスはパケットを破棄し、イベントログにその旨を記録します。
   - SCREEN 機構が異常な動きを検出し、イベントを記録するように構成されていてもパケットをブロックするようには構成されていない場合、セキュリティデバイスはイベントを ingress インターフェースの SCREEN カウンタリストに記録し、次の手順に進みます。
   - SCREEN 機構が異常な動きを検出しない場合、セキュリティデバイスはそのまま次の段階に進みます。

3. セッションモジュールは、パケットを既存のセッションと一致させるためセッションルックアップを実行します。

   - パケットが既存のセッションと適合しない場合、セキュリティデバイスは、1 番目のパケット処理、つまり手順 4 ～ 9 を実行します。
   - 逆に該当するセッションが見つかれば、既存のセッションエントリの情報を参照して、パケットを高速処理します。高速化処理では手順 4 ～ 8 はバイパスされます。これは、手順 4 ～ 8 で生成される情報がセッションの 1 番目のパケットの処理ですでに取得されているためです。

4. MIP (マップ IP) または VIP (仮想 IP) アドレスが使用されている場合、ルーティングテーブルが実際のホストアドレスを検索できるようにアドレスマッピングモジュールが MIP や VIP を解決します。

5. ルートルックアップの前に、ScreenOS は、ポリシーベースのルーティング (PBR) がないか、パケットを確認します。PBR がその受信インターフェースで有効な場合、次のアクションがパケットに適用されます。

   - その受信インターフェースにバインドされている PBR ポリシーが、パケットに適用されます。
   - インターフェースレベルで PBR ポリシーが存在しない場合、その受信インターフェースに関連付けられたゾーンにバインドされた PBR ポリシーが、パケットに適用されます。
   - ゾーンレベルで PBR ポリシーが存在しない場合、その受信インターフェースに関連付けられた VR にバインドされた PBR ポリシーが、パケットに適用されます。

注 : PBR の詳細については、*第 7 部 : ルーティング*を参照してください。

PBR が有効でない場合、ルートテーブルルックアップは、宛先アドレスに至るインターフェースを検索します。検索を行うと同時に、インターフェースモジュールはインターフェースがバインドされる宛先ゾーンを識別します。

インターフェースモジュールは、宛先ゾーンの決定に次の基準を使用します。

- 宛先ゾーンがセキュリティゾーンである場合、セキュリティゾーンがポリシールックアップに使用されます。
- 宛先ゾーンがトンネルゾーンの場合、対応するキャリアゾーンがポリシールックアップに使用されます。
- 宛先ゾーンがソースゾーンと同じであり、そのゾーンでイントラゾーンブロッキングが使用不可になっている場合、手順 6 と手順 7 が省かれてセッションが作成されます (手順 8)。イントラゾーンブロッキングが使用可能になっている場合、パケットがドロップされます。

6. ポリシーエンジンは、識別されたソースのアドレスと宛先ゾーンのアドレスの間のポリシーがないかポリシーセットリストを検索します。

   ポリシー内で構成されているアクションが、セキュリティデバイスがそのパケットを処理する方法を決定します。

   - アクションが **permit** の場合、セキュリティデバイスはパケットをその宛先に転送します。
   - アクションが **deny** の場合、セキュリティデバイスはパケットをドロップします。
   - アクションが **reject** の場合、セキュリティデバイスはパケットをドロップします。プロトコルが TCP である場合にはさらに、ソース IP アドレスにリセット (RST) を送信します。
   - アクションが **tunnel** の場合、セキュリティデバイスはパケットを VPN モジュールに転送します。VPN モジュールはパケットをカプセル化し、指定した VPN トンネル設定を使用して転送します。

7. ポリシーで NAT-Dst (宛先アドレス変換) が指定されている場合、NAT モジュールは IP パケットヘッダーにある元の宛先アドレスを異なるアドレスに変換します。

   ソースアドレス変換 (インターフェースベースの NAT またはポリシーベースの NAT-Src のいずれか) が指定されている場合、NAT モジュールは IP パケットヘッダーのソースアドレスを変換してから宛先または VPN モジュールに転送します。

   (同じポリシーで NAT-Dst および NAT-Src の両方が指定されている場合、セキュリティデバイスは最初に NAT-Dst を実行し、続いて NAT-Src を実行します。)

8. セッションモジュールは、セッションテーブルに手順 1 ～ 7 の結果が含まれた新しいエントリを作成します。

   セキュリティデバイスは、同じセッションの後続のパケットを処理するときに、セッションエントリで維持されている情報を使用します。

9. セキュリティデバイスは、セッションで指定された動作を実行します。

   主な動作には、ソースアドレス変換、VPN トンネルの選択と暗号化、暗号解読、パケット転送などがあります。

ジャンボフレーム

デバイスによっては、デバイスが処理できる最大パケットサイズ、すなわちメッセージ送信単位 (MTU) を増加させることにより、スループットを向上できます。お使いのデバイスがジャンボフレームをサポートしているか確認するには、ハードウェアのマニュアルを参照してください。

フレームサイズは 9830 ～ 1514 バイトまでの範囲です。デバイスをジャンボフレームモードにするには、最大フレームサイズを 9830 から 1515 以下の値に設定します。たとえば、**set envar max-frame-size = 9830** のようにします。通常の最大フレームサイズ (1514 バイト) にデバイスを戻すには、**unset envar max-frame-size** コマンドを使用します。または、**set envar max-frame-size = 1514** コマンドを使用できます。最大フレームサイズは、フレームの終わりにある 4 バイトのフレームチェックシーケンスを含みません。環境変数への変更を反映するには、システムを再起動しなければなりません。

ジャンボフレームモードでは、以下が該当します。

- 徹底監視 (DI) はサポートされません。
- 統合インターフェースを通って送信されたパケットは順序が乱れている可能性があります。
- NSRP 転送はサポートされません。
- ファイアウォールまたは VPN のスループットを最大化するには、少なくとも 4 つのセッション (ファイアウォール用) またはトンネル (VPN 用) が必要です。

ScreenOS アーキテクチャの例

次のセクションでは、前のセクションで説明した概念のいくつかを示す 4 つの例を挙げます。

- 「例 : (第 1 部) 6 つのゾーンを持つ企業」
- 16 ページの「例 : (第 2 部) 6 つのゾーンを持つインターフェース」
- 19 ページの「例 : (第 3 部) 2 つのルーティングドメイン」
- 20 ページの「例 : (第 4 部) ポリシー」

例 : (第 1 部) 6 つのゾーンを持つ企業

これまでのセクションで扱われた概念のいくつかを例証するために 4 部から成る例を示します。これは第 1 部です。第 2 部では各ゾーンのインターフェースを設定します。詳細については 16 ページの「例 : (第 2 部) 6 つのゾーンを持つインターフェース」を参照してください。ここでは、ある企業のために次の 6 つのゾーンを構成します。

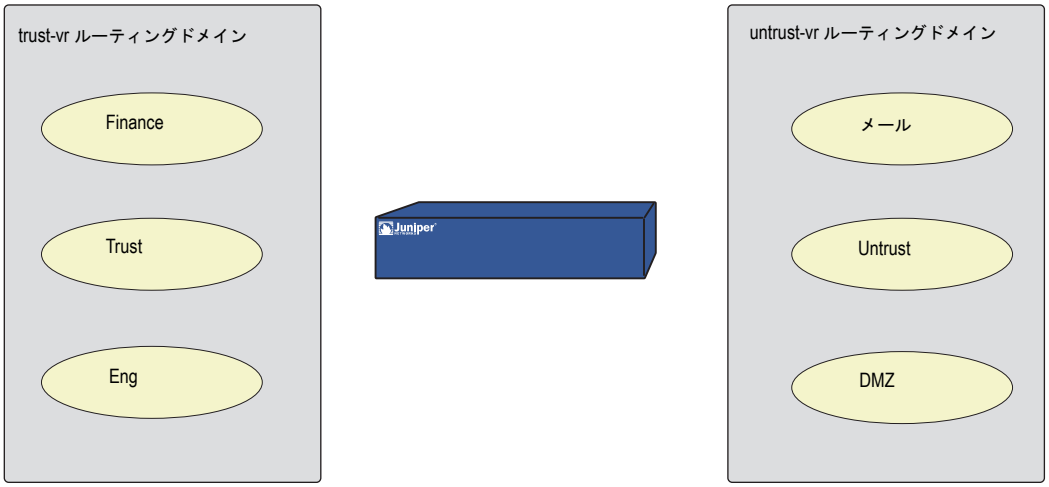
- Finance
- Trust

- Eng
- メール
- Untrust
- DMZ

Trust、Untrust、および DMZ ゾーンは構成済みです。Finance、Eng および Mail ゾーンを定義する必要があります。デフォルトでは、ユーザー定義ゾーンは trust-vr ルーティングドメインに配置されます。したがって、Finance ゾーンおよび Eng ゾーンに仮想ルーターを指定する必要はありません。ただし、Mail ゾーンは構成するだけでなく untrust-vr ルーティングドメインに置かれるように指定する必要があります。また、Untrust ゾーンと DMZ ゾーンの仮想ルーターバインディングを trust-vr から untrust-vr に変更する必要もあります。15 ページの図 10 を参照してください。

注 : 仮想ルーターとそのルーティングドメインの詳細については、*第 7 部: ルーティング*を参照してください。

図 10: ゾーンから仮想ルーターへのバインディング



WebUI

Network > Zones > New: 次のように入力してから **OK** をクリックします。

Zone Name: Finance
Virtual Router Name: trust-vr
Zone Type: Layer 3: (選択)

Network > Zones > New: 次のように入力してから **OK** をクリックします。

Zone Name: Eng
Virtual Router Name: trust-vr
Zone Type: Layer 3: (選択)

Network > Zones > New: 次のように入力してから **OK** をクリックします。

Zone Name: Mail
Virtual Router Name: untrust-vr
Zone Type: Layer 3: (**選択**)

Network > Zones > Edit (Untrust): Virtual Router Name ドロップダウンリストで **untrust-vr** を選択し、**OK** をクリックします。

Network > Zones > Edit (DMZ): Virtual Router Name ドロップダウンリストで **untrust-vr** を選択し、**OK** をクリックします。

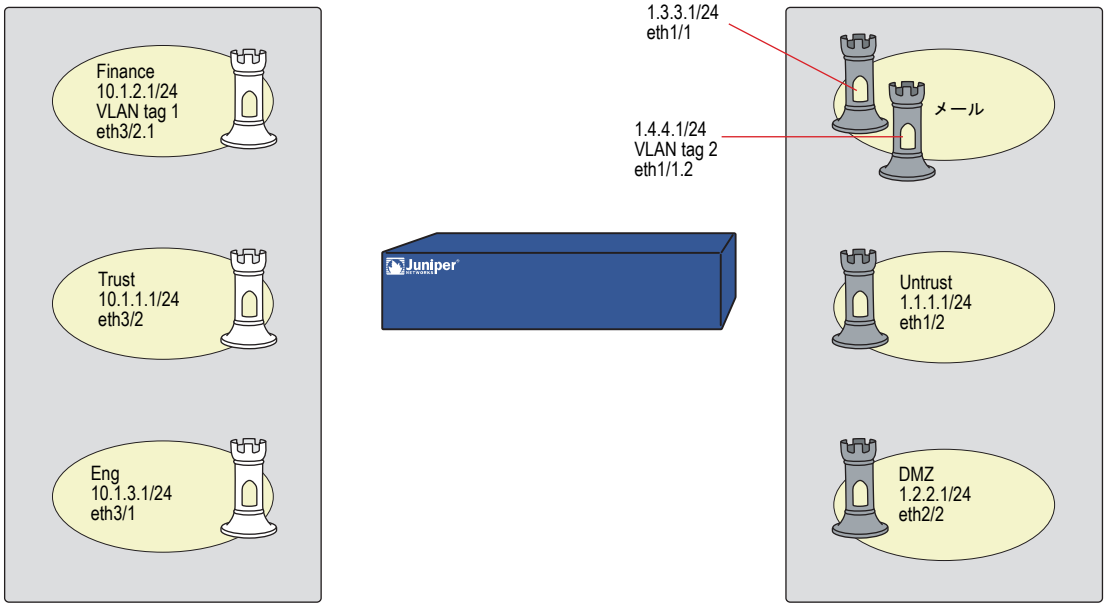
CLI

```
set zone name finance
set zone name eng
set zone name mail
set zone mail vrouter untrust-vr
set zone untrust vrouter untrust-vr
set zone dmz vrouter untrust-vr
save
```

例 : (第 2 部) 6 つのゾーンを持つインターフェース

これは、進行中の例の第 2 の 部分です。第 1 部ではゾーンが構成されました。詳細については、14 ページの「例 : (第 1 部) 6 つのゾーンを持つ企業」を参照してください。第 2 の部分では仮想ルーターが構成されます。詳細については 19 ページの「例 : (第 3 部) 2 つのルーティングドメイン」を参照してください。この部分の例では、ゾーンにインターフェースをバインドする方法、およびインターフェースに IP アドレスやさまざまな管理オプションを構成する方法を示します。図 11 を参照してください。

図 11: インターフェースからゾーンへのバインディング



WebUI

1. **インターフェース ethernet3/2**
   Network > Interfaces > Edit (ethernet3/2): 次のように入力してから **OK** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   Manageable: (選択)
   管理サービス : WebUI, Telnet, SNMP, SSH (選択)
   他のサービス : Ping (選択)

2. **インターフェース ethernet3/2.1**
   Network > Interfaces > Sub-IF New: 次のように入力してから **OK** をクリックします。

   Interface Name: ethernet3/2.1
   Zone Name: Finance
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.2.1/24
   VLAN Tag: 1
   他のサービス : Ping (選択)

3. **インターフェース ethernet3/1**
   Network > Interfaces > Edit (ethernet3/1): 次のように入力してから **OK** をクリックします。

   Zone Name: Eng
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.3.1/24
   他のサービス : Ping (選択)

4. **インターフェース ethernet1/1**
   Network > Interfaces > Edit (ethernet1/1): 次のように入力してから **OK** をクリックします。

   Zone Name: Mail
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.3.3.1/24

5. **インターフェース ethernet1/1.2**
   Network > Interfaces > Sub-IF New: 次のように入力してから **OK** をクリックします。

   Interface Name: ethernet1/1.2
   Zone Name: Mail
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.4.4.1/24
   VLAN Tag: 2

6. **インターフェース ethernet1/2**
   Network > Interfaces > Edit (ethernet1/2): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24
   Manageable: (選択)
   管理サービス : SNMP (選択)

7. **インターフェース ethernet2/2**
   Network > Interfaces > Edit (ethernet2/2): 次のように入力してから **OK** をクリックします。

   Zone Name: DMZ
   Static IP: (選択)
   IP Address/Netmask: 1.2.2.1/24

CLI

1. **インターフェース ethernet3/2**
   set interface ethernet3/2 zone trust
   set interface ethernet3/2 ip 10.1.1.1/24
   set interface ethernet3/2 manage ping
   set interface ethernet3/2 manage webui
   set interface ethernet3/2 manage telnet
   set interface ethernet3/2 manage snmp
   set interface ethernet3/2 manage ssh

2. **インターフェース ethernet3/2.1**
   set interface ethernet3/2.1 tag 1 zone finance
   set interface ethernet3/2.1 ip 10.1.2.1/24
   set interface ethernet3/2.1 manage ping

3. **インターフェース ethernet3/1**
   set interface ethernet3/1 zone eng
   set interface ethernet3/1 ip 10.1.3.1/24
   set interface ethernet3/1 manage ping

4. **インターフェース ethernet1/1**
   set interface ethernet1/1 zone mail
   set interface ethernet1/1 ip 1.3.3.1/24

5. **インターフェース ethernet1/1.2**
   set interface ethernet1/1.2 tag 2 zone mail
   set interface ethernet1/1.2 ip 1.4.4.1 /24

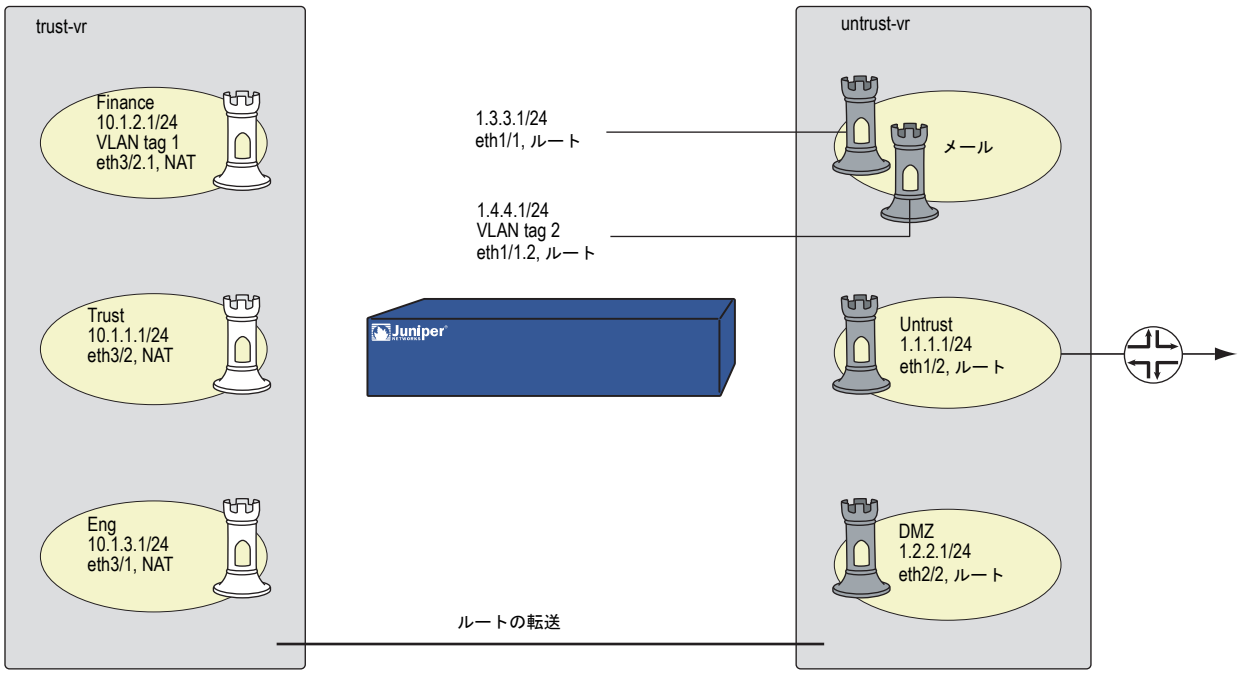
6. **インターフェース ethernet1/2**
   set interface ethernet1/2 zone untrust
   set interface ethernet1/2 ip 1.1.1.1/24
   set interface ethernet1/2 manage snmp

7. **インターフェース ethernet2/2**
   set interface ethernet2/2 zone dmz
   set interface ethernet2/2 ip 1.2.2.1/24
   save

例 : (第 3 部) 2 つのルーティングドメイン

これは、進行中の例の第 3 部です。前の部分では、さまざまなセキュリティゾーンのインターフェースを定義しました。詳細については 16 ページの「例 : (第 2 部) 6 つのゾーンを持つインターフェース」を参照してください。次の部分ではポリシーを設定します。詳細については 20 ページの「例 : (第 4 部) ポリシー」を参照してください。この例では、インターネットへのデフォルトゲートウェイのルートのみを構成します。他のルートは、インターフェース IP アドレスを作成したときに、セキュリティデバイスによって自動的に作成されます。19 ページの図 12 を参照してください。

図 12: ルーティングドメイン



WebUI

Network > Routing > Destination > (select trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Next Hop Virtual Router Name: (**選択**); untrust-vr

Network > Routing > Destination > (select untrust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: ethernet1/2
Gateway IP Address: 1.1.1.254

CLI

```
set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
set vrouter untrust-vr route 0.0.0.0/0 interface eth1/2 gateway 1.1.1.254
save
```

セキュリティデバイスは 表 1 および 表 2 のルートを自動的に作成します (一部例外あり)。

表 1: trust-vr のルートテーブル

アクセス先	使用するインターフェース	使用するゲートウェイ / 仮想ルーター	作成元
0.0.0.0/0	n/a	untrust-vr	ユーザーによる構成
10.1.3.0/24	eth3/1	0.0.0.0	セキュリティデバイス
10.1.1.0/24	eth3/2	0.0.0.0	セキュリティデバイス
10.1.2.0/24	eth3/2.1	0.0.0.0	セキュリティデバイス

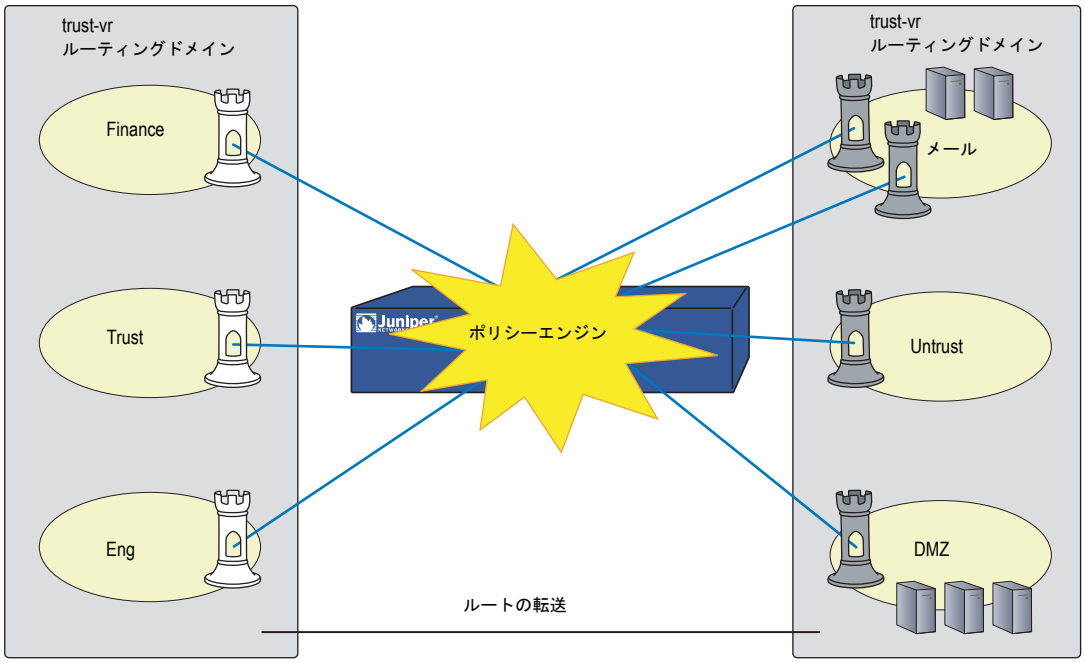
表 2: untrust-vr のルートテーブル

アクセス先	使用するインターフェース	使用するゲートウェイ / 仮想ルーター	作成元
1.2.2.0/24	eth2/2	0.0.0.0	セキュリティデバイス
1.1.1.0/24	eth1/2	0.0.0.0	セキュリティデバイス
1.4.4.0/24	eth1/1.2	0.0.0.0	セキュリティデバイス
1.3.3.0/24	eth1/1	0.0.0.0	セキュリティデバイス
0.0.0.0/0	eth1/2	1.1.1.254	ユーザーによる構成

例: (第 4 部) ポリシー

これは、進行中の例の最終部分です。前の部分は 19 ページの「例 : (第 3 部) 2 つのルーティングドメイン」で説明されています。この例では、新しいポリシーの構成方法を示します。図 13 を参照してください。

図 13: ポリシー



この例では、新しいポリシーの構成を始める前に新しいサービスグループを作成する必要があります。

注 : ゾーンを作成する場合、セキュリティデバイスは、そのゾーン内の全ホストに対して **Any** というアドレスを自動的に作成します。この例では、ホストに対してアドレス **Any** を利用します。

WebUI

1. **サービスグループ**

   Policy > Policy Elements > Services > Groups > New: 次のように入力してから **OK** をクリックします。

   Group name: Mail-Pop3

   Mail を選択し、< < ボタンを使って Available Members 列から Group Members 列にそのサービスを移動します。

   Pop3 を選択し、< < ボタンを使って Available Members 列から Group Members 列にそのサービスを移動します。

   Policy > Policy Elements > Services > Groups > New: 次のように入力してから **OK** をクリックします。

   Group name: Group name: HTTP-FTPGet

   HTTP を選択し、< < ボタンを使って Available Members 列から Group Members 列にそのサービスを移動します。

   FTP-Get を選択し、< < ボタンを使って Available Members 列から Group Members 列にそのサービスを移動します。

2. **ポリシー**

   Policy > Policies > (From: Finance, To: Mail) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), Any
   Destination Address:
   Address Book Entry: (**選択**), Any
   Service: Mail-Pop3
   Action: Permit

   Policy > Policies > (From: Trust, To: Mail) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), Any
   Destination Address:
   Address Book Entry: (**選択**), Any
   Service: Mail-Pop3
   Action: Permit

Policy > Policies > (From: Eng, To: Mail) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), Any
Destination Address:
    Address Book Entry: (選択), Any
Service: Mail-Pop3
Action: Permit

Policy > Policies > (From: Untrust, To: Mail) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), Any
Destination Address:
    Address Book Entry: (選択), Any
Service: Mail
Action: Permit

Policy > Policies > (From: Finance, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), Any
Destination Address:
    Address Book Entry: (選択), Any
Service: HTTP-FTPGet
Action: Permit

Policy > Policies > (From: Finance, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), Any
Destination Address:
    Address Book Entry: (選択), Any
Service: HTTP-FTPGet
Action: Permit

Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), Any
Destination Address:
    Address Book Entry: (選択), Any
Service: HTTP-FTPGet
Action: Permit

Policy > Policies > (From: Trust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), Any
Destination Address:
    Address Book Entry: (選択), Any
Service: HTTP-FTPGet
Action: Permit

Policy > Policies > (From: Eng, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), Any
Destination Address:
    Address Book Entry: (選択), Any
Service: HTTP-FTPGet
Action: Permit

Policy > Policies > (From: Eng, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), Any
Destination Address:
    Address Book Entry: (選択), Any
Service: FTP-Put
Action: Permit

Policy > Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), Any
Destination Address:
    Address Book Entry: (選択), Any
Service: HTTP-FTPGet
Action: Permit

CLI

1. **サービスグループ**
   set group service mail-pop3 add mail
   set group service mail-pop3 add pop3
   set group service http-ftpget add http
   set group service http-ftpget add ftp-get

2. **ポリシー**
   set policy from finance to mail any any mail-pop3 permit
   set policy from trust to mail any any mail-pop3 permit
   set policy from eng to mail any any mail-pop3 permit
   set policy from untrust to mail any any mail permit
   set policy from finance to untrust any any http-ftpget permit
   set policy from finance to dmz any any http-ftpget permit
   set policy from trust to untrust any any http-ftpget permit
   set policy from trust to dmz any any http-ftpget permit
   set policy from eng to untrust any any http-ftpget permit
   set policy from eng to dmz any any http-ftpget permit
   set policy from eng to dmz any any ftp-put permit
   set policy from untrust to dmz any any http-ftpget permit
   save

第 2 章
ゾーン

ゾーンは、セキュリティ測定が適用されるネットワークスペースのセグメント (セキュリティゾーン)、VPN トンネルインターフェースがバインドされる論理セグメント (トンネルゾーン)、または特定の機能を実行する物理エンティティあるいは論理エンティティ (機能ゾーン) のいずれかになります。

本章では、特にセキュリティゾーンに重点を置きながら、各タイプのゾーンを検討します。本章のセクションは、以下のようになります。

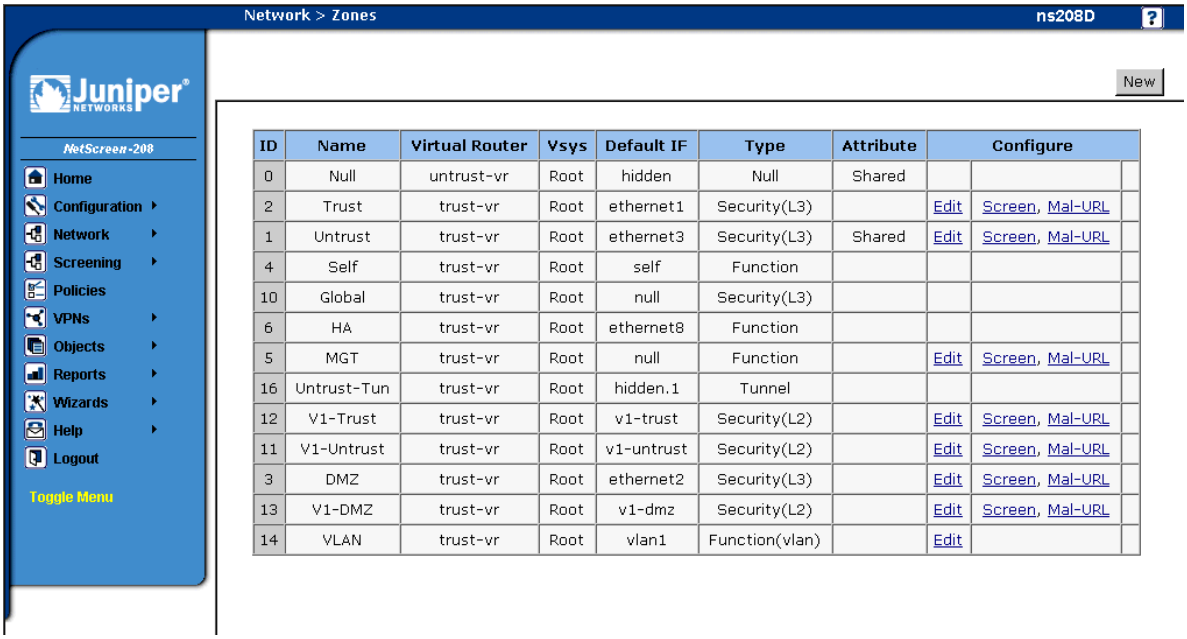
- 26 ページの「構成済みゾーンの表示」
- 28 ページの「セキュリティゾーン」
- 29 ページの「トンネルゾーンにトンネルインターフェースをバインドする」
- 30 ページの「セキュリティゾーンとトンネルゾーンの構成」
- 33 ページの「機能ゾーン」

構成済みゾーンの表示

初めてセキュリティデバイスを起動すると、多くの事前構成済みゾーンが表示されます。これらのゾーンを WebUI を使って表示する場合は、左側にあるメニュー列の **Network > Zones** をクリックします。図 14 を参照してください。

こららのゾーンを CLI を使って表示するには、**get zone** コマンドを使用します。27 ページの図 15 を参照してください。

図 14: WebUI の Network > Zones ページ



ID	Name	Virtual Router	Vsys	Default IF	Type	Attribute	Configure	
0	Null	untrust-vr	Root	hidden	Null	Shared		
2	Trust	trust-vr	Root	ethernet1	Security(L3)		Edit	Screen, Mal-URL
1	Untrust	trust-vr	Root	ethernet3	Security(L3)	Shared	Edit	Screen, Mal-URL
4	Self	trust-vr	Root	self	Function			
10	Global	trust-vr	Root	null	Security(L3)			
6	HA	trust-vr	Root	ethernet8	Function			
5	MGT	trust-vr	Root	null	Function		Edit	Screen, Mal-URL
16	Untrust-Tun	trust-vr	Root	hidden.1	Tunnel			
12	V1-Trust	trust-vr	Root	v1-trust	Security(L2)		Edit	Screen, Mal-URL
11	V1-Untrust	trust-vr	Root	v1-untrust	Security(L2)		Edit	Screen, Mal-URL
3	DMZ	trust-vr	Root	ethernet2	Security(L3)		Edit	Screen, Mal-URL
13	V1-DMZ	trust-vr	Root	v1-dmz	Security(L2)		Edit	Screen, Mal-URL
14	VLAN	trust-vr	Root	vlan1	Function(vlan)		Edit	

図 15 は、**get zone** コマンドの出力を示しています。

図 15: get zone コマンドの出力

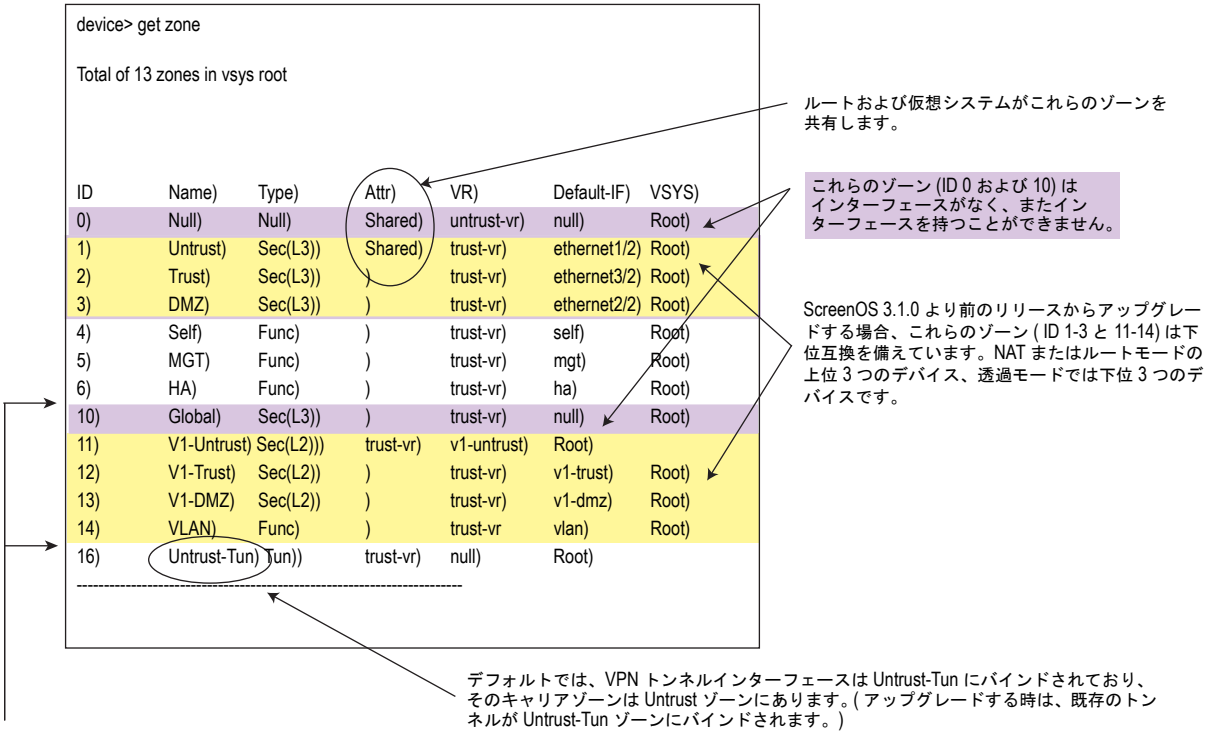


図 14 と 図 15 に示される事前構成済みゾーンは、以下の 3 つの異なるタイプに分類できます。

- セキュリティ : Untrust, Trust, DMZ, Global, V1-Untrust, V1-Trust, V1-DMZ
- トンネル : Untrust-Tun
- 機能ゾーン : Null、Self、MGT、HA、VLAN

セキュリティゾーン

各セグメントのニーズに応じてさまざまなセキュリティオプションを適用できるように、1 つのセキュリティデバイス上でネットワークをセグメントに分割し、複数のセキュリティゾーンを構成することができます。最小限、基本的にネットワークの 1 つのエリアを他から保護する 2 つのセキュリティゾーンを定義する必要があります。セキュリティプラットフォームには、複数のセキュリティアプライアンスを配備しなくても、多数のセキュリティゾーンを定義して、ネットワークセキュリティ設計上の細分性を高めることができるものもあります。

Global ゾーン

セキュリティゾーンには、アドレス帳があり、ポリシーで照会可能なので、セキュリティゾーンは識別することができます。グローバルゾーンは、これらの条件を満たします。しかし、インターフェースという、他のすべてのセキュリティゾーンがもつ 1 つの要素をもっていません。Global ゾーンは、マップ IP (MIP) と仮想 IP (VIP) アドレスのための記憶域として機能します。事前定義グローバルゾーンアドレス Any はすべての MIP、VIP、およびグローバルゾーンのその他のユーザー定義アドレスセットに適用されます。これらのアドレスに向かうトラフィックは他のアドレスにマップされるので、Global ゾーンはそれを通るトラフィックのインターフェースを必要としません。

Global ゾーンは、グローバルポリシーで使用するためのアドレスも含みます。グローバルポリシーに関する詳細については、164 ページの「グローバルポリシー」を参照してください。

注 : Global ゾーンをその宛先として使用するポリシーはすべて、NAT あるいはトラフィックシェーピングをサポートすることができません。

SCREEN オプション

Juniper Networks ファイアウォールは、1 つのセキュリティゾーンから別のセキュリティゾーンへの通過を必要とする接続試行をすべて検査して許可または拒否することによって、ネットワークの安全を確保します。すべてのセキュリティゾーン、および MGT ゾーンでは、セキュリティデバイスが潜在的に危険であると判断した種々のトラフィックを検出してブロックする、事前定義された SCREEN オプション一式を使用可能にすることができます。

利用可能な SCREEN オプションの詳細は、“ 第 4 部 : 攻撃の検出と防衛機能 ” を参照してください。

トンネルゾーンにトンネルインターフェースをバインドする

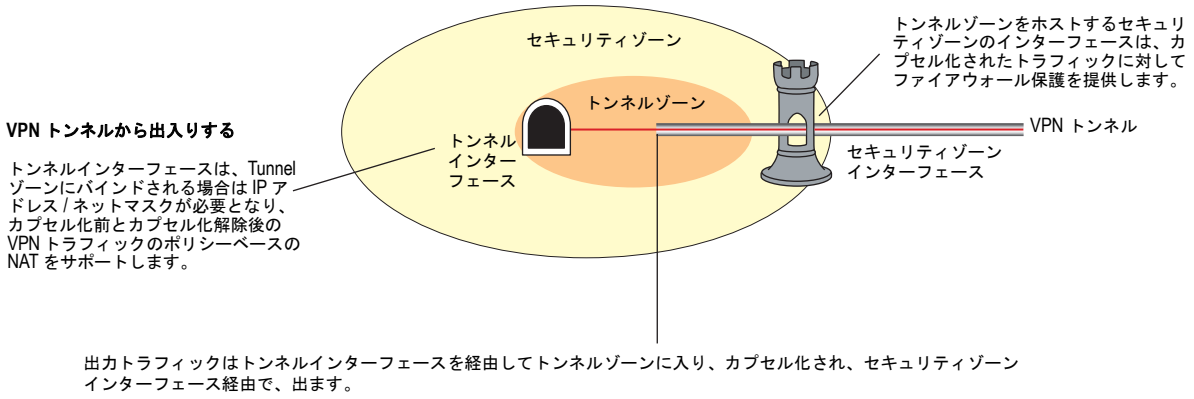
トンネルゾーンとは、1 つ以上のトンネルインターフェースをホストする論理セグメントです。トンネルゾーンは、「親子」関係のセキュリティゾーンに概念的に関連しています。「親」として動作するセキュリティゾーンは、キャリアゾーンとすることもでき、カプセル化されたトラフィックに対するファイアウォール保護を提供します。トンネルゾーンはパケットのカプセル化 / カプセル化解除を行い、MIP (マップされた IP) アドレスおよび DIP (動的 IP) プールをホストする IP アドレスやネットマスクを使ってトンネルインターフェースをサポートすることによって、ポリシーベース NAT サービスを提供できます。

セキュリティデバイスは、キャリアゾーンがトラフィックをトンネルの端点まで導くルーティング情報を使用します。デフォルトトンネルゾーンは、Untrust-Tun ゾーンであり、Untrust ゾーンと関係があります。仮想システムごとにキャリアゾーン 1 つにつき 1 つのトンネルゾーンのみで、他のトンネルゾーンを作成して、他のセキュリティゾーンにバインドすることができます。

注 : ルートシステムとすべての仮想システムは、Untrust ゾーンを共有することができます。しかし、各システムには個別の Untrust-Tun ゾーンがあります。

デフォルトでは、トンネルゾーンは trust-vr ルーティングドメインにありますが、トンネルゾーンを別のルーティングドメインに移動することもできます。図 16 を参照してください。

図 16: Tunnel ゾーンのルーティングドメイン



バージョン 3.1.0 以前の ScreenOS からアップグレードする場合、既存のトンネルインターフェースはデフォルトで、前もって構成された Untrust-Tun トンネルゾーンにバインドされます。それは前もって構成された Untrust セキュリティゾーンの「子」です。複数のトンネルゾーンを同じセキュリティゾーンにバインドできますが、トンネルゾーンを別のトンネルゾーンにバインドすることはできません。

この例では、トンネルインターフェースを作成し、tunnel.3 という名前を付けます。それを Untrust-Tun ゾーンにバインドし、IP アドレス 3.3.3.3/24 を割り当てます。次に、tunnel.3 に MIP (マップされた IP) アドレスを定義し、3.3.3.5 を Trust ゾーンのサーバーアドレスである 10.1.1.5 に変換します。Untrust-Tun ゾーンのキャリアゾーンである Untrust ゾーンも Trust ゾーンも trust-vr ルーチンドメインにあります。

WebUI

1. **トンネル インターフェース**
   Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

   Tunnel Interface Name: tunnel.3
   Zone (VR): Untrust-Tun (trust-vr)
   Fixed IP: (選択)
   IP Address/Netmask: 3.3.3.3/24

2. **MIP**
   Network > Interfaces > Edit (tunnel.8 を開く) > MIP > New: 次のように入力してから **OK** をクリックします。

   Mapped IP: 3.3.3.5
   Host IP Address: 10.1.1.5
   Netmask: 255.255.255.255
   Host Virtual Router Name: trust-vr

CLI

1. **トンネル インターフェース**
   set interface tunnel.3 zone Untrust-Tun
   set interface tunnel.3 ip 3.3.3.3/24

2. **MIP**
   set interface tunnel.3 mip 3.3.3.5 host 10.1.1.5
   save

セキュリティゾーンとトンネルゾーンの構成

最高性能の維持のために、いつも変更は保存し、ゾーンの作成後は再起動します。レイヤー 3 または レイヤー 2 セキュリティゾーンと Tunnel ゾーンの作成、変更、削除手順はほとんど一緒です。

注 : 定義済みセキュリティゾーンあるいは定義済みトンネルゾーンを編集することができても、削除することはできません。

ゾーンの作成

レイヤー 3 またはレイヤー 2 のセキュリティゾーンを作成する、あるいはトンネルゾーンを作成するには、WebUI か CLI のいずれかを使用します。

WebUI

Network > Zones > New: 次のように入力してから **OK** をクリックします。

Zone Name: ゾーンの名前を入力します。

Virtual Router Name: ゾーンを配置するルーティングドメインの仮想ルーターを選択します。

Zone Type:

Layer 3 を選択して、インターフェースをバインドすることができるゾーンを NAT またはルートモードで作成します。

Layer 2 を選択して、インターフェースをバインドすることができるゾーンを透過モードで作成します。

Tunnel ゾーンを作成してキャリアゾーンにバインドする場合は、**Tunnel Out Zone** を選択して、特定のキャリアゾーンをドロップダウンリストから選択します。

Block Intra-Zone Traffic: このオプションを選択して、同じセキュリティゾーン内のホスト間のトラフィックをブロックします。デフォルトでは、イントラゾーンブロッキングが無効です。

注 : レイヤー 2 セキュリティゾーンの名前には先頭に“L2-”が付きます (例 : “L2-Corp”または“L2-XNet”)。

CLI

```
set zone name zone [ l2 vlan_id_num | tunnel sec_zone ]
set zone zone block
set zone zone vrouter name_str
save
```

注 : レイヤー 2 のセキュリティゾーンを作成するときは、VLAN ID 番号を必ず 1 にしてください (VLAN1 用)。

ゾーンの変更

セキュリティゾーンまたはトンネルゾーンの名前を変更する、あるいはトンネルゾーンのキャリアゾーンを変更するには、まずゾーンを削除し、次に変更を加えたゾーンを作成し直します。イントラゾーンブロッキングオプションと既存するゾーン上の仮想ルーターを変更することができます。

注 : ゾーンを削除する前に、バインドしているすべてのインターフェースを最初にアンバインドする必要があります。

ゾーンの仮想ルーターを変更するときは、その前にバインドしているすべてのインターフェースを削除してください。

WebUI

1. **ゾーン名の変更**
   Network > Zones: (名前を変更したいセキュリティゾーン、トンネルゾーン、またはキャリアゾーンを変更したいトンネルゾーンの) **Remove** をクリックします 。

   削除を確認するプロンプトが表示されたら、**Yes** をクリックします。

Network > Zones > New: ゾーン設定に変更を加えて入力して、**OK** をクリックします。

2. **イントラゾーンブロッキングオプションあるいは仮想ルーターの変更**
   Network > Zones > Edit (変更するゾーン): 次のように入力してから **OK** をクリックします。

   Virtual Router Name: ドロップダウンリストからゾーンを移動するルーティングドメインの仮想ルーターを選択します。

   Block Intra-Zone Traffic: 使用可能にするには、チェックボックスをオンにします。無効にするには、クリアします。

CLI

1. **ゾーン名の変更**
   unset zone *zone*
   set zone name *zone* [l2 *vlan_id_num* | tunnel *sec_zone*]

2. **イントラゾーンブロッキングオプションあるいは仮想ルーターの変更**
   { set | unset } zone *zone* block
   set zone *zone* vrouter *name_str*
   save

ゾーンの削除

最高の性能を維持するため、必ず変更は保存し、ゾーンを作成後は再起動します。セキュリティゾーンあるいはトンネルゾーンを削除するには、以下のいずれかを行います。

WebUI

Network > Zones: **Remove** をクリックします (削除するゾーンの場合)。

削除を確認するプロンプトが表示されたら、**Yes** をクリックします。

CLI

unset zone *zone*
save

注 : ゾーンを削除する前に、バインドしているすべてのインターフェースを最初にアンバインドする必要があります。ゾーンからインターフェースをアンバインドするために、45 ページの「インターフェースをセキュリティゾーンにバインドする」を参照してください。

機能ゾーン

5 つの機能ゾーンは、Null、MGT、HA、Self、および VLAN です。各ゾーンには、表 3 に説明されているように単一の目的があります。

表 3: 機能ゾーン

ゾーン	解説
Null ゾーン	このゾーンは、他のゾーンにバインドされていない任意のインターフェースのための一時的なストレージとして機能します。
MGT ゾーン	このゾーンは、帯域外管理インターフェースである MGT をホストします。種々の攻撃から管理インターフェースを保護するために、このゾーンにファイアウォールオプションを設定できます。ファイアウォールオプションの詳細については、“ 第 4 部 : 攻撃の検出と防衛機能 ” を参照してください。
HA ゾーン	このゾーンは、高可用性インターフェースである HA1 と HA2 をホストします。HA ゾーンのインターフェースを設定することはできますが、ゾーン自体は構成できません。
セルフゾーン	このゾーンは、リモート管理接続のためのインターフェースをホストします。HTTP、SCS または Telnet 経由でセキュリティデバイスに接続する場合は、セルフゾーンに接続します。
VLAN ゾーン	このゾーンは VLAN1 インターフェースをホストします。VLAN1 インターフェースは、デバイスが透過モードにあるときにデバイスを管理し、VPN トラフィックを終了します。種々の攻撃から VLAN1 インターフェースを保護するために、このゾーンにファイアウォールオプションも設定できます。

第 3 章
インターフェース

物理インターフェースとサブインターフェースは、トラフィックのセキュリティゾーンへの出入りを可能にします。ネットワークトラフィックがセキュリティゾーンに出入りできるようにするには、インターフェースをそのセキュリティゾーンにバインドし、セキュリティゾーンがレイヤー 3 ゾーンであれば IP アドレスを割り当てます。次にトラフィックがゾーン間のインターフェースからインターフェースへと通過できるようにするポリシーを構成します。複数のインターフェースを 1 つのゾーンに割り当てることはできますが、1 つのインターフェースを複数のゾーンに割り当てることはできません。

本章のセクションは、以下のようになります。

- 35 ページの「インターフェースタイプ」
- 43 ページの「インターフェースの表示」
- 45 ページの「セキュリティゾーンインターフェースを構成する」
- 51 ページの「2 次 IP アドレスを作成する」
- 52 ページの「ループバックシステムインターフェース」
- 58 ページの「ループバックインターフェース」
- 62 ページの「インターフェース状態の変化」

インターフェースタイプ

このセクションでは、論理インターフェース、機能ゾーンインターフェースおよびトンネルインターフェースについて説明します。これらのインターフェースの表を表示する方法は、43 ページの「インターフェースの表示」を参照してください。

論理インターフェース

論理インターフェースの目的は、ネットワークトラフィックがゾーン間を通過するための通り道を提供することです。ScreenOS は以下のタイプの論理インターフェースに対応しています。

- 物理インターフェース
- ワイヤレスインターフェース

- ブリッジグループインターフェース
- サブインターフェース
- 統合インターフェース
- 冗長インターフェース
- 仮想セキュリティインターフェース

物理インターフェース

物理インターフェースの名前は、メディアタイプ、スロット番号 ((一部のデバイスの場合) 、およびインデックス番号からなります。たとえば、*ethernet3/2*、*ethernet0/2*、*wireless2*、*wireless0/2*、*bgroup2*、*serial0/0*、*serial0/2*、*bri0/0*、*または adsl0/2* のようになります。物理インターフェースを、トラフィックがゾーンを出入りするための出入口の働きをするあらゆるセキュリティゾーンにバインドできます。インターフェースがなければ、トラフィックはゾーンにアクセスすることもゾーンから出ることもできません。

インターフェースからゾーンへのバインディングの変更をサポートしてするセキュリティデバイスでは、3 つの物理イーサネットインターフェースが、V1-Trust、V1-Untrust、V1-DMZ という特定のレイヤー 3 セキュリティゾーンにあらかじめバインドされています。どのインターフェースがどのゾーンにバインドしているかは、各プラットフォームにより異なります。(セキュリティゾーンの詳細については、45 ページの「セキュリティゾーンインターフェースを構成する」を参照してください。)

ワイヤレスインターフェース

ワイヤレスインターフェースは、物理インターフェースと同様に、トラフィックがセキュリティゾーンに出入りするための出入口の働きをします。各ワイヤレスセキュリティデバイスは、最高 4 つのワイヤレスインターフェース (wireless0/0 ～ wireless0/3) が同時にアクティブになることを許可します。

ワイヤレスインターフェースは、Untrust セキュリティゾーンにバインドできません。(詳細は、**12**-115 ページの「ワイヤレス ローカル エリア ネットワーク」を参照してください。)

ブリッジグループインターフェース

セキュリティデバイスにはブリッジグループ (bgroups) をサポートするものがあります。bgroup を使えば、複数のイーサネットおよびワイヤレスインターフェースをグループ化できます。各 bgroup は、自身のブロードキャストドメインを構成し、グループ内のインターフェース間の高速イーサネットスイッチングを提供します。各 bgroup インターフェースに 1 つの IP アドレスを割り当てることができます。bgroup インターフェースは、あらゆるゾーンにバインドできます。

ブリッジグループで構成済みのデバイスについては、2 つの異なるブリッジグループ番号方式があります。いくつかのデバイスでは、構成済みの bgroup インターフェースが bgroup0 ～ bgroup3 によって識別されます。他のデバイスでは、構成済みの bgroup インターフェースが bgroup0/0 ～ bgroup0/2 によって識別されます。

PIM または mini-PIM のようなフィールドインストール可能なモジュールをサポートするいくつかのデバイスでは、モジュール上のイーサネットポートのいくつかまたはすべてを含む bgroup を作成できます。これらのデバイスで、bgroupx/y によって識別される bgroup を作成します。ここで、x はグループ化されたポートを含むモジュールのスロット番号、y はブリッジグループを作成するときに割り当てる番号です。

ブリッジグループインターフェースは、あらゆるゾーンにバインドできます。(詳細については、45 ページの「インターフェースをセキュリティゾーンにバインドする」を参照してください)。

サブインターフェース

サブインターフェースは、物理インターフェースと同様に、トラフィックがセキュリティゾーンに出入りするための出入口の働きをします。物理インターフェースは、複数の仮想サブインターフェースへ論理的に分けることが可能です。各仮想サブインターフェースは、必要な帯域幅を自分の元になる物理インターフェースから借りるため、その名前は物理インターフェース名の延長になり、たとえば、*ethernet3/2.1* や *ethernet0/2.1* のようになります。

サブインターフェースは、あらゆるレイヤー 3 ゾーンにバインドできます。サブインターフェースをその物理インターフェースと同じゾーンにバインドすることも、別のゾーンにバインドすることもできます。(詳細については、45 ページの「インターフェースをセキュリティゾーンにバインドする」を参照してください)。

統合インターフェース

セキュリティデバイスには、統合インターフェースをサポートするものがあります。統合インターフェースは、2 つ以上の物理インターフェースを集積したもので、この統合インターフェースの IP アドレスへ向かうトラフィック負荷は各物理インターフェースによって等しく分担されます。統合インターフェースを使用することによって、1 つの IP アドレスで使用可能な帯域幅を大幅に増加させることができます。また、統合インターフェースの中の 1 つに障害が発生した場合、他のインターフェースが、障害前より帯域幅が少なくなってはいますがトラフィック処理を継続できます。

注 : 統合インターフェースの詳細については、**11**-43 ページの「インターフェースの冗長性および フェールオーバー」を参照してください。

冗長インターフェース

2 つの物理インターフェースをバインドして 1 つの冗長インターフェースをつくり、この冗長インターフェースをセキュリティゾーンにバインドできます。2 つの物理インターフェースのうちの一方が 1 次インターフェースとして、その冗長インターフェースへ向かうすべてのトラフィックを処理します。もう一方の物理インターフェースは 2 次インターフェースとして、稼動中のインターフェースに障害が発生した場合にそなえてスタンバイしています。障害が発生すると、冗長インターフェースへ向かうトラフィックは 2 次インターフェースへフォールオーバーし、この 2 次インターフェースが新しい 1 次インターフェースになります。冗長インターフェースを使用することが、フェールオーバーがデバイスレベルに発展する前の最初の冗長化となります。

注： 冗長インターフェースの詳細については、**11**-43 ページの「インターフェースの冗長性および フェールオーバー」を参照してください。

仮想セキュリティインターフェース

VSI (仮想セキュリティインターフェース) は、VSD (仮想セキュリティデバイス) をつくる 2 台の セキュリティデバイスが、HA モードで動作するときに共有する仮想インターフェースです。ネットワークと VPN トラフィックは、VSI の IP アドレスと仮想 MAC アドレスを使用します。VSD はさらに、あらかじめ VSI をバインドしておいた物理インターフェース、サブインターフェースもしくは冗長インターフェースへトラフィックをマッピングします。2 台の セキュリティデバイスが HA モードで動作しているときは、デバイスのフェールオーバーの際に連続したサービスを提供したいセキュリティゾーンインターフェースを 1 台以上の 仮想セキュリティデバイス (VSD) にバインドする必要があります。インターフェースを VSD (仮想セキュリティデバイス) にバインドすると、VSI (仮想セキュリティインターフェース) になります。

注： VSI の詳細と VSI が HA クラスタで VSD とどのように機能するかについては、*第 11 部 : 高可用性*を参照してください。

機能ゾーンインターフェース

機能ゾーンインターフェースには「管理」や「HA」があり、それぞれ特別な目的があります。

管理インターフェース

セキュリティデバイスによっては、通常のネットワークユーザートラフィック以外の管理トラフィックを移動する、管理 (MGT) インターフェースという独立した物理インターフェースを通して、デバイスを管理できます。管理トラフィックをネットワークユーザートラフィックと切り離すことにより、セキュリティが大幅に強化され、安定した帯域幅管理が可能になります。

注： デバイスの管理向け構成については、**3**-1 ページの「管理」を参照してください。

高可用性インターフェース

高可用性 (HA) インターフェースは、HA 機能専用の物理ポートです。冗長グループの中で、一方のユニットは 1 次デバイスとして、ネットワークファイアウォール、VPN、トラフィックシェーピングの機能を行い、もう一方のユニットは、バックアップデバイスとして、1 次ユニットが故障した場合にファイアウォール機能を引き継ぐために待機しています。これを、アクティブ / パッシブ構成といいます。また、クラスタのどちらのユニットも、互いの 1 次ユニットとバックアップユニットになるように設定することもできます。これを、アクティブ / アクティブ構成といいます。この 2 つの構成については、*第 11 部 : 高可用性*で詳しく説明しています。

仮想 HA インターフェース

HA 専用インターフェースがないセキュリティデバイスでは、仮想 HA インターフェースが同じ機能を提供します。HA トラフィック専用の独立した物理ポートがないため、仮想 HA インターフェースはイーサネット物理ポートの 1 つにバインドする必要があります。セキュリティゾーンにネットワークインターフェースをバインドするのと同じ手順で、ネットワークインターフェースを HA ゾーンにバインドします。

トンネルインターフェース

トンネルインターフェースは、VPN トンネルへの出入口の働きをします。トラフィックは、トンネルインターフェースから VPN トンネルに出入りします。

トンネルインターフェースを VPN トンネルにバインドするとき、その トンネルインターフェースを特定の宛先へのルート内で参照し、それからその宛先を 1 つ以上のポリシー内で参照することができます。このアプローチにより、トラフィックのフローをトンネルを経て細かく制御できます。また、VPN トラフィックのための動的ルーティングもサポート可能になります。VPN トンネルにバインドされたトンネルインターフェースがない場合は、ポリシー自体の中で VPN トンネルを指定して、**tunnel** をアクションに選択してください。**Tunnel** アクションは許可を意味するため、VPN トンネルからのトラフィックをはっきりと拒否することはできません。

動的 IP (DIP) アドレスのプールをトンネル インターフェースと同じサブネットで使用して、ポリシーベース NAT を送信もしくは受信トラフィックで実施できます。ポリシーベース NAT をトンネル インターフェースで使用する代表的な理由は、VPN トンネルのどちらかの側で 2 サイト間の IP アドレス矛盾が発生するのを回避するためです。

ルートベースの VPN トンネルを トンネルインターフェースへバインドして、セキュリティデバイスがトラフィックをトンネルインターフェースと送受信できるようにする必要があります。ルートベース VPN トンネルをバインドする トンネルインターフェースは、番号あり (IP アドレス / ネットマスクあり) であっても番号なし (IP アドレス / ネットマスクなし) であっても構いません。トンネルインターフェースが番号なしの場合、トンネルインターフェースが IP アドレスを借りてくるインターフェースを指定する必要があります。セキュリティデバイスは、自分がトンネルに OSPF メッセージなどのトラフィックを送り出すとき、借りてきた IP アドレスをソースアドレスとして使用します。トンネルインターフェースは IP アドレスを、同じセキュリティゾーンのインターフェースから借りることも、また別のセキュリティゾーンのインターフェースからも借りることもでき、これはどちらのセキュリティゾーンも同じルーティングドメインの中にある場合に限ります。

専用の仮想ルーティングドメイン内にある 1 つのゾーンにすべての番号なしトンネルインターフェースをバインドし、そのゾーンにバインドされたループバックインターフェースから IP アドレスを借りることで、VPN トラフィックルーティングの安全な管理可能になります。たとえば、すべての番号なし トンネルインターフェースを 天 PNi という名のユーザー定義ゾーンにバインドし、これらの トンネルインターフェースが IP アドレスを借りる loopback.1 インターフェースもこの VPN ゾーンにバインドされているように構成します。この VPN ゾーンは、“vpn-vr” という名前のユーザー定義ルーティングドメインです。トンネルが導くすべての宛先アドレスをこの VPN ゾーンに入れます。これらのアドレスへのルートは トンネルインターフェースを指し、ポリシーは他のゾーンと VPN ゾーンとの間の VPN トラフィックを制御します。図 17 を参照してください。

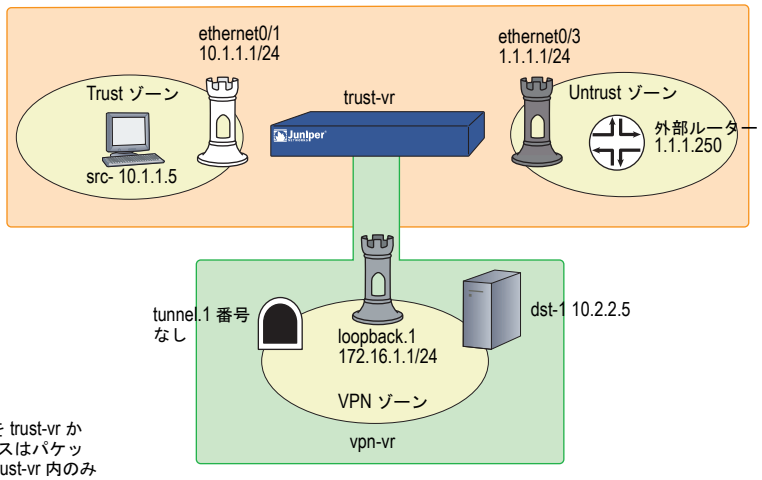
図 17: 番号なしトンネルインターフェースのバインディング

```
set vrouter name vpn-vr
set zone name vpn vrouter vpn-vr
set interface loopback.1 zone vpn
set interface loopback.1 ip 172.16.1.1/24
set interface tunnel.1 zone vpn
set interface tunnel.1 ip unnumbered loopback.1

src-1 と dst-1 のアドレスを構成します。
VPN トンネルを構成して tunnel.1 にバインドします。

set vrouter trust-vr route 10.2.2.5/32 vrouter vpn-vr
set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/3
gateway 1.1.1.250
set vrouter vpn-vr route 10.2.2.5 interface tunnel.1

set policy from trust to vpn scr-1 dst-1 any permit
```



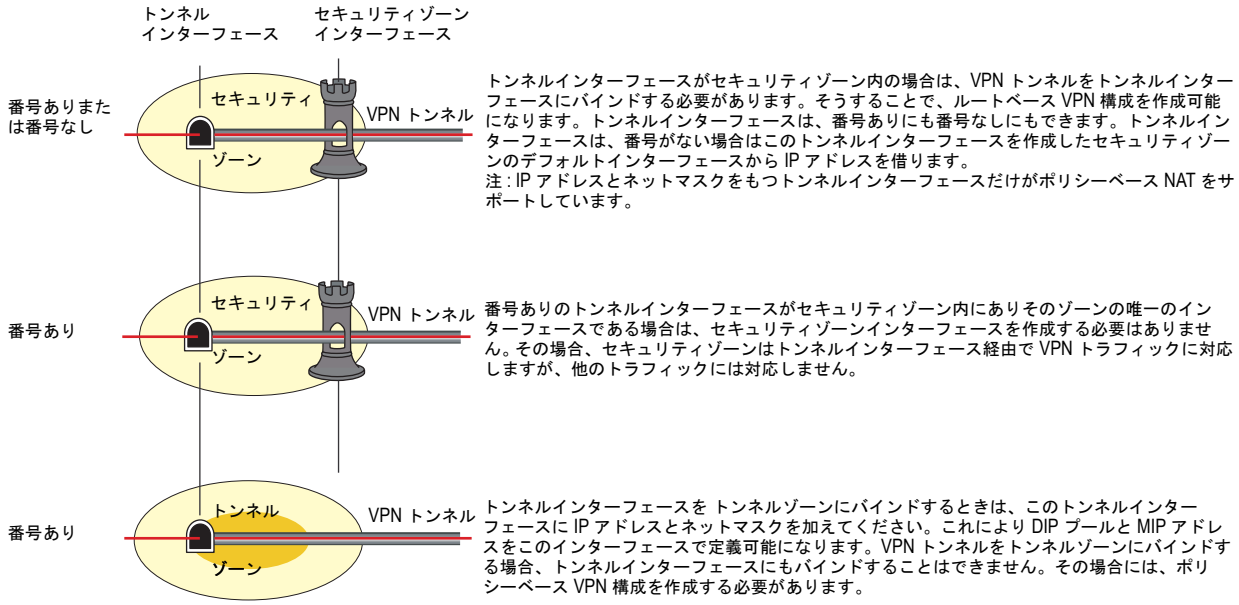
セキュリティデバイスは 10.2.2.5/32 に宛てたトラフィックを trust-vr から vpn-vr へ送ります。tunnel.1 が使用不可になると、デバイスはパケットをドロップします。デフォルトルート (0.0.0.0/0 への) は trust-vr 内のみであるため、デバイスはプレーンテキストのパケットを ethernet0/3 へ送信しようとはしません。

すべてのトンネルインターフェースをこうしたゾーンに入れることは非常に安全であるといえます。理由は、VPN に障害が発生することにより、対応付けられたトンネルインターフェースへのルートが非アクティブになり、トンネルするはずだったトラフィックがリダイレクトされてデフォルトルートのような非トンネルルートを使用してしまうといった可能性がなくなるためです。(このような問題の回避方法に関する提案については、5-68 ページの「ルートベース VPN (仮想プライベートネットワーク) のセキュリティ検討事項」を参照してください。)

トンネルインターフェースを、トンネルゾーンにバインドすることもできます。この場合、トンネルインターフェースには IP アドレスが必要になります。トンネル インターフェースを トンネル ゾーンにバインドするのは、NAT サービスをポリシーベース VPN トンネルが使用できるようにするためです。41 ページの図 18 を参照してください。

注 : ネットワークアドレス変換 (NAT) サービスには、インターフェースと同じサブネット内に定義された動的 IP (DIP) プールとマップ IP (MIP) アドレスが含まれます。

図 18: トンネルインターフェースからゾーンへのバインディング



VPN トンネルは、概念的にはパイプが走っているものと考えることができます。ローカルデバイスからリモートゲートウェイに延びており、トンネルインターフェースがこうしたパイプの開口部になります。パイプはかならずそこにあり、ルーティングエンジンがインターフェースの 1 つにトラフィックを導くといつでも使えるようになっています。

一般に、IP アドレスをトンネルインターフェースに割り当てるのは、そのトンネルインターフェースが、ソースアドレス変換 (NAT-Src) のための動的 IP (DIP) プールと宛先アドレス変換 (NAT-Dst) のためのマップ IP (MIP) アドレスをサポートするようにする場合です。VPN およびアドレス変換の詳細については、**5**-137 ページの「アドレスがオーバーラップする VPN サイト」を参照してください。IP アドレスとネットマスクをもつトンネルインターフェースを、セキュリティゾーンまたはトンネルゾーンのいずれかで作成できます。

トンネルインターフェースがアドレス変換に対応する必要がなく、構成でトンネルインターフェースをトンネルゾーンにバインドする必要がない場合は、トンネルインターフェースを番号なしに指定できます。番号のないトンネルインターフェースはセキュリティゾーンにバインドしてください。トンネルゾーンにはバインドできません。また、番号なしインターフェースがバインドされているセキュリティゾーンと同じ仮想ルーティングドメインの中にある IP アドレスを持つインターフェースを指定する必要があります。番号のないトンネルインターフェースは、IP アドレスをそのインターフェースから借ります。

注 : トンネル インターフェースをトンネルにバインドする方法の例は、**5**-77 ページの「サイト間 VPN (仮想プライベートネットワーク)」と **5**-157 ページの「ダイヤルアップ仮想プライベート ネットワーク」でルートベース VPN の例を参照してください。

VPN トンネル経由でマルチキャストパケットを伝送している場合には、トンネルインターフェース上で一般ルーティングのカプセル化 (GRE) を使用可能にすると、マルチキャストパケットをユニキャストパケットにカプセル化することができます。Juniper Networks セキュリティデバイスは、IP パケットを IPv4 ユニキャストパケットにカプセル化する、この GREv1 に対応しています。GRE の詳細については、7-155 ページの「トンネルインターフェース上に一般ルーティングのカプセル化を構成する」を参照してください。

トンネルインターフェースの削除

MIP (マップ IP) アドレスまたは DIP (動的 IP) アドレスプールのホストになっているトンネルインターフェースをいきなり削除することはできません。これらの機能のホストになっているトンネルインターフェースを削除する前に、まずこれらの機能を参照しているポリシーを削除する必要があります。それから、このトンネルインターフェースの MIP および DIP プールを削除してください。また、ルートベース VPN 構成が トンネルインターフェースを参照している場合は、先に VPN 構成を削除してからトンネルインターフェースを削除してください。

この例では、トンネルインターフェース tunnel.2 は、DIP プール 8 にリンクされています。DIP プール 8 は、Trust ゾーンから Untrust ゾーンへの vpn1 という名の VPN トンネルを流れる VPN トラフィックのポリシー (ID 10) で参照されています。トンネルインターフェースを削除するには、先にポリシーを削除 (またはポリシーから DIP プール 8 への参照を削除) してから DIP プールを削除します。その後で、tunnel.2 を vpn1 からアンバインドします。トンネルインターフェースに依存するすべての構成を削除した後で、このトンネルインターフェースを削除できます。

WebUI

1. **DIP プール 8 を参照するポリシー 10 の削除**
   Policy > Policies (From: Trust, To: Untrust): ポリシー ID 10 の **Remove** をクリックします。

2. **tunnel.2 にリンクされた DIP プール 8 の削除**
   Network > Interfaces > Edit (tunnel.2) > DIP: DIP ID 8 の **Remove** をクリックします。

3. **Tunnel.2 の vpn1 からのアンバインド**
   VPNs > AutoKey IKE > Edit (vpn1) > Advanced: Bind to: Tunnel Interface ドロップダウンリストで **None** を選択し、**Return** をクリックしてから **OK** をクリックします。

4. **tunnel.2 の削除**
   Network > Interfaces: tunnel.2 の **Remove** をクリックします。

CLI

1. **DIP プール 8 を参照するポリシー 10 の削除**
   unset policy 10
2. **tunnel.2 にリンクされた DIP プール 8 の削除**
   unset interface tunnel.2 dip 8
3. **Tunnel.2 の vpn1 からのアンバインド**
   unset vpn vpn1 bind interface
4. **tunnel.2 の削除**
   unset interface tunnel.2
   save

インターフェースの表示

セキュリティデバイスのすべてのインターフェースがリストされた表を表示できます。物理インターフェースはあらかじめ定義されているため、構成したかしないかに関係なくリストされます。サブインターフェースとトンネルインターフェースは、作成して構成したものだけがリストされます。

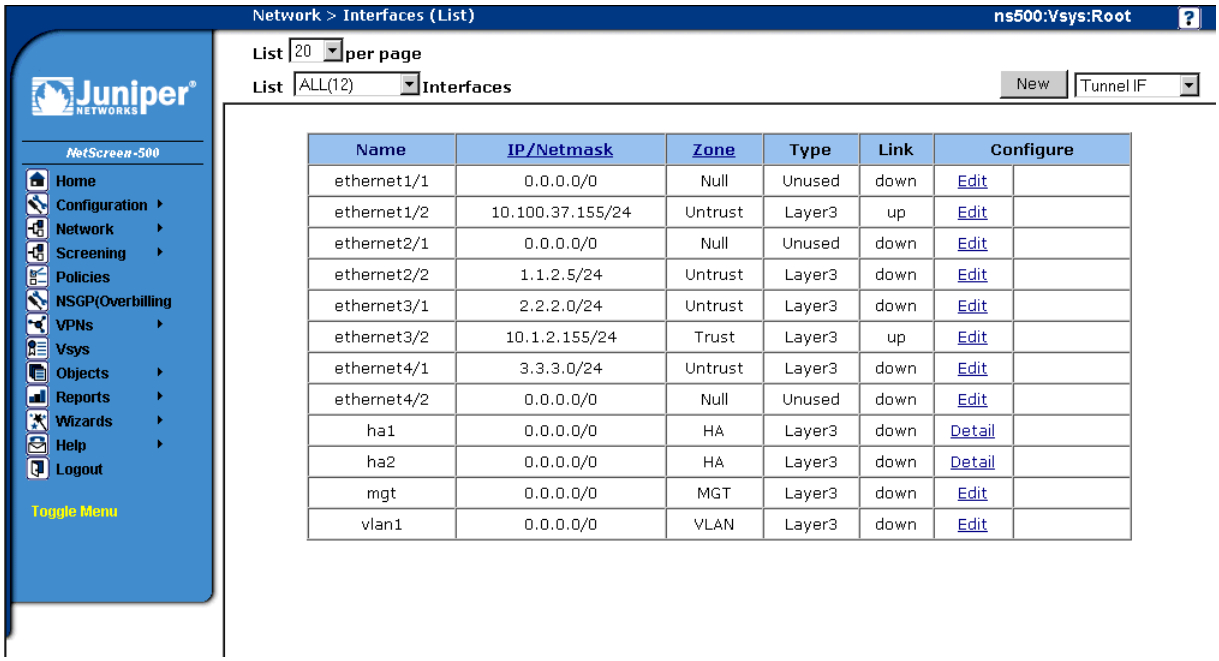
WebUI でインターフェース表を表示するには、**Network > Interfaces** をクリックします。表示するインターフェースのタイプを List Interfaces ドロップダウンリストで指定できます。

CLI でインターフェース表を表示するには、**get interface** コマンドを使用します。

インターフェース表には、それぞれのインターフェースに関する次の情報が表示されます。

- **Name:** インターフェースの名前を示すフィールドです。
- **IP/Netmask:** インターフェースの IP アドレスとネットマスクを示すフィールドです。
- **Zone:** インターフェースをバインドしているゾーンを示すフィールドです。
- **Type:** インターフェースタイプ (Layer 2、Layer 3、tunnel、redundant、aggregate、VSI) を示すフィールドです。
- **Link:** インターフェースがアクティブ (up) か非アクティブ (down) かを示すフィールドです。
- **Configure:** このフィールドで、インターフェースを変更や削除できます。

図 19: WebUI インターフェース表



Name	IP/Netmask	Zone	Type	Link	Configure	
ethernet1/1	0.0.0.0/0	Null	Unused	down	Edit	
ethernet1/2	10.100.37.155/24	Untrust	Layer3	up	Edit	
ethernet2/1	0.0.0.0/0	Null	Unused	down	Edit	
ethernet2/2	1.1.2.5/24	Untrust	Layer3	down	Edit	
ethernet3/1	2.2.2.0/24	Untrust	Layer3	down	Edit	
ethernet3/2	10.1.2.155/24	Trust	Layer3	up	Edit	
ethernet4/1	3.3.3.0/24	Untrust	Layer3	down	Edit	
ethernet4/2	0.0.0.0/0	Null	Unused	down	Edit	
ha1	0.0.0.0/0	HA	Layer3	down	Detail	
ha2	0.0.0.0/0	HA	Layer3	down	Detail	
mgt	0.0.0.0/0	MGT	Layer3	down	Edit	
vlan1	0.0.0.0/0	VLAN	Layer3	down	Edit	

図 20: CLI インターフェース表

```
ns500-> get interface

A - Active, I - Inactive, U - Up, D - Down, R - Ready

Interfaces in vsys Root:
Name            IP Address          Zone        MAC             VLAN State VSD Vsys
eth1/1          0.0.0.0/0           Null        0010.db0d.4ddc     -    D   -   Root
eth1/2          10.100.37.155/24    Untrust     0010.db0d.4dde     -    U   -   Root
eth2/1          0.0.0.0/0           Null        0010.db0d.4ddb     -    D   -   Root
eth2/2          1.1.2.5/24          Untrust     0010.db0d.4ddd     -    D   -   Root
eth3/1          2.2.2.0/24          Untrust     0010.db0d.4dd8     -    D   -   Root
eth3/2          10.1.2.155/24       Trust       0010.db0d.4dda     -    U   -   Root
eth4/1          3.3.3.0/24          Untrust     0010.db0d.4dd7     -    D   -   Root
eth4/2          0.0.0.0/0           Null        0010.db0d.4dd9     -    D   -   Root
mgt             0.0.0.0/0           MGT         0010.db0d.4dd0     -    D   -   Root
ha1             0.0.0.0/0           HA          0010.db0d.4dd5     -    D   -   Root
ha2             0.0.0.0/0           HA          0010.db0d.4dd6     -    D   -   Root
vlan1           0.0.0.0/0           VLAN        0010.db0d.4ddf     1    D   -   Root
null            0.0.0.0/0           Null        0010.dbff.0100     -    U   0   Root
ns500->
```

セキュリティゾーンインターフェースを構成する

このセクションでは、セキュリティゾーンインターフェースに関する次の要素の構成方法を説明します。

- インターフェースをセキュリティゾーンにバインドやアンバインドする
- アドレスをレイヤー 3 (L3) セキュリティゾーンインターフェースに割り当てる
- 物理インターフェースとサブインターフェースを変更する
- サブインターフェースを作成する
- サブインターフェースを削除する

注 : インターフェースへのトラフィック帯域幅の設定については、195 ページの「トラフィックシェーピング」を参照してください。管理およびインターフェースごとに使用可能なその他サービスオプションの詳細は、**3**-28 ページの「管理トラフィックのコントロール」を参照してください。

インターフェースをセキュリティゾーンにバインドする

物理インターフェースを L2 もしくは L3 のセキュリティゾーンにバインドできます。ADSL 用を除く WAN インターフェースは、L2 セキュリティゾーンにバインドできません。サブインターフェースは IP アドレスを必要とするため、L3 セキュリティゾーンにのみバインドできます。IP アドレスをインターフェースに割り当てる前に、そのインターフェースを L3 セキュリティゾーンにバインドします。ワイヤレスインターフェースは、Untrust セキュリティゾーンにバインドできません。

セキュリティデバイスによっては、複数のインターフェースをグループ化できるものがあります。インターフェースをグループに追加する前に、そのインターフェースを Null セキュリティゾーンに設定する必要があります。インターフェースをグループに追加した後で、接続を確立できるように、グループインターフェースをセキュリティゾーンに割り当てる必要があります。

この例では、ethernet0/5 を Trust ゾーンにバインドします。

WebUI

Network > Interfaces > Edit (ethernet0/5): Zone Name ドロップダウンリストから **Trust** を選択してから **Apply** をクリックします。

CLI

```
set interface ethernet0/5 zone trust
save
```

この例では、ethernet0/3 および ethernet0/4 を Null セキュリティゾーンに設定し、bgroup1 にインターフェースをグループ化して、グループを DMZ セキュリティゾーンにバインドしています。

WebUI

Network > Interfaces > Edit (ethernet0/3): Zone Name ドロップダウンリストから **Null** を選択してから **Apply** をクリックします。

Network > Interfaces > Edit (ethernet0/4): Zone Name ドロップダウンリストから **Null** を選択してから **Apply** をクリックします。

Network > Interfaces > Edit (bgroup1): Zone Name ドロップダウンリストから **DMZ** を選択してから **Apply** をクリックします。

Network > Interfaces > Edit (bgroup1): Bind to Current Bgroup 列で **ethernet0/3** および **ethernet0/4** をチェックしてから **Apply** をクリックします。

CLI

```
set interface ethernet0/3 zone null
set interface ethernet0/4 zone null
set interface bgroup1 port ethernet0/3
set interface bgroup1 port ethernet0/4
set interface bgroup1 zone DMZ
save
```

インターフェースをセキュリティゾーンからアンバインドする

インターフェースに番号がない場合は、あるセキュリティゾーンからアンバインドして別のセキュリティゾーンにバインドできます。インターフェースに番号がついている場合は、まずその IP アドレスとネットマスクを 0.0.0.0 に設定します。その後で、1 つのセキュリティゾーンからアンバインドして別のセキュリティゾーンにバインドし、(任意で) IP アドレス / ネットマスクを再び割り当てることができます。

この例で、ethernet0/3 には IP アドレス 210.1.1.1/24 があり、Untrust ゾーンにバインドされています。IP アドレスとネットマスクを 0.0.0.0/0 に設定し、Null (空) ゾーンにバインドします。

WebUI

Network > Interfaces > Edit (ethernet0/3): 次のように入力してから **OK** をクリックします。

Zone Name: Null
IP Address/Netmask: 0.0.0.0/0

CLI

```
set interface ethernet0/3 ip 0.0.0.0/0
set interface ethernet0/3 zone null
save
```

インターフェースをグループからアンバインドし、別のセキュリティゾーンに再割り当てするには、インターフェースを bgroup から解放する必要があります。bgroup からインターフェースを解放すると、インターフェースは Null セキュリティゾーンに置かれます。Null セキュリティゾーンに入ると、インターフェースは、IP アドレスを使って構成されているセキュリティゾーンにバインドできます。

WebUI

Network > Interfaces > Edit (bgroup1) > Bind Port: Bind to Current Bgroup 列で **ethernet0/3** を選択解除してから **Apply** をクリックします。

Network > Interfaces > Edit (ethernet0/3): Zone Name ドロップダウンリストから **Trust** を選択してから **Apply** をクリックします。

CLI

```
unset interface bgroup1 port ethernet0/3
set interface ethernet0/3 zone trust
save
```

L3 セキュリティゾーンインターフェースのアドレス設定

レイヤー 3 (L3) セキュリティゾーンのインターフェースまたはサブインターフェースを定義するときは、IP アドレスとネットマスクを割り当てる必要があります。インターフェースを trust-vr のゾーンにバインドする場合、インターフェースモードを NAT かルートに指定することもできます。(インターフェースをバインドするゾーンが untrust-v r にある場合、インターフェースは常にルートモードです。)

注 : NAT とルートモードの構成の例は、81 ページの「インターフェースモード」を参照してください。

インターフェースアドレスの割り当てを行うときに考慮する基本的な IP アドレスのタイプは、次の 2 つです。

- 公開アドレスは、ISP (インターネットサービスプロバイダ) がインターネットなどの公開ネットワークで使用するために提供するアドレスで、一意でなければなりません。
- 非公開アドレスは、ローカルネットワーク管理者が非公開ネットワークで使用するために割り当てます。別の管理者も、他の非公開ネットワークで使用するために非公開アドレスを割り当てできます。

注 : IP アドレスをインターフェースに加えると、セキュリティデバイスは ARP 要求によって、この IP アドレスがすでにローカルネットワークに存在しないかどうかを調べます。(このとき物理リンクが稼動している必要があります。) この IP アドレスがすでに存在する場合は、注意が表示されます。

公開 IP アドレス

インターフェースが公開ネットワークに接続する場合には、公開 IP アドレスが必要です。また、untrust-vr の L3 セキュリティゾーンが公開ネットワークに接続し、trust-vr のゾーンのインターフェースが Route モードの場合、trust-vr のゾーン内のすべてのインターフェースとホストのアドレスも、公開アドレスにする必要があります。公開 IP アドレスは、表 4 に示すように A、B、C の 3 つのクラスに分類されます。

表 4: 公開アドレスの範囲

アドレスクラス	アドレス範囲	除外アドレス範囲
A	0.0.0.0 – 127.255.255.255	10.0.0.0 – 10.255.255.255, 127.0.0.0 – 127.255.255.255
B	128.0.0.0 – 191.255.255.255	172.16.0.0 – 172.31.255.255
C	192.0.0.0 – 223.255.255.255	192.168.0.0 – 192.168.255.255

注 : D および E クラスのアドレスもあり、これらは特別な用途のために確保されています。

IP アドレスは 4 つのオクテットからなり、各オクテットは 8 ビット長です。クラス A アドレスでは、8 ビット目まではネットワーク ID を示し、残りの 24 ビットはホスト ID を示します (nnn.hhh.hhh.hhh)。クラス B アドレスでは、16 ビット目まではネットワーク ID を示し、残りの 16 ビットはホスト ID を示します (nnn.nnn.hhh.hhh)。クラス C アドレスでは、24 ビット目までがネットワーク ID を示し、最後の 8 ビットは、ホスト ID を示します (nnn.nnn.nnn.hhh)。

サブネットマスク (ネットマスク) を使用することで、ネットワークをさらに分割できます。ネットマスクは、ホスト ID の一部をマスクするもので、これによりマスクした部分はネットワーク ID のサブネットになります。たとえば、アドレス 10.2.3.4/24 の 24 ビットマスク は、最初の 8 ビット (1 番目のオクテット ー 010) がこの非公開クラス A アドレスのネットワーク部を示し、次の 16 ビット (2 番目と 3 番目のオクテット ー 002.003) がこのアドレスのサブネットワーク部を示し、最後の 8 ビット (4 番目のオクテットー 004) がアドレスのホスト部を示します。サブネットを使用してネットワークアドレスの大きな領域を小さな分割部分に狭めることで、IP データグラムの配信効率が大きく向上します。

注 : 24 ビットマスクのドット付き 10 進数は、255.255.255.0 です。

非公開 IP アドレス

インターフェースが非公開ネットワークに接続している場合、ローカルネットワーク管理者は任意のアドレスを割り当てることができます。しかし、RFC 1918、*Address Allocation for Private Internets* で定義されるように、非公開使用のために確保されたアドレス範囲 10.0.0.0/8、172.16.0.0 ～ 172.31.255.255、192.168.0.0/16 から 1 つのアドレスを使用することが一般的です。

untrust-vr の L3 セキュリティゾーンが公開ネットワークに接続し、trust-vr のゾーンにバインドされたインターフェースが NAT モードであれば、trust-vr のゾーン内のインターフェースおよびホストのアドレスはすべて、非公開アドレスにできます。

インターフェースのアドレスを設定する

この例では、ethernet0/5 に IP アドレス 210.1.1.1/24 を割り当てて、管理 IP アドレス 210.1.1.5 を与えます。(管理 IP アドレスは、セキュリティゾーンインターフェース IP アドレスと同じサブネット内にする必要があります。) 最後に、インターフェースを NAT モードに設定します。NAT モードは、すべての内部 IP アドレスを他のセキュリティゾーンにバインドされたデフォルトインターフェースに変換します。

注 : セキュリティゾーン内のデフォルトインターフェースとは、このセキュリティゾーンにバインドされた最初のインターフェースのことです。どのインターフェースがゾーンのデフォルトインターフェースになるのかを知るには、WebUI の Network > Zones の Default IF 列か、CLI で **get zone** コマンドを実行して出力される Default-If 列を参照してください。

WebUI

Network > Interfaces > Edit (ethernet0/5): 次のように入力してから **OK** をクリックします。

IP Address/Netmask: 210.1.1.1/24
Manage IP: 210.1.1.5

CLI

```
set interface ethernet0/5 ip 210.1.1.1/24
set interface ethernet0/5 manage-ip 210.1.1.5
save
```

インターフェース設定を変更する

物理インターフェース、サブインターフェース、冗長インターフェース、または仮想セキュリティインターフェース (VSI) を構成後は、次のいずれの設定内容も必要に応じて変更できます。

- IP アドレスとネットマスク
- 管理 IP アドレス
- (L3 ゾーンインターフェース) 管理およびネットワークサービス
- (サブインターフェース) サブインターフェース ID 番号と VLAN タグ番号
- (trust-vr の L3 セキュリティゾーンにバインドされたインターフェース) インターフェースモード : NAT または Route
- (物理インターフェース) トラフィック帯域幅の設定 (195 ページの「トラフィックシェーピング」を参照)
- (物理、冗長、統合インターフェース) 最大伝送単位 (MTU) サイズ
- (L3 インターフェース) 1 次サブネットと 2 次サブネットの間や 2 次サブネット間のトラフィックを含むトラフィックが、同じインターフェースを出入りするのを防ぎます (これは、CLI の **set interface** コマンドに **route-deny** オプションを使用して行います)。

一部のセキュリティデバイスの物理インターフェースでは、リンクの物理的状態を強制的に停止または稼動状態にできます。リンクの物理的状態を強制的に停止にすることで、インターフェースポートからのケーブルの切断をシミュレートできます。(これを行うには、CLI の **set interface** コマンドに **phy link-down** オプションを使用します。)

この例では、Trust ゾーンにバインドされたインターフェースである ethernet0/1 に変更を加えます。管理 IP アドレスを 10.1.1.2 から 10.1.1.12 に変更します。管理トラフィックのセキュリティを強化するために、管理サービスオプションも変更して SCS と SSL を使用可能にし、Telnet と WebUI を使用不可にします。

WebUI

Network > Interfaces > Edit (ethernet0/1): 次のように変更して **OK** をクリックします。

Manage IP: 10.1.1.12
Management Services: (**選択**) SSH、SSL; (**クリア**) Telnet、WebUI

CLI

```
set interface ethernet0/1 manage-ip 10.1.1.12
set interface ethernet0/1 manage ssh
set interface ethernet0/1 manage ssl
unset interface ethernet0/1 manage telnet
unset interface ethernet0/1 manage web
save
```

ルートシステムにサブインターフェースを作成する

ルートシステムまたは仮想システムの任意の物理インターフェース上にサブインターフェースを作成できます。サブインターフェースは、VLAN タグを使用して、このサブインターフェースへ向かうトラフィックと他のインターフェースへ向かうトラフィックを識別します。サブインターフェースは、必要な帯域幅を借りる物理インターフェースから始まっていますが、「親」インターフェースがバインドされているゾーンに限らず、どのゾーンにもサブインターフェースをバインドすることができます。その上、サブインターフェースの IP アドレスは、他のすべての物理インターフェースとサブインターフェースの IP アドレスとは異なるサブネットになければなりません。

注 : 冗長インターフェースと VSI 上にもサブインターフェースを構成することができます。冗長インターフェース上のサブインターフェースの構成を含む例については、**11**-96 ページの「Virtual System Failover」を参照してください。

この例では、ルートシステムの Trust ゾーンにサブインターフェースを作成します。Trust ゾーンにバインドされた ethernet0/1 でサブインターフェースを構成します。このサブインターフェースを、trust-vr にある “accounting” という名前のユーザー定義ゾーンにバインドします。それに、サブインターフェース ID 3、IP アドレス 10.2.1.1/24、VLAN タグ ID 3 を割り当てます。インターフェースモードは NAT です。

WebUI

Network > Interfaces > New Sub-IF: 次のように入力してから **OK** をクリックします。

Interface Name: ethernet0/1.3
Zone Name: accounting
IP Address/Netmask: 10.2.1.1/24
VLAN Tag: 3

CLI

```
set interface ethernet0/1.3 zone accounting
set interface ethernet0/1.3 ip 10.2.1.1/24 tag 3
save
```

サブインターフェースの削除

MIP (マップ IP) アドレス、VIP (仮想 IP) アドレス、または DIP (動的 IP) アドレスプールの上位となるサブインターフェースは、いきなり削除できません。これらの機能の上位となるサブインターフェースを削除する前に、まずこれらの機能を参照しているポリシーまたは IKE ゲートウェイを削除する必要があります。その後で、サブインターフェースの MIP、VIP、および DIP プールを削除します。

この例では、サブインターフェース ethernet0/1.1 を削除します。

WebUI

Network > Interfaces: ethernet0/1.1 の **Remove** をクリックします。

削除の確認を求めるメッセージが表示されます。

Yes をクリックしてサブインターフェースを削除します。

CLI

```
unset interface ethernet0/1.1
save
```

2 次 IP アドレスを作成する

各 ScreenOS インターフェースには、固有の *1 次* IP アドレスが 1 つずつあります。しかし、ときには 1 つのインターフェースに複数の IP アドレスが必要な場合もあります。たとえば、ある組織では新たに IP アドレス割当てを受けたものの、それを使用するために新たにルーターを設置したくないのかもしれません。またある組織では、たとえば LAN に 254 以上のホストが接続しており、ネットワークデバイス数がその組織のサブネットで対処できる数を超えているかもしれません。こうした問題を解決するために、Trust、DMZ、またはユーザー定義ゾーンのインターフェースに *2 次* IP アドレスを追加できます。

注 : Untrust ゾーンのインターフェースに複数の 2 次 IP アドレスを設定することはできません。

2 次アドレスには、それをどう導入できるかに影響を及ぼすいくつかの特性があります。それらは、次のようなものです。

- 2 つの 2 次 IP アドレスの間でサブネットアドレスが重複することはあり得ません。さらに、2 次 IP とセキュリティデバイス上のいずれの既存サブネットの間にも、サブネットアドレスの重複はありません。
- セキュリティデバイスを 2 次 IP アドレスによって管理する場合、このアドレスは常に 1 次 IP アドレスと同じ管理特性を持ちます。そのため、この 2 次 IP アドレスに別の管理構成を指定することはできません。
- ゲートウェイは 2 次 IP アドレスに構成できません。
- 2 次 IP アドレスを新規作成すると、セキュリティデバイスは、対応するルーティングテーブルのエントリを自動的に作成します。2 次 IP アドレスを削除すると、そのルーティングテーブルエントリを自動的に削除します。

2 つの 2 次 IP アドレスの間のルーティングを使用可能または使用不可にしても、ルーティングテーブルに変化はありません。たとえば、この両アドレス間のルーティングを使用不可にすると、セキュリティデバイスは、一方のインターフェースから他方のインターフェースへ向けられたパケットをドロップしますが、ルーティングテーブルに変化はありません。

この例では、IP アドレス 10.1.1.1/24 を持ち Trust ゾーンにバインドされた ethernet0/1 に、2 次 IP アドレスー 192.168.2.1/24 ーを設定します。

WebUI

Network > Interfaces > Edit (ethernet0/1) > Secondary IP: 次のように入力してから **Add** をクリックします。

IP Address/Netmask: 192.168.2.1/24

CLI

```
set interface ethernet0/1 ip 192.168.2.1/24 secondary
save
```

ループバックシステムインターフェース

インターフェースバックアップ機能により、1 次インターフェースに構成されたインターフェースからトラフィックを引き継ぐことができる、バックアップインターフェースを構成できます。どのタイプのインターフェースでも、そのプラットフォームでサポートされている他のタイプのインターフェースでバックアップできます。必要なのは、両方のインターフェースが Untrust ゾーンにあるということだけです。

1 次インターフェースがダウンしたり (ケーブルが外れている、または故障している) 、1 次インターフェースの宛先が到達不可能になったり、または 1 次インターフェースにバインドされているトンネルが非アクティブになった場合に、セキュリティデバイスがトラフィックを切り替えることができるように、バックアップインターフェースを設定します。1 次インターフェースを介した接続が回復したら、ScreenOS は、トラフィックをバックアップインターフェースから 1 次インターフェースに自動的に切り替えます。インターフェースバックアップ機能により、1 次インターフェースからバックアップインターフェースへ、またはバックアップインターフェースから 1 次インターフェースへ手動で切り替えることもできます。各 1 次インターフェースは、バックアップインターフェースを 1 つしか持つことができません。また、各バックアップインターフェースは、1 つしか 1 次インターフェースを持つことができません。

次のような状況が 1 次インターフェースで発生した場合に、セキュリティデバイスがバックアップインターフェースへ切り替えるように構成できます。

- ある IP アドレスが、インターフェースから到達不可能になった。
- インターフェースのある VPN トンネルが到達不可能になった。
- 事前に構成したルートが、インターフェースから到達不可能になった。

セキュリティデバイスが、これらの理由のいずれかでトラフィックをバックアップインターフェースに切り替えるためには、最初に、そのように 1 次インターフェースおよびバックアップインターフェースを構成する必要があります。また、1 次インターフェースおよびバックアップインターフェースについて、デフォルトルートを 1 つずつ構成する必要があります。バックアップインターフェース機能は、WebUI または CLI で構成できます。

バックアップインターフェースの構成

ScreenOS は、1 次インターフェースの活動を追跡または監視して、いつバックアップインターフェースに切り替えるかを判断します。以下のタイプのバックアップインターフェースを構成できます。

- IP トラッキング
- tunnel-if トラッキング
- ルートの監視

IP トラッキングバックアップインターフェースの構成

この例では、ScreenOS が、1 次インターフェース (ethernet0/0) 上の IP アドレス 10.1.1.1 を追跡し、このアドレスが到達不可能になったときにバックアップインターフェース (dialer1) に切り替えるように構成します。IP トラッキングの仕組みについては、**11**-50 ページの「IP トラッキングによるインターフェースフォールオーバー」を参照してください。

WebUI

1. **インターフェースの構成**
   Network > Interfaces > (ethernet0/0) Edit > Monitor > Add: 以下を入力して **Apply** をクリックします。

   Track IP: 10.1.1.1
   Weight: 200
   Interval: 2
   Threshold: 5

   Network > Interfaces > Backup: 以下を入力して **Apply** をクリックします。

   Primary interface (選択): ethernet0/0
   Backup Interface (選択): dialer1

2. **ルートの構成**
   Network > Routing > Destination > trust-tr New: 以下を入力して **Apply** をクリックします。

   IP Address/Netmask: 0.0.0.0/0
   interface (選択): ethernet0/0

   Network > Routing > Destination > trust-tr New: 以下を入力して **Apply** をクリックします。

   IP Address/Netmask: 0.0.0.0/0
   interface (選択): dialer1

CLI

1. **インターフェースの構成**
   set interface ethernet0/0 monitor track-ip
   set interface ethernet0/0 monitor track-ip threshold 100
   set interface ethernet0/0 monitor trackip ip 10.1.1.1 interval 2
   set interface ethernet0/0 monitor trackip ip 10.1.1.1 threshold 5
   set interface ethernet0/0 monitor trackip ip 10.1.1.1 weight 200
   set interface ethernet0/0 backup interface dialer1 type track-ip

2. **ルートの構成**
   set route 0.0.0.0/0 interface ether0/0
   set route 0.0.0.0/0 interface dialer1
   save

tunnel-if バックアップインターフェースの構成

この例では、ethernet0/0 で一方向の VPN トンネルを 1 対構成します。1 つは Router-1 上に、もう 1 つは Router-2 上に構成します。そして、Router-1 上のバックアップインターフェースに dialer1 を構成します。トンネルは、支社サイトの Trust ゾーンにあるホストと、企業サイトの Trust ゾーンにある SMTP サーバーを結びます。各サイトのゾーンは、trust-vr ルーティングドメインに存在します。

1 次 Untrust ゾーンインターフェース (ethernet0/0) を持つ両方のトンネルを外向きインターフェースに、バックアップ Untrust ゾーンインターフェース (dialer1) も持つバックアップ VPN トンネルを外向きインターフェースに構成します。セキュリティデバイスは、いつバックアップに切り替えるか判断するため、1 次 VPN トンネルを監視します。この判断は、バックアップウェイトを VPN 監視しきい値と比較して行います。しきい値は 100 に (**set vpnmonitor threshold 100**) 、バックアップウェイトは 200 に (**set vpn vpn backup-weight 200**) 設定します。1 次インターフェースが何かの理由で非アクティブになると、ScreenOS は、VPN 監視しきい値をバックアップウェイトと比較し、バックアップウェイトがしきい値より大きい場合、デバイスをバックアップに切り替えます。

VPN 監視の rekey 機能も有効にします。この機能では、フェールオーバーが発生したときでも、1 次インターフェースにある VPN トンネルの累計ウェイトが VPN 監視しきい値より大きくなった場合、セキュリティデバイスは、バックアップインターフェースから 1 次インターフェースにトラフィックを戻します。

支社サイトにあるセキュリティデバイスは、Untrust ゾーンインターフェースのアドレス、デフォルトゲートウェイ、DNS サーバーのアドレスを、2 つの異なる ISP から動的に取得します。ISP はそれぞれ別のプロトコルを使います。ISP-1 は DHCP を使って ethernet0/0 にアドレスを割り当て、ISP-2 は PPP で dialer1 にアドレスを割り当てます。企業サイトのセキュリティデバイスには、静的 IP アドレス (2.2.2.2) が割り当てられています。デフォルトゲートウェイの IP アドレスは 2.2.2.250 です。

VPN 監視の対象である宛先アドレスは、デフォルトである、リモートゲートウェイの IP アドレス (2.2.2.2) ではなく、サーバーのアドレス (10.2.2.10) になります。リモートゲートウェイの IP アドレスを使用して、それが到達不可能になると、1 次トンネルは必ずバックアップ : に切り替えます。

注 : この例は長いので、CLI による設定例のみを完全に示します。WebUI セクションでは、さまざまな設定要素が示されているページを開く手順を示します。各パラメータの設定値については、CLI コマンドを参照してください。

WebUI (Router-1)

1. **インターフェースの構成**
   Network > Interfaces > Edit (ethernet0/0)

   Network > Interfaces > Edit (bri1/0)

   Network > Interfaces > New Tunnel IF

2. **VPN の構成**
   VPNs > AutoKey IKE > New

   VPNs > AutoKey Advanced > Gateway > New

3. **非対称 VPN の構成**
   Network > Zones > Edit (Trust)

4. **バックアップインターフェースの構成**
   Network > Interfaces > Backup

5. **ルートの構成**
   Network > Routing > Destination > trust-vr

CLI (Router-1)

1. **インターフェースの構成**

```
set interface ethernet0/0 zone untrust
set interface ethernet0/0 dhcp client

set interface bri2/0 isdn switch-type etsi
set interface dialer1 zone untrust
set dialer pool name pool-1
set interface bri2/0 dialer-pool-member pool-1
set interface dialer1 dialer-pool pool-1

set ppp profile isdn-ppp
set ppp profile isdn-ppp auth type chap
set ppp profile isdn-ppp auth local-name juniper
set ppp profile isdn-ppp auth secret juniper
set ppp profile isdn-ppp passive
set ppp dialer1 ppp profile isdn-ppp

set interface tunnel.1 untrust
set interface tunnel.1 ip unnumbered interface bgroup0
set interface tunnel.2 untrust
set interface tunnel.2 ip unnumbered interface bgroup0
```

2. **VPN の構成**
   set ike gateway corp1 address 2.2.2.2 aggressive local-id ssg5ssg20-e0
   outgoing-interface ethernet0/0 preshare juniper1 sec-level basic
   set ike gateway corp1 address 2.2.2.2 aggressive local-id ssg5ssg20-dialer
   outgoing-interface dialer1 preshare juniper2 sec-level basic

   set vpn vpn1 gateway corp1 sec-level basic
   set vpn vpn1 bind interface tunnel.1
   set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 smtp
   set vpn vpn1 monitor source-interface bgroup0 destination-ip 10.2.2.10 rekey
   set vpn vpn1 backup-weight 200

   set vpn vpn2 gateway corp2 sec-level basic
   set vpn vpn2 bind interface tunnel.2
   set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 smtp
   set vpn vpn2 monitor source-interface bgroup0 destination-ip 10.2.2.10 rekey

3. **非対称 VPN の構成**
   set zone trust asymmetric-vpn

4. **バックアップインターフェースの構成**
   set interface ethernet0/0 backup interface dialer1 type tunnel-if
   set vpnmonitor threshold 100

5. **ルートの構成**
   set route 10.2.2.10/32 interface tunnel.1
   set route 10.2.2.10/32 interface tunnel.2
   set route 0.0.0.0/0 interface ethernet0/0
   save

WebUI (Router-2)

1. **インターフェースの構成**
   Network > Interfaces > Edit (bgroup1)

   Network > Interfaces > Edit (ethernet0/0)

   Network > Interfaces > New Tunnel IF

2. **アドレスの構成**
   Policy > Policy Elements > Addresses > List > New

3. **VPN の構成**
   VPNs > AutoKey IKE > New

   VPNs > AutoKey Advanced > Gateway > New

4. **非対称 VPN の構成**
   Network > Zones > Edit (Trust)

   Network > Interfaces > Edit (ethernet0/0)

5. **ルートの構成**
   Network > Routing > Destination > trust-vr

6. **ポリシーの構成**
   Policy > Policies (From Untrust to trust) > New

CLI (Router-2)

1. **インターフェースの構成**
   set interface bgroup zone trust
   set interface bgroup ip 10.2.2.1/24
   set interface bgroup nat
   set interface ethernet0/0 zone untrust
   set interface ethernet0/0 ip 2.2.2.2/24
   set interface tunnel.1 zone trust
   set interface tunnel.1 ip unnumbered interface bgroup0
   set interface tunnel.2 zone untrust
   set interface tunnel.2 ip unnumbered interface bgroup0

2. **アドレスの構成**
   set address untrust branch 10.1.1.0/24
   set address trust smtp-1 10.2.2.10/24
   set address trust http-1 10.2.2.15/32
   set group address trust servers add smtp-1
   set group service vpn-srv add smtp

3. **VPN の構成**
   set ike gateway branch1 dynamic ssg5ssg20-e0 aggressive outgoing-interface ethernet0/0 preshare juniper1 sec-level basic
   set ike gateway branch2 dynamic ssg5ssg20-dialer aggressive outgoing-interface ethernet0/0 preshare juniper2 sec-level basic

   set vpn vpn1 gateway branch1 sec-level basic
   set vpn vpn1 bind interface tunnel.1
   set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 smtp
   set vpn vpn2 gateway branch2 sec-level basic
   set vpn vpn2 bind interface tunnel.2
   set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 smtp

4. **非対称 VPN の構成**
   set zone trust asymmetric-vpn

5. **ルートの構成**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet 0/0 gateway 2.2.2.250

6. **ポリシーの構成**
   set policy from untrust to trust branch servers vpn-srv permit
   save

ルート監視バックアップインターフェースの構成

この例では、1 次インターフェース (ethernet0/0) に、ゲートウェイ 10.10.10.1 を使って、ネットワークセグメント 5.5.5.0/24 へのルートを構成します。また、dialer1 をバックアップインターフェースに構成し、同じネットワークセグメントへのルートを構成します。次に、1 次インターフェースのデフォルトルートを同じゲートウェイ (10.10.10.1) に、そして、dialer1 インターフェースのデフォルトルートを構成します。

WebUI

1. **インターフェースの構成**
   Network > Routing > Destination > trust-vr > New: 以下を入力して **Apply** をクリックします。

   IP Address/Netmask: 5.5.5.0/24
   Gateway: (選択)
   Interface: (選択) ethernet0/0
   Gateway IP Address: 10.10.10.1

   Network > Interfaces > Backup: 以下を入力して **Apply** をクリックします。

   1 次インターフェース : (選択) ethernet0/0
   バックアップインターフェース : (選択), dialup1
   Type: (選択) route vrouter: (選択) trust-vr
   IP Address/Netmask: 5.5.5.0/24

2. **Configure Route**
   Network > Routing > Source Interface (ethernet0/0) > New: 次のように入力してから **OK** をクリックします。

   Gateway: 10.10.10.1

   Network > Routing > Destination (trust-vr) > New: 次のように入力してから **OK** をクリックします。

   interface (選択): Null

CLI

```
set vrouter trust-vr route 5.5.5.0/24 interface ethernet0/0 gateway 10.10.10.1
set interface ethernet0/0 backup interface dialer1 type route vrouter trust-vr
    5.5.5.0/24
set route 0.0.0.0/0 interface ethernet0/0 gateway 10.10.10.1
set route 0.0.0.0/0 interface dialer1
save
```

ループバックインターフェース

ループバックインターフェースは、セキュリティデバイスの物理インターフェースをエミュレートする論理インターフェースです。ただし、物理インターフェースと異なり、ループバックインターフェースは、それが存在している NetScreen デバイスが作動している限り、常に稼動状態にあります。ループバックインターフェースには loopback.*id_num* の名前が付き、*id_num* は 1 以上の数字で、デバイスの固有のループバックインターフェースを表わします。物理インターフェースと同様、IP アドレスをループバックインターフェースに割り当ててセキュリティゾーンにバインドする必要があります。

注 : 指定できる最大の *id_num* 値は、プラットフォーム固有の値です。

ループバックインターフェースを定義すると、別のインターフェースをそのグループのメンバーとして定義できます。トラフィックがループバックインターフェースに到達するためには、そのループバックインターフェースのグループ内のいずれかのインターフェースを通って到着しなければなりません。物理インターフェース、サブインターフェース、トンネルインターフェース、冗長インターフェース、VSI など、あらゆるインターフェースタイプをループバックインターフェースグループのメンバーにできます。

ループバックインターフェースを作成したら、物理インターフェースと同様のいろいろな使い方ができます。

- 管理用ループバックインターフェースの設定
- ループバックインターフェースでの BGP の設定
- ループバックインターフェースでの VSI の設定
- ループバックインターフェースをソースインターフェースに設定

注 : ループバックインターフェースを HA ゾーンにバインドすることや、レイヤー 2 操作のために構成したり、冗長 / 統合インターフェースとして構成することはできません。
インターフェースとして構成することはできません。NTP, DNS, VIP, secondary IP, track IP, or WebAuth.

ループバックインターフェースを VPN 構成で出力インターフェースとして使用する場合、ループバックインターフェースは、出力物理インターフェースと同じゾーンにある必要があります。

MIP をループバックインターフェースに定義できます。定義すると MIP にインターフェースのグループがアクセス可能になり、これがループバックインターフェース特有の機能です。MIP を持つループバックインターフェースの使用については、**8**-71 ページの「MIP とループバックインターフェース」を参照してください。

セキュリティデバイスは、ループバックインターフェースの IP アドレスと、ループバックインターフェースに割り当てる管理 IP アドレスのどちらを使っても管理できます。

ループバックインターフェースを作成する

次の例では、ループバックインターフェース loopback.1 を作成し、Untrust ゾーンにバインドして、IP アドレス 1.1.1.27/24 を割り当てます。

WebUI

Network > Interfaces > New Loopback IF: 次のように入力してから **OK** をクリックします。

Interface Name: loopback.1
Zone: Untrust (選択)
IP Address/Netmask: 1.1.1.27/24

CLI

```
set interface loopback.1 zone untrust
set interface loopback.1 ip 1.1.1.27
save
```

注 : ループバックインターフェースは、別のゾーンに存在するネットワークやホストから直接アクセスできません。このインターフェースへのトラフィックの出入りを許可するポリシーを定義する必要があります。

管理用ループバックインターフェースの設定

次の例では、あらかじめ定義した loopback.1 インターフェースを、デバイスの管理インターフェースとして構成します。

WebUI

Network > Interfaces > loopback.1 > Edit: すべての管理オプションを選択して **OK** をクリックします。

CLI

```
set interface loopback.1 manage
save
```

ループバックインターフェースでの BGP の設定

ループバックインターフェースは、セキュリティデバイス上の BGP 動的ルーティングをサポートできます。次の例では、BGP を loopback.1 インターフェースで使用可能にします。

注 : BGP をループバックインターフェースで使用可能にするには、最初に BGP インスタンスを仮想ルーターに作成します (この仮想ルーター内でインターフェースをバインドするものとします)。Juniper Networks セキュリティデバイスでの BGP 構成については、*第 7 部: ルーティング* を参照してください。

WebUI

Network > Interfaces > loopback.1 > Edit: **Protocol BGP** を選択して、**OK** をクリックします。

CLI

```
set interface loopback.1 protocol bgp
save
```

ループバックインターフェースでの VSI の設定

NetScreen 冗長プロトコル (NSRP) のための仮想セキュリティインターフェース (VSI) をループバックインターフェースで構成できます。ループバックインターフェース上の VSI の物理的状態は、常に作動中となります。VSI はアクティブにすることも非アクティブにすることもでき、この VSI が属している VSD グループの状態によって決まります。

WebUI

Network > Interfaces > New VSI IF: 次のように入力してから **OK** をクリックします。

Interface Name: VSI Base: loopback.1
VSD Group: 1
IP Address/Netmask: 1.1.1.1/24

CLI

```
set interface loopback.1:1 ip 1.1.1.1/24
save
```

ループバックインターフェースをソースインターフェースに設定

ループバックインターフェースを、セキュリティデバイスから送出されるある特定のトラフィックのソースインターフェースとして使用できます。(ソースインターフェースをアプリケーションに定義すると、外部デバイスとやりとりするために指定されたソースインターフェースアドレスがアウトバウンドインターフェースアドレスの代わりに使用されます。次の例では、セキュリティデバイスが、syslog パケットを送信するためにあらかじめ定義した loopback.1 インターフェースを使用するように指定します。

WebUI

Configuration > Report Settings > Syslog: 以下を入力して **Apply** をクリックします。

Enable Syslog Messages: (選択)
Source interface: loopback.1 (選択)
Syslog Servers:
No.: 1 (選択)
IP/Hostname: 10.1.1.1
Traffic Log: (選択)
Event Log: (選択)

CLI

```
set syslog config 10.1.1.1 log all
set syslog src-interface loopback.1
set syslog enable
save
```

インターフェース状態の変化

インターフェースの状態は、表 5 に示す状態のいずれかです。

表 5: インターフェースの状態

状況	説明
物理的アップ	OSI (開放型システム間相互接続) モデルの Layer2 (Transparent モード) または Layer3 (Route モード) で動作する物理インターフェースに当てはまります。インターフェースが別のネットワークデバイスに配線されてそのデバイスとのリンクが確立されている場合は、そのインターフェースは物理的アップの状態です。
論理的アップ	物理インターフェースと論理インターフェースの両方 (サブインターフェース、冗長インターフェース、統合インターフェース) に該当します。インターフェースを通過するトラフィックが、ネットワーク上で指定したデバイス (トラックされる IP アドレス) に到達できる場合は、そのインターフェースは論理的アップの状態です。
物理的ダウン	インターフェースは、別のネットワークデバイスに配線されていない場合や配線されているがリンクを確立できない場合、物理的ダウンの状態です。また、次の CLI コマンドを使用してインターフェースを強制的に物理的ダウンの状態にすることもできます。**set interface *interface* phy link-down**.
論理的ダウン	インターフェースを通過するトラフィックが、ネットワーク上の (追跡された IP アドレスにある) 指定したデバイスに到達できない場合は、論理的ダウンの状態です。

インターフェースの物理状態は、論理状態に優先します。インターフェースが物理的アップの状態では、論理的アップと論理的ダウンのどちらにもなります。インターフェースが物理的ダウンの状態であると、論理状態は無関係になります。

インターフェースの状態がアップであると、そのインターフェースのすべてのルートがアクティブで使用可能になっています。インターフェースの状態がダウンである場合には、そのインターフェースが使用するすべてのルートが非アクティブになります。ただし、インターフェースの状態が物理的ダウンか論理的ダウンであるかによって、ダウン状態のインターフェースをトラフィックが通過できる可能性があります (76 ページの「ダウン状態のインターフェースとトラフィックフロー」を参照してください)。インターフェースの損失によるルートの損失を補うには、代替インターフェースを使用する代替ルートを構成します。

監視しているインターフェース状態を変えるアクションの設定方法によっては、監視される側のインターフェースがアップからダウンへ状態変化すると、監視する側のインターフェースがダウンからアップへ変化させることができます。こうした動作を構成するには、以下の CLI コマンドを使用します。

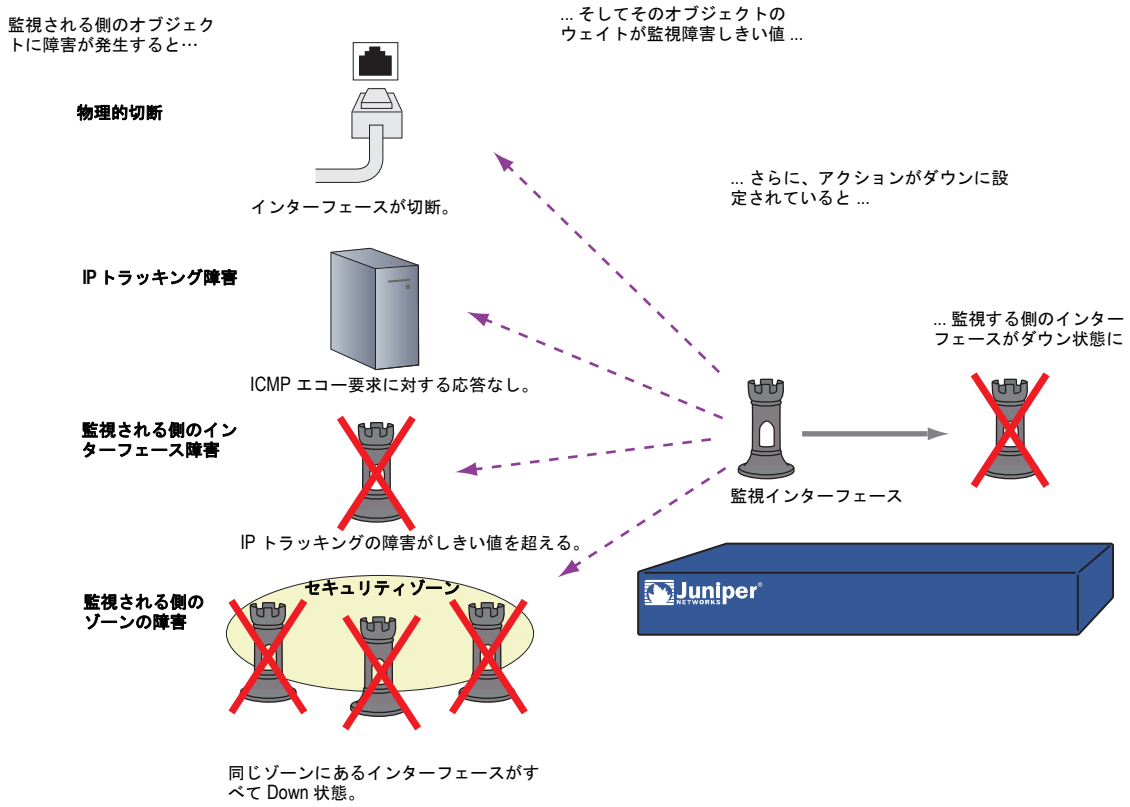
set interface *interface* monitor threshold *number* action up { logically | physically }

上記のコマンドを入力すると、セキュリティデバイスによって、監視する側のインターフェースが自動的にダウン状態に強制変更されます。監視される側のオブジェクト (トラック IP アドレス、インターフェース、ゾーン) に障害が発生した場合は、監視する側のインターフェースの状態は構成ごとに論理的アップまたは物理的アップのいずれかの状態になります。

インターフェースは、以下のイベントの 1 つ以上のオブジェクトを監視します。63 ページの図 21 を参照してください。各イベントは単体または複数で、監視する側のインターフェースの状態を Up から Down、および Down から Up へと変化させます。

- 物理的切断 / 再接続
- IP トラッキング障害 / 成功
- 監視される側のインターフェースの障害 / 成功
- 監視される側のセキュリティゾーンの障害 / 成功

図 21: インターフェース状態の監視



監視される側のオブジェクトに障害が発生してから成功する (インターフェースが再接続するか IP トラッキング再試行が成功する) と、監視する側のインターフェースが Up 状態に復帰します。監視される側のオブジェクトが成功してから監視する側のインターフェースが再アクティブ化されるまでに、約 1 秒の遅延があります。

上記の各イベントを以下のセクションで説明します。

物理的接続の監視

セキュリティデバイス上にある物理インターフェースはすべて、ネットワークデバイスと自分の物理的接続の状態を監視します。インターフェースが別のネットワークデバイスとのリンク接続が確立されている場合は、そのインターフェースは、物理的アップの状態で、そのインターフェースが使用するすべてのルートがアクティブになっています。

インターフェースの状態は、**get interface** コマンドから出力される State 列、および WebUI の Network > Interfaces にある Link 列に表示されます。アップまたはダウンです。

ルートの状態は、**get route id** *number* コマンドの status フィールド、および WebUI の Network > Routing > Routing Entries に表示されます。アスタリスク (*) があるルートがアクティブです。アスタリスク (*) がないルートは非アクティブです。

IP アドレスのトラッキング

セキュリティデバイスは、指定した IP アドレスをインターフェースから追跡することによって、1 つまたは複数の IP アドレスに到達できなくなった場合に、物理リンクがアクティブであっても、そのインターフェースに関連するすべてのルートを非アクティブにすることができます。非アクティブにされたルートは、セキュリティデバイスがそれらの IP アドレスに到達できるようになると、再びアクティブになります。

注 : このアクションは、一部の ScreenOS アプライアンスで、IP トラッキングが構成されているインターフェースと同じゾーンにバインドされたバックアップインターフェースへのフェールオーバーも起こします (**11**-50 ページの「IP トラッキングによるインターフェースフォールオーバー」を参照)。

ScreenOS は、レイヤー 3 パスモニタリング、または NSRP に使用されるものに類似した *IP トラッキング*を使用して、指定した IP アドレスに対するインターフェースからの到達可能性を監視します。例えば、インターフェースが直接ルーターに接続する場合、インターフェースの次のホップアドレスをトラックして、そのルーターがまだ到達可能かを判断することができます。インターフェースで IP トラッキングを構成すると、セキュリティデバイスはインターフェースにおいて、最大 4 つのターゲット IP アドレスにユーザー定義間隔で ping 要求を送信します。セキュリティデバイスは、これらのターゲットを監視し、応答を受信するかどうかを判断します。指定された回数試行してもターゲットから応答がない場合、その IP アドレスは宛先不明とみなされます。1 つまたは複数のターゲットから応答を引き出せない場合、セキュリティデバイスは、そのインターフェースに関連付けられているルートを非アクティブにします。同じ宛先への別のルートが利用可能な場合、セキュリティデバイスは、新しいルートを使用するようにトラフィックを転送します。

管理 IP アドレスを構成した以下のレイヤー 3 インターフェースで IP トラッキングを定義できます。

- セキュリティゾーンにバインドされた物理インターフェース (HA と MGT の機能ゾーン以外)

注 : インターフェースの動作モードには、レイヤー 2 (透過モード) またはレイヤー 3 (ルートモード) があります。

- サブインターフェース
- 冗長インターフェース
- 統合インターフェース

注 : インターフェースは冗長インターフェースまたは統合インターフェースの場合がありますが、冗長インターフェースや統合インターフェースのメンバーであることはできません。

仮想システムをサポートするデバイスでは、IP トラッキングを設定したインターフェースはルートシステムまたは仮想システム (vsys) に属すことができます。ただし、共有インターフェースでの IP トラッキングを設定する場合、ルートレベルでの設定しかできません。

注 : vsys からインターフェースモニタリングを設定することで、vsys に属するインターフェースから共有インターフェースを監視することができます。ただし、vsys 内からは共有インターフェースからのインターフェースモニタリングの設定ができません。詳細については、69 ページの「インターフェース監視」を参照してください。

それぞれのインターフェースについて、セキュリティデバイスがトラックする IP アドレスを最大 4 つ構成できます。単一のデバイスで、最大 64 のトラッキング IP アドレスを構成できます。この総数には、インターフェースベースの IP トラッキングまたは NSRP ベースの IP トラッキング、そしてルートレベルまたは vsys レベルでのトラック IP アドレスがすべて含まれます。

トラックされる IP アドレスは、インターフェースと同じサブネットワークにある必要はありません。トラックされるそれぞれの IP アドレスについて、以下を指定できます。

- 指定した IP アドレスに ping が送信される間隔 (秒単位)。
- ping が連続して失敗し IP アドレスへの接続が障害とみなされるまでの ping 試行回数。
- 障害がある IP 接続のウェイト (障害があるすべての IP 接続のウェイト合計が指定したしきい値を越えた時点で、インターフェースに関連付けられているルートは非アクティブになります)。

また、PPPoE クライアントまたは DHCP クライアントであるインターフェースのデフォルトのゲートウェイをトラッキングするように、セキュリティデバイスを構成することもできます。その場合、「動的」オプションを使用します。(CLI) **set interface** *interface* **monitor dynamic**、または (WebUI) Network > Interfaces > Edit (DHCP または PPPoE client interface) > Monitor > Track IP > Add から **Dynamic** を選択します。

注： セキュリティデバイスがトラックする IP アドレスを構成する場合には、ルーティングテーブルにその IP アドレスのホストルートは追加されません。

IP アドレスのトラッキングを構成する場合のしきい値には 2 つのタイプがあります。

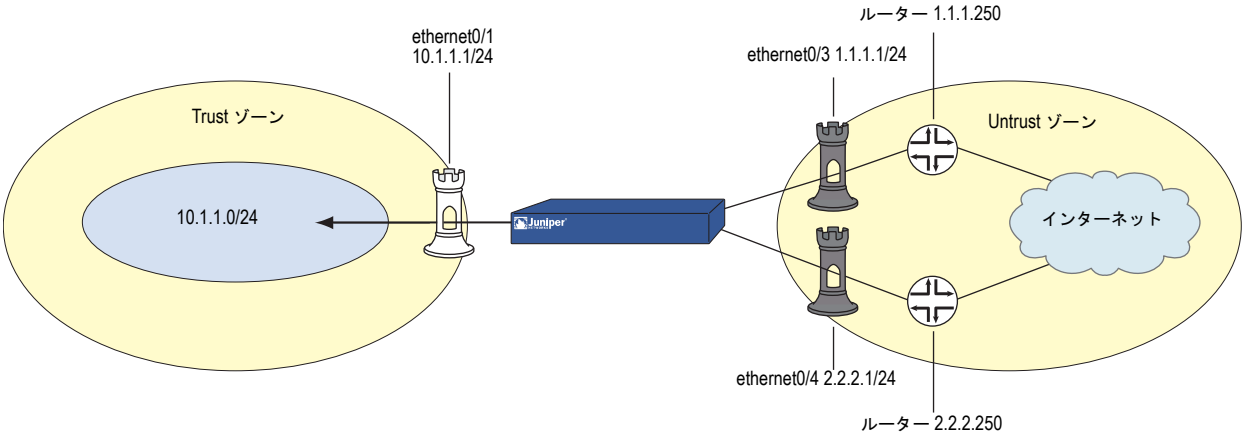
- トラックされる特定の IP アドレスの障害しきい値 - IP アドレスの追跡中に障害を起こす特定の IP アドレスから、ping 応答の引き出しに連続して失敗する回数。しきい値を超えていない場合は、そのアドレスとの接続性が良好なレベルであることを示し、しきい値を超えている場合は、不良なレベルであることを示します。各 IP アドレスについて、このしきい値を 1 から 200 までの任意の値で設定します。デフォルト値は 3 です。

- インターフェースの IP トラッキングの障害しきい値 - インターフェースで IP アドレスを追跡する際に、そのインターフェースに関連付けられているルートが非アクティブになる累積未遂のウェイト合計。このしきい値は 1 から 255 までの任意の値に設定できます。デフォルト値は 1 で、構成されたトラックされる IP アドレスの追跡に失敗すると、インターフェースに関連付けられているルートは非アクティブになります。

トラックされる IP アドレスに「*ウェイト*」または値を適用することによって、そのアドレスへの接続性の重要度を、他のトラックされる IP アドレスへの追跡に関連して調整することができます。相対的に重要度の高いアドレスには比較的大きなウェイトを割り当て、相対的に重要度の低いアドレスには比較的小さなウェイトを割り当てることができます。割り当てられたウェイトは、トラックされる特定の IP アドレスへの障害しきい値に達したときのみ有効になります。たとえば、あるインターフェースの IP トラッキング障害しきい値が 3 である場合、ウェイト 3 が割り当てられたトラックされる単一の IP アドレスに障害が起きるとそのインターフェースの IP トラッキング障害しきい値に達するため、インターフェースに関連付けられているルートは非アクティブになります。ウェイト 1 が割り当てられたトラックされる単一の IP アドレスに障害が起きた場合は、インターフェースの IP トラッキング障害しきい値には達しないため、そのインターフェースに関連付けられているルートはアクティブなままになります。

この例では、インターフェース ethernet0/1 は Trust ゾーンにバインドされ、10.1.1.1/24 というネットワークが割り当てられます。インターフェース ethernet0/3 と ethernet0/4 は Untrust ゾーンにバインドされます。ethernet0/3 インターフェースはネットワークアドレス 1.1.1.1/24 に割り当てられ、1.1.1.250 のルーターに接続されます。ethernet0/4 インターフェースはネットワークアドレス 2.2.2.1/24 が割り当てられ、2.2.2.250 のルーターに接続されます。図 22 を参照してください。

図 22: インターフェース IP トラッキング



デフォルトでは 2 つのルートが構成されます。一方は、ゲートウェイにルーターアドレス 1.1.1.250 を使用して ethernet0/3 をアウトバウンドインターフェースとして使用します。他方は、ゲートウェイにルーターアドレス 2.2.2.250 を使用して ethernet0/4 をアウトバウンドインターフェースとして使用し、数値 10 で構成されます。ethernet0/3 を使用するデフォルトのルートは、数値が小さいため優先ルートになります (静的ルートのデフォルトの数値は 1 です)。**get route** コマンドからの次の出力は、trust-vr のアクティブな 4 つのルートを示します (アクティブなルートはアスタリスク (*) で示されています)。ethernet0/3 経由のデフォルトルートはアクティブであり、ethernet0/4 経由のデフォルトルートは優先度が低いため非アクティブです。

図 23: get route コマンドの出力

```
device-> get route
untrust-vr (0 entries)
---------------------------------------------------------------------------
C - Connected, S - Static, A - Auto-Exported, I - Imported, R - RIP
iB - IBGP, eB - EBGP, O - OSPF, E1 - OSPF external type 1
E2 - OSPF external type 2
trust-vr (4 entries)
---------------------------------------------------------------------------
    ID   IP-Prefix    Interface Gateway     P     Pref  Mtr   Vsys
---------------------------------------------------------------------------
*   4    0.0.0.0/0    eth0/3    1.1.1.250   S     20    1     Root
*   2    1.1.1.0/24   eth0/3    0.0.0.0     C     0     0     Root
    3    0.0.0.0/0    eth0/4    2.2.2.250   S     20    10    Root
*   6    2.2.2.0/24   eth0/4    0.0.0.0     C     0     1     Root
*   5    10.1.1.0/24  eth0/1    0.0.0.0     C     20    1     Root
```

ethernet0/3 経由のルートを使用できなくなった場合は、ethernet0/4 経由のデフォルトルートがアクティブになります。ethernet0/3 インターフェースで IP トラッキングを使用可能にし、ルーターアドレス 1.1.1.250 を監視するように構成します。IP トラッキングが 1.1.1.250 に到達できない場合、ethernet0/3 インターフェースに関連付けられているすべてのルーターが、セキュリティデバイスで非アクティブになります。その結果、ethernet0/4 経由のデフォルトルートがアクティブになります。IP トラッキングが 1.1.1.250 に到達できるようになると、ethernet0/3　経由のデフォルトルートがアクティブになり、それと同時に、ethernet0/4 経由のデフォルトルートは ethernet0/3 経由のデフォルトルートよりも優先度が低いため非アクティブになります。

次のように、インターフェース障害しきい値が 5 である IP トラッキングを使用可能にし、ウェイト 10 が割り当てられたルーター IP アドレス 1.1.1.250 を監視するように ethernet0/3 インターフェースの IP トラッキングを構成します。

WebUI

Network > Interfaces > Edit (for ethernet0/3) > Monitor: 以下を入力して **Apply** をクリックします。

Enable Track IP: (選択)
Threshold: 5
> Monitor Track IP ADD: 次のように入力してから **Add** をクリックします。
Static: (選択)
Track IP: 1.1.1.250
Weight: 10

CLI

```
set interface ethernet0/3 monitor track-ip ip 1.1.1.250 weight 10
set interface ethernet0/3 monitor track-ip threshold 5
set interface ethernet0/3 monitor track-ip
save
```

この例では、ターゲットアドレスの障害しきい値はデフォルト値の 3 に設定されています。つまり、ターゲットが連続して 3 回 ping に応答しなかった場合、インターフェースの IP トラッキングの障害しきい値にウェイト 10 が適用されます。インターフェースの IP トラッキングの障害しきい値が 5 であるため、インターフェースに関連付けられているルートは、ウェイト 10 が適用されると、セキュリティデバイスで非アクティブになります。

図 24 のように CLI コマンド **get interface ethernet0/3 track-ip** を発行すると、インターフェースの IP トラッキングの状態を確認できます。

図 24: get interface コマンドの出力

```
device-> get interface ethernet0/3 track-ip
ip address  interval  threshold  wei   gateway  fail-count success-rate
1.1.1.250   1         1          10    0.0.0.0  343        46%
threshold: 5, failed: 1 ip(s) failed, weighted sum = 10
```

get route コマンドは、ethernet0/4 経由のデフォルトルートがアクティブになり、ethernet0/3 経由のすべてのルートがアクティブではなくなったことを示します。

図 25: アクティブ化されたインターフェースでの get route コマンドの出力

```
device-> get route
untrust-vr (0 entries)
-------------------------------------------------------------------------
C - Connected, S - Static, A - Auto-Exported, I - Imported, R - RIP
iB - IBGP, eB - EBGP, O - OSPF, E1 - OSPF external type 1
E2 - OSPF external type 2
trust-vr (4 entries)
-------------------------------------------------------------------------
   ID   IP-Prefix    Interface Gateway    P   Pref  Mtr   Vsys
-------------------------------------------------------------------------
    4   0.0.0.0/0    eth0/3    1.1.1.250  S   20    1     Root
    2   1.1.1.0/24   eth0/3    0.0.0.0    C   0     0     Root
*   3   0.0.0.0/0    eth0/4    2.2.2.250  S   20    10    Root
*   6   2.2.2.0/24   eth0/4    0.0.0.0    C   0     1     Root
*   5   10.1.1.0/24  eth0/1    0.0.0.0    C   20    1     Root
```

ethernet0/3 経由のルートはアクティブではなくなりましたが、IP トラッキングには ethernet0/3 に関連付けられているルートが使用され、ターゲット IP アドレスに ping 要求が継続して送信されることに注意してください。IP トラッキングが 1.1.1.250 に到達できるようになると、ethernet0/3 経由のデフォルトルートがセキュリティデバイスで再びアクティブになります。同時に、ethernet0/4 経由のデフォルトルートは、ethernet0/3 経由のデフォルトルートよりも優先度が低いため非アクティブになります。

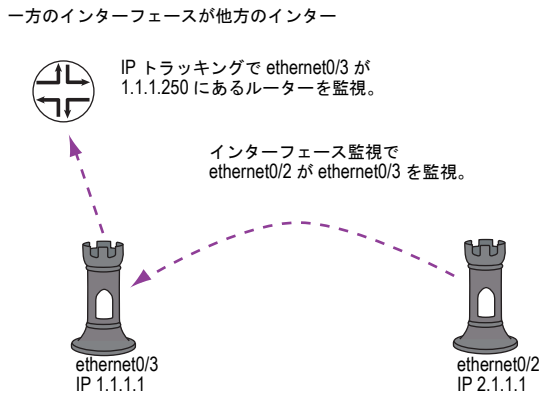
インターフェース監視

セキュリティデバイスは、インターフェースの物理状態と論理状態を監視してから、確認された変更に基づいてアクションを実行します。図 26 を参照してください。たとえば、表 6 で示すように、監視される側のインターフェースがアップからダウンに変化した場合には、以下の状況が発生する可能性があります。

表 6: 監視されるインターフェース

条件	結果
インターフェースの物理状態がアップからダウンに変化	この状態変化によって、ダウン状態になったインターフェースを監視している別のインターフェースもダウン状態になる可能性があります。この別のインターフェースを物理的ダウンにするか論理的ダウンにするかを指定できます。 いずれかのインターフェースが物理的ダウンの状態に変化する、または両方のインターフェースの合計ウェイトで物理的ダウンの状態になると、NSRP フェールオーバーが発生する可能性があります。NSRP デバイスや VSD グループのフェールオーバーは、インターフェースの物理状態が変化したときのみ発生します。
IP トラッキング障害によって、インターフェースの論理状態がアップからダウンに変化	この状態変化によって、ダウン状態になったインターフェースを監視している別のインターフェースもダウン状態になる可能性があります。最初のインターフェースが論理的ダウンになっても、別のインターフェースの状態を物理的ダウンにするか論理的ダウンにするかを指定できます。

図 26: Ethernet0/1 および Ethernet0/2 のインターフェース監視



インターフェースモニタリングを設定するには、次のいずれかを実行します。

WebUI

Network > Interfaces > Edit (監視するインターフェース) > Monitor > Edit Interface: 以下を入力して **Apply** をクリックします。

Interface Name: 監視するインターフェースを選択します。
Weight: 1 から 255 のウェイトを入力します。

CLI

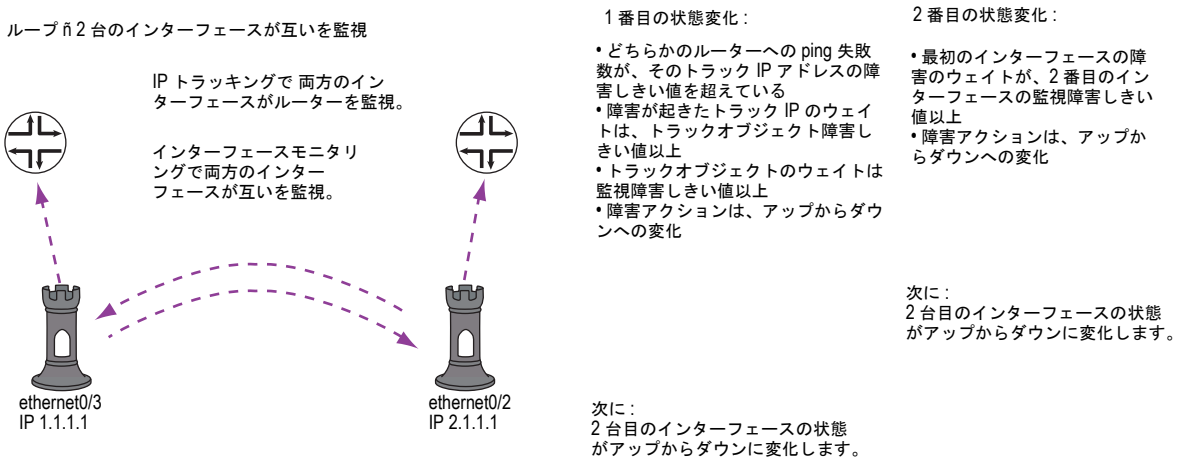
set interface *interface1* monitor interface *interface2* [weight *number*]
save

ウェイトを設定しない場合には、デフォルト値 255 が適用されます。

2 台のインターフェースが互いを監視する場合は、ループが形成されます。その場合、どちらかのインターフェースの状態が変化すると、他方のインターフェースの状態も変化します。71 ページの図 27 を参照してください。

注 : インターフェースは 同時に 1 つのループにしか入ることができません。1 台のインターフェースが複数のループに属する構成は、サポートしません。

図 27: ループ監視



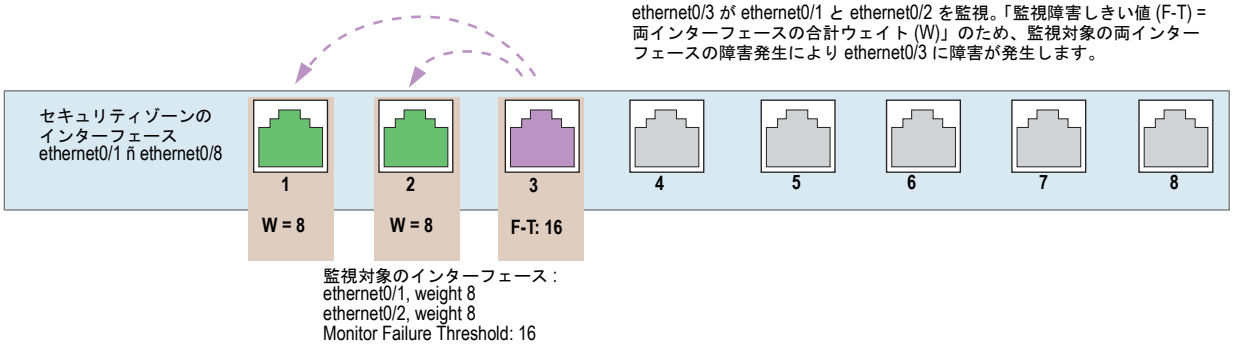
2 つのインターフェースの監視

この例では、ethernet0/3 を設定して 2 台のインターフェース ethernet0/1 と ethernet0/2 を監視します。監視する各インターフェースの重み (8 + 8) が監視障害しきい値と同じ (16) であるため、ethernet0/1 と ethernet0/2 の両方に障害が発生する (2 台の状態がアップからダウンへ変化する) と、同時に ethernet0/3 に障害が発生 (状態がアップからダウンへ変化) します。図 28 を参照してください。

注 : この例では、インターフェース ethernet0/1 と ethernet0/2 上での IP トラッキング構成は省かれます (64 ページの「IP アドレスのトラッキング」を参照)。IP トラッキングがない場合、ethernet0/1 と ethernet0/2 は、他のネットワークデバイスから物理的に切断されるか、他のネットワークデバイスとのリンクを維持できない場合にのみ障害が発生する可能性があります。

監視障害しきい値を 8 に設定する、または監視障害しきい値は 16 のままで監視する各インターフェースのウェイトを 16 に設定すると、ethernet0/1 または ethernet0/2 のいずれかに障害が発生すると ethernet0/3 に障害が発生する可能性があります。

図 28: 2 ループインターフェースの監視



WebUI

Network > Interfaces > Edit (for ethernet0/3) > Monitor > Edit Interface: 以下を入力して **Apply** をクリックします。

ethernet0/1: (**選択**), Weight: 8
ethernet0/2: (**選択**), Weight: 8

Network > Interfaces > Edit (ethernet0/3) > Monitor: Monitor Threshold フィールドに **16** と入力して、**Apply** をクリックします。

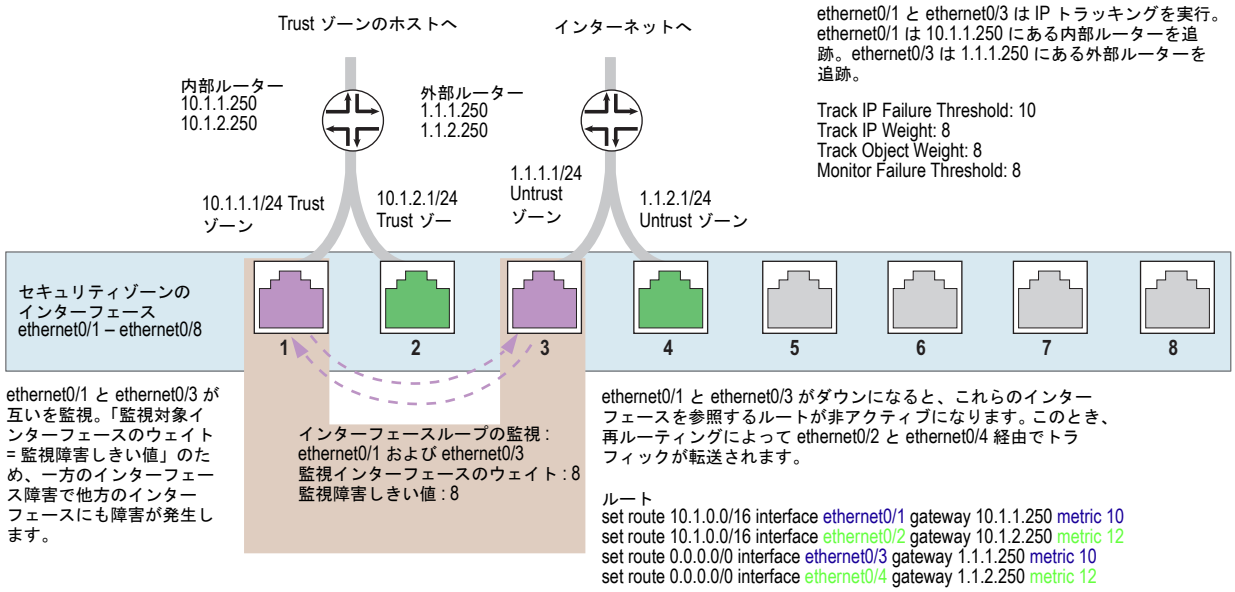
CLI

```
set interface ethernet0/3 monitor interface ethernet0/1 weight 8
set interface ethernet0/3 monitor interface ethernet0/2 weight 8
set interface ethernet0/3 monitor threshold 16
save
```

インターフェースループの監視

この例では最初に、2 台のインターフェース ethernet0/1 および ethernet0/3 の IP トラッキングを構成する必要があります。次に、2 台のインターフェースが互いを監視するように構成すると、一方のインターフェースが他方のインターフェースの状態を変えた場合に、後者のインターフェースも前者のインターフェースの状態を変えます。最後に、ルートのセットを 2 つ定義します。最初のセットでは ethernet0/1 と ethernet0/3 を経由してトラフックを転送します。第 2 のセットでも宛先アドレスは同じですが、ルートが下位のランクのメトリックであり、ルートには最初のセットとは異なる egress インターフェース (ethernet0/2 と ethernet0/4) および異なるゲートウェイが使用されます。この構成によって、最初のインターフェースセットに障害が発生すると、すべてのトラフィックが第 2 のセット経由に再ルーティングされます。すべてのゾーンは、trust-vr ルーティングドメインにあります。

図 29: 4 つのインターフェースのループの監視



WebUI

1. **IP トラッキング**

   Network > Interfaces > Edit (ethernet0/1) > Monitor: 以下を入力して **Apply** をクリックします。

   Enable Track IP: (選択)
   Monitor Threshold: 8
   Track IP Option: Threshold: 8
   Weight: 8

注 : インターフェースの状態を論理的または物理的ダウン (またはアップ) のいずれかに制御するには、**set interface** *interface* **monitor threshold** *number* **action { down | up } { logically | physically }** の CLI コマンドを使用する必要があります。物理的アップと物理的ダウンの状態は、Null ゾーン以外の任意のセキュリティゾーンにバインドされた物理インターフェースのみがなります。

> Monitor Track IP ADD: 次のように入力してから **Add** をクリックします。

Static: (選択)
Track IP: 10.1.1.250
Weight: 8
Interval: 3 Seconds
Threshold: 10

Network > Interfaces > Edit (ethernet0/3) > Monitor: 以下を入力して **Apply** をクリックします。

Enable Track IP: (選択)
Monitor Threshold: 8
Track IP Option: Threshold: 8
Weight: 8

> Monitor Track IP ADD: 次のように入力してから **Add** をクリックします。

Static: (選択)
Track IP: 1.1.1.250
Weight: 8
Interval: 3 Seconds
Threshold: 10

2. **インターフェースモニタリング**
Network > Interfaces > Edit (ethernet0/1) > Monitor > Edit Interface: 以下を入力して **Apply** をクリックします。

ethernet0/3: (選択), Weight: 8

Network > Interfaces > Edit (ethernet0/3) > Monitor > Edit Interface: 以下を入力して **Apply** をクリックします。

ethernet0/1: (選択), Weight: 8

3. **ルート**
Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.0.0/16
Gateway: (選択)
Interface: ethernet0/1
Gateway IP Address: 10.1.1.250
Metric: 10

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.0.0/16
Gateway: (選択)
Interface: ethernet0/2
Gateway IP Address: 10.1.2.250
Metric: 12

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet0/3
Gateway IP Address: 1.1.1.250
Metric: 10

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet0/4
Gateway IP Address: 1.1.2.250
Metric: 12

CLI

1. **IP トラッキング**
   set interface ethernet0/1 track-ip ip 10.1.1.250 weight 8
   set interface ethernet0/1 track-ip threshold 8
   set interface ethernet0/1 track-ip weight 8
   set interface ethernet0/1 track-ip
   set interface ethernet0/3 track-ip ip 1.1.1.250 weight 8
   set interface ethernet0/3 track-ip threshold 8
   set interface ethernet0/3 track-ip weight 8
   set interface ethernet0/3 track-ip

2. **インターフェースモニタリング**
   set interface ethernet0/1 monitor interface ethernet0/3 weight 8
   set interface ethernet0/1 monitor threshold 8 action down physically
   set interface ethernet0/3 monitor interface ethernet0/1 weight 8
   set interface ethernet0/3 monitor threshold 8 action down physically

3. **ルート**
   set vrouter trust-vr route 10.1.0.0/16 interface ethernet0/1 gateway 10.1.1.250 metric 10
   set vrouter trust-vr route 10.1.0.0/16 interface ethernet0/2 gateway 10.1.2.250 metric 12
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/3 gateway 1.1.1.250 metric 10
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/4 gateway 1.1.2.250 metric 12
   save

セキュリティゾーンの監視

インターフェースは、個々のインターフェースの監視に加えて、自身以外の任意のセキュリティゾーンにあるすべてのインターフェースを監視することができます。セキュリティゾーン全体に障害があるとされるには、そのゾーンにバインドされているすべてのインターフェースに障害が発生している必要があります。監視対象のゾーンにバインドされているインターフェースが 1 つでもアップの状態であると、そのゾーン全体がアップ状態であると見なされます。

インターフェースを構成してセキュリティゾーンを監視するには、以下のいずれかを行います。

WebUI

Network > Interfaces > Edit (監視するインターフェース) > Monitor > Edit Zone: 以下を入力して **Apply** をクリックします。

Zone Name: 監視するインターフェースを選択します。
Weight: 1 から 255 のウェイトを入力します。

CLI

set interface *interface* monitor zone *zone* [weight *number*]

ウェイトを設定しない場合には、デフォルト値 255 が適用されます。

ダウン状態のインターフェースとトラフィックフロー

インターフェースで IP アドレスを構成すると、セキュリティデバイスでは、特定の IP アドレスが最初のインターフェース経由で宛先不明になった場合、別のインターフェース経由で出力トラフィックを再ルーティングできます。ただし、セキュリティデバイスが IP トラッキングの障害によりインターフェースに関連付けられているルートを非アクティブにした場合でも、インターフェースは、物理的にはアクティブな状態のままでトラフィックを送受信できます。たとえば、セキュリティデバイスは、IP トラッキングが失敗した元のインターフェースで受信される可能性がある、既存のセッションの受信トラフィックを継続して処理します。また、セキュリティデバイスは、そのまま元のインターフェースを使用してターゲットに ping 要求を送信し、ターゲット IP アドレスが再び到達可能になるかどうかを判断します。このような状況でも、IP トラッキングが失敗してセキュリティデバイスによってルートが非アクティブになったインターフェースをトラフィックは通過します。

そのようなインターフェースでのセキュリティデバイスのセッショントラフィック処理方法は、次のように異なります。

- IP トラッキング機能を構成したインターフェースが、セッションの出口インターフェースとして機能する場合、セッション応答がそのインターフェースに到着し続けることもあり、セキュリティデバイスはそれらを処理します。

- IP トラッキングを構成したインターフェースがセッションの入口インターフェースとして機能する場合、**set arp always-on-dest** コマンドを適用すると、セキュリティデバイスはセッション応答を別のインターフェースに再ルーティングします。このコマンドを設定しない場合、セキュリティデバイスは、IP トラッキングが失敗したインターフェースを使用するルートを非アクティブにしたにもかかわらず、そのインターフェースからセッション応答を転送します。(デフォルトでは、このコマンドは設定されていません。)

  デフォルトでは、セキュリティデバイスは、新しいセッションの最初のパケットを受信すると、セッションのイニシエータの MAC アドレスをキャッシュします。CLI コマンド **set arp always-on-dest** を入力すると、セキュリティデバイスはセッションイニシエータの MAC アドレスをキャッシュしません。その代わり、セキュリティデバイスは、最初のパケットへの応答を処理する際に、ARP ルックアップを実行します。イニシエータの MAC アドレスが ARP テーブルに存在すると、セキュリティデバイスはそれを使用します。MAC アドレスが ARP テーブルに存在しない場合、セキュリティデバイスは宛先 MAC アドレスの ARP 要求を送信して、受信した MAC アドレスを ARP テーブルに追加します。セキュリティデバイスは、ルートが変更されるたびに ARP ルックアップを実行します。

「出口インターフェースでの障害」では、IP トラッキングが出口インターフェースと入口インターフェースで失敗した場合の異なるシナリオ、また後者の場合に **set arp always-on-dest** コマンドを使用するとどうなるかを説明します。

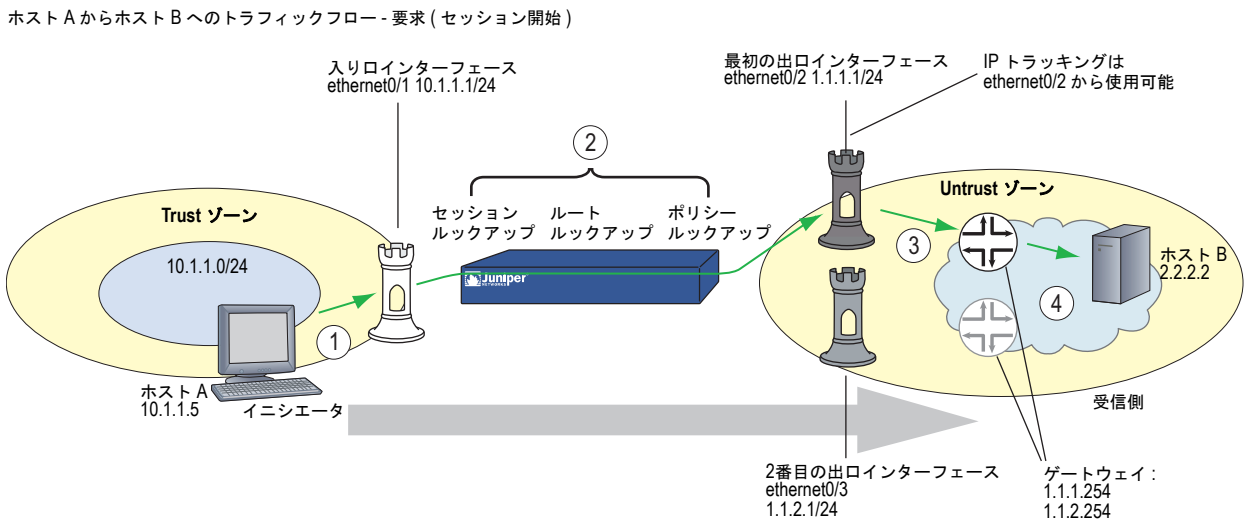
注 : 「出口インターフェースでの障害」では、IP トラッキングのルーティング変更方法、およびこれらの変更が、すべての Juniper Networks セキュリティデバイスを通過するパケットフローに与える影響を説明します。

出口インターフェースでの障害

次のシナリオでは、ホスト A からホスト B へのセッションの出口インターフェースである ethernet0/2 で IP トラッキングを構成します。図 30 に示すように、ホスト A がホスト B にパケットを送信してセッションを開始します。

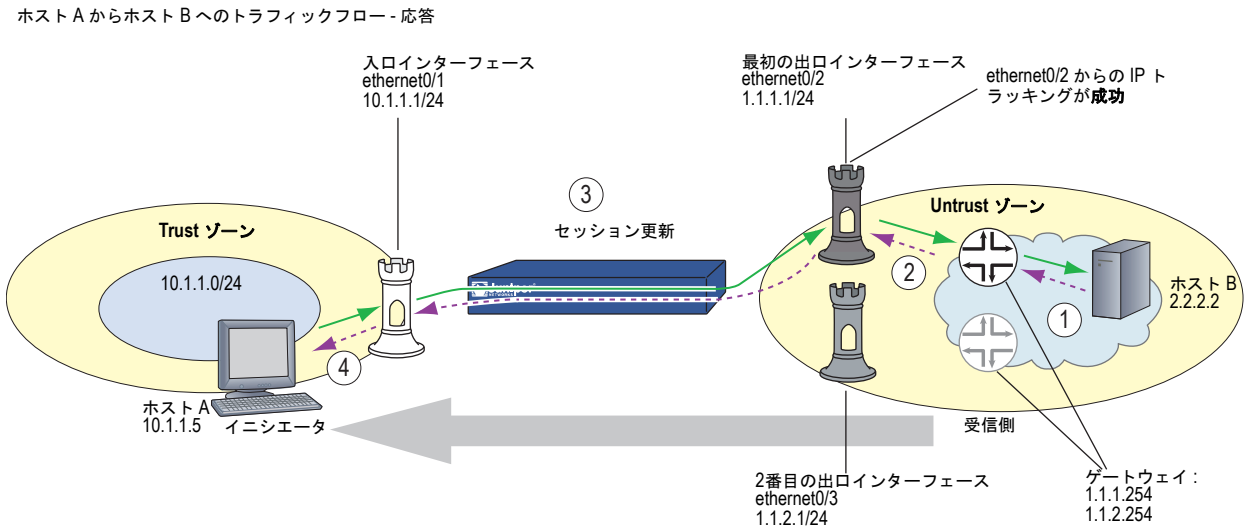
注 : まず、ホスト B へのルートを 2 つ作成し、両方の出口インターフェースを同じゾーンにおいて、再ルーティングの前後で同じポリシーがトラフィックに適用されるようにします。

図 30: ホスト A とホスト B の IP トラッキング



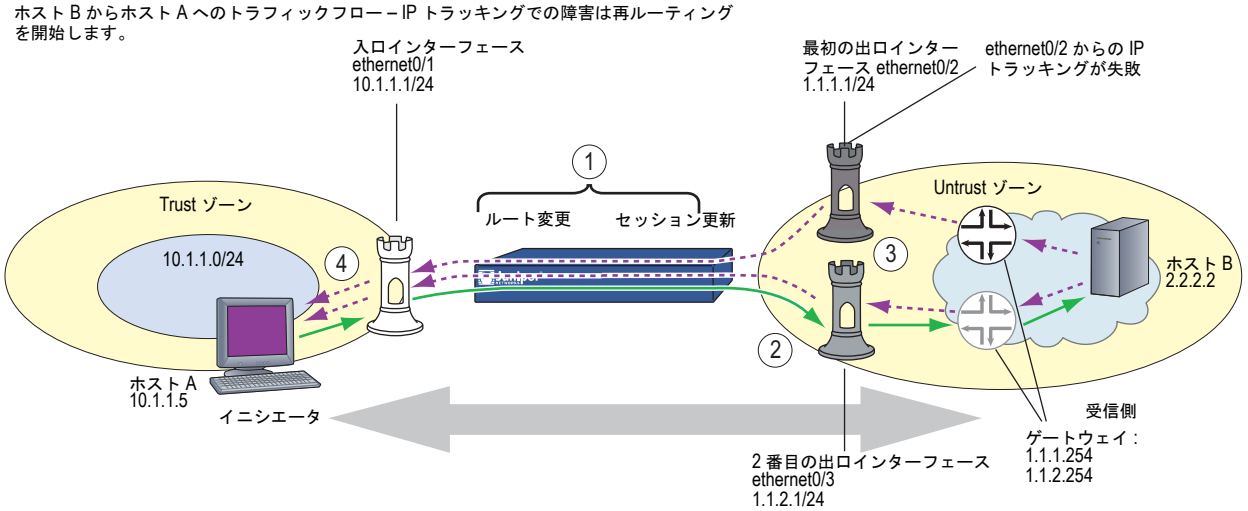
ホスト B がホスト A に応答すると、図 31 に示されているように、返信トラフィックはセキュリティデバイスを通って同様のパスで戻ります。

図 31: ホスト B からホスト A への出口トラフィックフロー



ethernet0/2 の IP トラッキングに障害がある場合、セキュリティデバイスは、ethernet0/2 を使用するルートを非アクティブにして、ホスト B へのアウトバウンドトラフィックに ethernet0/3 を使用します。ただし、ホスト B からホスト A への応答は、ethernet0/2 または etehrnet0/3 のどちらを経由しても到着でき、セキュリティデバイスは、応答を ethernet0/1 を経由してホスト A に転送します。図 32 を参照してください。

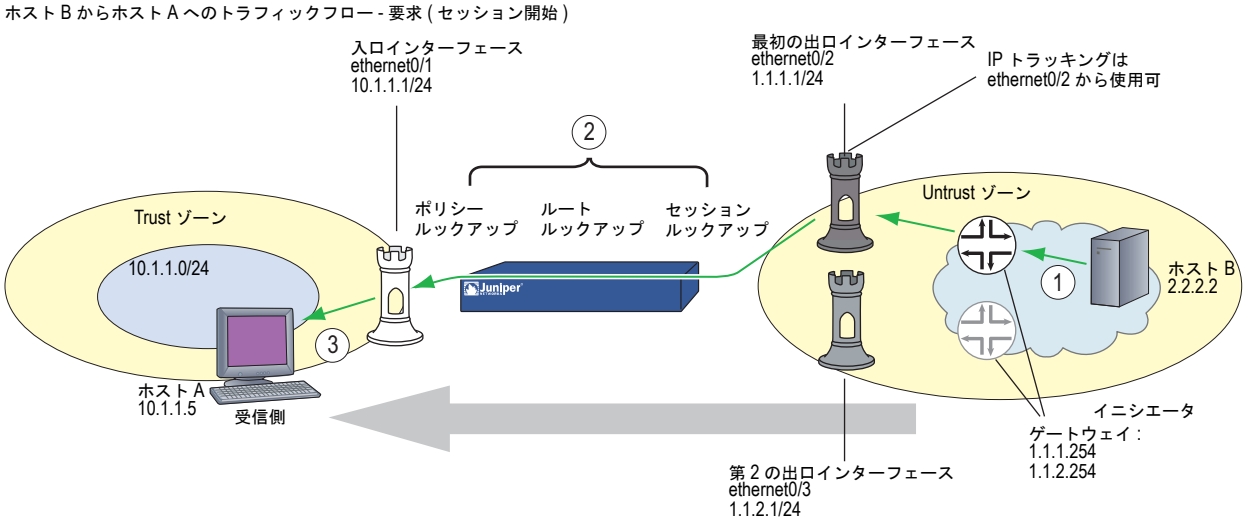
図 32: 出口 IP トラッキングの障害



出口インターフェースでの障害

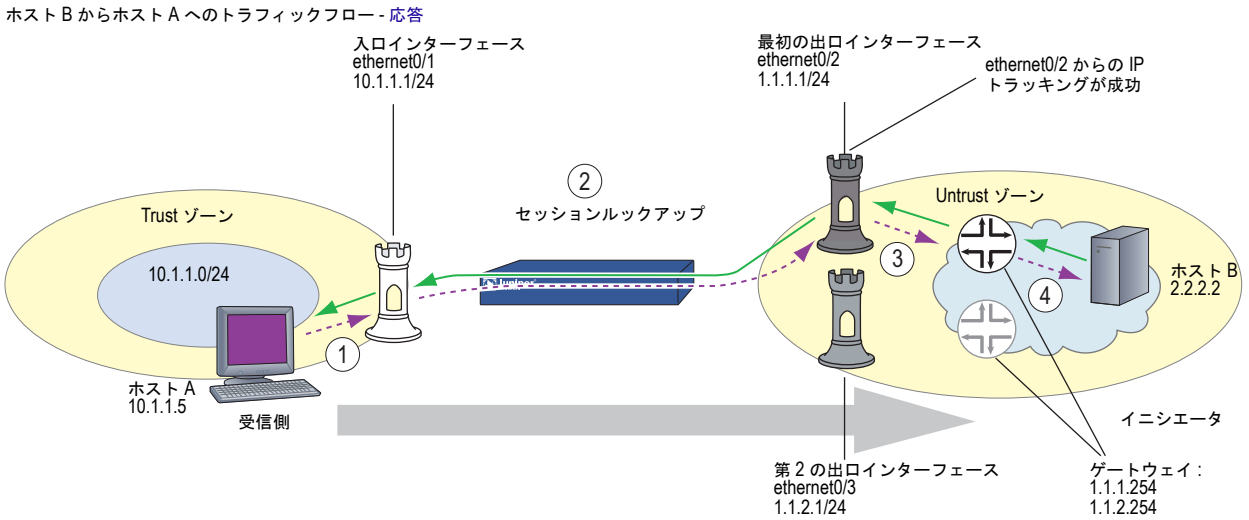
次のシナリオでは、再び ethernet0/2 で IP トラッキングを構成しますが、今回 ethernet0/2 は、ホスト B からホスト A へのセッションでセキュリティデバイスの入口インターフェースです。図 33 に示すように、ホスト A がホスト B にパケットを送信してセッションを開始します。

図 33: ホスト B からホスト A への入口トラフィックフロー



ホスト A がホスト B に応答すると、図 34 に示されているように、返信トラフィックはセキュリティデバイスを通って同様のパスで戻ります。

図 34: ホスト A からホスト B への入口トラフィックフロー



1. 10.1.1.5 のホスト A は、ホスト B (2.2.2.2) 宛てのパケットを 10.1.1.1 の ethernet0/1 に送信します。
2. セキュリティデバイスは、セッションルックアップを実行します。これは応答なので、デバイスは既存のセッションと照合し、セッションテーブルエントリをリフレッシュします。
3. デバイスは、1.1.1.254 のゲートウェイのキャッシュされた MAC アドレスを使用するか、または ARP ルックアップを実行して MAC アドレスを調べるかをして、パケットを ethernet0/2 を経由してゲートウェイに転送します。
4. 1.1.1.254 のゲートウェイで応答が受信されると、次のホップへパケットを転送します。ルーティングはホスト B が受信するまで続行されます。

ethernet0/2 の IP トラッキングに障害がある場合、セキュリティデバイスは ethernet0/2 を使用するルートを非アクティブにして、ホスト B へのアウトバウンドトラフィックに ethernet0/3 を使用します。しかし、ホスト B からホスト A への要求は ethernet0/2 を経由して到着でき、セキュリティデバイスは応答を ethernet0/1 を経由してホスト A に転送します。ホスト B からホスト A への要求のデータフローは、IP トラッキングの障害が発生した後でも、障害の前と見かけは変わりません。ただし、ホスト A からの応答は、**set arp always-on-dest** コマンドの適用状態によって、2 つの異なるパスのいずれかを通ります。

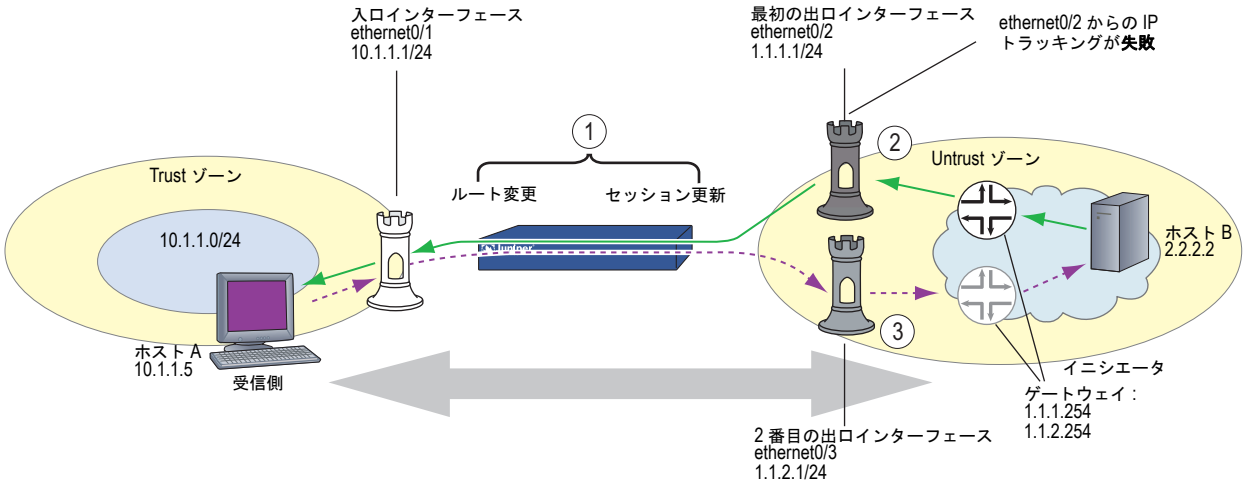
set arp always-on-dest コマンドが設定されている場合、セキュリティデバイスは、セッション内の最初のパケットへの応答を処理する場合かルートが変更される場合に、宛先 MAC アドレスの ARP 要求を送信します。(このコマンドが設定されていない場合、セキュリティデバイスは、セッションの最初の MAC アドレスをキャッシュして、応答を処理する際にそのキャッシュを使用します。デフォルトでは、このコマンドは設定されていません。)

ethernet0/2 で IP トラッキングに障害があると、セキュリティデバイスはまず ethernet0/2 を使用するすべてのルートを非アクティブにし、ルートルックアップを実行します。ホスト B へ到着するための、ethernet0/3 と 1.1.2.254 のゲートウェイを経由する別のルートを探します。その後、セッションテーブルをスキャンし、すべてのセッションを新しいルートに転送します。**set arp always-on-dest** コマンドを使用可能にした場合、セキュリティデバイスは、ホスト A から次のパケットへの応答を処理するとき、ARP ルックアップを実行します。これは、

パケットがルート変更によって影響を受けるセッションにあるからです。入口インターフェースではホスト B からのパケットが到着しますが、セキュリティデバイスは、ホスト A からのその後の応答すべてを ethernet0/3 を経由して 1.1.2.254 のゲートウェイに送信します。80 ページの図 35 を参照してください。

図 35: トラフィック再ルーティングでの入口 IP トラッキング障害

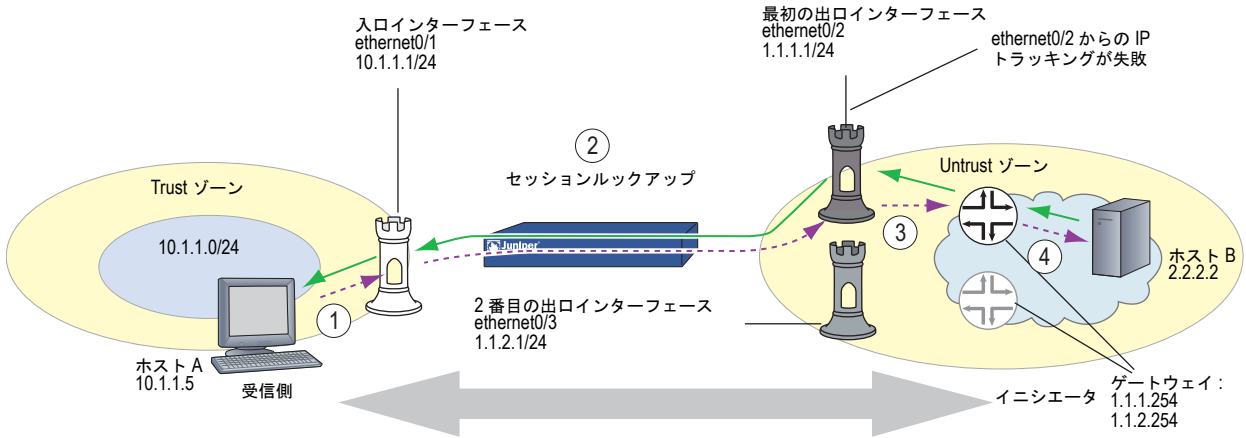
ホスト B からホスト A へのトラフィックフロー – IP トラッキングでの障害は再ルーティングを開始します。



unset arp always-on-dest コマンドを設定している場合 (デフォルトの構成) 、セキュリティデバイスは、ホスト B が最初のセッションパケットを送信したときにキャッシュされた MAC アドレスを、1.1.1.1 のゲートウェイに使用します。セキュリティデバイスは、ethernet0/2 を経由してセッション応答を継続して送信します。この場合、IP トラッキングで障害が発生しても、セキュリティデバイス経由のデータフローは変更されませんでした。

図 36: 再ルーティングのない入口 IP トラッキング障害

ホスト B からホスト A へのトラフィックフロー – IP トラッキングの障害は再ルーティングを開始しません。



第 4 章

インターフェースモード

インターフェースの動作モードには、NAT (ネットワークアドレス変換)、Route、透過の 3 種類があります。レイヤー 3 ゾーンに向かうインターフェースに IP アドレスが割り当てられていれば、そのインターフェースは、NAT モードまたは Route モードで動作させることができます。一方、レイヤー 2 ゾーン (v1-trust、v1-untrust、v1-dmz として定義済みのゾーンや、ユーザー定義の レイヤー 2 ゾーン) に向かうインターフェースは、透過モードに限ります。動作モードの選択は、インターフェースの設定時に行います。

注 : レイヤー 3 ゾーンに向かうインターフェースを NAT モードにした場合でも、実際にセキュリティデバイスが NAT を適用できるのは、Untrust ゾーンに伝送される途中でこのインターフェースを通過するトラフィックに限ります。Untrust ゾーン以外に向かうトラフィックに対しても、やはり NAT を施すことはありません。さらに、Untrust ゾーンインターフェースを NAT モードにすることも可能ですが、その場合でも NAT 処理が行われることはありません。

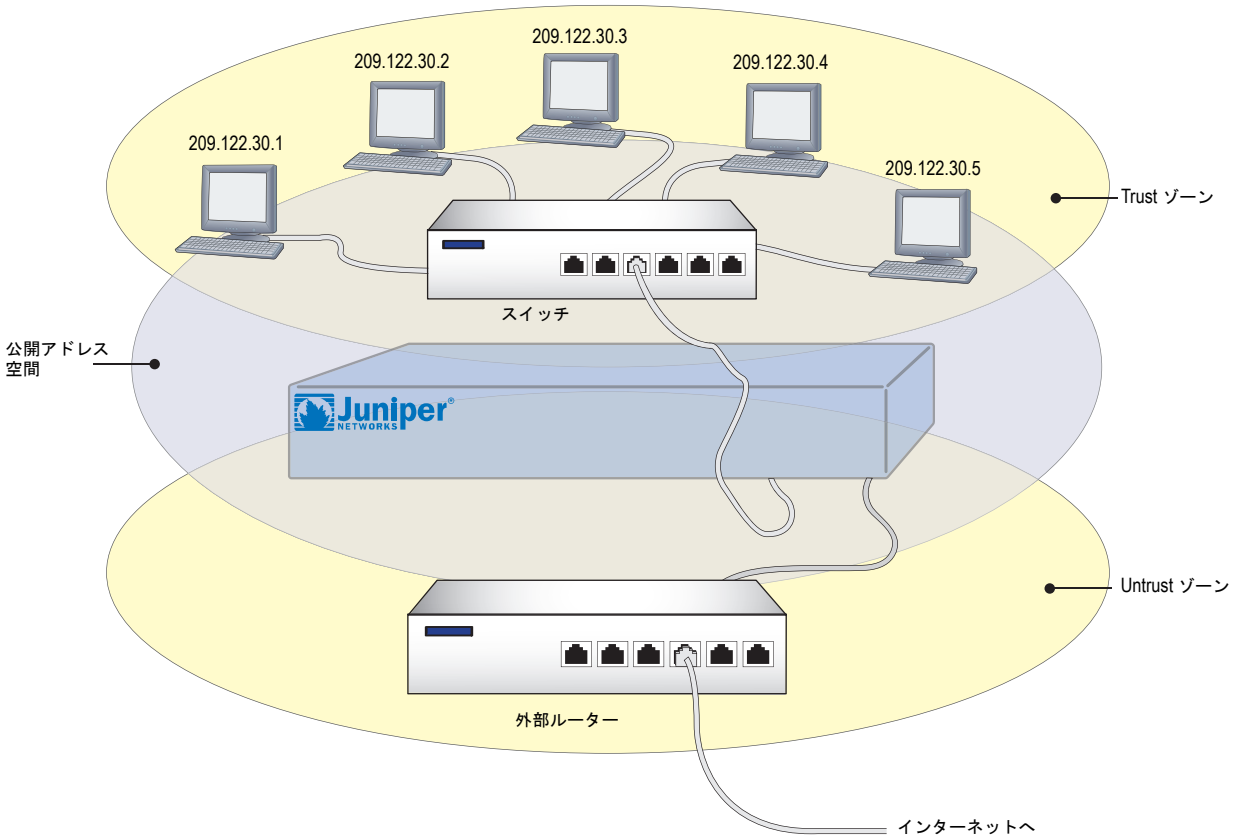
本章のセクションは、以下のようになります。

- 82 ページの「透過モード」
- 94 ページの「NAT モード」
- 100 ページの「Route モード」

透過モード

インターフェースを透過モードにした場合、セキュリティデバイスはファイアウォールを行き来するパケットに対し、IP パケットヘッダーのソース情報や宛先情報を変更することなく、フィルタを適用します。インターフェースはすべて、同じネットワークの一部であるように振る舞います。セキュリティデバイスは、レイヤー 2 スイッチやブリッジと同じように働きます。透過モードでは、インターフェースの IP アドレスは 0.0.0.0 と設定されるので、ユーザーからはセキュリティデバイスが透明である (見えない) ように見えます。図 37 を参照してください。

図 37: 透過モード



透過モードは、Web サーバーその他が受け取るトラフィックのソースが信頼できない場合に、サーバーを攻撃から保護する手段として有用です。透過モードには次のような利点があります。

- ルーターや保護対象サーバーの IP 設定を変更する必要はありません。
- マップ IP アドレスや仮想 IP アドレスを設定しなくても、正当なインバウンドトラフィックはサーバーに到達できます。

ゾーンの設定

ScreenOS では、特に操作をしなくても、機能ゾーンである VLAN ゾーンと、L2 セキュリティゾーンである V1-Trust、V1-Untrust、V1-DMZ の 3 つが生成されています。

VLAN ゾーン

VLAN ゾーンには、物理インターフェースと同等の構成と管理能力を持つ VLAN1 インターフェースがあります。セキュリティデバイスが透過モードの場合、デバイス管理や VPN トラフィックの終端として VLAN1 インターフェースを使うことになります。VLAN1 インターフェースの設定により、L2 セキュリティゾーンにあるホストでデバイス管理をするよう許可することができます。そのためには、VLAN1 インターフェースの IP アドレスを、L2 セキュリティゾーンにあるホストと同じサブネットから選んで設定する必要があります。

管理トラフィックに対しては、VLAN インターフェース IP よりも VLAN1 管理 IP の方が優先的に使われます。管理トラフィック用に VLAN1 管理 IP を設定しておけば、VLAN1 インターフェース IP はもっぱら VPN トンネルの終端用にのみ使うことができるのです。

定義済みのレイヤー 2 ゾーン

ScreenOS では、特に操作をしなくても V1-Trust、V1-Untrust、V1-DMZ という 3 つの L2 セキュリティゾーンが生成されています。この 3 つは同じ L2 ドメインを共有します。したがって、あるゾーンに対してインターフェースを設定すると、これは L2 ドメインに対して追加され、すての L2 ゾーンに属するあらゆるインターフェースから使えるようになるのです。L2 ゾーン内のホスト同士が通信するためには、すべて同じサブネット上に置かなければなりません。

前節でも述べたように NetScreen デバイスが透過モードであれば、その管理には VLAN1 インターフェースを使います。管理トラフィックが VLAN1 インターフェースに到達できるよう、VLAN1 インターフェース自身のほか、管理トラフィックが通過するゾーンすべてについて、管理オプションを有効にしておかなければなりません。デフォルトでは、V1-Trust ゾーンでは管理オプションがすべて有効になっています。その他のゾーンにあるホストで管理したい場合は、当該ホストが属するゾーンの管理オプションを有効にする必要があります。

注 : 各 Juniper Networks セキュリティプラットフォームの初期状態で、どの物理インターフェースが L2 ゾーンにバインドされているかについては、各プラットフォームのインストレーションガイドを参照してください。

トラフィックの転送

セキュリティデバイスを レイヤー 2 (L2) で動作させた場合、適切なポリシーを設定しない限りゾーン間でトラフィックが行き来することはありません。ポリシーの設定の詳細については、**2**-161 ページの「ポリシー」を参照してください。ポリシーを設定することにより、セキュリティデバイスでは次のようなことができます。

- ポリシーの条件に合致したトラフィックの許可または拒否
- ARP やその他 IP 以外の Layer 2 マルチキャスト / ブロードキャストトラフィックの許可これによりセキュリティデバイスは、スパニングツリープロ

トコルの L2 ブロードキャストトラフィックを受信および通過させて、LAN 間接続を実現できます。

- IP でも ARP でもないユニキャストトラフィックや IPSec トラフィックをすべて遮断

NetScreen デバイスの転送機能は、設定により次のように変更できます。

- IP でも ARP でもない L2 トラフィックを、マルチキャストやブロードキャストも含めてすべて遮断するには、**unset interface vlan1 bypass-non-ip-all** コマンドを入力します。
- IP 以外の L2 トラフィックをすべて通過させるには、**set interface vlan1 bypass-non-ip** コマンドを入力します。
- IP でも ARP でもないユニキャストトラフィックをすべて遮断する、という初期状態の動作に戻るには、**unset interface vlan1 bypass-non-ip** コマンドを入力します。

  設定ファイルに **unset interface vlan1 bypass-non-ip-all** と **unset interface vlan1 bypass-non-ip** の両方のコマンドを記述した場合、前者が常に有効になります。ゆえに、**unset interface vlan1 bypass-non-ip-all** コマンドを実行してしまった後で、IP でも ARP でもないユニキャストトラフィックを遮断する、という初期状態の動作に戻りたい場合は、まず **set interface vlan1 bypass-non-ip** コマンドを実行して、マルチキャスト、ユニキャスト、ブロードキャストトラフィックを含む、非 IP および非 ARP トラフィックがすべて通過できるようにする必要があります。次に **unset interface vlan1 bypass-non-ip** コマンドを実行すると、IP でも ARP でもないユニキャストトラフィックのみを遮断できます。

- IPSec トラフィックを終端せずに通過させるには、**set interface vlan1 bypass-others-ipsec** コマンドを実行します。すると、IPSec トラフィックはそのまま通過して、他の VPN 終端点に向かうようになります。

注： セキュリティデバイスのインターフェースを透過モードにした場合に、ルートを設定する目的は 2 つあります。すなわち、SNMP トラップなど自分自身が送出するトラフィックを伝送するため、およびカプセル化したり逆にそのカプセルを外したりした VPN トラフィックを転送するためです。

宛先不明のユニキャストの処理方式

ホストや各種ネットワークデバイス側で別デバイスの IP アドレスに関連付けられた MAC アドレスが不明の場合には、ARP (Address Resolution Protocol) を使います。この場合、同じサブネットに属するすべてのデバイスに向けたブロードキャストメッセージとして、ARP クエリ (arp-q) を送出します。arp-q は、該当する宛先 IP アドレスのデバイスに対して、ARP 応答 (arp-r) を返して MAC アドレスを通知するよう要求するものです。サブネット上の各デバイスは、arp-q を受け取るとその宛先 IP アドレスを確認し、それが自分自身でない場合は単にパケットをドロップします。arp-r を返すのは、IP アドレスが一致したデバイスだけです。その結果判明した IP アドレスと MAC アドレスの対応関係を、ARP キャッシュに保存しておきます。

セキュリティデバイスが透過モードならば ARP トラフィックは通過できますが、その際、各パケットのソース MAC アドレスを参照して、どのインターフェースの先に該当 MAC アドレスのデバイスがあるかを記録しておきます。実際にセキュリティデバイスは、すべてのパケットのソース MAC アドレスを調べ、インターフェースと MAC アドレスとの対応関係を転送テーブルに記録しています。次に、この情報が転送テーブルに保存されます。

注 : セキュリティデバイスを透過モードで動作させた場合、適切なポリシーを設定しない限り、ゾーン間でトラフィックが行き来することはありません。透過モードの場合に、どのようにトラフィックを転送するかについては、83 ページの「トラフィックの転送」を参照してください。

デバイスが宛先 MAC アドレス付きのユニキャストパケットを送信する場合に、その宛先 MAC アドレスが ARP キャッシュに保存されているが、セキュリティデバイスの転送テーブルには記録されていない、という状況も起こりえます。たとえば、セキュリティデバイスを再起動すると、転送テーブルはクリアされてしまいます。(転送テーブルは CLI コマンド **clear arp** で強制的にクリアすることもできます。) 透過モードのセキュリティデバイスがユニキャストパケットを受信したが、その宛先 MAC アドレスが転送テーブルに記録されていない場合、次のいずれかが起こります。

- このパケットのソースアドレスを基準としてポリシーを検索し、宛先として許可されているゾーンを判定します。次に、この各ゾーンにバインドされたインターフェースに、先頭パケットを一斉に送出 (フラッド) し、応答があったインターフェースを使って、以後の転送処理を続けます。これがフラッドオプションで、初期状態ではこちらが有効になっています。

- 先頭パケットをいったんドロップし、ARP クエリを、(送信元以外の) すべてのインターフェースに向けて送出 (フラッド) します。ARP クエリに加えて、TTL (time-to-live) 値を 1 にした trace-route パケット (ICMP echo 要求) を送出することもあります。ARP (または trace-route) に対する応答があれば、この応答を返したルーターまたはホストの MAC アドレスは先頭パケットの宛先 MAC アドレスと一致していることになるので、それに向けて以降のパケットを転送します。trace-route を使えば、宛先 MAC アドレスに該当するホストやルーターが隣接サブネット以外にある場合でも、宛先を見つけることができます。

注 : 以上のうち、ARP/trace-route 方式の方がより安全です。すべてのインターフェースに向けて送出するのが、先頭パケットではなく、ARP クエリや trace-route パケットだからです。

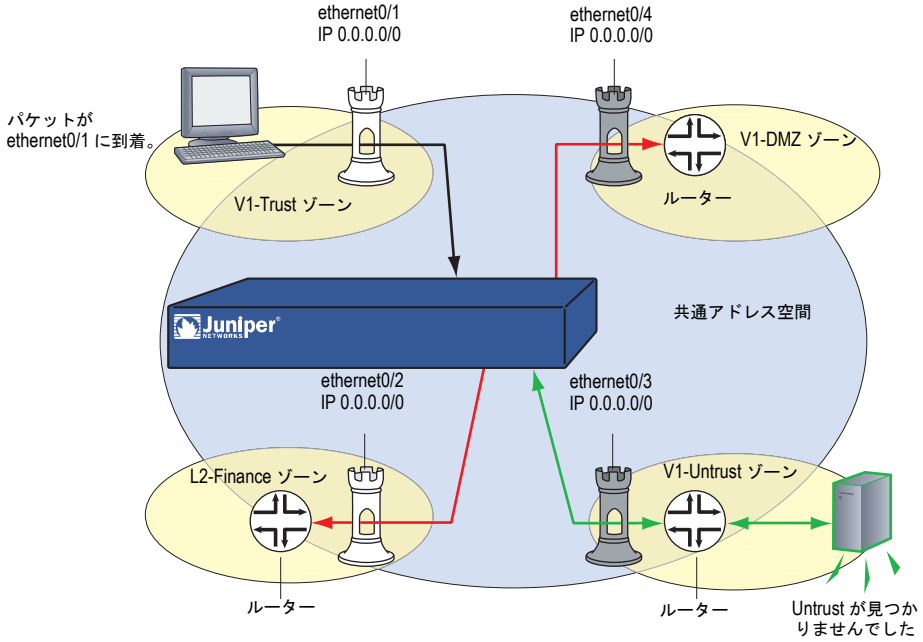
フラッド方式

フラッド方式の場合、多くのレイヤー 2 スイッチと同様の方法でパケットを転送します。スイッチには転送テーブルが備えられており、レイヤー 2 ドメインごとに MAC アドレスとポートの対応を管理しています。また、トラフィックを各デバイスに転送する際、どのインターフェースを使えばよいかという情報もここに記録しておきます。届いたパケットのフレームヘッダーに未知のソース MAC アドレスがあると、スイッチはその MAC アドレスを転送テーブルに追加します。また、当該パケットがどのインターフェースから届いたかについても記録します。あるパケットの宛先 MAC アドレスが転送テーブルに載っていない場合、

そのパケットを複製し、(送信元以外の) すべてのインターフェースに向けて一斉に送出 (フラッド) します。その結果、いずれかのインターフェースから応答があれば、当該 MAC アドレスのパケットはそのインターフェースに転送すればよいことが判明します。

フラッド方式を有効にした場合、セキュリティデバイスが受け取ったイーサネットフレームの宛先 MAC アドレスが転送テーブルに登録されていなければ、すべてのインターフェースに向けて一斉にパケットを送出します。

図 38: フラッド方式



セキュリティデバイスは ethernet0/2 に向けてパケットを送出するが、応答なし。

宛先不明のユニキャストパケットの処理方法としてフラッド方式を有効にするには、次のいずれかの操作を行います。

WebUI

Network > Interfaces > Edit (VLAN1): ブロードキャストオプションとして **Flood** を選択し、**OK** をクリックします。

CLI

```
set interface vlan1 broadcast flood
save
```

ARP/Trace-Route 方式

ARP 方式を選択して trace-route オプションも有効にした場合、受け取ったイーサネットフレームの宛先 MAC アドレスが転送テーブルに登録されていなければ、セキュリティデバイスは次のような処理を行います。

注 : ARP 方式を選択すると、デフォルトでは trace-route オプションも有効になっています。必要なければ trace-route オプションは無効にしても構いません。だしこの場合、宛先 IP アドレスが 入口 IP アドレスと同じサブネット上になければ、宛先 MAC アドレスを解決できません。 ((入口 IP アドレスについては、下の注を参照してください。)

1. セキュリティデバイスは、先頭パケットの宛先 MAC アドレスを確認します。(また、ソース MAC アドレスと対応するインターフェースが転送テーブルに載っていなければ、ここで追加します。)

2. セキュリティデバイスは、先頭パケットをドロップします。

3. ARP クエリ (arp-q) パケットと、TTL (time-to-live) 値を 1 にした trace-route パケット (ICMP echo 要求 または PING) の 2 つを生成し、送信元を除くすべてのインターフェースに向けて一斉に送出 (フラッド) します。どちらのパケットも、ソース IP アドレス、宛先 IP アドレスは、元の先頭パケットから転記します。arp-q パケットについては、ソース MAC アドレスとして VLAN1 の MAC アドレス、宛先 MAC アドレスとして ffff.ffff.ffff を設定します。また、trace-route パケットについては、ブロードキャストする ICMP echo 要求の先頭パケットに、ソース MAC アドレスと宛先 MAC アドレスを設定します。

   宛先 IP アドレスが入口 IP アドレスと同じサブネットに属していれば、MAC アドレスを記した ARP 応答 (arp-r) が返されるので、これ以降、どのインターフェースに向けてトラフィックを転送すればよいかが判明します。(88 ページの図 39、「ARP 方式」を参照してください。)

注 : 入口 IP アドレスとは、セキュリティデバイスに向けて直近にパケットを送信したデバイスの IP アドレスのことです。パケットを生成、送出したデバイス自身である場合もありますが、それを転送したルーターである場合もあります。

   宛先 IP アドレスが ingress IP アドレスと同じサブネットには属していない場合、trace-route には、宛先に行くルーターの IP アドレスと MAC アドレスが返されます。したがって、この MAC アドレス宛のトラフィックをどのインターフェースに向けて転送すべきかがわかります。(Figure 40 on page 89 を参照してください。)

注 : 実際には、trace-route により、サブネット上のすべてのルーターの IP アドレス、MAC アドレスが返されます。セキュリティデバイスは、先頭パケットの宛先 MAC アドレスと、arp-r パケットのソース MAC アドレスを比較して、目的とするルーターを判定し、どのインターフェースに向けて送出するべきかを判断します。

4. 以上の処理により判明した宛先 MAC アドレスとインターフェースの対応関係を、セキュリティデバイスは、転送テーブルに追加登録します。

5. これ以降、パケットは、すべて判明したインターフェースを使い、宛先に向けて転送されます。

宛先不明のユニキャストパケットの処理方法として ARP/trace-route 方式を有効にするには、次のいずれかの操作を行います。

WebUI

Network > Interfaces > Edit (VLAN1): ブロードキャストオプションとして **ARP** を選択し、**OK** をクリックします。

CLI

```
set interface vlan1 broadcast arp
save
```

注 : デフォルトでは trace-route オプションが有効になっています。trace-route オプションなしで ARP を使用するには、以下のコマンドを入力してください : **unset interface vlan1 broadcast arp trace-route** このコマンドにより trace-route オプションは解除されますが、ARP 方式は選択されたままです。

図 39 は、ARP 方式により宛先 MAC アドレスを解決する様子を示します。(宛先 IP アドレスが隣接サブネット上にある場合)

図 39: ARP 方式

注 : パケットヘッダーの該当する要素および MAC アドレスの最後の 4 桁のみが下に表示されています。

次のようなパケットが :

ethernet フレーム			IP データグラム	
dst	src	type	src	dst
11bb	11aa	0800	210.1.1.5	210.1.1.75

ethernet0/1 に到着し、転送先のテーブルが MAC アドレス 00bb.11bb.11bb のエントリがない、セキュリティ

ethernet フレーム			ARM メッセージ	
dst	src	type	src	dst
ffff	39ce	0806	210.1.1.5	210.1.1.75

デバイスが次の arp-r を ethernet0/2 で受信した場合、以下となります。

ethernet フレーム			ARM メッセージ	
dst	src	type	src	dst
39ce	11bb	0806	210.1.1.75	210.1.1.5

MAC アドレスとインターフェースとの対応関係が判明します。

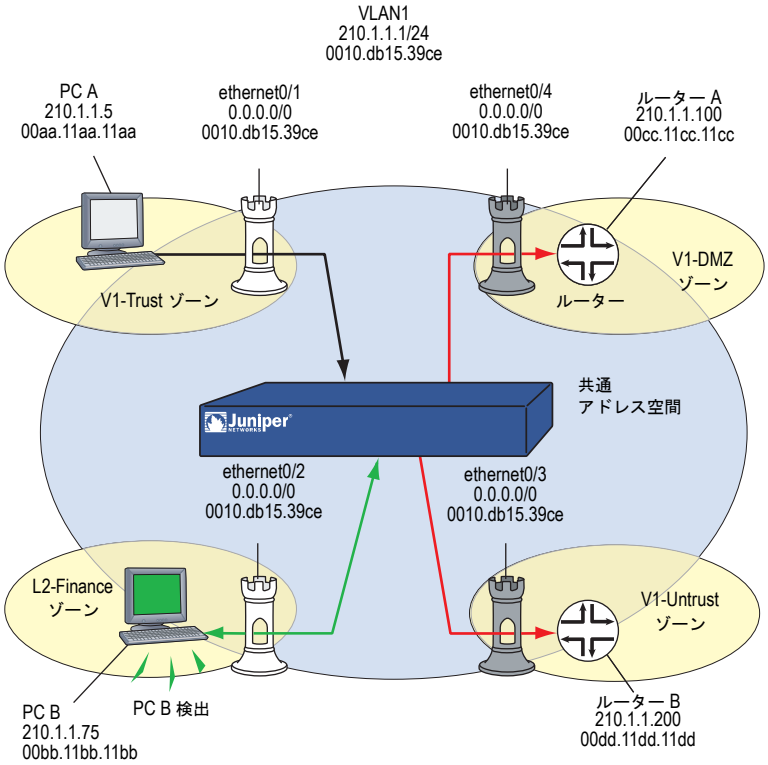


図 40 は、trace-route 方式により宛先 MAC アドレスを解決する様子を示します (宛先 IP アドレスが隣接サブネット上にない場合)。

図 40: Trace-Route

注 : パケットヘッダーの該当する要素および MAC アドレスの最後の 4 桁のみが下に表示されています。

次のようなパケットが :

ethernet フレーム			IP データグラム	
dst	src	type	src	dst
11dd	11aa	0800	210.1.1.5	195.1.1.5

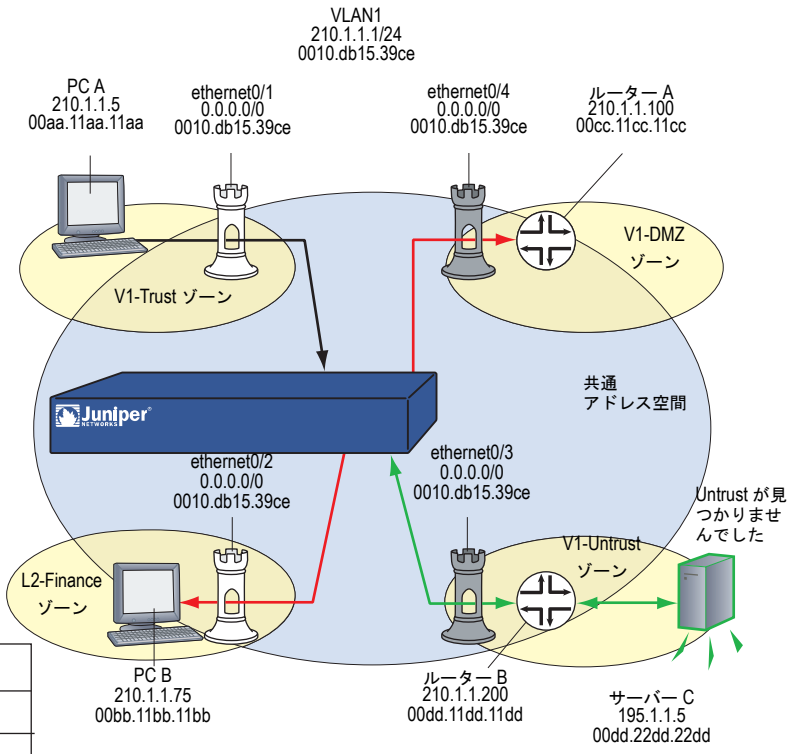
ethernet0/1 に到着し、転送先のテーブルが MAC アドレス 00bb.11bb.11bb のエントリがないと、セキュリティデバイスは次のトレースルートパケットを ethernet0/2, ethernet0/3, and ethernet0/4:

ethernet フレーム			ICMP メッセージ		
dst	src	type	src	dst	TTL
11dd	11aa	0800	210.1.1.5	195.1.1.5	1

デバイスが次の応答を ethernet0/3 で受信した場合、以下となります。

ethernet フレーム			ICMP メッセージ		
dst	src	type	src	dst	msg
11aa	11dd	0800	210.1.1.200	210.1.1.5	Time Exceeded

MAC アドレスとインターフェースとの 対応関係が判明します。



管理用の VLAN1 インターフェースの構成

ここでは VLAN1 インターフェース上に、次のような管理用のセキュリティデバイスを構成します。

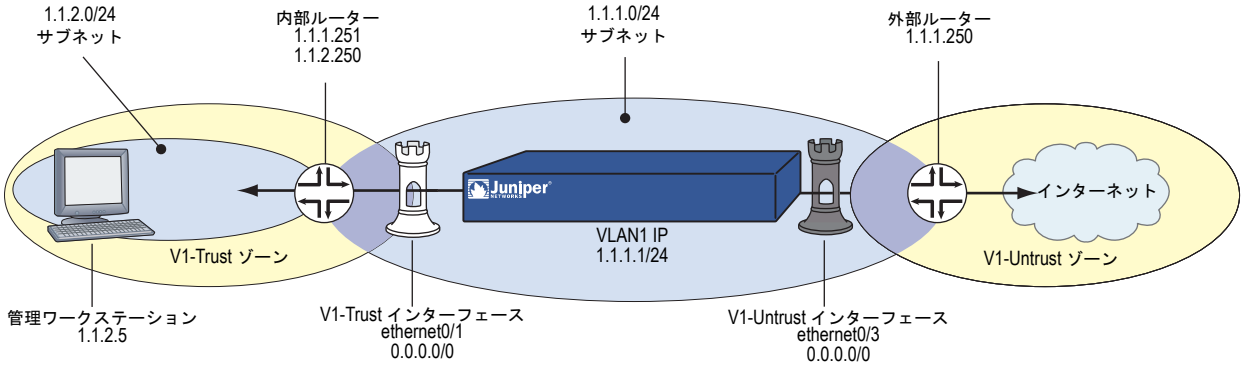
- VLAN1 インターフェースに IP アドレス 1.1.1.1/24 を割り当てます。
- Web、Telnet、SSH、Ping を、VLAN1 インターフェースおよび V1-Trust セキュリティゾーンの両方で使えるようにします。

注 : VLAN1 インターフェースおよび V1-Trust セキュリティゾーンの管理オプションは、デフォルトで使用可能になっています。ここでは例示の意味で、このオプションを有効にする手順も示します。明示的に無効にしていなければ、この操作は必要ありません。

レイヤー 2 セキュリティゾーンからデバイスを管理するためには、VLAN1 インターフェースとレイヤー 2 セキュリティゾーンのどちらについても、同じ管理オプションを設定する必要があります。

- Trust 仮想ルーター (レイヤー 2 セキュリティゾーンはすべて trust-vr ルーティングドメインにあります) にルートを追加して、セキュリティデバイスと隣接しないサブネット上にある管理ワークステーションとの間で、管理トラフィックが行き来できるようにします。セキュリティゾーンはすべて trust-vr ルーティングドメインにあります。

図 41: 透過 VLAN



WebUI

1. **VLAN1 インターフェース**
   Network > Interfaces > Edit (VLAN1): 次のように入力してから **OK** をクリックします。

   IP Address/Netmask: 1.1.1.1/24
   Management Services: WebUI, Telnet, SSH (選択)
   Other Services: Ping (選択)

2. **V1-Trust ゾーン**
   Network > Zones > Edit (V1-Trust): 次のように選択してから **OK** をクリックします。

   Management Services: WebUI, Telnet, SSH
   Other Services: Ping

3. **Route**
   Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 1.1.2.0/24
   Gateway: (選択)
   Interface: vlan1(trust-vr)
   Gateway IP Address: 1.1.1.251
   Metric: 1

CLI

1. **VLAN1 インターフェース**

```
set interface vlan1 ip 1.1.1.1/24
set interface vlan1 manage web
set interface vlan1 manage telnet
set interface vlan1 manage ssh
set interface vlan1 manage ping
```

2. **V1-Trust ゾーン**
   set zone v1-trust manage web
   set zone v1-trust manage telnet
   set zone v1-trust manage ssh
   set zone v1-trust manage ping

3. **ルート**
   set vrouter trust-vr route 1.1.2.0/24 interface vlan1 gateway 1.1.1.251 metric 1
   save

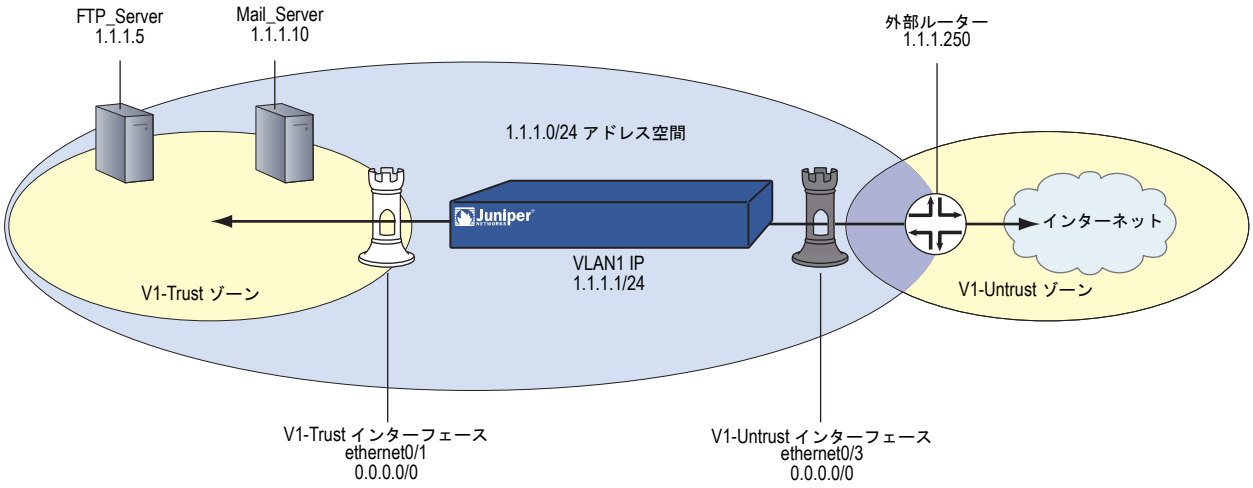
透過モードの構成

ここでは、透過モードのセキュリティデバイスで LAN を保護する基本的な構成例を示します。ポリシーを設定すると、V1-Trust ゾーンのすべてのホストからの出力トラフィック、メールサーバー宛のインバウンド SMTP サービス要求、および FTP サーバー宛のインバウンド FTP-GET サービス要求が許可できます。

管理トラフィックのセキュリティを向上するには、WebUI による管理用の HTTP ポート番号を 80 から 5555 に、CLI による管理用の Telnet ポート番号を 23 から 4646 に変更します。また、VLAN1 の IP アドレス 1.1.1.1/24 を使って、V1-Trust セキュリティゾーンからセキュリティデバイスを管理します。FTP サーバーとメールサーバーのアドレスも定義します。さらに、外部ルーター向けのデフォルトルートを 1.1.1.250 と設定して、セキュリティデバイスからこの外部ルーター宛のアウトバウンド VPN トラフィックを送信できるようにします。(V1-Trust ゾーン上のホストもすべて、デフォルトゲートウェイは 1.1.1.250 となります。)

注 : 透過モードのインターフェースを持つセキュリティデバイス用に VPN トンネルを構成する例については、5-148 ページの「透過モード VPN」を参照してください。

図 42: 基本的な透過モード



WebUI

1. **VLAN1 インターフェース**
   Network > Interfaces > Edit (VLAN1 インターフェース): 次のように入力してから **OK** をクリックします。

   IP Address/Netmask: 1.1.1.1/24
   Management Services: WebUI, Telnet (**選択**)
   Other Services: Ping (**選択**)

2. **HTTP ポート**
   Configuration > Admin > Management: HTTP Port フィールドに **5555** を入力してから、**Apply** をクリックします。

注 : デフォルトのポート番号は 80 です。不正アクセスを防ぐため、1,024 ～ 32,767 の範囲の適当な番号に変更するよう推奨します。デバイスを後で管理するためにログオンする場合は、ブラウザーの URL フィールドに以下を入力してください。http://1.1.1.1:5555 。

---

3. **インターフェース**
   Network > Interfaces > Edit (ethernet0/1): 次のように入力してから **OK** をクリックします。

   Zone Name: V1-Trust
   IP Address/Netmask: 0.0.0.0/0

   Network > Interfaces > Edit (ethernet0/3): 次のように入力してから **OK** をクリックします。

   Zone Name: V1-Untrust
   IP Address/Netmask: 0.0.0.0/0

4. **V1-Trust ゾーン**
   Network > Zones > Edit (v1-trust): 次のように選択してから **OK** をクリックします。

   Management Services: WebUI, Telnet
   Other Services: Ping

5. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 以下を入力し **OK** をクリックします。

   Address Name: FTP_Server
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 1.1.1.5/32
   Zone: V1-Trust

   Policy > Policy Elements > Addresses > List > New: 以下を入力し **OK** をクリックします。

   Address Name: Mail_Server
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 1.1.1.10/32
   Zone: V1-Trust

6. **Route**

   Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選択)
   Interface: vlan1(trust-vr)
   Gateway IP Address: 1.1.1.250
   Metric: 1

7. **ポリシー**

   Policy > Policies > (From: V1-Trust, To: V1-Untrust) New: 以下を入力し **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Any
   Destination Address:
   Address Book Entry: (選択), Any
   Service: Any
   Action: Permit

   Policy > Policies > (From: V1-Untrust, To: V1-Trust) New: 以下を入力し **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Any
   Destination Address:
   Address Book Entry: (選択), Mail_Server
   Service: Mail
   Action: Permit

   Policy > Policies > (From: V1-Untrust, To: V1-Trust) New: 以下を入力し **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Any
   Destination Address:
   Address Book Entry: (選択), FTP_Server
   Service: FTP-GET
   Action: Permit

CLI

1. **VLAN1**

   set interface vlan1 ip 1.1.1.1/24
   set interface vlan1 manage web
   set interface vlan1 manage telnet
   set interface vlan1 manage ping

2. **Telnet**

   set admin telnet port 4646

注 : デフォルトのポート番号は 23 番。不正アクセスを防ぐため、1,024 ～ 32,767 の範囲の適当な番号に変更するよう推奨します。変更後は、デバイス管理用にログインする際、アドレスを 1.1.1.1:4646 と入力してください。

---

3. **インターフェース**
   set interface ethernet0/1 ip 0.0.0.0/0
   set interface ethernet0/1 zone v1-trust
   set interface ethernet0/3 ip 0.0.0.0/0
   set interface ethernet0/3 zone v1-untrust

4. **V1-Trust ゾーン**
   set zone v1-trust manage web
   set zone v1-trust manage telnet
   set zone v1-trust manage ping

5. **アドレス**
   set address v1-trust FTP_Server 1.1.1.5/32
   set address v1-trust Mail_Server 1.1.1.10/32

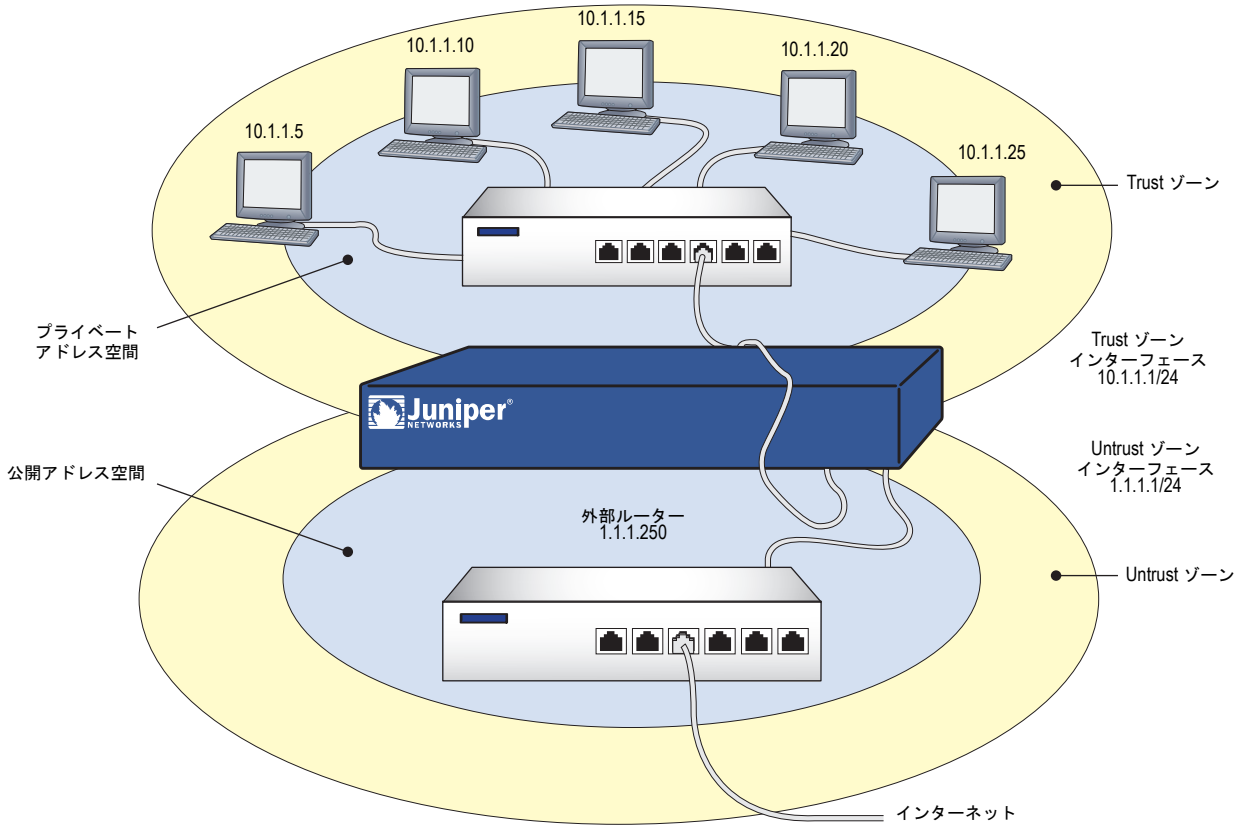
6. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway 1.1.1.250 metric 1

7. **ポリシー**
   set policy from v1-trust to v1-untrust any any any permit
   set policy from v1-untrust to v1-trust any Mail_Server mail permit
   set policy from v1-untrust to v1-trust any FTP_Server ftp-get permit
   save

NAT モード

入口インターフェースを NAT (Network Address Translation、ネットワークアドレス変換) モードにすると、セキュリティデバイスは、レイヤー 3 スイッチ (あるいはルーター) のように働いて、Untrust ゾーン向けのアウトバウンド IP パケットのヘッダーにあるソース IP アドレスとソースポート番号の 2 つを変換します。すなわち、パケットを送出したホストのソース IP アドレスを Untrust ゾーンインターフェースの IP アドレスに置き換えます。さらに、ソースポート番号も、セキュリティデバイスでランダムな番号を生成して置き換えます。

図 43: NAT トポロジ



応答パケットがセキュリティデバイスに到着したら、デバイスは、受信パケットの IP ヘッダーにある 2 つのコンポーネントを変換します。宛先アドレスとポート番号で、それぞれオリジナルの番号に戻るよう変換されます。セキュリティデバイスは、その宛先に向けてパケットを転送します。

NAT モードにすると、透過モードに比べてセキュリティが向上します。NAT モードの入口インターフェース (Trust ゾーンインターフェースなど) を経由してトラフィックを送信する場合、送信元ホストのアドレスが出口ゾーン (Untrust ゾーンなど) にあるホストに公開されることはありません。ただし、この 2 つのゾーンが同じ仮想ルーティングドメインに属し、セキュリティデバイスが DRP (動的ルーティングプロトコル) を使ってルートをアドバタイズしている場合は例外です。このような場合でも、ポリシーで許可されていない限り、Trust ゾーンアドレスにインバウンドトラフィックが到達することはありません (DRP を使う場合でも Trust ゾーンアドレスを隠蔽しておきたい場合は、Untrust ゾーンを untrust-vr、Trust ゾーンを trust-vr におき、内部アドレスに到達するルートを trust-vr から untrust-vr に向けて公開しないようにしてください。)

セキュリティデバイスが静的ルーティングを採用し、仮想ルーターが 1 つしかない場合は、インターフェースベースの NAT の働きにより、トラフィックがアウトバウンドであっても内部アドレスは隠蔽されます。インバウンドトラフィックについては、ポリシーの設定により制御します。インバウンドトラフィックに適用するポリシーで、宛先としてマップ IP (MIP) または仮想 IP (VIP) しか使わないようにすると、内部アドレスは隠蔽されたままになります。

さらに NAT には、公開 IP アドレスの使用を保持させる働きもあります。ネットワーク上のデバイスに対してすべてに公開 IP アドレスが与えられていない環境は珍しくありません。NAT サービスを使用すると、少数の公開 IP アドレスを使うだけで、プライベート IP アドレスを割り当てた何台ものホストからインターネットにアクセスできます。次の範囲の IP アドレスはプライベート IP ネットワーク用に予約されており、公開インターネット上で使うことはできません。

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

インバウンドおよびアウトバウンドの NAT トラフィック

NAT モードのインターフェースを経由してトラフィックを送信しているゾーンのホストから Untrust ゾーンへトラフィックを伝送できます (ポリシーで許可されている場合)。ScreenOS 5.0.0 までは、NAT モードのインターフェースの内側にあるホストが Untrust ゾーンからのトラフィックを受け取るためには、マップ IP (MIP) 、仮想 IP (VIP) 、VPN トンネルのいずれかを設定する必要がありました。しかし ScreenOS 5.0.0 以降では Untrust ゾーンを含め、どのゾーンからのトラフィックを受け取る場合でもこのような設定は不要になりました。ただし、アドレスを公開したくない、あるいはインターネット上に公開されることのないプライベートアドレスを使いたい場合には、MIP、VIP、VPN が今でも有効です。逆にそのような要請がないのであれば、MIP、VIP、VPN などを使わなくても、NAT モードのインターフェースを経由して Untrust ゾーンからのトラフィックを内側のホストが受信することは可能です。

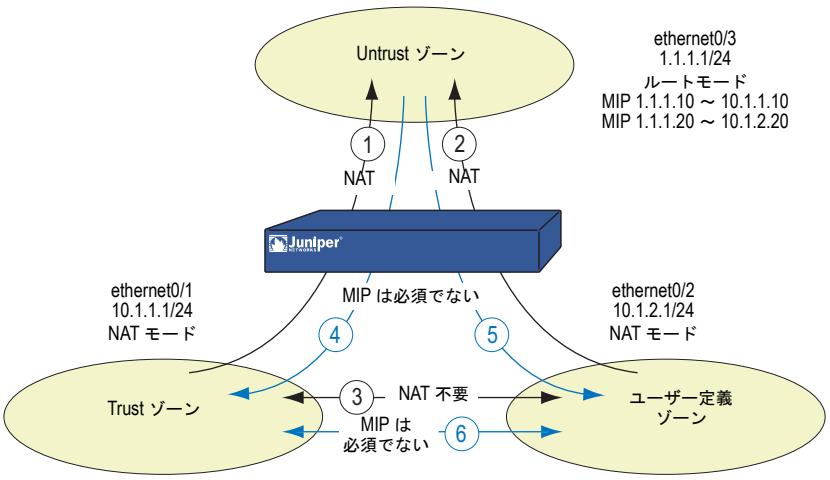
注 : 仮想 IP (VIP) アドレスは、Untrust ゾーンに向かうインターフェースにしか定義できません。

図 44: NAT トラフィックフロー

1. Trust ゾーンから Untrust ゾーンに向かうトラフィックに適用される、インターフェースベースの NAT。
2. ユーザー定義のゾーンから Untrust ゾーンに向かうトラフィックに適用される、インターフェースベースの NAT。

   (注記 : これはユーザー定義のゾーンと Untrust ゾーンが異なる仮想ルーティングドメインに属する場合にのみ可能。)
3. Trust ゾーンとユーザー定義ゾーンを行き来するトラフィックに適用される、インターフェースベースの NAT はありません。

4 & 5. Untrust ゾーンから Trust ゾーンまたはユーザー定義のゾーンに到達するトラフィックに対しては、MIP、VIP、VPN を適用できますが、必須ではありません。



注 : MIP の詳細については、8-61 ページの「マップ IP アドレス」を参照してください。VIP の詳細については、8-79 ページの「仮想 IP アドレス」を参照してください。

インターフェース設定

NAT モードでは次のようなインターフェース設定を定義します。ここで、*ip_addr1* および *ip_addr2* は IP アドレス、*mask* はネットマスク、*vlan_id_num* は VLAN タグ番号、*zone* はゾーン名、*number* は kbps 単位の帯域幅を表します。

ゾーンインターフェース	設定	ゾーンサブインターフェース
Trust、DMZ、ユーザー定義の各ゾーンのうち、NAT を適用するもの	IP: *ip_addr1* Netmask: *mask* Manage IP[1] : *ip_addr2* Traffic Bandwidth[2] : *number* NAT[3] : (選択)	IP: *ip_addr1* Netmask: *mask* VLAN Tag: *vlan_id_num* Zone Name: *zone* NAT[†]: (選択)
Untrust[4]	IP: *ip_addr1* Netmask: *mask* Manage IP[*]: *ip_addr2* Traffic Bandwidth[†]: *number*	IP: *ip_addr1* Netmask: *mask* VLAN Tag: *vlan_id_num* Zone Name: *zone*

1.管理 IP アドレスはインターフェースごとに設定できます。管理用のトラフィックに一般のネットワークトラフィックとは別の IP アドレスを割り当てるのが主な目的です。また、稼働率の高いデバイスにアクセスする際にも、管理用の IP アドレスを使用できます。
2.トラフィックシェーピング用に必要な場合に指定。
3.これによりインターフェースは NAT モードになります。Route をオンにすればインターフェースがルートモードになります。
4.Untrust ゾーンに向かうインターフェースを NAT モードにすることはできますが、セキュリティデバイスは、このインターフェースに対して NAT を適用することはありません。

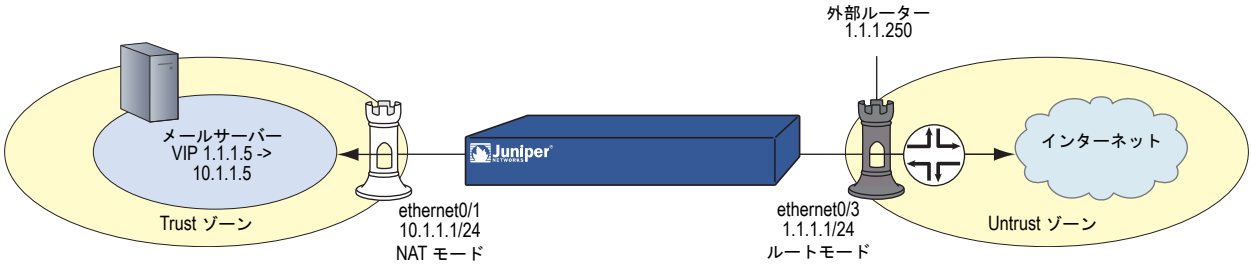
注 : NAT モードでは、任意のインターフェース (複数のインターフェース) から、システム IP アドレス、インターフェース IP アドレス、管理 IP アドレス、または MGT IP アドレスを使用して、セキュリティデバイスを管理できます。

NAT モードの構成

ここでは、Trust ゾーン内の単一のサブネットで構成される LAN の基本的な設定例を示します。LAN は NAT モードのセキュリティデバイスが保護しています。ポリシー設定により、Trust ゾーンに向かう出力トラフィックと、メールサーバーを宛先とする受信メールを許可します。受信メールは仮想 IP アドレスの機構によりメールサーバーに伝送されます。Untrust ゾーン、DMZ ゾーンはともに、trust-vr ルーティングドメインに属します。

注 : 図 45 を 101 ページの図 47、「Route モードのデバイス」の Route モードと比較してください。

図 45: NAT モードのデバイス



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet0/1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface Mode: NAT

注 : デフォルトでは、Trust ゾーンにバインドされたどのインターフェースも NAT モードになっています。そのため、Trust ゾーンにバインドされたインターフェースではこのオプションはすでに有効にしています。

   Network > Interfaces > Edit (ethernet0/3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24
   Interface Mode: Route

注 : セキュリティデバイスの Untrust ゾーンにある IP アドレスが、ISP により動的に割り当てられている場合は、IP アドレスとネットマスクを空のままにしておき、**Obtain IP using DHCP** をオンにしてください。ISP が PPPoE (Point-to-Point Protocol over Ethernet) を使っている場合は、**Obtain IP using PPPoE** をオンにし、**Create new PPPoE settings** ボタンを押して、名前とパスワードを入力してください。

---

2. **VIP**
   Network > Interfaces > Edit (ethernet0/3) > VIP: 次のように入力してから **Add** をクリックします。

   Virtual IP Address: 1.1.1.5

   Network > Interfaces > Edit (ethernet0/3) > VIP > New VIP Service: 次のように入力してから **OK** をクリックします。

   Virtual Port: 25
   Map to Service: Mail
   Map to IP: 10.1.1.5

注 : 仮想 IP (VIP) アドレスについては 8-79 ページの「仮想 IP アドレス」を参照してください。

3. ルート

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: ethernet0/3
Gateway IP Address: 1.1.1.250

4. ポリシー

Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), Any
Service: Any
Action: Permit

Policy > Policies > (From: Untrust, To: Global) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), VIP(1.1.1.5)
Service: MAIL
Action: Permit

CLI

1. インターフェース

```
set interface ethernet0/1 zone trust
set interface ethernet0/1 ip 10.1.1.1/24
set interface ethernet0/1 nat
set interface ethernet0/3 zone untrust
set interface ethernet0/3 ip 1.1.1.1/24
set interface ethernet0/3 route
```

注 : **set interface ethernet***n* **nat** コマンドは、セキュリティデバイスが NAT モードで動作しているかどうかの確認に使います。

セキュリティデバイスの Untrust ゾーンの IP アドレスが、ISP により動的に割り当てられている場合は、**set interface untrust dhcp** というコマンドを実行してください。一方、ISP が PPPoE (Point-to-Point Protocol over Ethernet) を使っている場合は、**set pppoe** コマンドと **exec pppoe** というコマンドを実行します。詳細は、*ScreenOS CLI Reference Guide: IPv4 Command Descriptions を参照してください。*

2. VIP

```
set interface ethernet0/3 vip 1.1.1.5 25 mail 10.1.1.5
```

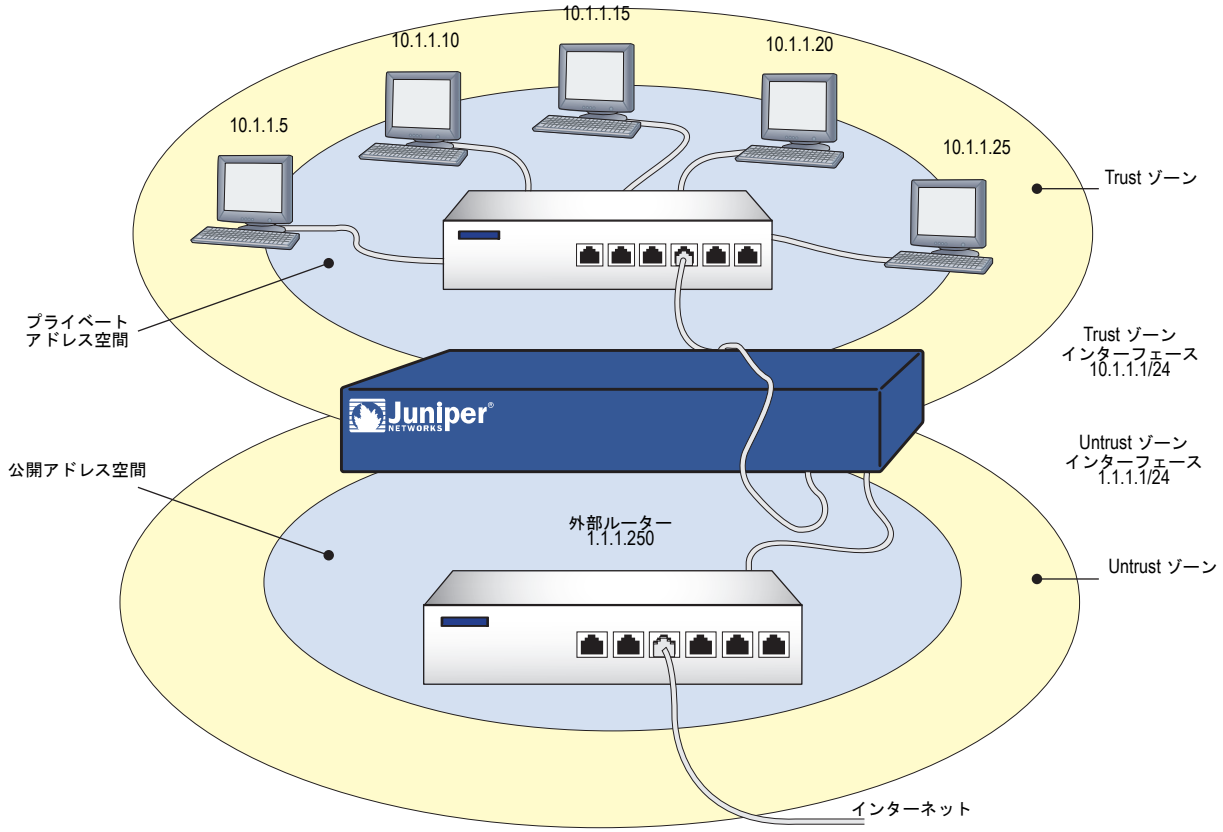
3. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/3 gateway 1.1.1.250

4. **ポリシー**
   set policy from trust to untrust any any any permit
   set policy from untrust to global any vip(1.1.1.5) mail permit
   save

Route モード

インターフェースが Route モードの場合、セキュリティデバイスは NAT-Src を適用することなく、ゾーン間を行き来するトラフィックのルーティングを行います。したがって、IP パケットヘッダー中のソースアドレスおよびソースポート番号は変換されません。NST-Src と違って、マップ IP (MIP) アドレスや仮想 IP (VIP) アドレスを設定しなくても、宛先ゾーンインターフェースがルートモードであれば、インバウンドトラフィックがホストに到達できます。透過モードと違い、各ゾーンのインターフェースは別々のサブネットに属します。

図 46: NAT トポロジ



インターフェースレベルでソースネットワークアドレス変換 (NAT-Src) を適用して、出力トラフィックのソースアドレスを宛先ゾーンインターフェースの IP アドレスに変換する必要はありません。NAT-Src はポリシーの設定に従い、選択的に適用することになります。どのトラフィックを転送し、どのトラフィックに NAT-Src を適用するかの設定は、ソースアドレスや内向き / 外向きを条件として指定したポリシーを定義して行います。ネットワークトラフィックに対する NAT

の場合、動的 IP (DIP) プールから取得した宛先ゾーンインターフェースのアドレスに変換します。この DIP プールは、宛先ゾーンインターフェースと同じサブネットにあります。一方、VPN トラフィックに対しては、トンネルインターフェース IP アドレス、またはこれに対応する DIP プールから取得したアドレスに変換します。

注 : ポリシーベースの NAT の設定については 8-13 ページの「ソースネットワークアドレス変換」を参照してください。

インターフェース設定

ルートモードでは次のようなインターフェース設定を定義します。ここで、*ip_addr1* および *ip_addr2* は IP アドレス、*mask* はネットマスク、*vlan_id_num* は VLAN タグ番号、*zone* はゾーン名、*number* は kbps 単位の帯域幅を表します。

表 7: インターフェースの設定

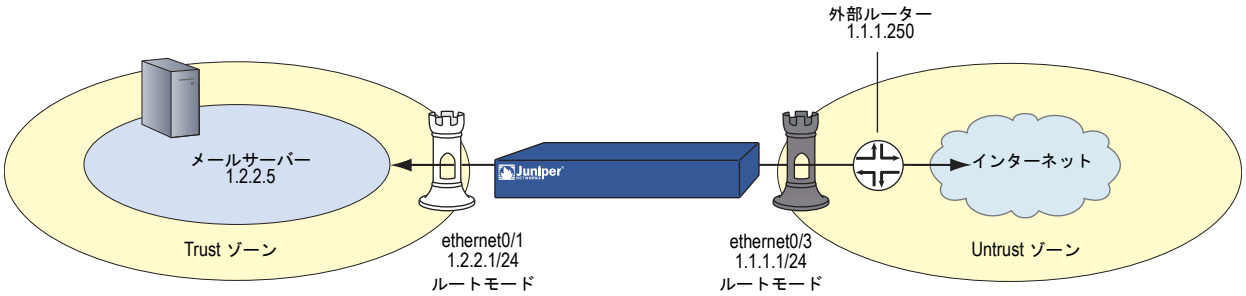
ゾーンインターフェース	設定	ゾーンサブインターフェース
Trust、Untrust、DMZ、ユーザー定義の各ゾーン	IP: *ip_addr1* Netmask: *mask* Manage IP[1] : *ip_addr2* Traffic Bandwidth[2] : *number* Route[3] : (選択)	IP: *ip_addr1* Netmask: *mask* VLAN Tag: *vlan_id_num* Zone Name: *zone* Route[†]: (選択)

1.管理 IP アドレスはインターフェースごとに設定できます。管理用のトラフィックに一般のネットワークトラフィックとは別の IP アドレスを割り当てるのが主な目的です。また、稼働率の高いデバイスにアクセスする際にも、管理用の IP アドレスを使用できます。
2.トラフィックシェーピング用に必要な場合に指定。
3.これによりインターフェースはルートモードになります。NAT をオンにすると NAT モードになります。

Route モードの構成

97 ページの「NAT モードの構成」では、Trust ゾーン LAN にあるホストに、プライベート IP アドレスとマップ IP (メールサーバー用) が割り当てられていました。次の例では、同じようにネットワークがルートモードのセキュリティデバイスによって保護されていますが、ホストには公開 IP アドレスが割り当てられているため、メールサーバー用に MIP を割り当てる必要がないことに注意してください。セキュリティゾーンはどちらも trust-vr ルーティングドメインにあります。

図 47: Route モードのデバイス



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet0/1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (**ある場合は選択する**)
   IP Address/Netmask: 1.2.2.1/24
   次のように入力してから OK をクリックします。
   Interface Mode: Route

   Network > Interfaces > Edit (ethernet0/3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (**ある場合は選択する**)
   IP Address/Netmask: 1.1.1.1/24

注 : **Route** を選択したので、セキュリティデバイスは Route モードで動作します。Trust ゾーンを行き来するトラフィックに NAT を適用することはありません。

セキュリティデバイスの Untrust ゾーンにある IP アドレスが、ISP により動的に割り当てられている場合は、IP アドレスとネットマスクを空のままにしておき、**Obtain IP using DHCP** をオンにしてください。ISP が PPPoE (Point-to-Point Protocol over Ethernet) を使っている場合は、**Obtain IP using PPPoE** をオンにし、**Create new PPPoE settings** リンクを押して、名前とパスワードを入力してください。

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 以下を入力し **OK** をクリックします。

   Address Name: **メールサーバー**
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 1.2.2.5/32
   Zone: Trust

3. **Route**
   Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (**選択**)
   Interface: ethernet0/3
   Gateway IP Address: 1.1.1.250

4. **ポリシー**
   Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), Any
   Destination Address:
   Address Book Entry: (**選択**), Any

Service: Any
Action: Permit

Policy > Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), Mail Server
Service: MAIL
Action: Permit

CLI

1. **インターフェース**
   set interface ethernet0/1 zone trust
   set interface ethernet0/1 ip 1.2.2.1/24
   set interface ethernet0/1 route
   set interface ethernet0/3 zone untrust
   set interface ethernet0/3 ip 1.1.1.1/24
   set interface ethernet0/3 route

注 : **set interface ethernet** *number* **route** コマンドで、セキュリティデバイスを Route モードにします。

---

2. **アドレス**
   set address trust mail_server 1.2.2.5/24
3. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/3 gateway 1.1.1.250
4. **ポリシー**
   set policy from trust to untrust any any any permit
   set policy from untrust to trust any mail_server mail permit
   save

第 5 章

ポリシー用ビルディングブロック

本章では、ポリシーで参照するコンポーネント、すなわちビルディングブロックについて説明します。本章のセクションは、以下のようになります。

- 105 ページの「アドレス」
- 110 ページの「サービス」
- 143 ページの「動的 IP プール」
- 158 ページの「反復スケジュールの設定」

注 : ユーザー認証についての詳細は、“ 第 9 部 : ユーザー認証 ” を参照してください。

アドレス

ScreenOS は、他のすべてのデバイスのアドレスを位置とネットマスクによって分類します。各ゾーンは、アドレスおよびアドレスグループのリストを独自に所有しています。

各ホストには単一の IP アドレスのみが定義されているため、255.255.255.255 (このホスト以外のすべてを認識する) のネットマスク設定を行う必要があります。

サブネットは、IP アドレスとネットマスク (たとえば 255.255.255.0 や 255.255.0.0) を持ちます。

各ホストとサブネットを出入りするトラフィックの許可、拒否またはトンネリングを行うポリシーを構成するには、その前に、各ホストとサブネットのエントリを ScreenOS アドレスリストに作成する必要があります。これらは、ゾーンごとに構成されます。

注 : “Any” に対するアドレスエントリを作成する必要はありません。この用語は、各ゾーン内に物理的に配置されたすべてのデバイスに自動的に適用されます。

アドレスエントリ

Juniper Networks ファイアウォール、VPN、およびトラフィックシェーピング機能の多くは、1 つ以上の複数のアドレスリストでアドレスを定義してからでないと設定できません。セキュリティゾーンのアドレスリストには、ホストまたはサブネットの IP アドレスやドメイン名があります。ホストやサブネットのトラフィックは、許可、ブロック、暗号化、またはユーザー認証のいずれかが行われます。

注： アドレスエントリにドメイン名を使用するには、その前に DNS（ドメイン名システム) サービス用のセキュリティデバイスを構成する必要があります。DNS 構成の詳細については、219 ページの「ドメイン名システムサポート」を参照してください。

ScreenOS 命名規則（アドレスに対して作成する名前に適用する) については、x ページの「コマンドラインインターフェースの規則」を参照してください。

アドレスの追加

この例では、Trust ゾーンのアドレスとして IP アドレス 10.1.10.0/24 を持つサブネット Sunnyvale_Eng を追加して、Untrust ゾーンのアドレスとしてアドレス www.juniper.net を追加します。

WebUI

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Sunnyvale_Eng
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.1.10.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Juniper
IP Address/Domain Name:
Domain Name: (**選択**), www.juniper.net
Zone: Untrust

CLI

```
set address trust Sunnyvale_Eng 10.1.10.0/24
set address untrust Juniper www.juniper.net
save
```

アドレスの変更

この例では、この部署がソフトウェアエンジニアリングを専門とし、異なる IP アドレス 10.1.40.0/24 を持つことを指定するように、アドレス Sunnyvale_Eng のアドレスエントリを変更します。

WebUI

Policy > Policy Elements > Addresses > List > Edit (for Sunnyvale_Eng): 次のように名前と IP アドレスを変更してから、**OK** をクリックします。

Address Name: Sunnyvale_SW_Eng
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.40.0/24
Zone: Trust

CLI

```
unset address trust Sunnyvale_Eng
set address trust Sunnyvale_SW_Eng 10.1.40.0/24
save
```

注 : アドレスまたはアドレスグループを定義してポリシーと関連付けると、そのアドレス位置を他のゾーンに変更する (Trust から Untrust へのように) ことはできません。その位置を変更するには、最初に基礎を成すポリシーから分離する必要があります。

アドレスの削除

この例では、アドレス“Sunnyvale_SW_Eng”のアドレスエントリを削除します。

WebUI

Policy > Policy Elements > Addresses > List: Sunnyvale_SW_Eng の Configure 列にある **Remove** をクリックします。

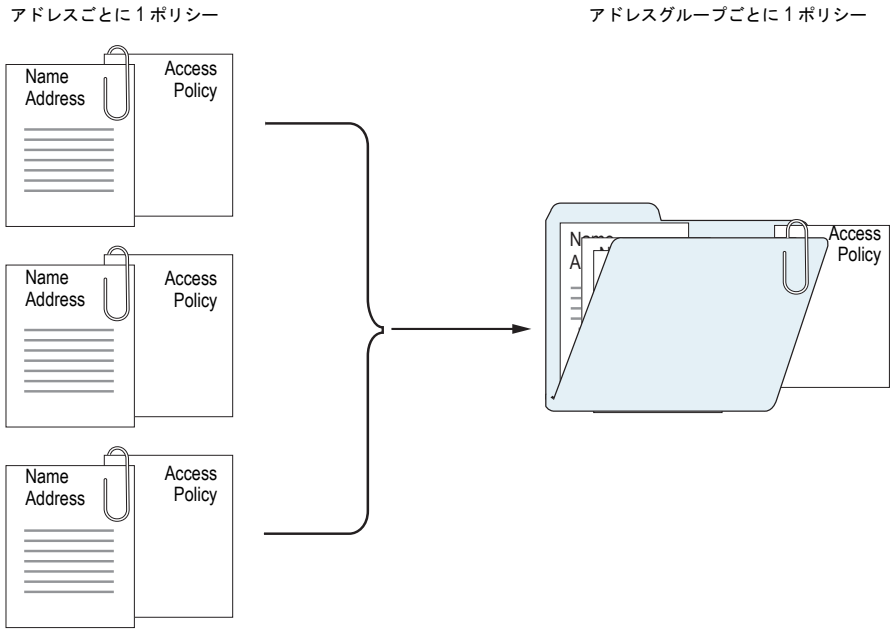
CLI

```
unset address trust “Sunnyvale_SW_Eng”
save
```

アドレスグループ

106 ページの「アドレスエントリ」では、個別のホストやサブネット用のアドレス帳エントリを作成、変更、および削除する方法を説明しました。アドレスリストにアドレスを追加すると、ポリシーがどのように各アドレス入力に影響するかを管理することは困難になります。ScreenOS によって、アドレスのグループを作成できます。多数のアドレスエントリではなく、少数のグループを管理できます。グループへの変更は、そのグループの各アドレスエントリに適用されます。

図 48: アドレスグループ



アドレスグループオプションは、次の機能を備えています。

- 任意のゾーンでアドレスグループを作成できます。
- 既存のユーザーを用いてアドレスグループを作成したり、空アドレスグループを作成した後にユーザーを入力することできます。
- アドレスグループは、他のアドレスグループのメンバーになれます。

注 : グループにそのグループ自身がメンバーとして偶発的に含まれていないことを確認するために、あるグループが他のグループに追加されると、セキュリティデバイスはサニティチェックを行います。たとえば、グループ A をグループ B のメンバーとして追加すると、セキュリティデバイスは A が既に B をメンバーとして含んでいないか自動的にチェックします。

- 個別のアドレス帳エントリのように、ポリシーのアドレスグループエントリを参照できます。
- 内部で各グループメンバー用に個別のポリシーを作成することによって、各グループのメンバーにポリシーが適用されます。ユーザーが 1 つのグループに作成するポリシーは 1 つですが、実際には、そのグループの各メンバー（各ユーザー用に構成した各サービス用と同様に) に内部ポリシーが作成されます。

注 : セキュリティデバイスによって自動的に各アドレスグループメンバーにポリシーが適用されるため、ユーザー側で各アドレス用に 1 つずつポリシーを作成する必要はありません。さらに、高速でルックアップを行う ASIC にこれらのポリシーを書き込みます。

- ユーザー側で個人のアドレスブックエントリをアドレス帳から削除すると、セキュリティデバイス側でそのエントリが属していたすべてのグループからも自動的にそのエントリが削除されます。

次の制約がアドレスグループに適用されます。

- アドレスグループは同じゾーンに属するアドレスのみを含みます。
- グループ名と同じアドレス名は使用できません。Paris という名前が、個別アドレス入力に使用される場合、グループ名に使用することはできません。
- ポリシーでアドレスグループが参照される場合、そのグループは削除できません。ただし、編集することはできます。
- 単一のポリシーがアドレスグループに割り当てられた場合、そのポリシーが各グループメンバーに個別に適用され、セキュリティデバイス側で ACL（アクセス制御リスト) に各メンバーのエントリを作成します。特別な警戒が必要でない場合、特にソースアドレスと宛先アドレスがともにアドレスグループであり指定されたサービスがサービスグループである場合は、利用可能なポリシーリソース数を超えることも可能です。
- 定義済みのアドレスである Any、All Virtual IPs および Dial-Up VPN は、グループに追加できません。

アドレスグループを作成する

以下の例で、すでに Trust ゾーン用アドレス帳に入力済みの 2 つのアドレス、つまり Santa Clara Eng および Tech Pubs を含む HQ 2nd Floor という 1 つのグループを作成します。

WebUI

Policy > Policy Elements > Addresses > Groups > (Zone: Trust) New: 以下のグループ名を入力して、以下のアドレスを移動し、**OK** をクリックします。

Group name: HQ 2nd Floor

Santa Clara Eng を選択し、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

Tech Pubs を選択し、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

CLI

```
set group address trust “HQ 2nd Floor” add “Santa Clara Eng”
set group address trust “HQ 2nd Floor” add “Tech Pubs”
save
```

アドレスグループエントリの編集

この例では、HQ 2nd Floor アドレスグループに (すでにアドレス帳に入力済みのアドレス) Support を追加します。

WebUI

Policy > Policy Elements > Addresses > Groups > (Zone: Trust) Edit (HQ 2nd Floor): 次のアドレスを移動してから **OK** をクリックします。

Support を選択し、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

CLI

```
set group address trust “HQ 2nd Floor” add Support
save
```

メンバおよびグループの削除

この例では、HQ 2nd Floor アドレスグループからメンバー“Support”を削除し、以前に作成したアドレスグループ“Sales”を削除します。

WebUI

Policy > Policy Elements > Addresses > Groups > (Zone: Trust) Edit (HQ 2nd Floor): 次のアドレスを移動してから **OK** をクリックします。

Support を選択し、> > ボタンを使用して Group Members 列から Available Members 列にアドレスを移動します。

Policy > Policy Elements > Addresses > Groups > (Zone: Trust): Sales 用の Configure コラムで **Remove** をクリックします。

CLI

```
unset group address trust “HQ 2nd Floor” remove Support
unset group address trust Sales
save
```

注 : グループからすべての名前を削除しても、セキュリティデバイス側ではそのグループを自動的には削除しません。

サービス

サービスとは、プロトコルスタンダードが存在するトラフィックのタイプです。各サービスは、FTP 用に TCP/ ポート 21、Telnet 用に TCP/ ポート 23 などのように、サービスと関連付けられたトランスポートプロトコルと宛先ポート番号を持ちます。ポリシーを作成する場合、そのポリシー用にサービスを指定する必要があります。そのサービスブックから 1 つの定義済みサービス、あるいは作成した顧客サービスまたはサービスグループを 1 つ選択できます。Policy Configuration ページ（Web UI) の Service ドロップダウンリストから、または **get service** コマンド（CLI) から、ポリシーで使用可能なサービスを表示できます。

定義済みサービス

WebUI または CLI から、セキュリティデバイスにある定義済みサービスやカスタムサービス、サービスグループのリストを表示できます。

- WebUI を使用する場合
  - Policy > Policy Elements > Services > Predefined
  - Policy > Policy Elements > Services > Custom
  - Policy > Policy Elements > Services > Groups
- CLI を使用する場合

  get service [group | predefined | user]

注 : 各定義済みのサービスは 1 ～ 65535 のソースポート範囲を持ち、有効なポート番号の全セットがこの範囲に含まれます。これによって、攻撃者がこの範囲外のソースポートを使用してアクセスを取得するのを防ぎます。定義済みのサービスに対して異なるソースポート範囲を使用する必要がある場合は、顧客サービスを作成します。詳細については、123 ページの「顧客サービス」を参照してください。

このセクションでは、以下の定義済みサービスについて説明します。

- 112 ページの「インターネット制御メッセージプロトコル」
- 115 ページの「インターネット関連の定義済みサービス」
- 116 ページの「Microsoft リモートプロシージャコールサービス」
- 118 ページの「動的ルーティングプロトコル」
- 118 ページの「ストリーミングビデオ」
- 119 ページの「Sun リモートプロシージャコールサービス」
- 120 ページの「セキュリティおよびトンネルサービス」
- 120 ページの「IP 関連サービス」
- 120 ページの「インスタントメッセージサービス」
- 121 ページの「管理サービス」
- 122 ページの「メールサービス」
- 122 ページの「UNIX サービス」
- 122 ページの「その他のサービス」

以下のページでは、次の項目について詳しく説明します。

- 128 ページの「ICMP（インターネット制御メッセージプロトコル）カスタムサービスの削除」
- 129 ページの「リモートシェル ALG」
- 129 ページの「Sun リモートプロシージャコール (RPC) アプリケーションレイヤーゲートウェイ」
- 130 ページの「Microsoft リモートプロシージャコール ALG のカスタマイズ」
- 132 ページの「リアルタイムストリーミングプロトコル（RTSP）アプリケーション レイヤーゲートウェイ」

インターネット制御メッセージプロトコル

ICMP(インターネット制御メッセージプロトコル) は、IP の一部であり、ネットワークの照会 (ICMP クエリーメッセージ) 、エラーパターンについてのフィードバックのネットワークからの受信 (ICMP エラーメッセージ) を行う方法を提供します。ただし、ICMP はエラーメッセージの配信を保証したり、損失したすべてのデータグラムを報告したりしないため、信頼性の高いプロトコルではありません。ICMP コードとタイプコードで、ICMP クエリーメッセージと ICMP エラーメッセージが記述されます。

特定のタイプの ICMP メッセージを許可または拒否して、ネットワークセキュリティを向上させることができます。ICMP メッセージのタイプの中には、悪用して、ネットワークのセキュリティを脅かす可能性のある情報を入手できるものがあります。たとえば、ICMP、TCP、UDP パケットは、トポロジなどのネットワークに関する情報やアクセスリストのフィルタリング特性を含む、ICMP エラーメッセージを返すように構成できます。112 ページの表 8 に、ICMP メッセージ名と対応するコード、タイプ、説明を示します。

表 8: ICMP 情報

ICMP メッセージ名	Type	コード	説明
ICMP-ANY	all	all	ICMP-ANY は、ICMP を使用しているすべてのプロトコルに影響します。 ICMP-ANY を拒否すると、ICMP を使用してネットワークに ping を送信したり監視したりしようとする試みを妨げます。 ICMP-ANY を許可すると、すべての ICMP メッセージが許可されます。
ICMP-ADDRESS-MASK ■ 要求 ■ 応答	 17 18	 0 0	ICMP アドレスマスククエリーは、ブートストラップサーバーからのローカルサブネットマスクを必要とするシステムに使用されます。 ICMP アドレスマスク要求メッセージを拒否すると、ディスクがないシステムに悪影響を与えることがあります。 ICMP アドレスマスク要求メッセージを許可すると、第三者がネットワーク内のホストのオペレーティングシステムに指紋を残すことが可能になる場合があります。
ICMP-DEST-UNREACH	3	0	ICMP 宛先不明エラーメッセージは、宛先ホストがパケットを拒否するように構成されていることを表します。 コード 0、1、4、5 は、ゲートウェイからのパケットに指定できます。コード 2 と 3 はホストからのパケットに指定できます (RFC 792)。 ICMP 宛先不明エラーメッセージを拒否すると、ホストがセキュリティデバイスの背後で稼働しているという推測を取り除くことができます。 ICMP 宛先不明エラーメッセージを許可すると、セキュリティフィルタリングなど、ネットワークについて推測できます。

表 8: ICMP 情報 (続き)

ICMP メッセージ名	Type	コード	説明
ICMP Fragment Needed	3	4	ICMP フラグメント化エラーメッセージは、フラグメント化が必要であるが、don 稚 fragment フラグが設定されていることを表します。 インターネット（Untrust）からトラステッドネットワークへのこれらのメッセージは、拒否することを推奨します。
ICMP Fragment Reassembly	11	1	ICMP フラグメント再アセンブリ時間超過エラーは、フラグメントメッセージを再アセンブリしているホストが時間切れとなり、パケットをドロップしたことを表します。このメッセージはときどき送信されます。 インターネット（Untrust）からトラステッドネットワークへのこれらのメッセージは、拒否することを推奨します。
ICMP-HOST-UNREACH	3	1	ICMP ホスト不明エラーメッセージは、ルーティングテーブルエントリが特定のホストをリストしていないか、または無限大としてリストしていることを表します。このエラーは、フラグメント化できないゲートウェイが、フラグメント化が必要なパケットを受信したときに、そのゲートウェイによって送信されることが時々あります。 インターネット（Untrust）からトラステッドネットワークへのこれらのメッセージは、拒否することを推奨します。 これらのメッセージを許可すると、第三者が消去プロセスによって内部ホストの IP アドレスを判別したり、ゲートウェイとフラグメンテーションについて推測できるようになります。
ICMP-INFO ■ 要求 ■ 応答	 15 16	 0 0	ICMP-INFO クエリーメッセージにより、ディスクのないホストシステムは、ネットワークの照会や自己構成を行うことができます。 ICMP アドレスマスク要求メッセージを拒否すると、ディスクがないシステムに悪影響を与えることがあります。 ICMP アドレスマスク要求メッセージを許可すると、第三者がネットワークセグメントに情報クエリーをブロードキャストして、コンピュータのタイプを判断できるようになる可能性があります。
ICMP-PARAMETER-PROBLEM	12	0	ICMP パラメータ問題エラーメッセージは、不正なヘッダーパラメータがあるのでパケットが廃棄された場合に、これを通知します。 インターネット（Untrust）からトラステッドネットワークへのこれらのメッセージは、拒否することを推奨します。 ICMP パラメータ問題エラーメッセージを許可すると、第三者がネットワークについて推測できるようになります。
ICMP-PORT-UNREACH	3	3	ICMP ポート不明エラーメッセージは、特定のポートを要求するデータグラムを処理しているゲートウェイが、使用できない、またはネットワークでサポートされていないことを表します。 インターネット（Untrust）からトラステッドネットワークへのこれらのメッセージは、拒否することを推奨します。 ICMP ポート不明エラーメッセージを許可すると、特定のプロトコルに使用しているポートを第三者が判断できるようになります。
ICMP-PROTOCOL-UNREACH	3	2	ICMP プロトコル不明エラーメッセージは、特定のプロトコルを要求するデータグラムを処理しているゲートウェイが、使用できない、またはネットワークでサポートされていないことを表します。 インターネット（Untrust）からトラステッドネットワークへのこれらのメッセージは、拒否することを推奨します。 ICMP プロトコル不明エラーメッセージを許可すると、ネットワークが実行しているプロトコルを第三者が判断できるようになります。
ICMP-REDIRECT	5	0	ICMP 転送ネットワークエラーメッセージは、ルーターによって送信されます。 インターネット（Untrust）からトラステッドネットワークへのこれらのメッセージは、拒否することを推奨します。

表 8: ICMP 情報（続き）

ICMP メッセージ名	Type	コード	説明
ICMP-REDIRECT-HOST	5	1	ICMP 転送メッセージは、別のパスで送信される、特定のホストを宛先とするデータグラムを表します。
ICMP-REDIRECT-TOS-HOST	5	3	ICMP 転送 TOS（サービスのタイプ）およびホストエラーは、メッセージタイプです。
ICMP-REDIRECT-TOS-NET	5	2	ICMP 転送 TOS およびネットワークエラーは、メッセージタイプです。
ICMP-SOURCE-QUENCH	4	0	ICMP 送信元エラーメッセージは、パケットを受け取り、キューに入れて、ネクストホップに送信するために使用できるバッファのスペースが、ルーターにないことを表します。 これらのメッセージを拒否しても、内部ネットワークのパフォーマンスが助長されたり障害となったりすることはありません。 これらのメッセージを許可すると、ルーターが混雑していることを第三者に知られ、攻撃対象となってしまいます。
ICMP-SOURCE-ROUTE-FAIL	3	5	ICMP ソースルート失敗エラーメッセージ。 インターネット（Untrust）からのこれらのメッセージは、拒否することを推奨します。
ICMP-TIME-EXCEEDED	11	0	ICMP TTL（生存時間）超過エラーメッセージは、パケットが宛先に到達する前にパケットの TTL 設定がゼロになったことを表します。これにより、再送信されたパケットが処理される前に、古いパケットが確実に廃棄されます。 トラステッドネットワークからインターネットへのこれらのメッセージは、拒否することを推奨します。
ICMP-TIMESTAMP			ICMP-TIMESTAMP クエリーメッセージは、時間を同期し、大規模で多様なネットワークでの時間配信を調整する機構を提供します。
■ 要求	13	0	
■ 応答	14	0	
ping（ICMP エコー）	8	0	ping（Packet Internet Groper）は、特定のホストが IP アドレス .0/0 エコー応答でアクセス可能かどうかを調べるユーティリティです。 ping 機能を拒否すると、ホストがアクティブかどうかを調べることができなくなります。 ping を許可すると、第三者が DoS（サービス拒否）攻撃やスマーフ攻撃を実行できるようになります。
ICMP-ECHO-FRAGMENT-ASSEMBLY-EXPIRE	11	1	ICMP フラグメントエコー再アセンブリ時間切れエラーメッセージは、再アセンブリ時間を超過したことを表します。 これらのメッセージは、拒否することを推奨します。
traceroute			traceroute は、特定のホストにアクセスするパスを示すユーティリティです。
■ 転送	30	0	インターネット（Untrust）から内部ネットワーク（Trust）へのこのユーティリティは、拒否することを推奨します。
■ 破棄	30	1	

ICMP 不明エラーの処理

異なったセキュリティのレベルに対して、ダウンストリームからの ICMP 不明エラーに対するデフォルトの行動は、次のように処理されます。

- ICMP タイプ 3 コード 4 メッセージに対して、セッションを閉じません。

  ICMP メッセージは、セッションをドロップせずに通過します。しかし、パケットはセッションごとにドロップされます。

- どの種類の ICMP 不明メッセージを受信しても、セッションを閉じません。

- セッションは、ICMP 不明メッセージを保管し、1 を通過するメッセージの数を制限します。

  1 つの ICMP 不明メッセージが、デバイスごとにグローバルに生成されます。残りの ICMP 不明メッセージはドロップされます。

インターネット関連の定義済みサービス

表 9 に、インターネット関連の定義済みサービスを示します。ネットワーク要件によって、これらのサービスのいずれかまたはすべてを許可あるいは拒否できます。各エントリについて、サービス名、デフォルトの受信ポート、およびサービスの説明を示します。

表 9: 定義済みサービス

サービス名	ポート	サービスの説明
AOL	5190-5193	America Online ISP（インターネットサービスプロバイダ）は、インターネット、チャット、およびインスタントメッセージサービスを提供します。
DHCP-Relay	67(デフォルト)	動的ホスト設定
DHCP	68 (client) 67 (server)	DHCP（動的ホスト構成プロトコル）は、ネットワークアドレスを割り当て、サーバーからホストへ構成パラメータを配信します。
DNS	53	DNS（ドメイン名システム）は、ドメイン名を IP アドレスに変換します。
FTP ■ FTP-Get ■ FTP-Put	20（データ） 21（制御）	FTP（ファイル転送プロトコル）によって、マシン間でファイルを送受信できます。ANY（GET または PUT）を拒否または許可したり、GET または PUT のどちらかを選択して許可あるいは拒否できます。GET は別のマシンからファイルを受信し、PUT は別のマシンにファイルを送信します。 アントラステッドソース（インターネット）からの FTP サービスは、拒否することを推奨します。
Gopher	70	Gopher は、インターネットサーバーのコンテンツをファイルの階層構造のリストに整理し、表示します。 ネットワーク構造が公開されるのを避けるため、Gopher のアクセスを拒否することを推奨します。
HTTP	8080	HTTP（ハイパーテキスト転送プロトコル）は、WWW（World Wide Web）が使用する、基礎となるプロトコルです。 HTTP サービスを拒否すると、ユーザーはインターネットを表示できなくなります。 HTTP サービスを許可すると、トラステッドホストはインターネットを表示できるようになります。
HTTP-EXT	—	拡張された非標準ポートを使用する HTTP（ハイパーテキスト転送プロトコル）
HTTPS	443	SSL（Secure Socket Layer）を使用する HTTP（ハイパーテキスト転送プロトコル）は、インターネットを通して機密文書を送信するためのプロトコルです。 HTTPS を拒否すると、ユーザーはインターネット上でのショッピングや、セキュリティ保護されたパスワードのやり取りを必要とする特定のオンラインリソースにアクセスできなくなります。 HTTPS を許可すると、トラステッドホストは、パスワードのやり取り、オンラインショッピング、ユーザーログインを必要とする、保護された各種オンラインリソースにアクセスできるようになります。
インターネットロケータサービス	—	インターネットロケータサービスには、LDAP、ユーザーロケータサービス、TSL/SSL 上の LDAP が含まれます。
IRC	6665-6669	IRC（Internet Relay Chat）を使用して、インターネットに接続し、ライブで会話に参加できます。

表 9: 定義済みサービス (続き)

サービス名	ポート	サービスの説明
LDAP	389	LDAP（Lightweight Directory Access Protocol）は、情報ディレクトリにアクセスするために使用するプロトコルセットです。
PC-Anywhere	—	PC-Anywhere は、リモート制御およびファイル転送ソフトウェアです。
TFTP	69	TFTP は、単純なファイル転送のためのプロトコルです。
WAIS	ó	WAIS（Wide Area Information Server）は、インターネット上の文書を検索するプログラムです。

Microsoft リモートプロシージャコールサービス

表 10 に、定義済みの Microsoft サービス、各サービスに関連するパラメータ、各サービスの簡単な説明を示します。パラメータには、UUID（Universal Unique Identifier）および TCP/UDP ソースポートと宛先ポートが含まれます。UUID は、ハードウェアアドレス、タイムスタンプ、シード値から生成される 128 ビットの一意の番号です。

表 10: Microsoft サービス

サービス	パラメータ /UUID	説明
MS-RPC-EPM	135 e1af8308-5d1f-11c9-91a4-08002b14a0fa	Microsoft RPC（リモートプロシージャコール）EPM（エンドポイントマッパー）プロトコル
MS-RPC-ANY	ó	任意の Microsoft リモートプロシージャコール (RPC) サービス
MS-AD	4 メンバー	Microsoft Active Directory サービスグループには、以下が含まれます。 ■ MS-AD-BR ■ MS-AD-DRSUAPI ■ MS-AD-DSROLE ■ MS-AD-DSSETUP
MS-EXCHANGE	6 メンバー	Microsoft Exchange サービスグループには、以下が含まれます。 ■ MS-EXCHANGE-DATABASE ■ MS-EXCHANGE-DIRECTORY ■ MS-EXCHANGE-INFO-STORE ■ MS-EXCHANGE-MTA ■ MS-EXCHANGE-STORE ■ MS-EXCHANGE-SYSATD
MS-IIS	6 メンバー	Microsoft IIS サーバーグループには、以下が含まれます。 ■ MS-IIS-COM ■ MS-IIS-IMAP4 ■ MS-IIS-INETINFO ■ MS-IIS-NNTP ■ MS-IIS-POP3 ■ MS-IIS-SMTP

表 10: Microsoft サービス (続き)

サービス	パラメータ /UUID	説明
MS-AD-BR	ecec0d70-a603-11d0-96b1-00a0c91ece30 16e0cf3a-a604-11d0-96b1-00a0c91ece30	Microsoft Active Directory バックアップと復元サービス
MS-AD-DRSUAPI	e3514235-4b06-11d1-ab04-00c04fc2dcd2	Microsoft Active Directory レプリケーションサービス
MS-AD-DSROLE	1cbcad78-df0b-4934-b558-87839ea501c9	Microsoft Active Directory DSROLE サービス
MS-AD-DSSETUP	3919286a-b10c-11d0-9ba8-00c04fd92ef5	Microsoft Active Directory セットアップサービス
MS-DTC	906b0ce0-c70b-1067-b317-00dd010662da	Microsoft 分散トランザクションコーディネータサービス
MS-EXCHANGE-DATABASE	1a190310-bb9c-11cd-90f8-00aa00466520	Microsoft Exchange データベースサービス
MS-EXCHANGE-DIRECTORY	f5cc5a18-4264-101a-8c59-08002b2f8426 f5cc5a7c-4264-101a-8c59-08002b2f8426 f5cc59b4-4264-101a-8c59-08002b2f8426	Microsoft Exchange ディレクトリサービス
MS-EXCHANGE-INFO-STORE	0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde 1453c42c-0fa6-11d2-a910-00c04f990f3b 10f24e8e-0fa6-11d2-a910-00c04f990f3b 1544f5e0-613c-11d1-93df-00c04fd7bd09	Microsoft Exchange インフォメーションストアサービス
MS-EXCHANGE-MTA	9e8ee830-4459-11ce-979b-00aa005ffebe 38a94e72-a9bc-11d2-8faf-00c04fa378ff	Microsoft Exchange MTA サービス
MS-EXCHANGE-STORE	99e66040-b032-11d0-97a4-00c04fd6551d 89742ace-a9ed-11cf-9c0c-08002be7ae86 a4f1db00-ca47-1067-b31e-00dd010662da a4f1db00-ca47-1067-b31f-00dd010662da	Microsoft Exchange ストアサービス
MS-EXCHANGE-SYSATD	67df7c70-0f04-11ce-b13f-00aa003bac6c f930c514-1215-11d3-99a5-00a0c9b61b04 83d72bf0-0d89-11ce-b13f-00aa003bac6c 469d6ec0-0d87-11ce-b13f-00aa003bac6c 06ed1d30-d3d3-11cd-b80e-00aa004b9c30	Microsoft Exchange システムアテンダントサービス
MS-FRS	f5cc59b4-4264-101a-8c59-08002b2f8426 d049b186-814f-11d1-9a3c-00c04fc9b232 a00c021c-2be2-11d2-b678-0000f87a8f8e	Microsoft ファイルレプリケーションサービス
MS-IIS-COM	70b51430-b6ca-11d0-b9b9-00a0c922e750 a9e69612-b80d-11d0-b9b9-00a0c922e70	Microsoft Internet Information Server COM GUID/UUID サービス
MS-IIS-IMAP4	2465e9e0-a873-11d0-930b-00a0c90ab17c	Microsoft Internet Information Server IMAP4 サービス
MS-IIS-INETINFO	82ad4280-036b-11cf-972c-00aa006887b0	Microsoft Internet Information Server 管理サービス
MS-IIS-NNTP	4f82f460-0e21-11cf-909e-00805f48a135	Microsoft Internet Information Server NNTP サービス
MS-IIS-POP3	1be617c0-31a5-11cf-a7d8-00805f48a135	Microsoft Internet Information Server POP3 サービス
MS-IIS-SMTP	8cfb5d70-31a4-11cf-a7d8-00805f48a135	Microsoft Internet Information Server SMTP サービス

表 10: Microsoft サービス（続き）

サービス	パラメータ /UUID	説明
MS-ISMSERV	68dcd486-669e-11d1-ab0c-00c04fc2dcd2 130ceefb-e466-11d1-b78b-00c04fa32883	Microsoft サイト間メッセージングサービス
MS-MESSENGER	17fdd703-1827-4e34-79d4-24a55c53bb37 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc	Microsoft Messenger サービス
MS-MQQM	fdb3a030-065f-11d1-bb9b-00a024ea5525 76d12b80-3467-11d3-91ff-0090272f9ea3 1088a980-eae5-11d0-8d9b-00a02453c33 5b5b3580-b0e0-11d1-b92d-0060081e87f0 41208ee0-e970-11d1-9b9e-00e02c064c39	Microsoft Windows メッセージキュー管理サービス
MS-NETLOGON	12345678-1234-abcd-ef00-01234567cffb	Microsoft Netlogon サービス
MS-SCHEDULER	1ff70682-0a51-30e8-076d-740be8cee98b 378e52b0-c0a9-11cf-822d-00aa0051e40f 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53	Microsoft スケジューラサービス
MS-WIN-DNS	50abc2a4-574d-40b3-9d66-ee4fd5fba076	Microsoft Windows DNS サーバー
MS-WINS	45f52c28-7f9f-101a-b52b-08002b2efabe 811109bf-a4e1-11d1-ab54-00a0c91e9b45	Microsoft WINS サービス

動的ルーティングプロトコル

ネットワーク要件によって、これらの動的ルーティングプロトコルから生成されたメッセージとパケットを許可あるいは拒否できます。表 11 に、サポートされている各動的ルーティングプロトコルの名前、ポート、および説明を示します。

表 11: 動的ルーティングプロトコル

動的ルーティングプロトコル	ポート	説明
RIP	520	RIP は、一般的な距離ベクトルルーティングプロトコルです。
OSPF	89	OSPF は、一般的なリンク状態ルーティングプロトコルです。
BGP	179	BGP は、外部 / ドメイン間ルーティングプロトコルです。

ストリーミングビデオ

表 12 に、サポートされている各ストリーミングビデオサービスの名前、デフォルトポート、および説明を示します。ネットワーク要件によって、これらのサービスのいずれかまたはすべてを許可あるいは拒否できます。

表 12: ストリーミングビデオサービス

サービス	ポート	説明
H.323	TCP ソース 1-65535、TCP 宛先 1720、1503、389、522、1731 UDP ソース 1 ～ 65535、UDP ソース 1719	H.323 は、視聴覚会議データがどのようにネットワーク経由で伝送されるかを定義する、ITU（国際電気通信連合）によって認定された規格です。

表 12: ストリーミングビデオサービス (続き)

サービス	ポート	説明
NetMeeting	TCP ソース 1-65535、TCP 宛先 1720、1503、389、522 UDP ソース 1719	Microsoft NetMeeting は、TCP を使用してインターネットを介したテレビ会議（映像と音声）サービスを提供します。
Real media	TCP ソース 1 ～ 65535、TCP 宛先 7070	Real Media は、ストリーミング ビデオ オーディオ技術です。
RTSP	554	ストリーミングメディアアプリケーション用の RTSP（リアルタイムストリーミングプロトコル）
SIP	5056	SIP（Session Initiation Protocol）は、セッションを作成、変更、終了するためのアプリケーションレイヤー制御プロトコルです。
VDO Live	TCP ソース 1 ～ 65535、TCP 宛先 7000 ～ 7010	VDOLive は拡張可能なビデオストリーミング技術です。

Sun リモートプロシージャコールサービス

表 13 に、Sun RPC ALG（リモートプロシージャコール アプリケーションレイヤーゲートウェイ）の各サービスの名前、パラメータ、正式名称を示します。

表 13: RPC ALG サービス

サービス	プログラム番号	正式名称
SUN-RPC-PORTMAPPER	111 100000	Sun PRC ポートマッパープロトコル
SUN-RPC-ANY	任意	任意の Sun RPC サービス
SUN-RPC-PROGRAM-MOUNTD	100005	Sun RPC マウントデーモン
SUN-RPC-PROGRAM-NFS	100003 100227	Sun RPC ネットワークファイルシステム
SUN-RPC-PROGRAM-NLOCKMGR	100021	Sun RPC ネットワークロックマネージャ
SUN-RPC-PROGRAM-RQUOTAD	100011	Sun RPC リモートクォータデーモン
SUN-RPC-PROGRAM-RSTATD	100001	Sun RPC リモートステータスデーモン
SUN-RPC-PROGRAM-RUSERD	100002	Sun RPC リモートユーザーデーモン
SUN-RPC-PROGRAM-SADMIND	100232	Sun RPC リモート管理デーモン
SUN-RPC-PROGRAM-SPRAYD	100012	Sun RPC SPRAY デーモン
SUN-RPC-PROGRAM-STATUS	100024	Sun RPC STATUS
SUN-RPC-PROGRAM-WALLD	100008	Sun RPC WALL デーモン
SUN-RPC-PROGRAM-YPBIND	100007	Sun RPC イエローページバインドサービス

セキュリティおよびトンネルサービス

表 14 に、サポートされている各サービスを挙げ、各エントリのデフォルトのポートと説明を示します。

表 14: サポートされているプロトコルサービス

サービス	ポート	説明
IKE	UDP ソース 1 ～ 65535、UDP 宛先 500 4500（NAT-Traversal に使用）	IKE は、ISAKMP で使用するために認証済みの鍵マテリアルを取得するプロトコルです。 自動 IKE を構成する場合は、次の 3 つの事前に定義されたフェーズ 1 またはフェーズ 2 のプロポーザルから選択できます。 ■ Standard (標準): AES と 3DES ■ Basic (基本): DES および 2 つの異なるタイプの認証アルゴリズム ■ Compatible (互換): 一般的に使用される 4 つの認証および暗号化アルゴリズム
L2TP	1723	L2TP は、リモートアクセス用に PPTP（ポイントツーポイントトンネリングプロトコル）と L2F（レイヤー 2 転送）を組み合わせます。
PPTP	—	PPTP（ポイントツーポイントトンネリングプロトコル）によって、企業は、公共のインターネット上でプライベート*トンネル*を介してプライベートネットワークを拡張できます。

IP 関連サービス

表 15 に、定義済みの IP 関連サービスを示します。エントリごとに、デフォルトのポートおよびサービスの説明も示しています。

表 15: IP 関連サービス

サービス	ポート	説明
Any	—	任意のサービス
TCP-ANY	1-65535	TCP（トランスポート制御プロトコル）を使用する任意のプロトコル
		TCPMUX ポート 1
UDP-ANY	137	UDP（ユーザーデータグラムプロトコル）を使用する任意のプロトコル

インスタントメッセージサービス

表 16 に、定義済みのインターネットメッセージサービスを示します。エントリごとに、サービスの名前、デフォルトポートまたは割り当てられているポート、およびサービスの説明を示しています。

表 16: インターネットメッセージサービス

サービス	ポート	説明
Gnutella	6346（デフォルト）	Gnutella ファイル共有プロトコルは、分散ネットワーク上で動作するパブリックドメインのファイル共有プロトコルです。任意のポートを割り当てることができますが、デフォルトのポートは 6346 です。
MSN	1863	Microsoft Network Messenger は、インスタントメッセージを送信したり、オンラインで会話ができるユーティリティです。

サービス	ポート	説明
NNTP	119	NNTP（Network News Transport Protocol）は、USENET メッセージを投稿、配布、検索するのに使用するプロトコルです。
SMB	445	IP 上の SMB（サーバーメッセージブロック）プロトコルを使用して、ネットワーク上のサーバーでのファイルの読み込みおよび書き込みができます。
YMSG	5010	Yahoo! メッセンジャーは、他のユーザーがオンラインかどうかを調べたり、インスタントメッセージの送信やオンラインでの会話ができるユーティリティです。

管理サービス

表 17 に、定義済みの管理サービスを示します。エントリごとに、サービスの名前、デフォルトポートまたは割り当てられているポート、およびサービスの説明を示しています。

表 17: 管理サービス

サービス	ポート	説明
NBNAME	137	NetBIOS ネームサービスは、UDP ポート 137 で送信されたすべての NetBIOS 名パケットを表示します。
NDBDS	138	IBM が公開している NetBIOS データグラムサービスは、ブロードキャスト媒体に接続している PC に、リソースを見つけ、セッションの開始と終了を行うコネクションレス（データグラム）サービスを提供します。信頼性が低く、パケットは順序付けが行われません。
NFS	—	ネットワークファイルシステムは、UDP を使用して、異なるタイプのコンピュータに保存されている共有ファイルへのアクセスをネットワークユーザーに許可します。SUN RPC は、NFS のビルディングブロックです。
NS Global	—	NS-Global は、Juniper Networks ファイアウォール /VPN デバイスの中央管理プロトコルです。
NS Global PRO	—	NS Global-PRO は、Juniper Networks ファイアウォール /VPN デバイスファミリーの拡張可能な監視システムです。
NSM	—	NetScreen-Security Manager
NTP	123	NTP（Network Time Protocol）は、コンピュータを時間の基準に同期する方法を提供します。
RLOGIN	513	RLOGIN は、リモートホスト上で端末セッションを開始します。
RSH	514	RSH は、リモートホスト上でシェルコマンドを実行します。
SNMP	161	SNMP（簡易ネットワーク管理プロトコル）は、複雑なネットワークを管理するためのプロトコルのセットです。
SQL*Net V1	66	SQL*Net バージョン 1 は、データの作成、アクセス、変更、保護を行うことができるデータベース言語です。
SQL*Net V2	66	SQL*Net バージョン 2 は、データの作成、アクセス、変更、保護を行うことができるデータベース言語です。
MSSQL	1433（デフォルトのインスタンス）	Microsoft SQL は、データの作成、アクセス、変更、保護を行うことができる独自のデータベースサーバーツールです。
SSH	22	セキュアシェルは、セキュアでないチャネル上で、強力な認証とセキュアな通信を通じてネットワーク上の別のコンピュータにログインするプログラムです。
SYSLOG	514	syslog は、システムロガーにメッセージを送信する UNIX プログラムです。
Talk	517-518	talk は、ユーザーの端末から別のユーザーの端末にラインをコピーする視覚的な通信プログラムです。
Telnet	23	Telnet は、端末デバイスと端末指向プロセスを相互にインターフェースさせる標準的な方法を提供する UNIX プログラムです。

表 17: 管理サービス (続き)

サービス	ポート	説明
WinFrame	—	WinFrame は、非 Windows マシンのユーザーが Windows アプリケーションを実行できる技術です。
X-Windows	—	X-Windows は、Motif と OpenLook がベースとする、ウィンドウおよびグラフィックシステムです。

メールサービス

表 18 に、定義済みのメールサービスを示します。各サービスの名前、デフォルトのまたは割り当てられているポート番号、サービスの説明も示しています。

表 18: メールサービス

サービス	ポート	説明
IMAP	143	IMAP（インターネットメッセージアクセスプロトコル）は、メッセージを取り込むのに使用されるプロトコルです。
Mail（SMTP）	25	SMTP（簡易メール転送プロトコル）は、サーバー間でメッセージを送信するためのプロトコルです。
POP3	110	ポストオフィスプロトコルは、電子メールを取り込むのに使用されるプロトコルです。

UNIX サービス

表 19 に、定義済みの UNIX サービスを示します。エントリごとに、サービスの名前、デフォルトポートまたは割り当てられているポート、およびサービスの説明を示しています。

表 19: UNIX サービス

サービス	ポート	説明
FINGER	79	Finger は、ユーザーについての情報を提供する UNIX プログラムです。
UUCP	117	UUCP（Unix-to-Unix Copy Protocol）は、直接シリアル接続またはモデム接続を介して 2 台のコンピュータ間でファイルを転送できる UNIX ユーティリティです。

その他のサービス

表 20 に、定義済みのその他のサービスを示します。エントリごとに、サービス名、デフォルトまたは割り当てられているポート、サービスの説明を示しています。

表 20: その他のサービス

サービス	ポート	説明
CHARGEN	19	CHARGEN（Character Generator Protocol）は、UDP または TCP ベースのデバッギングおよび測定ツールです。
DISCARD	9	DISCARD（Discard Protocol）は、ポート 9 に送信された TCP または UDP データの廃棄プロセスを記述するアプリケーションレイヤープロトコルです。
IDENT	113	IDENT（Identification Protocol）は、TCP クライアント認証に使用される TCP/IP アプリケーションレイヤープロトコルです。

表 20: その他のサービス (続き)

サービス	ポート	説明
LPR	515 リッスン、721 ～ 731 ソース範囲（両者を包む）	LPR（Line Printer Daemon Protocol）は、印刷サービスに使用される TCP ベースのプロトコルです。
RADIUS	1812	RADIUS（リモート認証ダイヤルインユーザーサービス）は、認証と課金のために使用されるサーバープログラムです。
SQLMON	1434（SQL 監視ポート）	SQL 監視（Microsoft）
VNC	5800	VNC（Virtual Network Computing）は、インターネットに接続されている別のコンピュータやモバイルデバイスの表示ややり取りを容易にします。
WHOIS	43	ネットワークディレクトリサービスプロトコルは、ドメイン名をルックアップする方法です。
IPSEC-NAT	ó	IPSEC-NAT は、ISAKMP および ESP パケットのネットワークアドレス変換を許可します。
SCCP	2000	Cisco Station Call Control Protocol は、シグナリング接続制御ポート（SCCP）を使用して、高可用性とフロー制御を提供します。
VOIP	—	VoIP（Voice over IP）サービスグループは、インターネットを介した音声サービスを提供します。H.323 と SIP（Session Initiation Protocol）を含みます。

顧客サービス

定義済みサービスの代わりに、顧客サービスを簡単に作成することができます。各顧客サービスには以下の属性を割り当てることができます。

- 名前
- トランスポートプロトコル
- TCP または UDP を使用するサービスのソースポート番号と宛先ポート番号
- ICMP を使用するサービスのタイプとコード値
- タイムアウト値

ルートシステムで事前に定義しておいた顧客サービスと同じ名前で仮想システム (vsys) に顧客サービスを作成する場合、この仮想システムの顧客サービスは、指定したトランスポートプロトコル (TCP、UDP または ICMP) でデフォルトであるタイムアウト値をとります。ルートシステムにある顧客サービスが独自のタイムアウト値を有しており、仮想システムに作成する同名の顧客サービスについてカスタムタイムアウトをデフォルトと異なる値に定義するには、以下の順番で仮想システムとルートシステムの顧客サービスを作成します。

1. まず仮想システム上に、カスタムタイムアウトを設定した顧客サービスを作成します。
2. 次に、ルートシステム上に別の顧客サービスを作成します。名前は同じにしますが、タイムアウト値は別にします。

次の例では、カスタムサービスの追加、変更、削除を行う方法を説明します。

注 : ScreenOS ネーミング規則 (顧客サービスに対して作成する名前に適用される) については、x ページの「コマンドラインインターフェースの規則」を参照してください。

顧客サービスの追加

顧客サービスをサービスブックに追加するには、次の情報が必要です。

- サービスの名前 : この例では“cust-telnet”
- ソースポート番号の範囲 : 1–65535.
- サービス要求を受信する外部ポート番号 : たとえば 23000–23000.
- サービスが使用しているプロトコル。TCP、UDP、またはその他インターネット規格に定義されたプロトコル。この例では、プロトコルは TCP です。

WebUI

Policy > Policy Elements > Services > Custom > New: 次のように入力してから **OK** をクリックします。

Service Name: cust-telnet
Service Timeout: Custom (**選択**), 30 (**入力**)
Transport Protocol: TCP (**選択**)
Source Port Low: 1
Source Port High: 65535
Destination Port Low: 23000
Destination Port High: 23000

CLI

```
set service cust-telnet protocol tcp src-port 1-65535 dst-port 23000-23000
set service cust-telnet timeout 30
save
```

注 : タイムアウト値は、分単位です。設定しない場合、顧客サービスのタイムアウト値は 180 分です。サービスのタイムアウトを望まない場合は、**never** を入力してください。

顧客サービスの変更

この例では、宛先ポート範囲を 23230 ～ 23230 に変更することによって顧客サービス cust-telnet を変更します。

set service *service_name* **clear** コマンドを使用して、サービスブックからサービスを削除せずに顧客サービスの定義を削除します。

WebUI

Policy > Policy Elements > Services > Custom > Edit (for cust-telnet): 次のように入力してから **OK** をクリックします。

Destination Port Low: 23230
Destination Port High: 23230

CLI

```
set service cust-telnet clear
set service cust-telnet + tcp src-port 1-65535 dst-port 23230-23230
save
```

顧客サービスの削除

この例では、顧客サービス cust-telnet を削除します。

WebUI

Policy > Policy Elements > Services > Custom: cust-telnet の Configure コラムにある **Remove** をクリックします。

CLI

```
unset service cust-telnet
save
```

サービスタイムアウトの設定

サービスについて設定するタイムアウト値によって、セッションタイムアウトが決まります。定義済みサービスまたはカスタムサービスのタイムアウトしきい値が設定できます。デフォルトのサービスタイムアウトを使用したり、カスタムタイムアウトを指定できます。またタイムアウトを使用しないことも可能です。サービスタイムアウトの動作は、仮想システム（vsys）セキュリティドメインでもルートレベルと同じです。

サービスタイムアウトの構成とルックアップ

サービスタイムアウト値は、サービスエントリデータベースと、対応する仮想システム TCP および UDP ポートベースのタイムアウトテーブルに保存されます。サービスタイムアウト値を設定すると、セキュリティデバイスは、これらのテーブルを新しい値で更新します。また、サービスエントリデータベースには、デフォルトのタイムアウト値があり、これは定義済みサービスから取得されます。タイムアウトを設定できますが、デフォルト値は変更できません。

複数のルールエントリを持つサービスは、同じタイムアウト値を共有します。複数のサービスが同じプロトコル宛先ポート範囲を共有する場合、すべてのサービスは、構成された最後のタイムアウト値を共有します。

単一のサービスエントリの場合、サービスタイムアウトのルックアップは、次の順序で実行されます。

1. 設定されている場合、サービスエントリデータベースで指定されているタイムアウト

2. 定義済みサービスで指定されている場合は、サービスエントリデータベースのデフォルトのタイムアウト

3. プロトコルベースのデフォルトのタイムアウトテーブル

表 21: プロトコルベースのデフォルトのタイムアウトテーブル

プロトコル	デフォルトのタイムアウト（分）
TCP	30
UDP	1
ICMP	1
OSPF	1
その他	30

マルチセルポリシー構成で作成された非表示のグループを含むサービスグループ、および定義済みサービス“ANY”（タイムアウトが設定されていない場合）では、サービスタイムのルックアップは次の順序で実行されます。

1. タイムアウトが設定されている場合は、仮想システム TCP および UDP ポートベースのタイムアウトテーブル

2. プロトコルベースのデフォルトのタイムアウトテーブル

考慮事項

タイムアウトを設定する際には、以下の点に注意してください。

- サービスに複数のサービスルールエントリが含まれている場合、すべてのルールエントリは同じタイムアウトを共有します。タイムアウトテーブルは、プロトコル（UDP と TCP の場合。他のプロトコルはデフォルトを使用）に一致する各ルールエントリについて更新されます。サービスタイムアウトは、1 度だけ定義します。たとえば、2 つのルールを持つサービスを作成する場合、以下のコマンドは、両方のルールのタイムアウトを 20 分に設定します。

  ```
  set service test protocol tcp dst-port 1035-1035 timeout 20
  set service test + udp src-port 1-65535 dst-port 1111-1111
  ```

- 複数のサービスに同じプロトコルと重複する宛先ポートが構成されている場合、構成された最新のサービスタイムアウトが、ポートベースのテーブルにある他のタイムアウトを上書きします。例えば、次のように表示されます。

  ```
  set service ftp-1 protocol tcp src 0-65535 dst 2121-2121 timeout 10
  set service telnet-1 protocol tcp src 0-65535 dst 2100-2148 timeout 20
  ```

  この構成では、telnet-1 の宛先ポート番号（2100 ～ 2148）が、ftp-1 の宛先ポート番号（2121）と重複しており、ftp-1 を定義した後に telnet-1 を定義したので、セキュリティデバイスは、サービスグループの宛先ポート 2121 に 20 分のタイムアウトを適用します。

  複数のサービスが、同じプロトコルおよび重複する宛先ポート範囲を使用する場合に、サービスタイムアウトを変更するには、サービスを設定解除してから、新しいタイムアウト値で設定し直す必要があります。これは、再起動時にサービスは、変更時刻ではなく作成時刻に基づいてロードされるためです。

  誤ったタイムアウトがサービスに適用されてしまうのを避けるため、重複する宛先ポート番号を持つサービスを作成しないでください。

- サービスタイムアウトを設定解除すると、サービスエントリデータベースにあるプロトコルベースのデフォルトのタイムアウトが使用され、サービスエントリとポートベースの両方のタイムアウトテーブルが、デフォルト値に更新されます。

  変更したサービスが、他のサービスと重複する宛先ポートを使用している場合、プロトコルベースのデフォルトのタイムアウトは希望する値ではないことがあります。この場合、必要なタイムアウトが有効になるためには、セキュリティデバイスを再起動するか、サービスタイムアウトを設定し直します。

- 定義済みサービスを変更し再起動すると、変更したサービスが、構成での最後のサービスとはならない場合があります。これは、定義済みサービスはカスタムサービスの前にロードされ、再起動すると、カスタムサービスに対する変更が先に行われていた場合でも、定義済みサービスの変更より後に表示されるためです。

  たとえば、以下のサービスを作成します。

  ```
  set service my_service protocol tcp dst-port 179-179 timeout 60
  ```

  そして、定義済みサービス BGP のタイムアウトを以下のように変更します。

  ```
  set service bgp timeout 75
  ```

  セキュリティエントリデータベースに書き込まれたので、BGP サービスは 75 分のタイムアウト値を使用します。ただし、BGP が使用するポート 179 のタイムアウトも、TCP ポートベースのタイムアウトテーブルで 75 に変更されてしまいます。再起動後、BGP サービスは、単一のサービスとして、サービスエントリデータベースから取得する 75 分のタイムアウトを使用し続けます。しかし、ポート 179 の TCP ポートベースのタイムアウトテーブルにある現在のタイムアウトは 60 です。これは、**get service bgp** コマンドを入力して確認できます。

  これは、単一のサービスには影響しません。しかし、サービスグループに BGP または my_service を追加すると、60 分のタイムアウト値が宛先ポート 179 に使用されます。これは、サービスグループのタイムアウトが、ポートベースのタイムアウトテーブル（設定されている場合）から取得されるためです。

  定義済みサービスのタイムアウトを変更した場合に起こる状態を確実に予測するため、たとえば以下のように類似のサービスを作成できます。

  ```
  set service my-bgp protocol tcp dst-port 179-179 timeout 75
  ```

例

次の例では、FTP 定義済みサービスのタイムアウトしきい値を 75 分に変更します。

WebUI

Policy > Policy Elements > Services > Predefined > Edit (FTP): 次のように入力してから **OK** をクリックします。

Service Timeout: Custom (**選択**), 75 (**入力**)

CLI

```
set service FTP timeout 75
save
```

ICMP（インターネット制御メッセージプロトコル）カスタムサービスの削除

ScreenOS は、定義済みサービスまたはカスタムサービスとして、いくつかの ICMP メッセージだけでなく ICMP（インターネット制御メッセージプロトコル）もサポートします。顧客 ICMP サービスを構成する場合は、タイプおよびコードを定義する必要があります。ICMP にはさまざまなメッセージタイプがあります。例えば、次のように表示されます。

タイプ 0 = エコー要求メッセージ

タイプ 3 = 宛先不明メッセージ

注： ICMP のタイプとコードの詳細については RFC 792、*Internet Control Message Protocol* を参照してください。

ICMP メッセージタイプはメッセージコードを持つこともできます。表 22 に示すように、コードによってメッセージに関する詳細な情報を提供できます。

表 22: メッセージの説明

メッセージタイプ	メッセージコード
5 = 転送	0 = ネットワーク (またはサブネット) のデータグラムを転送する
	1 = ホストのデータグラムを転送する
	2 = サービスおよびネットワークのタイプのデータグラムを転送する
	3 = サービスおよびホストのタイプのデータグラムを転送する
11 = 時間超過コード	0 = 転送時の超過生存時間
	1 = フラグメント再アセンブリ時間の超過

ScreenOS は、任意のタイプまたはコードを 0 ～ 255 の範囲内でサポートします。

この例では、トランスポートプロトコルとして ICMP を使用して host-unreachable という名前の顧客サービスを定義します。タイプは 3 (宛先不明) で、コードは 1 (ホスト不明) です。タイムアウト値を 2 分に設定します。

WebUI

Policy > Policy Elements > Services > Custom: 次のように入力してから **OK** をクリックします。

Service Name: host-unreachable
Service Timeout: Custom (**選択**), 2 (**入力**)
Transport Protocol: ICMP (**選択**)
ICMP Type: 3
ICMP Code: 1

CLI

```
set service host-unreachable protocol icmp type 5 code 0
set service host-unreachable timeout 2
save
```

リモートシェル ALG

RSH ALG（リモートシェルアプリケーションレイヤーゲートウェイ）によって、ユーザーはリモートホスト上でシェルコマンドを実行できます。Juniper Networks セキュリティデバイスは、透過モード（L2）、Route モード（L3）、および NAT モードでの RSH サービスをサポートしますが、RSH トラフィックのポート変換はサポートしません。

Sun リモートプロシージャコール (RPC) アプリケーションレイヤーゲートウェイ

Sun リモートプロシージャコールは、オープンネットワークコンピューティングリモートプロシージャコール（ONC RPC）とも呼ばれ、あるホストで実行されているプログラム側から、別のホストで実行されているプログラムにあるプロシージャを呼び出す手段です。RPC サービスの数は多く、ブロードキャストが必要なため、RPC サービスのトランスポートアドレスはそのサービスのプログラム番号とバージョン番号に基づいて動的にネゴシエートされます。RPC プログラムの番号とバージョン番号をトランスポートアドレスにマッピングするために、バインディングプロトコルがいくつか定義されています。

Juniper Networks セキュリティデバイスは、定義済みサービスとして Sun RPC をサポートするため、構成したポリシーに基づいてトラフィックを許可および拒否できます。アプリケーションレイヤーゲートウェイ（ALG）によって、Sun RPC の動的トランスポートアドレスネゴシエーション機構を処理する機能、およびプログラム番号に基づいてファイアウォールポリシーを実施する機能が、セキュリティデバイスに提供されます。RPC 要求をすべて許可または拒否するファイアウォールポリシーや、特定のプログラム番号で RPC 要求を許可または拒否するファイアウォールポリシーを定義できます。また、ALG は受信した要求と送信した要求について、ルートモードと NAT モードをサポートします。

一般的な RPC 呼び出し手順

クライアントがリモートサービスを呼び出す際には、そのサービスのトランスポートアドレスを検索する必要があります。TCP/UDP の場合は、ポート番号を検索します。この場合での一般的な手順は以下のとおりです。

1. クライアントが、リモートマシン上の RPCBIND サービスに GETPORT メッセージを送信します。GETPORT メッセージには、プログラム番号と、呼び出すリモートサービスのバージョン番号とプロシージャ番号が含まれています。

2. RPCBIND サービスがポート番号で応答します。

3. 返されたポート番号を使用して、クライアントがリモートサービスを呼び出します。

4. リモートサービスがクライアントに応答します。

また、クライアントは CALLIT メッセージを使用して、リモートサービスのポート番号を知ることなくそのサービスを直接呼び出すこともできます。この場合、以下の手順に従います。

1. クライアントが、リモートマシン上の RPCBIND サービスに CALLIT メッセージを送信します。CALLIT メッセージには、プログラム番号と、呼び出すリモートサービスのバージョン番号とプロシージャ番号が含まれています。

2. RPCBIND がクライアントのサービスを呼び出します。

3. 呼び出しが成功すると、RCPBIND がクライアントに応答します。応答には、呼び出しの結果とサービスのポート番号が含まれています。

Sun RPC サービスのカスタマイズ

Sun RPC サービスは動的にネゴシエートされたポートを使用するため、固定の TCP/UDP ポートに基づいた正規のサービスオブジェクトを使用してセキュリティポリシーでサービスを許可することができません。代わりに、プログラム番号を使用して Sun RPC サービスオブジェクトを作成する必要があります。たとえば、NFS は 100003 と 100227 の 2 つのプログラム番号を使用します。対応する TCP/UDP ポートは動的です。プログラム番号を許可するには、前記の 2 つの番号が含まれた sun-rpc-nfs サービスオブジェクトを作成します。ALG は、プログラム番号を、動的にネゴシエートされた TCP/UDP ポートにマップして、構成したポリシーに基づいてサービスを許可または拒否します。

この例では、サービスオブジェクト my-sunrpc-nfs を作成して、プログラム ID 100003 と 100227 によって識別された Sun RPC ネットワークファイルシステムを使用します。

WebUI

Policy > Policy Elements > Services > Sun RPC Services > New: 以下を入力して **Apply** をクリックします。

Service Name: my-sunrpc-nfs
Service Timeout: (**選択**)
Program ID Low: 100003
Program ID High: 100003
Program ID Low: 100227
Program ID High: 100227

CLI

```
set service my-sunrpc-nfs protocol sun-rpc program 100003-100003
set service my-sunrpc-nfs + sun-rpc program 100227-100227
save
```

Microsoft リモートプロシージャコール ALG のカスタマイズ

Microsoft リモートプロシージャコール（MS RPC）は、分散コンピューティング環境（DCE）RPC の Microsoft による実装です。MS RPC は Sun RPC (129 ページの「Sun リモートプロシージャコール (RPC) アプリケーションレイヤーゲートウェイ」を参照) と同様に、あるホストで実行されているプログラム側から別のホストで実行されているプログラムにあるプロシージャを呼び出す手段です。RPC サービスの数は多く、ブロードキャストが必要なため、RPC サービスのトランスポートアドレスはそのサービスのプログラムの UUID (Universal Unique Identifier, ユニバーサル固有識別子) に基づいて動的にネゴシエートされます。特定の UUID をトランスポートアドレスにマッピングするために、バインディングプロトコルとしてエンドポイントマッパーが定義されています。

Juniper Networks セキュリティデバイスは、定義済みサービスとして MS RPC をサポートするため、構成したポリシーに基づいてトラフィックを許可および拒否できます。ALG によって、MS RPC の動的トランスポートアドレスネゴシエーション機構を処理する機能、および UUID に基づいてファイアウォールポリシーを実施する機能が、セキュリティデバイスに提供されます。RPC 要求をすべて

許可または拒否するファイアウォールポリシーや、特定の UUID 番号で RPC 要求を許可または拒否するファイアウォールポリシーを定義できます。また、ALG は受信した要求と送信した要求について、ルートモードと NAT モードをサポートします。

MS RPC サービスは動的にネゴシエートされたポートを使用するため、固定 TCP/UDP ポートに基づいた正規のサービスオブジェクトを使用してセキュリティポリシーでサービスを許可することができません。代わりに、UUID を使用して MS RPC サービスオブジェクトを作成する必要があります。たとえば Microsoft Exchange インフォメーションストアサービスでは、以下の 4 つの UUID が使用されます。

- 0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde
- 1453c42c-0fa6-11d2-a910-00c04f990f3b
- 10f24e8e-0fa6-11d2-a910-00c04f990f3b
- 1544f5e0-613c-11d1-93df-00c04fd7bd09

対応する TCP/UDP ポートは動的です。UUID を許可するには、前記の 4 つの UUID が含まれた ms-exchange-info-store サービスオブジェクトを作成します。ALG が、前記の 4 つの UUID に基づいて、動的にネゴシエートされた TCP/UDP ポートにプログラム番号をマップして、構成したポリシーに基づいてサービスを許可または拒否します。

この例では、サービスオブジェクト my-ex-info-store を作成します。このオブジェクトには、Microsoft Exchange インフォメーションストアサービスの UUID が含まれます。

WebUI

Policy > Policy Elements > Services > MS RPC: 以下を入力して **Apply** をクリックします。

```
Service Name: my-ex-info-store
UUID: 0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde
UUID: 1453c42c-0fa6-11d2-a910-00c04f990f3b
UUID: 10f24e8e-0fa6-11d2-a910-00c04f990f3b
UUID: 1544f5e0-613c-11d1-93df-00c04fd7bd09
```

CLI

```
set service my-ex-info-store protocol ms-rpc uuid
    0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde
set service my-ex-info-store + ms-rpc uuid
    1453c42c-0fa6-11d2-a910-00c04f990f3b
set service my-ex-info-store + ms-rpc uuid
    10f24e8e-0fa6-11d2-a910-00c04f990f3b
set service my-ex-info-store + ms-rpc uuid
    1544f5e0-613c-11d1-93df-00c04fd7bd09
save
```

リアルタイムストリーミングプロトコル（RTSP）アプリケーション レイヤーゲートウェイ

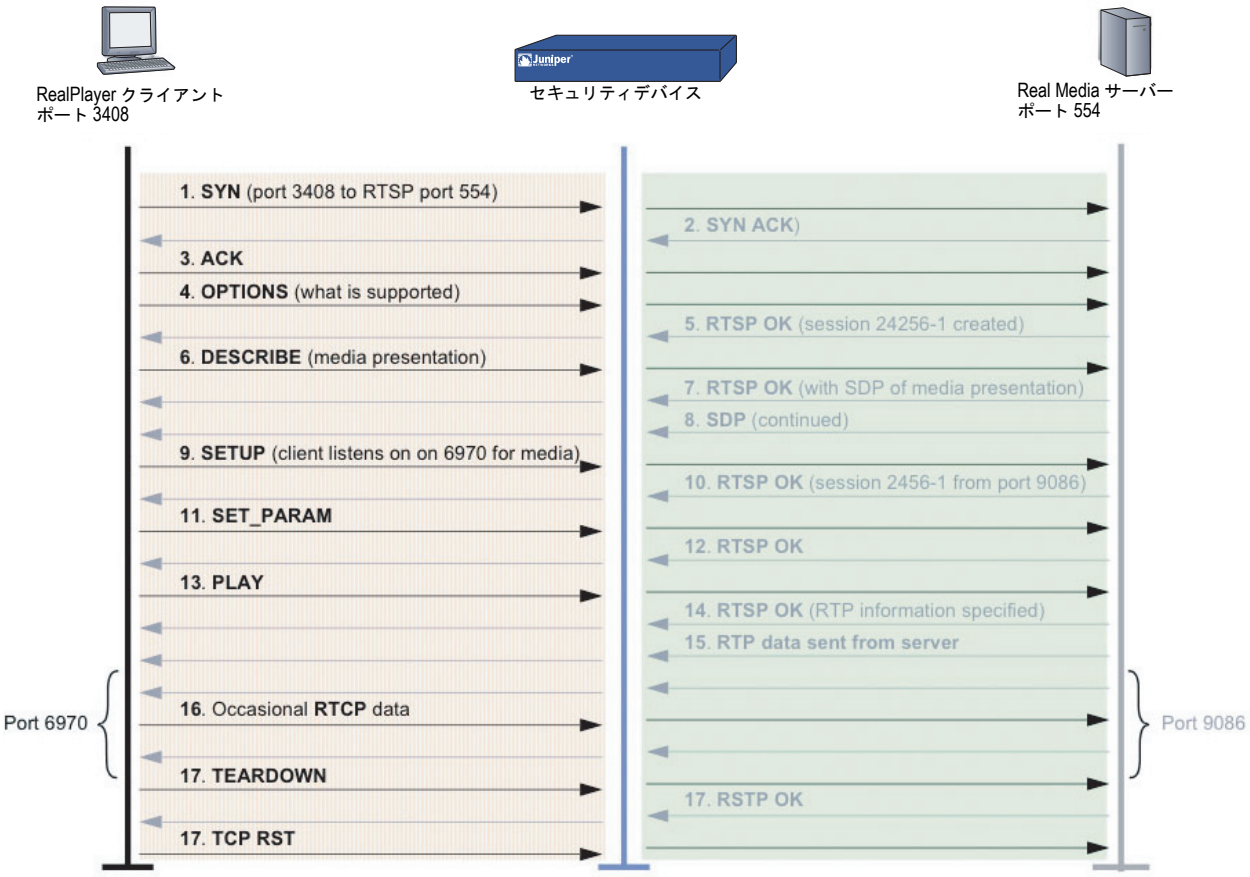
リアルタイムストリーミングプロトコル（RTSP）とは、1 つ以上の同期化された音声やビデオなどのマルチメディアストリームの配信を制御する際に使用される、アプリケーションレイヤープロトコルです。RTSP にはデータストリーム自体を配信する機能はありますが（制御ストリームで連続メディアストリームをインタリーブする）、RTSP の一般的な用途は、マルチメディアサーバーのネットワークリモート制御です。RTSP は配信チャネル (UDP、マルチキャスト UDP、TCP など) を選択し、RTP (リアルタイムプロトコル) に基づいた配信機構を選択する手段として設計されました。また、RTSP は SDP（セッション記述プロトコル）を使用して、1 つ以上のサーバーから配信されるストリームから成るプレゼンテーションの統合制御、および 1 つのサーバーから配信される複数ストリームから成るプレゼンテーションの非統合制御を行うためにクライアントに情報を提供する手段となります。データのソースはライブフィードや保存されたクリップです。

Juniper Networks セキュリティデバイスは、サービスとして RTSP をサポートするため、構成したポリシーに基づいて RTSP トラフィックを許可および拒否できます。RTSP は、制御接続の確立中にパケットペイロードに入れられて伝送される動的に割り当てられたポート番号を使用します。そのため ALG が必要です。ALG は、動的に割り当てられたポート番号を追跡し、それに従ってピンホールをオープンします。NAT モードでは、ALG は必要に応じて IP アドレスとポートを変換します。セキュリティデバイスは、Route モードと透過モードで RTSP をサポートします。また、インターフェースベースかつポリシーベースの NAT モードでも RTSP をサポートします。

133 ページの図 49 は、一般的な RTSP セッションを示しています。クライアントがセッションを起動して (たとえば、ユーザーが RealPlayer の Play ボタンをクリックする)、RTSP サーバーとの TCP 接続をポート 554 で確立します。クライアントは次に、OPTIONS メッセージ (メッセージはメソッドともいいます) を送信してサーバーがサポートする音声機能やビデオ機能を検索します。サーバーは、サーバーの名前とバージョンおよびセッション識別子（例 : 24256-1）を指定して OPTIONS メッセージに応答します。（メソッドの詳細については、**6**-14 ページの「SIP 要求方法」および RFC 2326 のセクション 11 を参照してください。）

次にクライアントが、指定した実際のメディアファイルの URL が含まれている DESCRIBE メッセージを送信します。サーバーが、SDP 形式を使用したメディア記述を付けて DESCRIBE メッセージに応答します。その次に、クライアント側から SETUP メッセージが送信されます。SETUP メッセージでは、RTP/RTCP や RDT などのストリームメディアについてクライアントが受け入れ可能なトランスポート機構が指定され、メディアを受信するポートが指定されます。NAT を使用する場合、RTSP ALG はポートを追跡して、必要に応じて変換します。サーバー側で SETUP メソッドに応答してトランスポートプロトコルを 1 つ選択してから、クライアントとサーバーの両方がメディアを転送する機構について同意します。最後にクライアントが PLAY メソッドを送信して、サーバーからクライアントにメディアのストリーミングを開始します。

図 49: 一般的な RTSP セッション



RTSP 要求メソッド

134 ページの表 23 に、リソース（メディアオブジェクト）上で実行できるメソッド、情報が流れる方向、メソッドの重要度（必須、推奨、オプション）を示します。プレゼンテーションが参照する情報には、ネットワークアドレス、コード化などがあります。さらには、完全なメディアフィードとしてクライアントに提供される 1 つ以上のストリームから成るセットについての内容などがあります。ストリームとは単一のメディアインスタンスであり、たとえば音声やビデオなど、セッション内のソースが作成するすべてのパケットのことです。

表 23: RTSP 要求メソッド

メソッド	方向	オブジェクト	要件	説明
OPTIONS	クライアントからサーバー	プレゼンテーション、ストリーム	クライアントからサーバーは必須	クライアント側で、サーバーがサポートする音声やビデオの機能についてサーバーを要求します。また、サーバーの名前やバージョン、セッション ID も要求します。
	サーバーからクライアントへ	プレゼンテーション、ストリーム	サーバーからクライアントはオプション	
DESCRIBE	クライアントからサーバー	プレゼンテーション、ストリーム	推奨	クロックレートやカラーテーブル、その他トランスポート独立情報などのメディア初期化情報を交換するため、クライアント側にとってメディアストリームの再生に必要なメソッドです。通常、クライアント側からは要求するファイルの URL を送信します。サーバー側からは、SDP 形式でのメディア説明を付けて応答します。
ANNOUNCE	クライアントからサーバー	プレゼンテーション、ストリーム	オプション	クライアント側では、このメソッドを使用して要求 URL によって識別されたプレゼンテーションまたはメディアオブジェクトの記述をポストします。サーバー側では、このメソッドを使用してリアルタイムでセッション記述を更新します。
	サーバーからクライアントへ	プレゼンテーション、ストリーム		
SETUP	クライアントからサーバー	ストリーム	必須	クライアント側で受け入れ可能なトランスポート機構を指定します。メディアストリームを受信するポートや、トランスポートプロトコルなどが指定されます。
GET_PARAMETER	クライアントからサーバー	プレゼンテーション、ストリーム	オプション	URL で指定されたプレゼンテーションやストリームのパラメータ値を取得します。このメソッドはエンティティボディを使用せずに、クライアントやサーバーの起動状態をテストします。Ping も起動状態のテストに使用できます。
	サーバーからクライアントへ			
SET_PARAMETER	クライアントからサーバー	プレゼンテーション、ストリーム	オプション	クライアントはこのメソッドを使用して、URL で指定されたプレゼンテーションやストリームのパラメータ値を設定します。ファイアウォールの条件により、トランスポートパラメータの設定には使用できません。
	サーバーからクライアントへ			
PLAY	クライアントからサーバー	プレゼンテーション、ストリーム	必須	SETUP で指定したトランスポート機構を使用してのデータ送信をサーバーに指示します。クライアントは、すべての SETUP 要求が成功するまで PLAY 要求を発行しません。サーバー側では PLAY 要求は順番にキューに入ります。アクティブの PLAY 要求が完了するまでは新しい PLAY 要求の実行は遅延されます。PLAY 要求には指定した範囲が含まれますが、含まれない場合もあります。指定した範囲には、世界協定時刻 (UTC) で指定された再生開始の時間パラメータが含まれる場合があります。このパラメータは、さまざまなソースからのストリーム同期化にも使用できます。

表 23: RTSP 要求メソッド (続き)

メソッド	方向	オブジェクト	要件	説明
PAUSE	クライアントからサーバー	プレゼンテーション、ストリーム	推奨	アクティブなプレゼンテーションの配信を一時的に停止します。要求 URL によって特定のストリームが指定される場合、特に音声ストリームの場合はミュートに相当します。再生や記録が再開される際にはトラックの同期化が維持されますが、SETUP にあるタイムアウトパラメータで指定された時間 PAUSE が継続されると、サーバー側でセッションがクローズされる可能性があります。PAUSE 要求によって、キューにある PLAY 要求はすべて破棄されます。
RECORD	クライアントからサーバー	プレゼンテーション、ストリーム	オプション	プレゼンテーションの記述で定義されたメディアの範囲の記録を開始します。UTC タイムスタンプに開始時間と終了時間が示されています。そうでない場合は、サーバー側でプレゼンテーションの記述にある開始時間と終了時間を使用します。
REDIRECT	サーバーからクライアントへ	プレゼンテーション、ストリーム	オプション	別のサーバーへの接続が必要であることをクライアントに通知します。このメソッドには場所の情報が含まれ、その新しい URL についての範囲パラメータが含まれる場合もあります。この URL についてクライアントがメディアの受信を継続するには、クライアント側から現在のセッションについての TEARDOWN 要求と、新しいセッションについての SETUP 要求を発行する必要があります。
TEARDOWN	クライアントからサーバー	プレゼンテーション、ストリーム	必須	所定の URL についてのストリームの配信を停止して、ストリームの関連リソースを解放します。すべてのトランスポートパラメータがセッション記述で定義されていない場合には、セッションの再生を再開する前に SETUP 要求を発行する必要があります。

RTSP ステータスコード

RTSP はステータスコードを使用して、クライアントやサーバーの要求についての情報を提供します。ステータスコードには、マシン可読の 3 桁の結果コードと、人間側で可読のリーズンフレーズが含まれています。リーズンフレーズを表示するかどうかは、クライアント側で選択できます。ステータスコードを表 24 に示します。

表 24: RSTP ステータスコード

コード	番号	説明
通知	100 ～ 199	要求が受信され、処理中である
成功	200 ～ 299	アクションの受信、解釈、承認が正常に行われた
転送	300 ～ 399	要求を完了するにはさらにアクションを起こす必要がある
クライアントエラー	400 ～ 499	要求が不正な構文を含み、実行できない
サーバーエラー	500 ～ 599	サーバーが明らかに有効な要求の実行に失敗した

表 25 に、RTSP 1.0 で定義されるすべてのステータスコードと、推奨されるリーズンフレーズを示します。リーズンフレーズは、プロトコルの動作に影響を与えずに改変または再定義できます。

表 25: RTSP 1.0 ステータスコード

ステータスコード	リーズンフレーズ	ステータスコード	リーズンフレーズ
100	Continue（継続）	414	Request-URI Too Large（Request-URL が長すぎる）
200	OK	415	Unsupported Media Type（サポートされていないメディアタイプ）
201	Created（作成された）	451	Unsupported Media Type（サポートされていないメディアタイプ）
250	Low on Storage Space（保存スペースが少ない）	452	Conference Not Found（会議が見つからない）
300	Multiple Choices（複数の選択肢がある）	453	Not Enough Bandwidth（帯域不足）
301	Moved Permanently（恒久的に移動した）	454	Session Not Found（セッションが見つからない）
303	See Other（他を参照）	455	Method Not Valid in This State（このステータスではメソッドが無効）
304	Not Modified（未変更）	456	Header Field Not Valid for Resource（リソースのヘッダーフィールドが無効）
305	Use Proxy（プロキシを使用せよ）	457	Invalid Range（無効な範囲）
400	Bad Request（不正な要求）	458	Parameter is Read-Only（パラメータが読取専用）
401	Unauthorized（認可されていない）	459	Aggregate operation not allowed（統合動作が許可されていない）
402	Payment Required（料金支払いが必要）	460	Only aggregate operation allowed（統合動作のみが許可されている）
403	Forbidden（禁止）	461	Unsupported transport（サポートされていないトランスポート）
404	Not Found（見つからない）	462	Destination unreachable（宛先不明）
405	Method Not Allowed（メソッドが許可されていない）	500	Internal Server Error（サーバー内部エラー）
406	Not Acceptable（受け入れ不能）	501	Not Implemented（実装されていない）
407	Proxy Authentication Required（プロキシ認証が必要）	502	Bad Gateway（不正なゲートウェイ）
408	Request Time-out（要求がタイムアウトした）	503	Service Unavailable（サービスを利用できない）
410	Gone（リソースがもう存在しない）	504	Gateway Time-out（ゲートウェイがタイムアウトした）

表 25: RTSP 1.0 ステータスコード (続き)

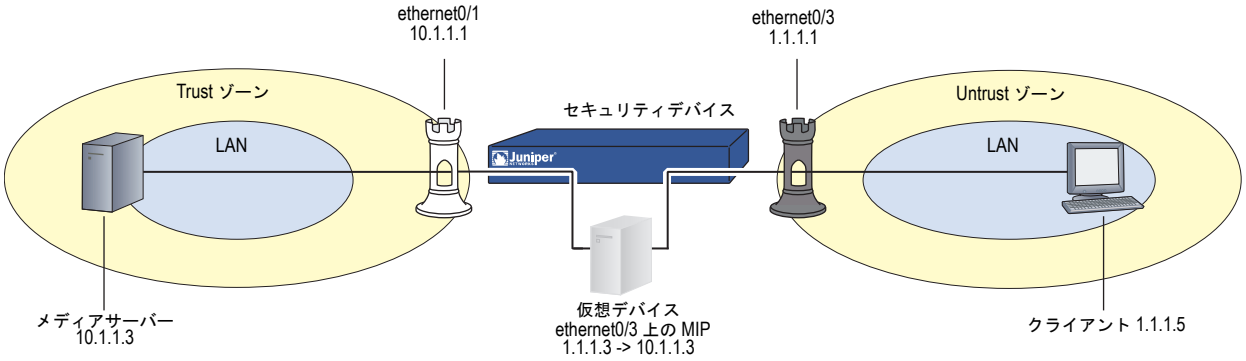
ステータスコード	リーズンフレーズ	ステータスコード	リーズンフレーズ
411	Length Required（長さが必要）	505	RTSP Version not supported（サポートされていない RTSP バージョン）
412	Precondition Failed（前提条件が失敗）	551	Option not supported（オプションがサポートされていない）
413	Request Entity Too Large（要求のエンティティが大きすぎる）		

注 : ステータスコードの詳細な定義については RFC 2326、*Real Time Streaming Protocol (RTSP)* を参照してください。

プライベートドメイン内でのメディアサーバーの構成

この例では、メディアサーバーが Trust ゾーンに、クライアントが Untrust ゾーンにあります。ethernet0/3 インターフェース上の MIP を Trust ゾーンに配置してから、ポリシーを作成して、Untrust ゾーン内のクライアントから Trust ゾーン内のメディアサーバーへの RTSP トラフィックを許可します。

図 50: RTSP プライベートドメイン



WebUI

1. **インターフェース**

   Network > Interfaces > Edit (ethernet0/1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   Manage IP: 10.1.1.2

   Network > Interfaces > Edit (ethernet0/3): 以下を入力して **Apply** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24
   Manage IP: 1.1.1.2

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: Media_server
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.3/24
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: クライアント
   IP Address/Domain Name:
   IP/Netmask: (選択), 1.1.1.5/24
   Zone: Untrust

3. **MIP**
   Network > Interfaces > Edit (ethernet0/3) > MIP > New: 次のように入力してから **OK** をクリックします。

   Mapped IP: 1.1.1.3
   Host IP Address: 10.1.1.5

4. **ポリシー**
   Policy > Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), client
   Destination Address:
   Address Book Entry: (選択), MIP(1.1.1.3)
   Service: RTSP
   Action: Permit

CLI

1. **インターフェース**
   set interface ethernet0/1 trust
   set interface ethernet0/1 ip 10.1.1.1
   set interface ethernet0/3 untrust
   set interface ethernet0/3 ip 1.1.1.1

2. **アドレス**
   set address trust media_server 10.1.1.3/24
   set address untrust client 1.1.1.5

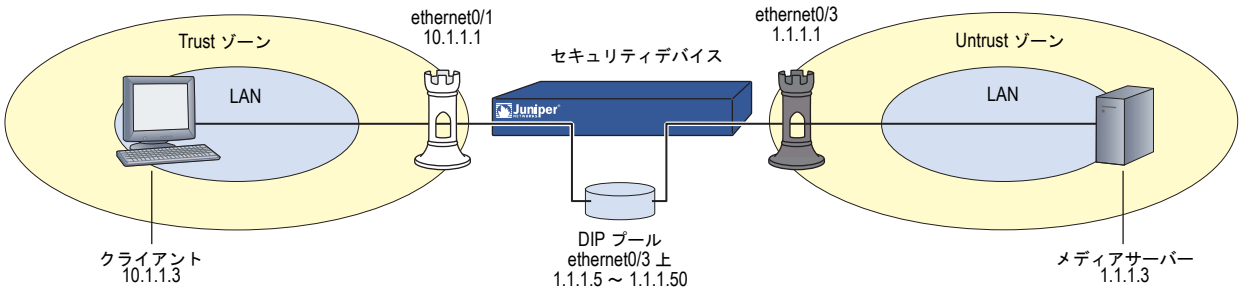
3. **MIP**
   set interface ethernet0/3 mip (1.1.1.3) host 10.1.1.3

4. **ポリシー**
   set policy from untrust to trust client mip(1.1.1.3) rtsp permit
   save

パブリックドメイン内でのメディアサーバーの構成

この例では、メディアサーバーが Untrust ゾーンに、クライアントが Trust ゾーンにあります。ethernet0/3 インターフェースに DIP プールを配置すると、メディアサーバーが Untrust ゾーンからクライアントへ応答する際に NAT が機能します。次にポリシーを作成して、Trust ゾーンから Untrust ゾーンへの RTSP トラフィックを許可します。

図 51: RTSP パブリックドメイン



WebUI

1. **インターフェース**

   Network > Interfaces > Edit (ethernet0/1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   Manage IP: 10.1.1.2

   Network > Interfaces > Edit (ethernet0/3): 以下を入力して **Apply** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24
   Manage IP: 1.1.1.2

2. **アドレス**

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: client
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.3/24
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: Media_server
   IP Address/Domain Name:
   IP/Netmask: (選択), 1.1.1.3/24
   Zone: Untrust

3. **DIP プール**
   Network > Interfaces > Edit (ethernet0/3) > DIP > New: 次のように入力してから **OK** をクリックします。

   ID: 5
   IP Address Range: (選択) 1.1.1.5 ~ 1.1.1.50
   Port Translation: (選択)

4. **ポリシー**
   Policy > Policies > (From: Trust, To: Untrust) > New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry (選択): client
   Destination Address:
   Address Book Entry (選択): media_server
   Service: RTSP
   Action: Permit

   > Advanced: 次のように入力してから **OK** をクリックします。

   NAT:
   Source Translation: (選択)
   (DIP on): 5 (1.1.1.5-1.1.1.50)/port-xlate

CLI

1. **インターフェース**
   set interface ethernet0/1 zone trust
   set interface ethernet0/1 ip 10.1.1.1
   set interface ethernet0/3 zone untrust
   set interface ethernet0/3 ip 1.1.1.1/24

2. **アドレス**
   set address trust client ip 10.1.1.3/24
   set address untrust media_server ip 1.1.1.3/24

3. **DIP プール**
   set interface ethernet0/3 dip 5 1.1.5 1.1.1.50

4. **ポリシー**
   set policy from trust to untrust client media_server rtsp nat dip 5 permit
   save

サービスグループ

サービスグループとは、1 つの名前で収集したサービスのセットです。いくつかのサービスを含むグループを作成すると、グループレベルのサービスをポリシーに適用できるため、管理が容易となります。

ScreenOS サービスグループオプションは、次の機能を備えています。

- 各サービスブックエントリは、1 つまたは複数のグループで参照できます。
- 各サービスグループには、定義済みおよびユーザ定義サービスブックエントリを含めることができます。

サービスグループは次の制限を受けます。

- サービスグループは、サービスと同じ名前をもつことはできません。したがって“FTP”というサービス名を持つ場合、“FTP”というサービスグループ名をもつことはできません。
- サービスグループがポリシーで参照される場合、そのグループを編集することはできますが、ポリシーでのグループへの参照を削除してからでないと削除することはできません。
- 顧客サービスブックエントリがサービスブックから削除されると、そのエントリは参照されているすべてのグループからも削除されます。
- 1 つのサービスグループに他のサービスグループをメンバーとして含めることはできません。
- 包括的サービス用語“ANY”を、グループに追加することはできません。
- サービスは 1 度につき 1 つのグループの部分になれます。

サービスグループの作成

この例では、IKE、FTP、および LDAP サービスを含む、grp1 という名前のサービスグループを作成します。

WebUI

Policy > Policy Elements > Services > Groups > New: 以下のグループ名を入力して、以下のサービスを移動し、**OK** をクリックします。

Group Name: grp1

IKE を選択し、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

FTP を選択し、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

LDAP を選択し、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

CLI

```
set group service grp1
set group service grp1 add ike
set group service grp1 add ftp
set group service grp1 add ldap
save
```

注 : 存在しないサービスグループにサービスを追加しようとすると、セキュリティデバイスがそのグループを作成します。また、他のグループを参照するグループが、そのグループ自身を参照リストに含まないことを確認してください。

サービスグループを変更する

この例では、141 ページの「サービスグループの作成」で作成した grp1 という名前のサービスグループのメンバーを変更します。IKE、FTP、および LDAP サービスを削除し、HTTP、FINGER、および IMAP を追加します。

WebUI

Policy > Policy Elements > Services > Groups > Edit (grp1): 次のサービスを移動してから **OK** をクリックします。

IKE を選択し、> > ボタンを使用して、Group Members 列から Available Members 列に移動します。

FTP を選択し、> > ボタンを使用して、Group Members 列から Available Members 列に移動します。

LDAP を選択し、> > ボタンを使用して、Group Members 列から Available Members 列に移動します。

HTTP を選択し、< < ボタンを使って Available Members 列から Group Members 列にサービスを移動します。

Finger を選択し、< < ボタンを使用して Available Members 列から Group Members 列にサービスを移動します。

IMAP を選択し、< < ボタンを使用して Available Members 列から Group Members 列にサービスを移動します。

CLI

```
unset group service grp1 clear
set group service grp1 add http
set group service grp1 add finger
set group service grp1 add imap
save
```

サービスグループを削除する

この例では、波 rp1・という名前のサービスグループを削除します。

WebUI

Policy > Policy Elements > Services > Groups: **Remove** (grp1) をクリックします。

CLI

```
unset group service grp1
save
```

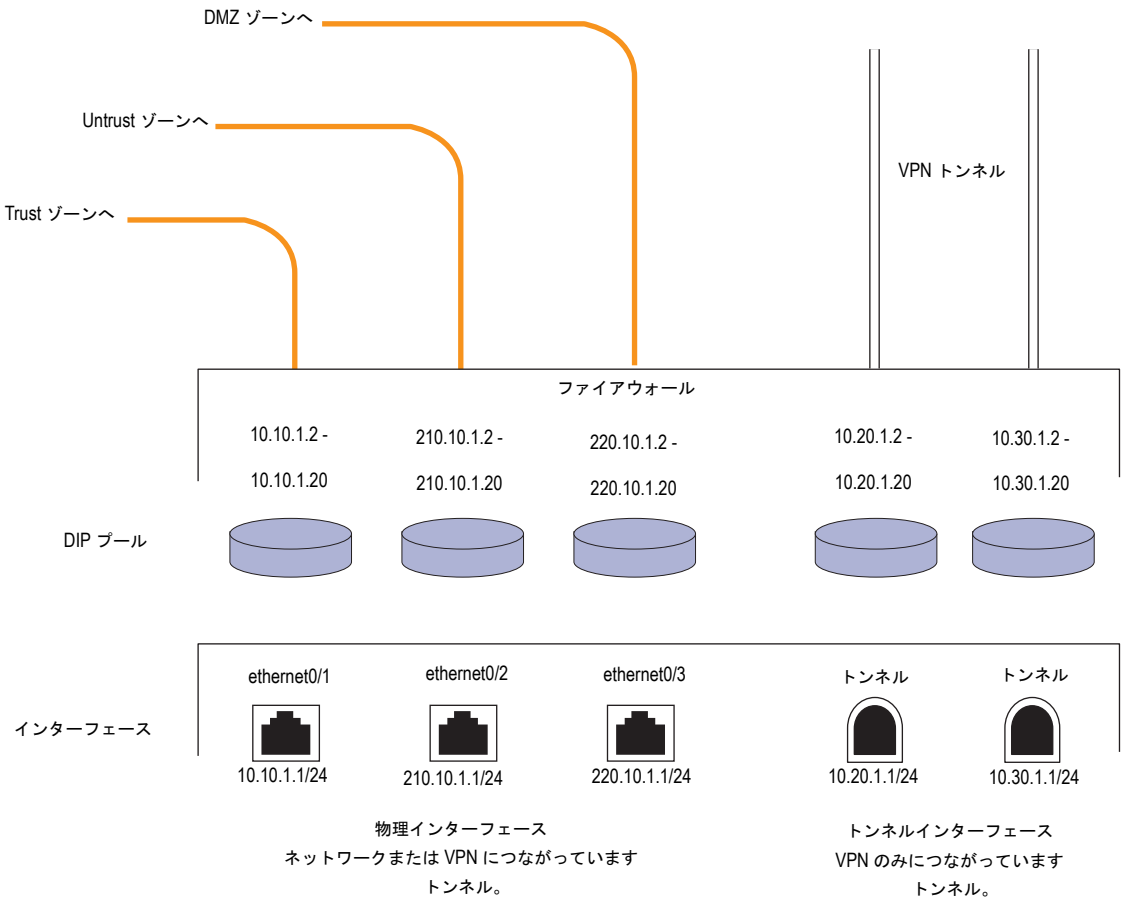
注： グループからメンバーをすべて削除しても、セキュリティデバイスはそのグループを自動的には削除しません。

動的 IP プール

動的 IP（DIP）プールとは、セキュリティデバイスが、IP パケットヘッダーのソース IP アドレス（NAT-src）上でネットワークアドレス変換を行う際に、動的または決定論的に選択できる IP アドレスの範囲です。(決定論的ソースアドレス変換については、8-19 ページの「NAT-Src - DIP プールからアドレスシフティングによりアドレス取得」を参照してください)。DIP プールのアドレスの範囲がインターフェース IP アドレスと同じサブネット内にある場合、プールは、インターフェース IP アドレス、ルーター IP アドレス、およびそのサブネットに存在する可能性がある MIP (マップ IP) または VIP (仮想 IP) のアドレスを除外する必要があります。アドレスの範囲が拡張インターフェースのサブネット内にある場合は、プールは拡張インターフェース IP アドレスを除外する必要があります。

DIP (動的 IP) プールにリンクできるインターフェースは、ネットワークトラフィックや VPN トラフィックの物理インターフェースとサブインターフェース、そして VPN トンネルトのみのトンネルインターフェースの 3 種類があります。

図 52: DIP インターフェース



ポートアドレス変換

ポートアドレス変換（PAT）を使用すると、同じ IP アドレス、つまり割り当てられたポート番号のリストを維持するセキュリティデバイスを、複数のホストが共有し、どのセッションがどのホストに属するかを識別できます。PAT を使用可能にすると、最大 64,500 台のホストで 1 つの IP アドレスを共有できます。

NetBEUI (NetBIOS Extended User Interface) や WINS (Windows Internet Naming Service) などのように、特定のポート番号が必要で、PAT が適用されていないと正しく機能しないアプリケーションもあります。そのようなアプリケーションでは、DIP を適用する際には PAT を実行しない (固定ポートを使用する) ように指定できます。固定ポート DIP では、セキュリティデバイスは、オリジナルホストの IP アドレスをハッシュし、自身のホストハッシュテーブルに保存するので、セキュリティデバイスは、正しいセッションを各ホストに関連付けることができます。

PAT の DIP Pool を作成する

この例では、ローカルサイトのユーザーがリモートサイトの FTP サーバーに到達できるように VPN トンネルを作成します。ただし、両サイトの内部ネットワークは、同じ秘密アドレススペース 10.10.1.0/24 を使用します。このアドレスの重複問題を解決するには、ローカルのセキュリティデバイス上の Untrust ゾーンにトンネルインターフェースを作成し、IP アドレス 10.10.1.1/24 を割り当てて、そのアドレスを、アドレス範囲が 10.10.1.2 ～ 10.10.1.2 でポートアドレス変換が使用可能な DIP プールに関連付けます。

また、リモートサイトの管理者は、10.20.2.1/24 などの中立アドレススペース内の IP アドレスを持つトンネルインターフェースを作成し、その FTP サーバーに、10.1.1.5 をホストする 10.20.2.5 のように、MIP (マップ IP) アドレスを設定する必要があります。

注 : この例には、トンネルインターフェースとそれに関する DIP プールの構成のみが含まれます。この方法に必要な構成手順を示す完全な例は、5-137 ページの「アドレスがオーバーラップする VPN サイト」を参照してください。

WebUI

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

```
Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Fixed IP: ( 選択 )
        IP Address/Netmask: 10.10.1.1/24
```

Network > Interfaces > Edit (tunnel.1) > DIP > New: 次のように入力してから **OK** をクリックします。

```
ID: 5
IP Address Range: 10.10.1.2 ~ 10.10.1.2
Port Translation: ( 選択 )
In the same subnet as the interface IP or its secondary IPs: ( 選択 )
```

注 : 続けて利用可能な表示された ID 番号を使用するか、または異なる番号を入力することができます。

CLI

```
set interface tunnel.1 zone untrust-tun
set interface tunnel.1 ip 10.10.1.1/24
set interface tunnel.1 dip 5 10.10.1.2 10.10.1.2
save
```

注 : PAT はデフォルトで使用可能になっているため、使用可能にするための引数はありません。上記で定義されたものと同じ DIP プールを PAT なしで (つまり、固定ポートナンバーで) 作成するには、次のように行います。

(WebUI) Network > Interfaces > Edit (tunnel.1) > DIP > New: Port Translation チェックボックスをクリアして **OK** をクリックします。

(CLI) set interface tunnel.1 dip 5 10.10.1.2 10.10.1.2 fix-port

DIP プールの変更

この例では、既存の DIP プール (ID 5) のアドレス範囲を 10.20.1.2 - 10.20.1.2 から 10.20.1.2 - 10.20.1.10 に変更します。この DIP プールは tunnel.1 と関連付けられています。CLI を介して DIP プール範囲を変更するには、まず既存の DIP プールを削除 (または設定を解除) してから、新規プールを作成する必要があります。

注 : この特定の DIP プールを使用するポリシーはありません。ポリシーが DIP プールを使用している場合、DIP プールを変更するには、その前にポリシーを削除するか、または DIP プールを使用しないように変更する必要があります。

WebUI

Network > Interfaces > Edit (tunnel.1) > DIP > Edit (ID 5): 次のように入力してから **OK** をクリックします。

IP Address Range: 10.20.1.2 ~ 10.20.1.10

CLI

```
unset interface tunnel.1 dip 5
set interface tunnel.1 dip 5 10.20.1.2 10.20.1.10
save
```

スティッキー DIP アドレス

ホストが NAT（ネットワークアドレス変換）を必要とするポリシーに適合するいくつかのセッションを開始し、DIP（動的 IP）プールからポート変換が可能なアドレスを割り当てられると、セキュリティデバイスは各セッションに対して異なるソース IP アドレスを割り当てます。そのようなランダムなアドレスの割り当ては、各セッションに同じソース IP アドレスを必要とする複数のセッションを作成するサービスでは問題となることがあります。

注： ポート変換を行わない DIP プールの場合は、セキュリティデバイスは、同じホストからのすべての同時セッションに対して 1 つの IP アドレスを割り当てます。

たとえば、AIM (AOL インスタントメッセージ) クライアントの使用時には、複数セッションに同じ IP アドレスを持つことが重要です。ログオン時に 1 つのセッションを作成し、チャットするごとに別のセッションを作成します。AIM サーバーが新しいチャットが認証済みユーザーに属することを確認するには、ログインセッションのソース IP アドレスをチャットセッションのソース IP アドレスに適合させる必要があります。適合しない場合 (おそらく、NAT プロセス中に DIP プールからランダムに割り当てられたため)、AIM サーバーはチャットセッションを拒否します。

セキュリティデバイスが、複数の同時セッションについて同じ IP アドレスを DIP プールからホストに割り当てるように、CLI コマンド **set dip sticky** を入力して、「スティッキー」DIP アドレス機能を使用可能できます。

異なるサブネットでの DIP の使用

アウトバウンドファイアウォールトラフィックのソース IP アドレスを、egress インターフェースのアドレスと異なるサブネットのアドレスに変換する必要がある場合、拡張インターフェースオプションを使用できます。このオプションによって、セカンド IP アドレスおよびそれに付随する DIP プールを、異なるサブネットにあるインターフェース上に移植できます。それによって、ポリシー単位ベースで NAT を使用可能にして、変換用の拡張インターフェース上に作られた DIP プールを指定することができます。

この例では、2 つの支社が中央オフィスへのリース回線を持っています。中央オフィスは支社に対して、中央オフィスが割り当てた許可 IP アドレスのみを使用するよう要求します。ただし、支社はインターネットトラフィック用の ISP とは異なる IP アドレスを受け取ります。中央オフィスと通信するために、拡張インターフェースオプションを使用して、中央オフィスに送信したパケット内のソース IP アドレスを許可アドレスに変換するように、各支社のセキュリティデバイスを構成します。支社 A と支社 B の許可 IP アドレスおよび割り当て IP アドレスは次のとおりです。

表 26: 支社の許可 IP アドレス

	割り当て IP アドレス (ISP より) Untrust ゾーン物理インターフェースに使用	許可 IP アドレス (中央オフィスより) Untrust ゾーン拡張インターフェース DIP に使用
支社 A	195.1.1.1/24	211.10.1.1/24
支社 B	201.1.1.1/24	211.20.1.1/24

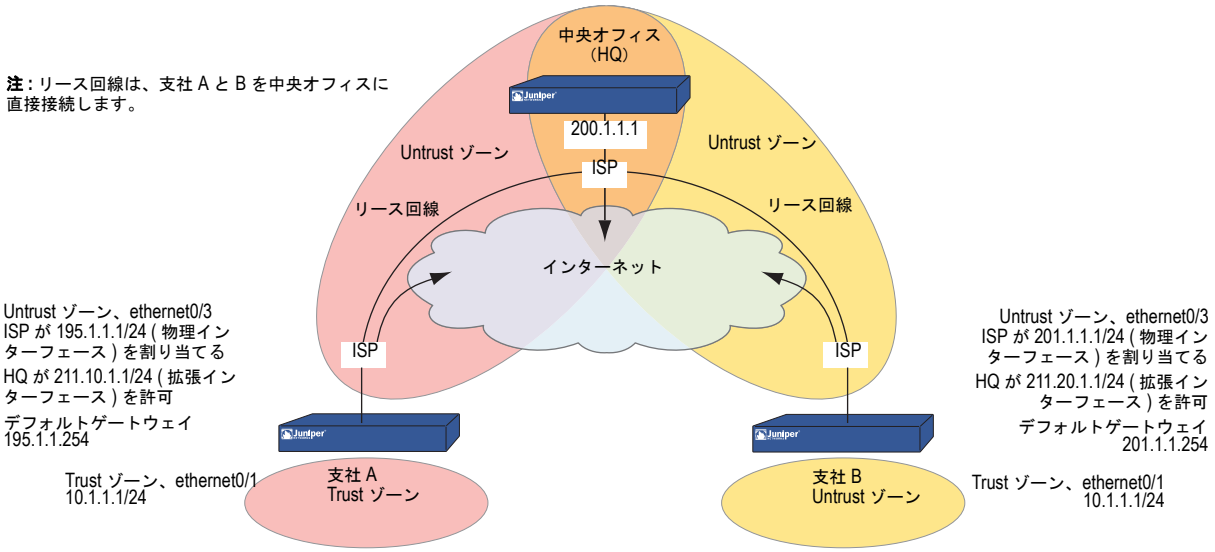
両方のサイトのセキュリティデバイスは Trust ゾーンと Untrust ゾーンを持ちます。セキュリティゾーンはすべて trust-vr ルーティングドメインにあります。ethernet0/1 を Trust ゾーンにバインドして、IP アドレス 10.1.1.1/24 を割り当てます。ethernet0/3 を Untrust ゾーンにバインドして、ISP によって割り当てられた IP アドレスを割り当てます。支社 A には 195.1.1.1/24、支社 B には 201.1.1.1/24 を割り当てます。次に、許可 IP アドレスを含む DIP プールで ethernet0/3 上に拡張インターフェースを作成します。

- 支社 A: 拡張インターフェース IP 211.10.1.10/24、DIP プール 211.10.1.1 - 211.10.1.1、PAT 使用可能

- 支社 B: 拡張インターフェース IP 211.20.1.10/24、DIP プール 211.20.1.1 - 211.20.1.1、PAT 使用可能

NAT モードで Trust ゾーンインターフェースを設定します。中央オフィスに送られるトラフィックを除いて、すべてのアウトバウンドトラフィックのソースアドレスとして Untrust ゾーンインターフェース IP アドレスが使用されます。ソースアドレスを拡張インターフェースの DIP プールにあるアドレスに変換するポリシーを中央オフィスに対して構成します (DIP プール ID 番号は 5 です。(DIP プール ID 番号は 5 です。IP アドレスが 1 つ含まれており、ポートアドレス変換で最高 64,500 ホストのセッションを処理できます。) 中央オフィスがインバウンドトラフィックに使用する MIP アドレスは 200.1.1.1 で、これは各セキュリティデバイス上の Untrust ゾーンアドレス帳に “HQ” と入力します。

図 53: 別のサブネットの DIP



注 : 各 ISP は、リース回線の終端にあるサイトを宛先とするトラフィックのルートで、リース回線を使用するための設定を行う必要があります。ISP は、ローカルのセキュリティデバイスから受信するその他すべてのトラフィックをインターネットにルーティングします。

WebUI (支社 A)

1. インターフェース

Network > Interfaces > Edit (ethernet0/1): 次のように入力してから **OK** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24
Interface Mode: NAT

Network > Interfaces > Edit (ethernet0/3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 195.1.1.1/24
Interface Mode: Route

Network > Interfaces > Edit (for ethernet0/3) > DIP > New: 次のように入力してから **OK** をクリックします。

ID: 5
IP Address Range: 211.10.1.1 ~ 211.10.1.1
　　Port Translation: (**選択**)
Extended IP/Netmask: 211.10.1.10/255.255.255.0

2. **アドレス**
Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: HQ
IP Address/Domain Name:
　　IP/Netmask: (**選択**), 200.1.1.1/32
Zone: Untrust

3. **ルート**
Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
　　Interface: ethernet0/3
　　Gateway IP address: 195.1.1.254

4. **ポリシー**
Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
　　Address Book Entry: (**選択**), Any
Destination Address:
　　Address Book Entry: (**選択**), Any
Service: Any
Action: Permit

Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
　　Address Book Entry: (**選択**), Any
Destination Address:
　　Address Book Entry: (**選択**), HQ
Service: Any
Action: Permit
Position at Top: (**選択**)

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: (**選択**)
　(DIP on): 5 (211.10.1.1-211.10.1.1)/X-late

WebUI (支社 B)

1. **インターフェース**
   Network > Interfaces > Edit (ethernet0/1): 次のように入力してから **OK** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet0/3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 201.1.1.1/24
   Interface Mode: Route

   Network > Interfaces > Edit (ethernet0/3) > DIP > New: 次のように入力してから **OK** をクリックします。

   ID: 5
   IP Address Range: 211.20.1.1 ~ 211.20.1.1
   Port Translation: (選択)
   Extended IP/Netmask: 211.20.1.10/255.255.255.0

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: HQ
   IP Address/Domain Name:
   IP/Netmask: (選択), 200.1.1.1/32
   Zone: Untrust

3. **ルート**
   Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選択)
   Interface: ethernet0/3
   Gateway IP address: 201.1.1.254

4. **ポリシー**
   Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Any
   Destination Address:
   Address Book Entry: (選択), Any
   Service: Any
   Action: Permit

Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), HQ
Service: Any
Action: Permit
Position at Top: (**選択**)

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: (**選択**)
DIP On: (**選択**), 5 (211.20.1.1-211.20.1.1)/X-late

CLI (支社 A)

1. **インターフェース**
```
set interface ethernet0/1 zone trust
set interface ethernet0/1 ip 10.1.1.1/24
set interface ethernet0/1 nat
set interface ethernet0/3 zone untrust
set interface ethernet0/3 ip 195.1.1.1/24
set interface ethernet0/3 route
set interface ethernet0/3 ext ip 211.10.1.10 255.255.255.0 dip 5 211.10.1.1
```
2. **アドレス**
```
set address untrust hq 200.1.1.1/32
```
3. **ルート**
```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/3 gateway 195.1.1.254
```
4. **ポリシー**
```
set policy from trust to untrust any any any permit
set policy top from trust to untrust any hq any nat src dip 5 permit
save
```

CLI (支社 B)

1. **インターフェース**
```
set interface ethernet0/1 zone trust
set interface ethernet0/1 ip 10.1.1.1/24
set interface ethernet0/1 nat
set interface ethernet0/3 zone untrust
set interface ethernet0/3 ip 201.1.1.1/24
set interface ethernet0/3 route
set interface ethernet0/3 ext ip 211.20.1.10 255.255.255.0 dip 5 211.20.1.1
```
2. **アドレス**
```
set address untrust hq 200.1.1.1/32
```
3. **ルート**
```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/3 gateway 201.1.1.254
```
4. **ポリシー**
```
set policy from trust to untrust any any any permit
set policy top from trust to untrust any hq any nat src dip 5 permit
save
```

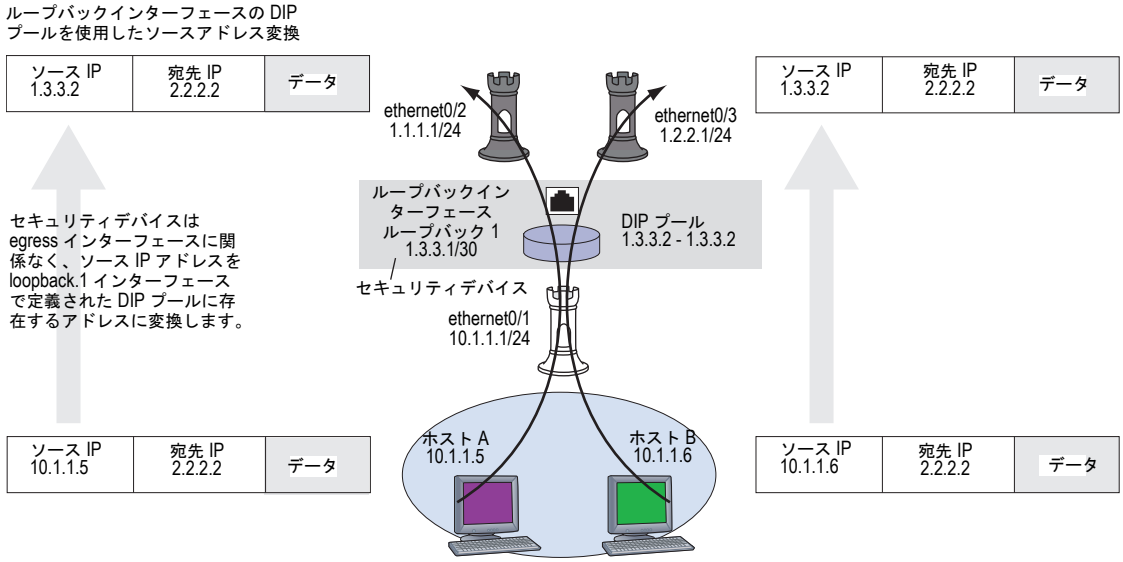
ループバックインターフェースでの DIP の使用

ループバックインターフェースとは、このインターフェースを持つデバイスが作動している限り、常に作動状態となる論理インターフェースです。ソースアドレス変換を実行する際に、関連するループバックインターフェースグループに属するインターフェースのグループがアクセスできるように、ループバックインターフェース上に DIP (動的 IP) アドレスのプールを作成することができます。セキュリティデバイスがそのような DIP プールから引き出すアドレスは、ループバックインターフェース IP アドレスと同じサブネット内に存在し、メンバーインターフェースのいずれのサブネットにも存在しません。（DIP プールのアドレスは、インターフェース IP アドレスと重複できず、またループバックインターフェースでも定義されたどの MIP アドレスとも重複できません。）

注 : ループバックインターフェースについては、58 ページの「ループバックインターフェース」を参照してください。

DIP プールをループバックインターフェースに配置する主な用途は、ソースアドレスを同じアドレスまたはアドレス範囲に変換することですが、パケットによって使用する egress インターフェースが異なることがあります。

図 54: ループバック DIP



この例では、セキュリティデバイスは異なる ISP (インターネットサービスプロバイダー) から、2 つの Untrust ゾーンインターフェース用の次の IP アドレスを受信します。ISP-1 および ISP-2

- ethernet0/2, 1.1.1.1/24, ISP-1
- ethernet0/3, 1.2.2.1/24, ISP-2

Untrust ゾーンにこれらのインターフェースをバインドし、上記の IP アドレスを割り当てます。さらに、Trust ゾーンに ethernet0/1 をバインドし、IP アドレス 10.1.1.1/24 を割り当てます。

セキュリティデバイスで、Trust ゾーンから Untrust ゾーンのリモートオフィスへ向かうアウトバウンドトラフィックのソースアドレスを変換することにします。変換されたアドレスは同じ IP アドレス (1.3.3.2) となる必要があります。これは、リモートオフィスがこの IP アドレスからのみのインバウンドトラフィックを許可するポリシーを持つためです。2 つの ISP がデバイスに割り当てたアドレスに加えて、既に公開 IP アドレス 1.3.3.1 および 1.3.3.2 を取得しており、これらのアドレスを使用していることは両方の ISP に通知済みです。

IP アドレス 1.3.3.1/30 を持つループバックインターフェース loopback.1 を構成して、そのインターフェースに 1.3.3.2 - 1.3.3.2 の DIP プールを構成します。DIP プールの ID 番号は 10 です。次に、ethernet0/1 と ethernet0/2 を loopback.1 のループバックグループのメンバーにします。

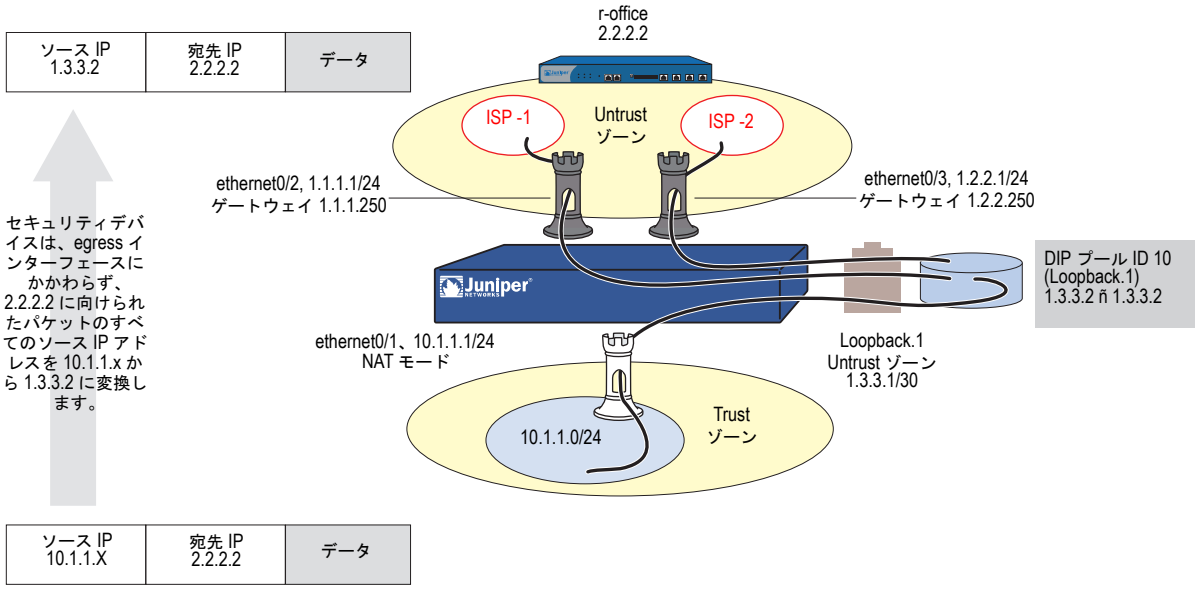
IP アドレスが 2.2.2.2/32 で r-office という名前のリモートオフィスのアドレスを定義します。さらに、ethernet0/1 と ethernet0/2 インターフェース用にそれぞれ、ISP-1 と ISP-2 のルーターをポイントするデフォルトルートを定義します。

アウトバウンドトラフィックが使用する 2 つのゲートウェイへのルートを定義します。他のルートよりも優先するルートはないため、ルートにメトリックは一切含めません。アウトバウンドトラフィックはいずれかのルートに従うと考えられます。

注： ルート優先度を指示するには、メトリックを両方のルートに含めて、優先するルートに高いメトリック、すなわち 1 に近い方の値を与えます。

最後に、NAT-Src（ソースネットワークアドレス変換）を用いるポリシーを作成し、トラフィックをリモートオフィスにアウトバウンドします。ポリシーは DIP プール ID 10 を参照します。

図 55: ループバック DIP ポリシー



WebUI

1. インターフェース

Network > Interfaces > New Loopback IF: 次のように入力してから **OK** をクリックします。

Interface Name: loopback.1
Zone: Untrust (trust-vr)
IP Address/Netmask: 1.3.3.1/30

Network > Interfaces > Edit (ethernet0/1): 次のように入力してから **OK** をクリックします。

As member of loopback group: loopback.1
Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24
Interface Mode: NAT

Network > Interfaces > Edit (ethernet0/2): 次のように入力してから **OK** をクリックします。

As member of loopback group: loopback.1
Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24
Interface Mode: Route

Network > Interfaces > Edit (ethernet0/3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.2.2.1/24
Interface Mode: Route

2. DIP プール

Network > Interfaces > Edit (lookback.1) > DIP > New: 次のように入力してから **OK** をクリックします。

ID: 5
IP Address Range: 1.3.3.2 ~ 1.3.3.2
Port Translation: (選択)

3. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: r-office
IP Address/Domain Name:
IP/Netmask: (選択), 2.2.2.2/32
Zone: Untrust

4. **ルート**
   Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (**選択**)
   Interface: ethernet0/2
   Gateway IP address: 1.1.1.250

   Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (**選択**)
   Interface: ethernet0/3
   Gateway IP address: 1.2.2.250

5. **ポリシー**
   Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), Any
   Destination Address:
   Address Book Entry: (**選択**), r-office
   Service: Any
   Action: Permit

   > Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

   NAT:
   Source Translation: (**選択**)
   DIP On: (**選択**), 10 (1.3.3.2-1.3.3.2)/port-xlate

CLI

1. **インターフェース**

```
set interface loopback.1 zone untrust
set interface loopback.1 ip 1.3.3.1/30
set interface ethernet0/1 zone trust
set interface ethernet0/1 ip 10.1.1.1/24
set interface ethernet0/1 nat
set interface ethernet0/2 zone untrust
set interface ethernet0/2 ip 1.1.1.1/24
set interface ethernet0/2 loopback-group loopback.1
set interface ethernet0/3 zone untrust
set interface ethernet0/3 ip 1.2.2.1/24
set interface ethernet0/3 loopback-group loopback.1
```

2. **DIP プール**

```
set interface loopback.1 dip 10 1.3.3.2 1.3.3.2
```

3. **アドレス**

```
set address untrust r-office 2.2.2.2/32
```

4. **ルート**

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/2 gateway 1.1.1.250
set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/3 gateway 1.2.2.250
```

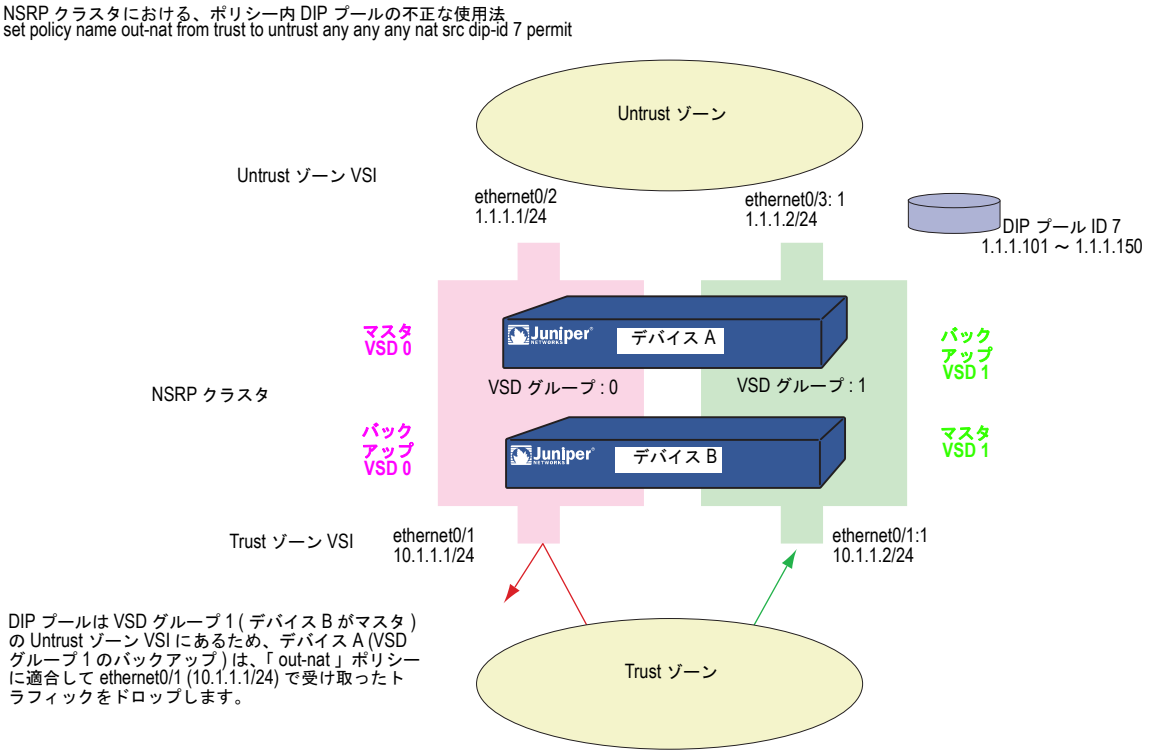
5. **ポリシー**

```
set policy from trust to untrust any r-office any nat src dip-id 10 permit
save
```

DIP グループを作成する

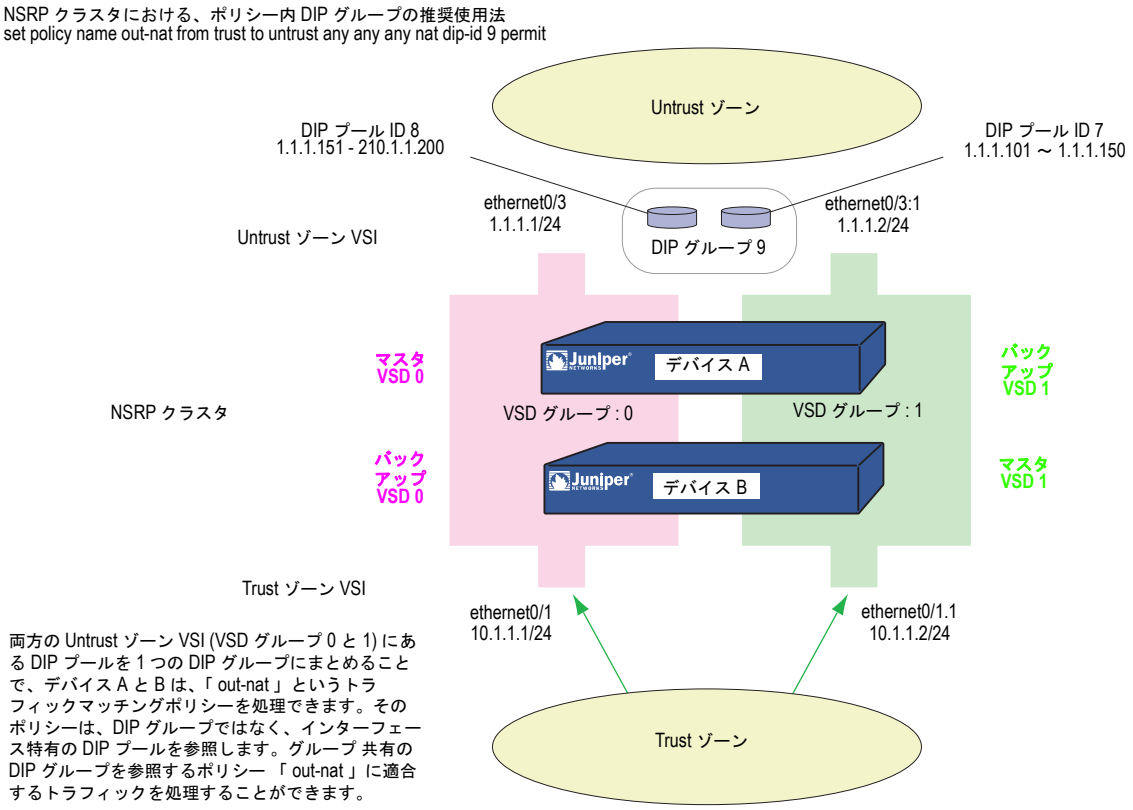
2 つのセキュリティデバイスを 1 つの冗長クラスタにグループ化し、アクティブ / アクティブ構成で HA（高可用性）を提供する場合、両方のデバイスは同じ構成を共有し、トラフィックを同時に処理します。1 つの VSI に配置された動的 IP（DIP プールを使用して、NAT（ネットワークアドレス変換）を実行するポリシーを定義すると、問題が発生することがあります。この VSI は、VSI がバインドされた VSD グループの 1 次デバイスとして機能するセキュリティデバイス上でのみアクティブなため、他のセキュリティデバイス（VSD グループのバックアップとして機能する）に送信されたトラフィックは、その DIP プールを使用できずドロップされます。

図 56: 1 つの VSI を持つ NAT での DIP 問題



この問題を解決するには、2 つの DIP プール (各 VSD グループの Untrust ゾーン VSI に 1 つずつ) を作成してこれらを 1 つの DIP グループにまとめ、ポリシーで参照します。ポリシーが DIP グループを指定する場合でも、各 VSI は自身の VSD プールを使用します。

図 57: 1 つの DIP グループ内に 2 つの DIP プールを作成



注 : セキュリティデバイスの HA 用の設定に関する詳細については、“ 第 11 部 : 高可用性 ” を参照してください。

この例では、アクティブ / アクティブ HA ペアである 2 つのセキュリティデバイス（デバイス A と B）で、NAT サービスを提供します。

2 つの DIP プール、つまり ethernet0/3 の DIP 5 (1.1.1.20 ～ 1.1.1.29) および ethernet0/3:1 の DIP 6 (1.1.1.30 ～ 1.1.1.39) を作成します。そしてそれらを結合して DIP 7 として識別される DIP グループとし、これをポリシーで参照します。

VSD グループ 0 と 1 の VSI は次のとおりです。

- Untrust ゾーン VSI ethernet0/3 1.1.1.1/24 (VSD グループ 0)
- Untrust ゾーン VSI ethernet0/3:1 1.1.1.1/24 (VSD グループ 1)
- Trust ゾーン VSI ethernet0/1:1 10.1.1.1/24 (VSD グループ 0)
- Trust ゾーン VSI ethernet0/1:1 10.1.1.1/24 (VSD グループ 1)

この例では、すでに NSRP クラスタにデバイス A と B を設定しており、VSD グループ 1 を作成して（VSD グループ 0 は、NSRP クラスタにデバイスを入れた際に ScreenOS 側で自動的に作成されます)、上記のインターフェースを構成していると仮定しています。（NSRP に セキュリティデバイスを設定する詳細について、“ 第 11 部 : 高可用性 ” を参照してください。）

WebUI

1. **DIP プール**
   Network > Interfaces > Edit (ethernet0/3) > DIP > New: 次のように入力してから **OK** をクリックします。

   ID: 5
   IP Address Range: 1.1.1.20 ñ 1.1.1.29
   Port Translation: (**選択**)

   Network > Interfaces > Edit (ethernet0/3:1) > DIP > New: 次のように入力してから **OK** をクリックします。

   ID: 6
   IP Address Range: 1.1.1.30 ñ 1.1.1.39
   Port Translation: (**選択**)

注 : 現行バージョンでは、DIP グループの定義は CLI からのみで可能です。

---

2. **ポリシー**
   Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), Any
   Destination Address:
   Address Book Entry: (**選択**), Any
   Service: Any
   Action: Permit

   > Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

   NAT:
   Source Translation: (**選択**)
   DIP On: (**選択**), 7

CLI

1. **DIP プール**
   set interface ethernet0/3 dip 5 1.1.1.20 1.1.1.29
   set interface ethernet0/3:1 dip 6 1.1.1.30 1.1.1.39

2. **DIP グループ**
   set dip group 7 member 5
   set dip group 7 member 6

3. **ポリシー**
   set policy from trust to untrust any any any nat src dip-id 7 permit
   save

反復スケジュールの設定

スケジュールとは構成可能なオブジェクトであり、1 つまたは複数のポリシーと関連付けてポリシーがいつ有効となるかを定義できます。スケジュールを適用すると、ネットワークトラフィックフローの制御およびネットワークセキュリティを強化できます。

スケジュールを定義する場合、次のパラメータに対する値を入力してください。

- **Schedule Name:** Policy Configuration ダイアログボックスの Schedule ドロップダウンリストに表示される名前。スケジュールを確認しやすいようにわかりやすい名前を選択してください。名前は一意であることが必要で、19 文字に制限されます。
- **Comment:** 任意の追加情報。
- **Recurring:** スケジュールを 1 週間ごとに繰り返すには、これを使用可能にします。

  Start and End Times: 開始時間と終了時間の両方を設定する必要があります。同じ日に 2 つまでの期間を指定できます。
- **Once:** そのスケジュールを 1 度だけ開始し終了するには、このパラメータを使用可能にします。

  mm/dd/yyyy hh:mm: 開始日時と終了日時の両方を入力する必要があります。

この例では、Tom という名前の短期社員が、仕事の後に私的な目的でその企業のインターネットアクセスを使用しています。勤務時間外のスケジュールを作成し、標準勤務時間外にその社員のコンピュータ (10.10.4.5/32) からのアウトバウンド TCP/IP トラフィックを拒否するポリシーに、このスケジュールを関連付けます。

WebUI

1. **スケジュール**
   Policy > Policy Elements > Schedules > New: 次のように入力してから **OK** をクリックします。

   Schedule Name: After Hours
   Comment: For non-business hours
   Recurring: (**選択**)
   Period 1:

Weekday	Start Time	End Time
Sunday	00:00	23:59
Monday	00:00	06:00
Tuesday	00:00	06:00
Wednesday	00:00	06:00
Thursday	00:00	06:00
Friday	00:00	06:00
Saturday	00:00	23:59

Period 2:

Weekday	Start Time	End Time
Sunday	17:00	23:59
Monday	17:00	23:59
Tuesday	17:00	23:59
Wednesday	17:00	23:59
Thursday	17:00	23:59
Friday	17:00	23:59
Saturday	17:00	23:59

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Tom
Comment: Temp
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.5/32
Zone: Trust

3. ポリシー

Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Name: No Net
Source Address:
Address Book Entry: (選択), Tom
Destination Address:
Address Book Entry: (選択), Any
Service: HTTP
Action: Deny
Schedule: After Hours

CLI

1. スケジュール

set schedule “after hours” recurrent sunday start 00:00 stop 23:59
set schedule “after hours” recurrent monday start 00:00 stop 06:00 start 17:00 stop 23:59
set schedule “after hours” recurrent tuesday start 00:00 stop 06:00 start 17:00 stop 23:59
set schedule “after hours” recurrent wednesday start 00:00 stop 06:00 start 17:00 stop 23:59
set schedule “after hours” recurrent thursday start 00:00 stop 06:00 start 17:00 stop 23:59
set schedule “after hours” recurrent friday start 00:00 stop 06:00 start 17:00 stop 23:59
set schedule “after hours” recurrent saturday start 00:00 stop 23:59 comment “for non-business hours”

2. アドレス

set address trust tom 10.1.1.5/32 “temp”

3. ポリシー

set policy from trust to untrust tom any http deny schedule “after hours”
save

第 6 章

ポリシー

デフォルトでは、セキュリティデバイスは Untrust ゾーン内のトラフィックを除いて、セキュリティゾーン間のすべてのトラフィック（ゾーン間トラフィック）を拒否し、同じゾーンにバインドされたインターフェース間のすべてのトラフィック（ゾーン内トラフィック）を許可します。特定のゾーン間トラフィックに対してセキュリティデバイスを通過することを許可するには、デフォルトよりも優先されるゾーン間ポリシーを作成する必要があります。同様に、特定のゾーン内トラフィックがセキュリティデバイスを通過しないようにするには、ゾーン内ポリシーを作成する必要があります。

本章では、ポリシーの実行内容と、ポリシーを形成するさまざまな要素がどのように関連しているかを説明します。本章のセクションは、以下のようになります。

- 162 ページの「基本要素」
- 163 ページの「3 種類のポリシー」
- 165 ページの「ポリシーセットリスト」
- 166 ページの「定義済みポリシー」
- 177 ページの「適用されるポリシー」

注： セキュリティデバイスのマルチキャストルーティングを構成する場合には、マルチキャストポリシーの構成が必要な場合があります。マルチキャストポリシーについては **7**-157 ページの「マルチキャストポリシー」を参照してください。

基本要素

ポリシーは、2 点間で、一方向に指定されたタイプのトラフィックの許可、拒否、またはトンネルを行います。トラフィック (または 「サービス」) のタイプ、2 つの端点の位置、呼び出されたアクションが、ポリシーの基本要素を形成します。その他のコンポーネントが存在することが可能な場合でも、表 27 に示す要素が必要になります。これらの要素が組み合わされてポリシーの核が形成されます。

表 27: 基本となるポリシー要素

要素	解説
Direction	2 つのセキュリティゾーン (ソースゾーンから宛先ゾーン) 間のトラフィックの方向
Source Address	トラフィックを発するアドレス
Destination Address	トラフィックの送り先となるアドレス
Service	送信されるトラフィックのタイプ
Action	上記の 4 つの基準（deny、permit、reject、または tunnel）を満たすトラフィックの受信時にセキュリティデバイスが実行するアクション **注記 :** 「トンネル」アクション（VPN または L2TP トンネル）- 暗黙的な permit (許可) の概念が含まれています。

例えば、以下の CLI コマンドで指定されるポリシーは、Trust ゾーン内の任意のアドレスから DMZ ゾーンの 都 erver1î と名づけられた FTP サーバーへの FTP トラフィックを許可します。

```
set policy from trust to untrust any server1 ftp permit
```

- **方向** : **from trust to untrust** (Trust ゾーンから Untrust ゾーンへ)
- **Source Address**: **any** (Trust ゾーン内の任意のアドレス。any は、ゾーン内の任意のアドレスに適用される定義済みアドレスを表します)
- **Destination Address**: **server1** (Untrust ゾーンのアドレス帳内のユーザー定義アドレス)
- **サービス** : **ftp** (ファイル転送プロトコル)
- **アクション** : **permit** (セキュリティデバイスは、このトラフィックにファイアウォールを通過することを許可します)

3 種類のポリシー

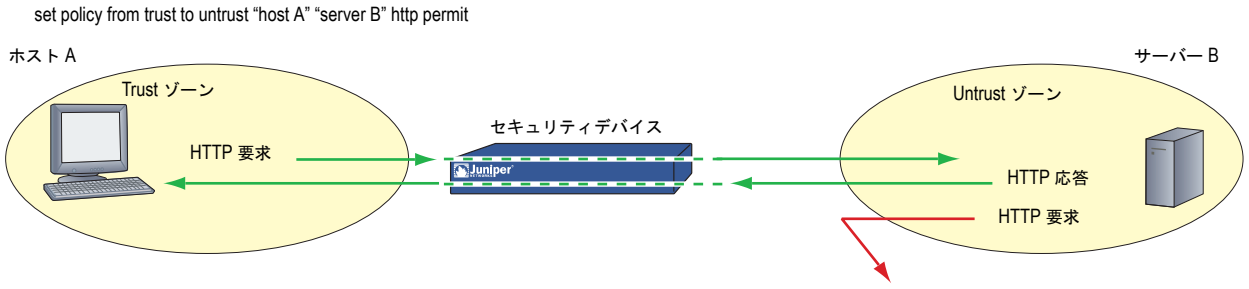
以下の 3 種類のポリシーによって、トラフィックのフローを制御することができます。

- **ゾーン間ポリシー**－セキュリティゾーンから別のセキュリティゾーンに到達することを許可するトラフィックの種類を制御することができます。
- **ゾーン内ポリシー**－同一ゾーン内にバインドされているインターフェースを通過することを許可するトラフィックの種類を制御することもできます。
- **グローバルポリシー**－セキュリティゾーンに関係なく、アドレス間のトラフィックを制御することができます。

地域間ポリシー

地域間ポリシーは、セキュリティゾーン間のトラフィック制御を提供します。地域間ポリシーを設定すると、ゾーンから別のゾーンへのトラフィックを許可 (permit)、拒否 (deny)、トンネル (tunnel) することができます。パケット状態監視のテクニックを使用して、セキュリティデバイスは、サービス要求に対する応答を許可できるように、アクティブな TCP セッションとアクティブな UDP「擬似」セッションのテーブルを維持しています。たとえば、Trust ゾーンのホスト A から Untrust ゾーンのホスト B への HTTP 要求を許可するポリシーがある場合、セキュリティデバイスはサーバー B からホスト A への HTTP 応答を受信すると、セキュリティデバイスは受信したパケットをテーブルと照らし合わせてチェックします。承認済みの HTTP 要求への応答となるパケットを見つけると、セキュリティデバイスは、パケットが Untrust ゾーンのサーバー B からファイアウォールを通過して Trust ゾーンのホスト A に到達することを許可します。(ホスト A によって開始されたトラフィックへの応答だけでなく) サーバー B によって開始されたホスト A へのトラフィックを許可するには、Untrust ゾーンのサーバー B から Trust ゾーンのホスト A までの 2 つ目のポリシーを作成する必要があります。

図 58: ゾーン間ポリシー

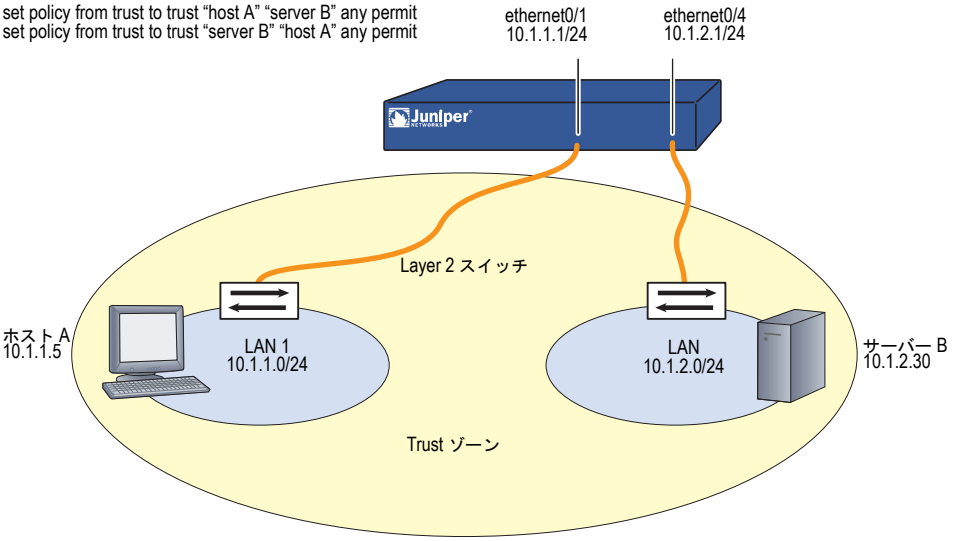


注 : サーバー B からの HTTP 要求を許可するポリシーは存在しないので、セキュリティデバイスはこの要求を拒否します。

ゾーン内ポリシー

ゾーン内ポリシーは、同一のセキュリティゾーンにバインドされたインターフェース間のトラフィック制御を提供します。ソースアドレスと宛先アドレスは同一セキュリティゾーン内にありますが、セキュリティデバイス上の異なるインターフェースを介して到達します。地域間ポリシーのように、ゾーン内ポリシーでも一方向に流れるトラフィックを制御します。データパスのどちらか一方の端点で開始されるトラフィックを許可するには、2 つのポリシー (それぞれの方向に 1 つずつ) を作成する必要があります。

図 59: ゾーン内ポリシー



ゾーン内ポリシーは、インターフェースレベル (**set interface** *interface* **nat**) に設定されている場合、VPN トンネルまたはソース NAT (Network Address Translation, ネットワークアドレス変換機能) をサポートしません。ただし、ポリシーベースの NAT-Src および NAT-Dst はサポートされます。また、ポリシーが宛先アドレスとしてマップ IP (MIP) を参照するときにも宛先アドレス変換機能をサポートします。(NAT-Src、NAT-Dst、MIP の詳細については、“ 第 8 部 : アドレス変換 ” を参照してください。

グローバルポリシー

地域間ポリシーやゾーン内ポリシーとは異なり、グローバルポリシーは特定のソースゾーンと宛先ゾーンを参照することはありません。グローバルポリシーは、ユーザー定義 Global ゾーンアドレス、または定義済み Global ゾーンアドレス “Any” を参照します。これらのアドレスは、複数のセキュリティゾーンにまたがることもできます。たとえば、複数のゾーンとのアクセスを提供しようとする場合は、Global ゾーンアドレスを “any” として指定してグローバルポリシーを作成することができます。これらのアドレス は、すべてのゾーンのすべてのアドレスを包含するものです。

注 : グローバルポリシーはこのリリースの時点では、ネットワークアドレス変換機能 (NAT-Src)、VPN トンネル、透過モードをサポートしていません。ただし、MIP または VIP をグローバルポリシーの宛先アドレスとして指定できます。

ポリシーセットリスト

セキュリティデバイスは、ゾーン間ポリシー、ゾーン内ポリシー、およびグローバルポリシーの各ポリシーに 1 つずつ異なるポリシーセットリストを維持しています。

セキュリティデバイスが新しいセッションを開始するパケットを受信すると、デバイスは ingress インターフェースに着目し、インターフェースがバインドされているソースゾーンを認識します。次に、セキュリティデバイスはルートルックアップを実行して egress インターフェースを調べ、そのインターフェースがバインドされている宛先ゾーンを決定します。セキュリティデバイスは、ソースゾーンと宛先ゾーンを使用してポリシールックアップを実行し、以下の順序でポリシー群リストを調べることができます。

1. ソースゾーンと宛先ゾーンが異なる場合、セキュリティデバイスはゾーン間ポリシーセットリストでポリシールックアップを実行します。

   (または)

   ソースゾーンと宛先ゾーンが同一の場合は、セキュリティデバイスはゾーン内ポリシー群リストでポリシールックアップを実行します。

2. ゾーン間またはゾーン内ポリシールックアップを実行して一致するポリシーが見つからない場合、セキュリティデバイスは次にグローバルポリシー群リストを調べて一致するポリシーを検索します。

3. ゾーン間ポリシーとグローバルポリシーのルックアップを実行し、一致するポリシーが見つからなかった場合、次に示すように、セキュリティデバイスはデフォルトの許可 (permit)/ 拒否 (deny) ポリシーをパケットに適用します。
   unset/set policy default-permit-all

   (または)

   ゾーン内ポリシーとグローバルポリシーのルックアップを実行し、一致するポリシーが見つからなかった場合、次に示すように、セキュリティデバイスはそのゾーンのゾーン内ブロッキング設定をパケットに適用します。
   unset/set zone *zone* **block**

セキュリティデバイスは、最上位から最下位までポリシー群リストを 1 つずつ検索します。そのため、リストでは特定性の低いポリシーの上に特定性の高いポリシーを配置する必要があります。(ポリシーの順序については、193 ページの「ポリシーの再順序付け」を参照してください。)

定義済みポリシー

ファイアウォールは、入口と出口が 1 ポイントしかないネットワーク境界を提供します。すべてのトラフィックはこのポイントを通過しなければならないため、地域間ポリシー、ゾーン内ポリシー、グローバルポリシー用のポリシーセットリストを実装することによって、トラフィックの予備選択と転送を行うことができます。

ポリシーを使用すると、1 つのセキュリティゾーンから別のセキュリティゾーンに通過しようとしているトラフィックの拒否 (deny)、許可 (permit)、リジェクト (拒否して TCP RST または ICMP ポートの宛先不明メッセージをソースホスト送信)、暗号化 (encrypt) と解読 (decrypt)、認証 (authenticate)、優先 (prioritize)、スケジュール (schedule)、フィルタ (filter)、監視 (monitor) を行うことができます。どのユーザーと何のデータが出入り可能で、いつどこに転送できるかを決定します。

注 : 仮想システムをサポートするセキュリティデバイスでは、ルートシステムで設定されたポリシーは、仮想システムで設定されたポリシーには影響を及ぼしません。

ポリシーとルール

A 1 つのユーザー定義可能ポリシーは、1 つ以上の論理ルールを内部的に生成し、またそれぞれの論理ルールはソースアドレス、宛先アドレス、サービスというコンポーネント群から形成されています。コンポーネントは、メモリーリソースを消費します。コンポーネントを参照する論理ルールは、メモリーリソースを消費しません。

ポリシーでソースアドレスと宛先アドレスの複数のエントリやグループ、およびサービスコンポーネントを使用するかどうかによりますが、論理ルールの数は、1 つのポリシーを作成してすぐわかる見かけ上の数よりもはるかに大きくなることがあります。たとえば、以下のポリシーは 125 個の論理ルールを生成します。

1 つのポリシー: 5 つのソースアドレス x 5 つの宛先アドレス x 5 つのサービス = 125 個の論理ルール

ただし、セキュリティデバイスは、論理ルールごとにコンポーネントを複製することはありません。ルールは、同一のコンポーネント群をさまざまに組み合わせて役立てます。たとえば、125 個の論理ルールを生成する上記のポリシーは、以下のようにわずか 15 個のコンポーネントに帰することになります。

5 つのソースアドレス + 5 つの宛先アドレス + 5 つのサービス = 15 個のコンポーネント

これら 15 個のコンポーネントはさまざまな方法で組み合わされ、1 つのポリシーによって 125 個の論理ルールが生成されます。複数の論理ルールに対して同一のコンポーネント群を異なる組み合わせで使用することを許可することによって、セキュリティデバイスが消費するリソースは、それぞれの論理ルールがコンポーネントと 1 対 1 関係になっている場合よりもはるかに少なくなります。

新しいポリシーのインストールにかかる時間は、セキュリティデバイスが追加、削除、修正するコンポーネントの数に比例するので、コンポーネントの数が少ないほどポリシーをインストールする時間が短縮されます。また、多数の論理ルールが少数のコンポーネント群を共有できることによって、ScreenOS では、それぞれのルールが専用のコンポーネントを必要とする場合に可能なポリシーよりも多くのポリシーを作成することが可能になり、作成できるルールが多くなります。

ポリシーの構成

ポリシーには、以下の要素を含む必要があります。

- ID(自動的に生成されますが、CLI でユーザーが定義できます)
- ゾーン (ソースおよび宛先)
- アドレス (ソースおよび宛先)
- サービス
- アクション (deny, permit, reject, tunnel)

ポリシーには、以下の要素を含む必要があります。

- アプリケーション
- 名前
- VPN トンネル
- L2TP トンネリング
- 徹底監視 (Deep Inspection)
- ポリシーリストの最上位の配置
- ソースアドレス変換
- 宛先アドレス変換
- ユーザー認証
- HA セッションバックアップ
- Web フィルタリング
- ロギング
- カウンティング
- トラフィックアラームしきい値
- スケジュール
- ウィルス対策スキャン
- トラフィックシェーピング

このセクションの以下の部分で、上記の要素を順番に 1 つずつ解説します。

ID

自分で定義するか セキュリティデバイスが自動的に割り当てるかどうかにかかわらず、すべてのポリシーには ID 番号があります。CLI: **set policy id** *number* の *set policy コマンドを通じてのみ、ポリシーの ID 番号を定義できます。*EID 番号がわかると、ポリシーを変更するためにさらにコマンドを発行して、ポリシーの内容を入力できます。(構成コンテキストのより詳細な情報は、187 ページの「ポリシーの内容の入力」を参照してください。

ゾーン

ゾーンには、セキュリティ測定が適用されるネットワークスペースのセグメント (セキュリティゾーン)、VPN トンネルインターフェースがバインドされる論理セグメント (トンネルゾーン)、または特定の機能を実行する物理的あるいは論理的エンティティ (機能ゾーン) の可能性があります。ポリシーはトラフィックに対して、2 つのセキュリティゾーンの間 (地域間ポリシー)、または同一ゾーンにバインドされている 2 つのインターフェース間 (ゾーン内ポリシー) をフローすることを許可します。(詳細については、25 ページの「ゾーン」、163 ページの「地域間ポリシー」、および 164 ページの「ゾーン内ポリシー」を参照してください。

アドレス

アドレスとは、あるセキュリティゾーンにおける、ファイアウォールとの位置関係によってホストやネットワークなどのネットワークデバイスを識別するオブジェクトのことです。個々のホストは、マスク 255.255.255.255 を使用して指定されます。これはアドレスの 32 ビットすべてが重要であることを示しています。ネットワークは、どのビットが重要であるかを示すサブネットマスクを使用して指定されます。特定のアドレスのポリシーを作成するには、最初に関連するホストとネットワークのエントリをアドレス帳に作成する必要があります。

他のアドレス帳入力のように、アドレスグループを作成して、それらのアドレスグループにポリシーを適用することもできます。アドレスグループをポリシーの要素として使用する場合は、セキュリティデバイスがグループ内の各アドレスにポリシーを適用するため、利用可能な内部論理ルールとそれらのルールで形成されるコンポーネントの数は、予想よりも急速に減少することがありますので注意してください。このことは、ソースと宛先の両方にアドレスグループを使用する場合には特に危険です。(詳細については、166 ページの「ポリシーとルール」を参照してください)。

サービス

サービスとは、Telnet、FTP、SMTP、HTTP のようなアプリケーションサービスを使用するために標準的で一般に認められた TCP と UDP のポート番号などのレイヤー 4 情報を使用してアプリケーションプロトコルを識別するオブジェクトのことです。ScreenOS には、定義済みの主なインターネットサービスが含まれています。また、顧客サービスを定義することもできます。

どのサービスを許可、拒否、暗号化、認証、ロギング、カウントするかを指定するポリシーを定義することができます。

アクション

アクションとは、ファイアウォールが受信したトラフィックに対してファイアウォールが実行する内容を説明したオブジェクトのことです。

- **Deny** は、パケットのファイアウォール通過をブロックします。
- **Permit** は、パケットのファイアウォール行き来を許可します。
- **Reject** は、パケットのファイアウォール通過をブロックします。セキュリティデバイスはパケットをドロップします。このとき、TCP トラフィックの場合には TCP リセット（RST）セグメントをソースホストクライアントに送信し、UDP トラフィックの場合には ICMP メッセージ「destination unreachable, port unreachable」（タイプ 3、コード 3）を送信します。TCP や UDP 以外のトラフィックの場合は、deny アクションの場合と同様に、ソースホストへは通知されずにパケットがドロップされます。

注 : セキュリティデバイスは、RST 以外の任意のコードビットが設定されている TCP セグメントを受信（およびドロップ）後に、TCP RST を送信します。

ingress インターフェースがレイヤー 2 またはレイヤー 3 で動作しており、プロトコルが TCP である場合、TCP RST にあるソース IP アドレスは元の（ドロップされた）パケットにある宛先 IP アドレスです。ingress インターフェースがレイヤー 2 で動作しておりプロトコルが UDP である場合、ICMP メッセージ内のソース IP アドレスは元のパケットにある宛先 IP アドレスです。ただし、ingress インターフェースがレイヤー 3 で動作しておりプロトコルが UDP である場合には、ICMP メッセージ内のソース IP アドレスは ingress インターフェースのソース IP アドレスです。

- **Tunnel** 出力 IP パケットをカプセル化し、受信 IP パケットをカプセルから取り出します。IPSec VPN トンネルでは、どの VPN トンネルを使用するかを指定します。L2TP トンネルでは、どの L2TP トンネルを使用するかを指定します。L2TP-over-IPSec では、IPSec VPN トンネルと L2TP トンネルの両方を指定します。

注 : L2TP-over-IPSec では、IPSec VPN トンネルのソースアドレスと宛先アドレスは、L2TP トンネルのものと同じでなければなりません。

セキュリティデバイスは、以前に示された条件、つまり、ゾーン (ソースおよび宛先)、アドレス (ソースおよび宛先)、およびサービスです。

アプリケーション

アプリケーションオプションでは、ポリシーで参照したレイヤー 4 サービスにマップされるレイヤー 7 アプリケーションを指定します。事前定義されたサービスがすでにレイヤー 7 アプリケーションにマップされています。しかし、カスタムサービスの場合、サービスをアプリケーションに明示的にリンクする必要があり、ポリシーに ALG（アプリケー

注 : ScreenOS は、DNS、FTP、H.323、HTTP、RSH、SIP、Telnet、TFTP などの数多くのサービスについて ALG をサポートします。

ALG をカスタムサービスに適用するには、次の 2 つの手順を実行します。

- カスタムサービスを名前、タイムアウト値、トランスポートプロトコル、ソースおよび宛先ポートで定義する
- ポリシーを構成するときに、適用する ALG のサービスおよびアプリケーションのタイプを参照する

カスタムサービスに徹底監視を適用する方法については、**4**-154 ページの「顧客サービスとアプリケーションのマッピング」を参照してください。

名前

目的を識別するための便利な手段を与えるために、ポリシーに内容を説明する名前を付けることができます。

注 : ポリシーに作成する名前に適用される ScreenOS ネーミング規則に関する詳細は、x ページの「コマンドラインインターフェースの規則」を参照してください。

VPN トンネル

構成済みの任意の VPN トンネルには、1 つ以上のポリシーを適用することができます。WebUI では、VPN トンネルオプションがすべての VPN トンネルのドロップダウンリストを提供します。CLI では、**get vpn** コマンドによって、利用できるすべてのトンネルが表示されます。(詳細については、**5**-77 ページの「サイト間 VPN (仮想プライベートネットワーク)」および **5**-157 ページの「ダイヤルアップ仮想プライベート ネットワーク」を参照してください。)

VPN トンネルの両端の VPN 構成がポリシーベースの NAT を使用している場合は、両方のゲートウェイデバイスの管理者はインバウンドとアウトバウンドのポリシー (合計で 4 つのポリシー) をそれぞれ作成する必要があります。VPN ポリシーが一致ペアを形成する（すなわち、ソースアドレスと宛先アドレスが逆になっている以外はインバウンドとアウトバウンドの各ポリシー構成のすべてが同じ）場合は、1 つのポリシーを構成してから **Modify matching bidirectional VPN policy** チェックボックスをオンにすることで、逆方向の 2 つ目のポリシーを自動的に作成することができます。新しいポリシーを構成するとき、このチェックボックスはデフォルトでオフになっています。一致ペアのメンバーとなっている既存のポリシーの変更では、チェックボックスはデフォルトでオンになっているため、1 つのポリシーに加えられた変更は、すべてもう一方に伝播します。

注 : このオプションは、WebUI によってのみ利用できます。ソースアドレス、宛先アドレス、またはサービスなどのポリシーコンポーネントに複数のエントリがあるときにはサポートされません。

L2TP トンネリング

構成済みの任意の L2TP（レイヤー 2 トンネリングプロトコル）トンネルには、1 つ以上のポリシーを適用できます。WebUI では、L2TP オプションがすべての L2TP トンネルのドロップダウンリストを提供します。CLI では **get l2tp** *tunn_str* **active** コマンドを使用すると、アクティブな L2TP トンネルの状態が表示されま

す。また、**get l2tp all** コマンドを使用すると、利用できるすべてのトンネルが表示されます。VPN トンネルと L2TP トンネルの端点が同一の場合は、この 2 つのトンネルを組み合わせてそれぞれの特徴を組み合わせたトンネルを作成できます。これは、L2TP-over-IPSec と呼ばれています。

注 : 透過モードのセキュリティデバイスは L2TP をサポートしません。

徹底監視 (Deep Inspection)

徹底監視（DI: Deep Inspection）は、ネットワークとトランスポートレイヤーだけでなく、アプリケーションレイヤーの内容とプロトコルの特性を調べることによって、ネットワークとトランスポートレイヤーで許可されるトラフィックをフィルタリングするためのメカニズムです。DI の目標は、Juniper Networks ファイアウォールが許可するトラフィック中に存在する可能性がある攻撃や異常動作を検知し保護することにあります。

注 : OSI（開放型システム間相互接続）モデルでは、ネットワークレイヤーはレイヤー 3 で、トランスポートレイヤーはレイヤー 4、アプリケーションレイヤーはレイヤー 7 です。OSI モデルは、ネットワークプロトコルアーキテクチャのネットワーク業界標準モデルです。OSI モデルは 7 つのレイヤーから成り立っています。

攻撃からの保護に関するポリシーを構成するには、以下の 2 つを選択します。使用する攻撃グループ (または複数の攻撃グループ)、および攻撃が検知された場合にとるべきアクションです。(詳細については、**4**-117 ページの「徹底監視 (Deep Inspection)」を参照してください)。

ポリシーリストの最上位の配置

ScreenOS では、新たに作成されたポリシーは、デフォルトではポリシーセットリストの最下位に配置されます。ポリシーを再配置する必要がある場合は、193 ページの「ポリシーの再順序付け」で説明されているポリシー再順序付け方法のいずれかを使用することができます。新たに作成されたポリシーをポリシーセットリストの最上位に再配置する余分なステップを回避するには、WebUI で **Position at Top** オプションをオンにするか、CLI の **set policy** コマンド (**set policy top**) でキーワード **top** を使用します。

ソースアドレス変換

ポリシーレベルでソースアドレス変換 (NAT-src) を適用できます。NAT-Src では、受信または出力のいずれかのネットワークトラフィックと VPN トラフィック上のソースアドレスを変換することができます。新しいソースアドレスは、ダイナミック IP (IP)　プールまたは出口インターフェースのいずれかから指定できます。NAT-Src はソースポートアドレス変換 (PAT) もサポートします。使用可能な NAT-Src オプションについては、**8**-13 ページの「ソースネットワークアドレス変換」を参照してください。

注 : インターフェースレベルで NAT (ネットワークアドレス変換) と呼ばれるソースアドレス変換を実行することもできます。インターフェースレベルの NAT-Src または NAT については、94 ページの「NAT モード」を参照してください。

宛先アドレス変換

ポリシーレベルで宛先アドレス変換 (NAT-dst) を適用できます。NAT-Dst では、受信または出力のいずれかのネットワークトラフィックと VPN トラフィック上の宛先アドレスを変換することができます。NAT-Dst は宛先ポートマッピングもサポートします。すべての NAT-Dst オプションについては、**8**-27 ページの「宛先ネットワークアドレス変換」を参照してください。

ユーザー認証

このオプションを選択するには、トラフィックがファイアウォールを行き来したり VPN トンネルに入れるようになる前に、ソースアドレスの認証ユーザーがユーザー名とパスワードを入力して自分の識別を認証することが必要になります。セキュリティデバイスは、ローカルデータベースや外部 RADIUS、SecurID、または LDAP 認証サーバーを使用して認証チェックを実行します。

注 : 認証を必要とするポリシーが IP アドレスのサブネットに適用される場合には、そのサブネットのそれぞれの IP アドレスに認証が必要になります。

（Telnet を実行している Unix ホストのように）ホストが複数の認証ユーザーアカウントをサポートしている場合には、最初のユーザー認証の後に、そのホストのその他すべてのユーザーが認証されることなく、最初のユーザーの権限を引き継いでセキュリティデバイスを介してトラフィックを通過させることができます。

ScreenOS には、以下の 2 つの認証スキームが提供されています。

- ランタイム認証 : セキュリティデバイスは、認証が使用可能になっているポリシーに一致する HTTP、FTP、または Telnet トラフィックを受信すると、認証ユーザーにログオンするようにプロンプトします。
- WebAuth: セキュリティデバイスを介してトラフィックを送信する前に、ユーザーは自分自身を認証する必要があります。

ランタイム認証

ランタイム認証の手順では、以下を実行します。

1. 認証ユーザーが HTTP、FTP または Telnet 接続要求を宛先アドレスに送信すると、セキュリティデバイスはパケットを代行受信し、バッファに格納します。
2. セキュリティデバイスが認証ユーザーにログインプロンプトを送信します。
3. このプロンプトに対して、認証ユーザーは自分のユーザー名とパスワードを入力します。
4. セキュリティデバイスが認証ユーザーのログイン情報を認証します。

   認証が成功すると、認証ユーザーと宛先アドレスの間で接続が確立されます。

最初の接続要求では、ポリシーには Telnet、HTTP、FTP　の 3 つのサービスのうち 1 つまたはすべてが含まれていなければなりません。Telnet、HTTP、または FTP です。これらのサービスの 1 つまたはすべてを含むポリシーのみが、認証手順を開始することができます。ユーザー認証に関わるポリシーでは、以下のサービスのいずれかを使用することができます。

- Any（“any”には 3 つの必要なサービスすべてが含まれるため）
- Telnet、FTP、または HTTP
- 使用予定の 1 つ以上のサービス、および認証手順を開始するのに必要な 3 つのサービス (Telnet、FTP、または HTTP) のうち 1 つ以上のサービスを含むサービスグループ。たとえば、FTP、Netmeeting、H.323 サービスをサポートする“Login”という名前のカスタムサービスグループを作成することができます。ポリシーを作成する時には、「ログイン」をサービスとして指定します。

認証に成功した後の接続では、ポリシーで指定されているすべてのサービスが有効になります。

注 : 認証が使用可能になっているポリシーでは、DNS (ポート番号 53) はサービスとしてサポートされていません。

事前ポリシーチェック認証 (WebAuth)

WebAuth 認証の手順では、以下を実行します。

1. 認証ユーザーが WebAuth サーバーの IP アドレスに HTTP 接続します。
2. セキュリティデバイスが認証ユーザーにログインプロンプトを送信します。
3. このプロンプトに対して、認証ユーザーは自分のユーザー名とパスワードを入力します。
4. セキュリティデバイスまたは外部認証サーバーが認証ユーザーのログイン情報を認証します。

   認証が成功した場合は、WebAuth 方式によって認証を実行するポリシーで指定されたとおりに、セキュリティデバイスが宛先へのトラフィックの開始を認証ユーザーに許可します。

注 : これら 2 つのユーザー認証方法についての詳細は、**9**-44 ページの「ポリシーで認証ユーザーを参照する」を参照してください。

特定のユーザーグループ、ローカルまたは外部ユーザー、またはグループ表現式を選択することによって、ポリシーが適用される認証ユーザーの範囲を制限または拡大することができます。グループ表現に関するより詳細な情報は、**9**-4 ページの「グループ式」を参照してください。ポリシーで認証ユーザーまたはユーザーグループを参照しない (WebUI では、**Allow Any** オプションを選択) 場合は、指定された認証サーバーのすべての認証ユーザーにポリシーが適用されます。

注： ScreenOS は、認証権限と認証ユーザーのログオンしたホストの IP アドレスをリンクします。すべての NAT 割り当てに対して 1 つの IP アドレスを使用している NAT デバイスの背後に存在するホストから 1 人のユーザーをセキュリティデバイスが認証すると、その NAT デバイスの背後に存在する他のホストのユーザーも同一の権限を自動的に受け取ります。

HA セッションバックアップ

高可用性（HA）のために NSRP クラスタ内に 2 台の セキュリティデバイスがある場合は、どのセッションをバックアップし、どのセッションをバックアップしないかを指定することができます。バックアップしたくないセッションのトラフィックについては、HA セッションのバックアップオプションを使用不可にしてあるポリシーを適用します。WebUI で **HA Session Backup** チェックボックスをクリアにします。CLI では、**set policy** コマンドで、**no-session-backup** 引数を使用します。デフォルトでは、NSRP クラスタ内のセキュリティデバイスはセッションをバックアップします。

Web フィルタリング

Web フィルタリングは、URL フィルタリングという別名でも呼ばれ、インターネットアクセスを管理して不適切な Web コンテンツへのアクセスを防ぎます。詳細については、**4**-98 ページの「Web フィルタリング」を参照してください。

ロギング

ポリシーでロギングを使用可能にすると、セキュリティデバイスはそのポリシーが適用されるすべての接続についてログを作成します。WebUI または CLI のどちらからでもログを閲覧することができます。WebUI では、**Reports > Policies > Logging**（表示するログを含むポリシー）をクリックします。CLI では、**get log traffic policy** *id_num* コマンドを使用します。

注： ログとグラフの表示方法の詳細については、**3**-55 ページの「セキュリティ デバイスの監視」を参照してください。

カウンティング

ポリシーでカウンティングを使用可能にすると、セキュリティデバイスはこのポリシーが適用されるトラフィックの合計バイト数をカウントし、履歴グラフに情報を記録します。WebUI でポリシーの履歴グラフを閲覧するには、**Reports > Policies > Counting**（表示するトラフィックカウントを含むポリシー）をクリックします。

トラフィックアラームしきい値

ポリシーによって許可されたトラフィックが指定されたバイト数 / 秒、バイト数 / 分、またはこれら両方を超過した時にアラームを鳴らすしきい値を設定できます。トラフィックアラームでは、セキュリティデバイスが合計バイト数を監視する必要があるため、カウンティング機能も使用可能にする必要があります。

注： トラフィックアラームについての詳細は、**3**-69 ページの「トラフィック警告」を参照してください。

スケジュール

スケジュールをポリシーに関連付けることによって、いつポリシーが有効になるかを決めることができます。スケジュールは、反復ベースおよびワンタイムイベントとして構成することができます。スケジュールは、ネットワークトラフィックのフローを制御し、ネットワークセキュリティを強化するための強力なツールを提供します。後者の例では、重要なデータを社外に送信する社員のことを心配している場合に、通常の勤務時間後にアウトバウンド FTP-Put と MAIL トラフィックをブロックするポリシーを設定することもできます。

WebUI では、**Policy > Policy Elements > Schedules** ページでスケジュールを定義します。CLI では、**set schedule** コマンドを使用します。

注 : WebUI では、スケジュールされたポリシーは、現在の時刻が定義されたスケジュールから外れていることを示すために灰色のバックグラウンドで表示されます。スケジュールされたポリシーがアクティブになると、白のバックグランドで表示されます。

ウィルス対策スキャン

Juniper Networks セキュリティデバイスの中には、FTP、HTTP、IMAP、POP3、および SMTP トラフィックをフィルタリングするために構成できる内部 AV スキャナをサポートするものがあります。内部 AV スキャナがウィルスを検知すると、パケットがドロップされ、トラフィックを発信したクライアントにウィルスを報告するメッセージが送信されます。

注 : ウィルス対策スキャンの詳細については、175 ページの「ウィルス対策スキャン」を参照してください。

トラフィックシェーピング

トラフィックの制御とシェーピングのパラメータは、それぞれのポリシーに設定することができます。表 28 は、トラフィックシェーピングパラメータを示します。

表 28: トラフィックシェーピングパラメータ

パラメータ	解説
Guaranteed Bandwidth	キロビット / 秒 (kbps) での保証スループット。このしきい値以下のトラフィックは、トラフィック管理やシェーピングメカニズムの影響を一切受けることなく、最も高い優先順位で通過します。
Maximum Bandwidth	キロビット / 秒 (kbps) での接続タイプで利用可能なセキュアな帯域幅。このしきい値を超えるトラフィックは、減速されたりドロップされます。 **注 :** 10 kbps 未満のレートをしきい値に使用しないことをお勧めします。このしきい値以下のレートでは、トラフィック管理の目的を損なうようなドロップパケットと過剰な再試行を招くことになります。
Traffic Priority	トラフィックの帯域幅が保証設定と最大設定の間にある場合は、セキュリティデバイスは最初に優先順位の高いトラフィックを通過させ、優先順位の高いトラフィックがない場合に限って、それよりも優先順位の低いトラフィックを通過させます。優先順位には 8 つのレベルがあります。
DiffServ Codepoint Marking	差別化されたサービス (DiffServ) は、優先順位の階層内の場所でトラフィックをタグ (あるいはマーキング) するためのシステムです。8 つの ScreenOS 優先順位レベルを DiffServ システムにマッピングすることができます。デフォルトでは、ScreenOS システムで最も高い優先順位（優先順位 0）は、IP パケットヘッダー内の DiffServ フィールド（RFC 2474 を参照）、または TOS バイトの IP precedence フィールド（RFC 1349 を参照）の最初の 3 ビット（111）にマッピングされます。ScreenOS システムで最も低い優先順位（優先順位 7）は、TOS DiffServ システムの（000）にマッピングされます。DSCP を使用可能に設定すると、ScreenOS は ToS バイトの最初の 3 ビットを IP precedence 優先順位で上書きします。DSCP を使用可能に設定し、*dscp-byte* **value** を設定すると、ScreenOS は ToS バイトの最初の 6 ビットを DSCP 値で上書きします。 **注記 :** いくつかのデバイスでは、システム全体に渡る環境変数の設定により、明示的に DSCP マーキングを有効にする必要があります。ポリシーで使用する前に、ご使用のデバイスで明示的に DSCP マーキングを有効にする必要があるかどうかはハードウェアのマニュアルを参照してください。必要な場合は、以下のコマンドを使用して、DSCP マーキングをシステム全体で有効にします。**set envar ipsec-dscp-mark = yes**. この変数は、WebUI を使って設定できません。システム全体で DSCP マーキングを無効にするには、**unset envar ipsec-dscp-mark** を使用します。

注 : トラフィック管理とシェーピングについての詳細は、195 ページの「トラフィックシェーピング」を参照してください。

ScreenOS の優先順位レベルと DiffServ システムとの間のマッピングを変更するには、次の CLI コマンドを使用します。

set traffic-shaping ip_precedence *number0 number1 number2 number3 number4 number5 number6 number7*

ここで、*number0* は優先順位 0 のマッピング（TOS DiffServ システムで最も高い優先順位）で、*number1* は優先順位 1 のマッピング、というように続きます。

IP precedence をクラスセレクタのコードポイントに包含させる、つまり DiffServ フィールドにある 2 番目の 3 ビットを消去して **ip_precedence** で設定した優先順位レベルをダウンストリームルーターによって正しく保存および処理させるようにするには、以下の CLI コマンドを使用します。

set traffic-shaping dscp-class-selector

適用されるポリシー

このセクションは、以下のポリシーの管理について説明します。ポリシーの閲覧、作成、変更、順序付け、再順序付け、削除です。

ポリシーの閲覧

WebUI でポリシーを閲覧するには、**Policies** をクリックします。ポリシーをソースゾーンと宛先ゾーンに分けて表示するには、**From** および **To** ドロップダウンリストからゾーン名を選択し、**Go** をクリックします。CLI では、**get policy** [**all** | **from** *zone* **to** *zone* | **global** | **id** *number*] コマンドを使用します。

ポリシーの作成

2 つのゾーン間をフローするトラフィックを許可するには、これらのゾーン間のトラフィックを許可 (permit)、拒否 (deny と reject)、トンネル (tunnel) するポリシーを作成します。セキュリティデバイスがポリシーで参照されるソースゾーンと宛先アドレス間のゾーン内トラフィックをルーティングできる唯一のネットワークデバイスである場合は、同一ゾーン内のトラフィックを制御するポリシーを作成することもできます。また、グローバルポリシーを作成することもできます。グローバルポリシーは Global ゾーンのアドレス帳内のソースアドレスと宛先アドレスを使用します。

たとえば、Trust ゾーンと Untrust ゾーン間など、2 つのゾーン間の双方向トラフィックを許可するには、Trust から Untrust へ進むポリシーを作成し、次に Untrust から Trust への 2 番目のポリシーを作成する必要があります。ニーズに合わせて、ポリシーは同一または別の IP アドレスを使用でき、ソースアドレスと宛先アドレスのみが逆になります。

ルートシステムや仮想システムなど同じシステム内にある任意のゾーンの間でポリシーを定義できます。ルートシステムと仮想システム間でポリシーを定義するには、ゾーンの 1 つが共有ゾーンである必要があります。(仮想システムに関連した共有ゾーンについては、“ 第 10 部 : 仮想 システム ” を参照してください。)

ゾーン間ポリシーメールサービスの作成

この例では、電子メールトラフィックのフローを制御する 3 つのポリシーを作成します。

最初のポリシーでは、Trust ゾーンの内部ユーザーが DMZ ゾーンのローカルメールサーバーから電子メールを送受信することを許可します。このポリシーは、内部ユーザーから発信された MAIL サービス (すなわち SMTP サービス) と POP3 サービスが Juniper Networks ファイアウォールを通過してローカルメールサーバーに到達することを許可します。

2 番目と 3 番目のポリシーでは、DMZ ゾーンのローカルメールサーバーと Untrust ゾーンのリモートメールサーバーの間にあるファイアウォールを MAIL サービスが通過することを許可します。

ただし、異なるセキュリティゾーンの間のトラフィックを制御するポリシーを作成する前にまず、これらのポリシーを適用する環境を設計する必要があります。最初の手順では、ゾーンへのインターフェースをバインドし、以下のとおりにインターフェース IP アドレスを割り当てます。

- Trust ゾーンに ethernet0/1 をバインドし、IP アドレス 10.1.1.11/24 を設定
- DMZ ゾーンに ethernet0/2 をバインドし、IP アドレス 1.2.2.1/24 を設定
- Untrust ゾーンに ethernet0/3 をバインドし、IP アドレス 1.1.1.1/24 を設定

セキュリティゾーンはすべて trust-vr ルーティングドメインにあります。

2 番目の手順では、以下のとおりにポリシーで使用するアドレスを作成します。

- corp_net という名前の Trust ゾーンのアドレスを定義し、IP アドレス 10.1.1.0/24 を設定
- mail_svr という名前の DMZ ゾーンのアドレスを定義し、IP アドレス 1.2.2.5/32 を設定
- r-mail_svr という名前の Untrust ゾーンのアドレスを定義し、IP アドレス 2.2.2.5/32 を設定

3 番目の手順では、2 つの事前定義された MAIL サービスと POP3 サービスを含む MAIL-POP3 という名前のサービスグループを作成します。

4 番目の手順では、ethernet0/3 経由で 1.1.1.250 にある外部ルーターをポイントする trust-vr ルーティングのデフォルトルートを設定します。

手順 1 ～ 4 を終了すると、保護されたネットワークの内外へ電子メールを送信、検索、配信することを許可するのに必要なポリシーを作成できます。

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet0/1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet0/2): 次のように入力してから **OK** をクリックします。

   Zone Name: DMZ
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.2.2.1/24

   Network > Interfaces > Edit (ethernet0/3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: corp_net
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 10.1.1.0/24
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: Mail_svr
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 1.2.2.5/32
   Zone: DMZ

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: r-mail_svr
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 2.2.2.5/32
   Zone: Untrust

3. **サービスグループ**
   Policy > Policy Elements > Services > Groups: 以下のグループ名を入力して、以下のサービスを移動し、**OK** をクリックします。

   Group Name: MAIL-POP3

   MAIL を選択し、< < ボタンを使用して、Available Members 列から Group Members 列にサービスを移動します。

   POP3 を選択し、< < ボタンを使用して、Available Members 列から Group Members 列にサービスを移動します。

4. **ルート**
   Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (**選択**)
   Interface: ethernet0/3
   Gateway IP Address: 1.1.1.250

5. **ポリシー**
   Policy > Policies > (From: Trust, To: Untrust) > New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), corp_net
   Destination Address:
   Address Book Entry: (**選択**), mail_svr
   Service: Mail-POP3
   Action: Permit

Policy > Policies > (From: DMZ, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), mail_svr
Destination Address:
Address Book Entry: (選択), r-mail_svr
Service: MAIL
Action: Permit

Policy > Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), r-mail_svr
Destination Address:
Address Book Entry: (選択), mail_svr
Service: MAIL
Action: Permit

CLI

1. **インターフェース**
```
set interface ethernet0/1 zone trust
set interface ethernet0/1 ip 10.1.1.1/24
set interface ethernet0/2 zone dmz
set interface ethernet0/2 ip 1.2.2.1/24
set interface ethernet0/3 zone untrust
set interface ethernet0/3 ip 1.1.1.1/24
```
2. **アドレス**
```
set address trust corp_net 10.1.1.0/24
set address dmz mail_svr 1.2.2.5/32
set address untrust r-mail_svr 2.2.2.5/32
```
3. **サービスグループ**
```
set group service MAIL-POP3
set group service MAIL-POP3 add mail
set group service MAIL-POP3 add pop3
```
4. **ルート**
```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/3 gateway 1.1.1.250
```
5. **ポリシー**
```
set policy from trust to dmz corp_net mail_svr MAIL-POP3 permit
set policy from dmz to untrust mail_svr r-mail_svr MAIL permit
set policy from untrust to dmz r-mail_svr mail_svr MAIL permit
save
```

ゾーン間ポリシー群の作成

この零細ソフトウェア企業の ABC デザインでは、内部ネットワークを 2 つのサブネットに分けました。この 2 つのサブネットは Trust ゾーン内にあります。サブネットには、以下のものがあります。

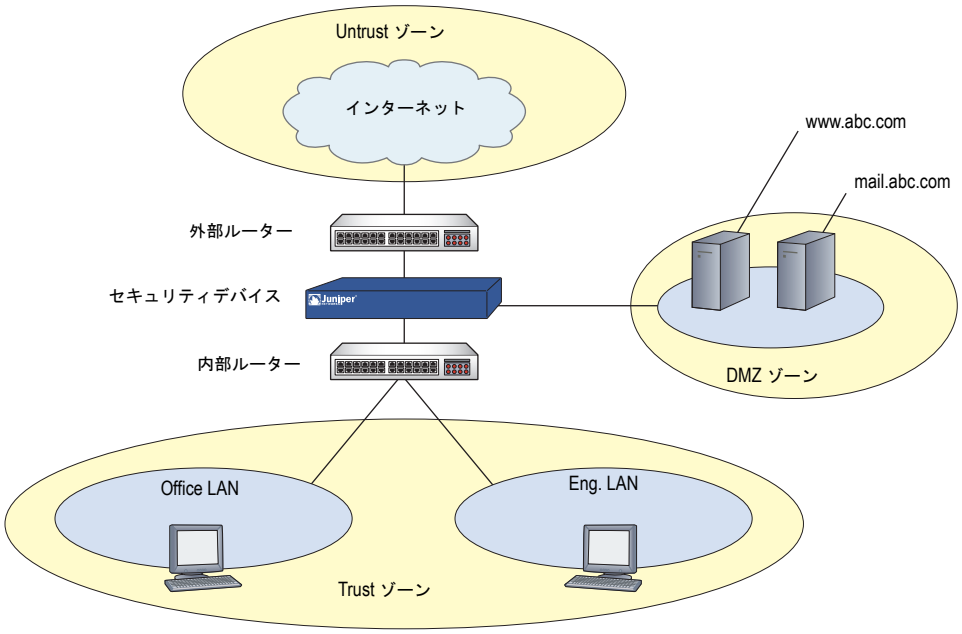
- エンジニアリング (定義済みアドレス“Eng”付き)
- その他の社内部署（“Office”というアドレスが定義済み）

ABC デザインには、Web サーバーとメールサーバーのための DMZ ゾーンもあります。

以下の例では、次のユーザーに対する典型的なポリシー群が示されています。

- “Eng”では、FTP-Put、IMAP、MAIL、POP3 を除いて、アウトバウンドトラフィックのためのすべてのサービスを使用することができます。
- “Office”は、WebAuth を介して自分自身を認証するという条件で、E メールを使用したり、インターネットにアクセスすることができます。(WebAuth ユーザー認証については、9-43 ページの「認証ユーザー」を参照してください。
- Trust ゾーンの全員は、DMZ ゾーンの Web サーバーとメールサーバーにアクセスできます。
- Untrust ゾーンのリモートメールサーバーは、DMZ ゾーンのローカルメールサーバーにアクセスできます。
- システム管理者のグループ (定義済みアドレス“sys-admins”) もあり、このシステム管理者は、DMZ ゾーンのサーバーへの完全なユーザーアクセスと管理アクセスを備えています。

図 60: 地域間ポリシーセット



この例では、必要なインターフェース、アドレス、サービスグループ、およびルートはすでに構成されていることを想定しています。これらの構成方法の詳細については、35 ページの「インターフェース」、105 ページの「アドレス」、140 ページの「サービスグループ」、および“ 第 7 部 : ルーティング ” を参照してください。

表 29: 構成するポリシー

From Zone - Src Addr	To Zone - Dest Addr	サービス	アクション
Trust - Any	Untrust - Any	Com (サービスグループ : FTP-Put, IMAP, MAIL, POP3)	Reject
Trust - Eng	Untrust - Any	Any	Permit
Trust - Office	Untrust - Any	Internet (サービスグループ : FTP-Get, HTTP, HTTPS)	Permit(+ WebAuth)

From Zone - Src Addr	To Zone - Dest Addr	サービス	アクション
Untrust - Any	DMZ - mail.abc.com	MAIL	Permit
Untrust - Any	DMZ - www.abc.com	Web (サービスグループ : HTTP, HTTPS)	Permit
Trust - Any	DMZ - mail.abc.com	Email（サービスグループ : IMAP, MAIL, POP3)	Permit
Trust - Any	DMZ - www.abc.com	Internet (サービスグループ : FTP-Get, HTTP, HTTPS)	Permit
Trust - sys-admins	DMZ - Any	Any	Permit
DMZ - mail.abc.com	Untrust - Any	MAIL	Permit

注 : デフォルトのポリシーはすべて Deny (拒否) になります。

WebUI

1. **Trust から Untrust へ**

   Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Eng
   Destination Address:
   Address Book Entry: (選択), Any
   Service: Any
   Action: Permit

   Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Office
   Destination Address:
   Address Book Entry: (選択), Any
   Service: インターネット Z
   Action: Permit

   > Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

   認証 : (選択)
   WebAuth: (選択)

注 : Internet は、FTP-Get、HTTP、HTTPS というメンバーを含むサービスグループです。

Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), Any
Service: Com
Action: Reject
Position at Top: (選択)

注 : Com は、FTP-Put、MAIL、IMAP、POP3 というメンバーを含むサービスグループです。Untrust ゾーンから Trust ゾーンへのトラフィックでは、デフォルトの Deny（拒否）ポリシーがすべてを拒否します。

2. Untrust から DMZ へ

Policy > Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), Any
Destination Address:
    Address Book Entry: (選択), mail.abc.com
Service: MAIL
Action: Permit

Policy > Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), Any
Destination Address:
    Address Book Entry: (選択), www.abc.com
Service: Web
Action: Permit

注 : Web は HTTP と HTTPS というメンバーを含むサービスグループです。

3. Trust から DMZ へ

Policy > Policies > (From: Trust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), Any
Destination Address:
    Address Book Entry: (選択), mail.abc.com
Service: Email
Action: Permit

注 : e-mail は、MAIL、IMAP、POP3 を含むサービスグループです。

Policy > Policies > (From: Trust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), Any
Destination Address:
    Address Book Entry: (選択), www.abc.com
Service: インターネット Z
Action: Permit

Policy > Policies > (From: Trust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), sys-admins
Destination Address:
Address Book Entry: (**選択**), Any
Service: Any
Action: Permit

4. **DMZ から Untrust へ**

Policy > Policies > (From: DMZ, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), mail.abc.com
Destination Address:
Address Book Entry: (**選択**), Any
Service: MAIL
Action: Permit

CLI

1. **Trust から Untrust へ**

```
set policy from trust to untrust eng any any permit
set policy from trust to untrust office any Internet permit webauth
set policy top from trust to untrust any any Com reject
```

注 : Internet は、FTP-Get、HTTP、HTTPS というメンバーを含むサービスグループです。
Com は、FTP-Put、MAIL、IMAP、POP3 というメンバーを含むサービスグループです。

2. **Untrust から DMZ へ**

```
set policy from untrust to dmz any mail.abc.com mail permit
set policy from untrust to dmz any www.abc.com Web permit
```

注 : Web は HTTP と HTTPS というメンバーを含むサービスグループです。

3. **Trust から DMZ へ**

```
set policy from trust to dmz any mail.abc.com e-mail permit
set policy from trust to dmz any www.abc.com Internet permit
set policy from trust to dmz sys-admins any any permit
```

注 : e-mail は、MAIL、IMAP、POP3 を含むサービスグループです。
Internet は、FTP-Get、HTTP、HTTPS というメンバーを含むサービスグループです。

4. **DMZ から Untrust へ**

```
set policy from dmz to untrust mail.abc.com any mail permit
save
```

ゾーン内ポリシーの作成

この例では、Trust ゾーン内の企業 LAN の機密サーバーへのアクセスを会計士のグループに許可するゾーン内ポリシーを作成します。最初に ethernet0/1 を Trust ゾーンにバインドし、IP アドレス 10.1.1.1/24 を割り当てます。次に、ethernet0/2 を Trust ゾーンにバインドし、IP アドレス 10.1.5.1/24 を割り当てます。Trust ゾーンでイントラゾーンブロッキングを使用可能にします。次に、2 つのアドレスを定義します。1 つは会社が自社の財務記録を保存するサーバー用のアドレス (10.1.1.100/32) で、もう 1 つは会計部門のホストが置かれているサブネット用のアドレス (10.1.5.0/24) です。それらのホストからサーバーへのアクセスを許可するゾーン内ポリシーを作成します。

WebUI

1. **Trust ゾーン ― インターフェースとブロッキング**

   Network > Interfaces > Edit (ethernet0/1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように選択してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet0/1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.5.1/24
   次のように選択してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Zones > Edit (Trust): 次のように入力してから **OK** をクリックします。

   Block Intra-Zone Traffic: (選択)

2. **アドレス**

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: Hamilton
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.100/32
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: accounting
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.5.0/24
   Zone: Trust

3. **ポリシー**
   Policy > Policies > (From: Trust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), accounting
   Destination Address:
   Address Book Entry: (**選択**), Hamilton
   Service: Any
   Action: Permit

CLI

1. **Trust ゾーン ― インターフェースとブロッキング**
   set interface ethernet0/1 zone trust
   set interface ethernet0/1 ip 10.1.1.1/24
   set interface ethernet0/1 nat
   set interface ethernet0/2 zone trust
   set interface ethernet0/2 ip 10.1.5.1/24
   set interface ethernet0/2 nat
   set zone trust block

2. **アドレス**
   set address trust Hamilton 10.1.1.100/32
   set address trust accounting 10.1.5.0/24

3. **ポリシー**
   set policy from trust to trust accounting Hamilton any permit
   save

グローバルポリシーの作成

この例では、当社の ウェブサイト www.juniper.net にどのゾーンのどのホストにもアクセスを許可するグローバルポリシーを作成します。グローバルポリシーは多数のセキュリティデバイスが存在する場合に、大変便利なショートカットとなります。この例では、*n* 個の地域間ポリシーで実行していたことを 1 つのグローバルポリシーで実行します (ここでは *n* = ゾーン数)。

注 : IP アドレスの代わりにドメイン名を使用するには、セキュリティデバイス上で構成された DNS サービスがあることを確認します。

WebUI

1. **グローバルアドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: Server1
   IP Address/Domain Name:
   Domain Name: (**選択**), www.juniper.net
   Zone: Global

2. ポリシー
Policy > Policies > (From: Global, To: Global) > New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), server1
Service: HTTP
Action: Permit

CLI

1. グローバルアドレス
set address global server1 www.juniper.net

2. ポリシー
set policy global any server1 http permit
save

ポリシーの内容の入力

CLI を通じてポリシーを構成する際に、まずポリシーを作成した後で、追加や変更を行うポリシーの内容を入力できます。たとえば、最初に以下のポリシーを作成します。

```
set policy id 1 from trust to untrust host1 server1 HTTP permit attack
    HIGH:HTTP:SIGS action close
```

たとえば、別のソースや宛先アドレス、別のサービスや別の攻撃グループを追加するなどポリシーの一部を変更する場合、ポリシー 1 の内容を入力してから関連コマンドを入力できます。

```
set policy id 1
device(policy:1)-> set src-address host2
device(policy:1)-> set dst-address server2
device(policy:1)-> set service FTP
device(policy:1)-> set attack CRITICAL:HTTP:SIGS
```

また、すべてを削除しない限り、1 つのポリシーのコンポーネントに対して複数の項目を削除できます。たとえば、上記の構成から server2 を削除できますが、server2 および server1 の両方は削除できません。宛先アドレスが残らなくなるからです。

ポリシーコンポーネントごとの複数の項目

ScreenOS では、ポリシーの以下のコンポーネントに対して複数の項目を追加できます。

- ソースアドレス
- 宛先アドレス
- サービス
- 攻撃グループ

リリース 5.0.0 よりも前の ScreenOS では、複数のソースアドレスと宛先アドレスまたはサービスを所有するための唯一の方法は、まずポリシーに複数のメンバーを持つアドレスまたはサービスグループを作成し、次にそのグループの参照を作成することです。ScreenOS 5.0.0 では引き続きポリシーのアドレスおよびサービスグループを使用できます。さらに、ポリシーコンポーネントに直接、余分な項目の追加のみもできます。

注： ポリシーで参照される最初のアドレスまたはサービスが Any である場合、それには論理的に何も追加できません。ScreenOS はこの種の構成の誤りを防ぎ、必要に応じてエラーメッセージを表示します。

ポリシーコンポーネントに複数の項目を追加するには、以下のいずれかを行います。

WebUI

アドレスとサービスを追加するには、項目を追加するコンポーネントの隣の **Multiple** ボタンをクリックします。攻撃グループを追加するには、**Attack Protection** ボタンをクリックします。Available Members コラムにある項目を選択し、**< <** キーを使用して、Active Members コラムに移動します。ほかの項目でこのアクションを繰り返すことができます。完了してから **OK** をクリックしてポリシー構成ページに戻ります。

CLI

以下のコマンドで、ポリシーの内容を入力します。

```
set policy id number
```

次に、以下のいずれかのコマンドを適宜使用します。

```
device(policy:number)-> set src-address string
device(policy:number)-> set dst-address string
device(policy:number)-> set service string
device(policy:number)-> set attack string
```

アドレス否定の設定

ソースまたは宛先のいずれかとして指定されたものを除いたすべてのアドレスに適用されるようにポリシーを構成できます。たとえば、P-T_contractors アドレスグループを除いた全員にインターネットアクセスを許可するポリシーを作成するとします。そのためには、アドレス否定オプションを使用します。

WebUI では、このオプションはポリシー構成ページの **Source Address** または **Destination Address** のいずれかの隣の **Multiple** ボタンをクリックすると表示されるポップアップで選択できます。

CLI では、ソースアドレスまたは宛先アドレスのすぐ前に、感嘆符 (!) を挿入します。

注： アドレス否定はポリシーコンポーネントレベルで行われ、否定されたコンポーネントのすべての項目に適用されます。

この例では、Trust ゾーンのすべてのアドレスに対して、エンジニアリングが次々と機能指定をポストする vulcan と呼ばれる FTP サーバーを除いたすべての FTP サーバーにアクセスすることを許可するゾーン内ポリシーを作成します。

ただし、ポリシーを作成する前にまず、それに適用する環境を設定する必要があります。まず、Trust ゾーンのイントラゾーンブロッキングを有効にします。ゾーン内ブロッキングでは、同じゾーンにバインドされた 2 つのインターフェースの間をセキュリティデバイスが通過する前にポリシーをルックアップすることが必要です。

2 番目に、2 つのインターフェースを Trust ゾーンにバインドし、以下のとおり IP アドレスに割り当てます。

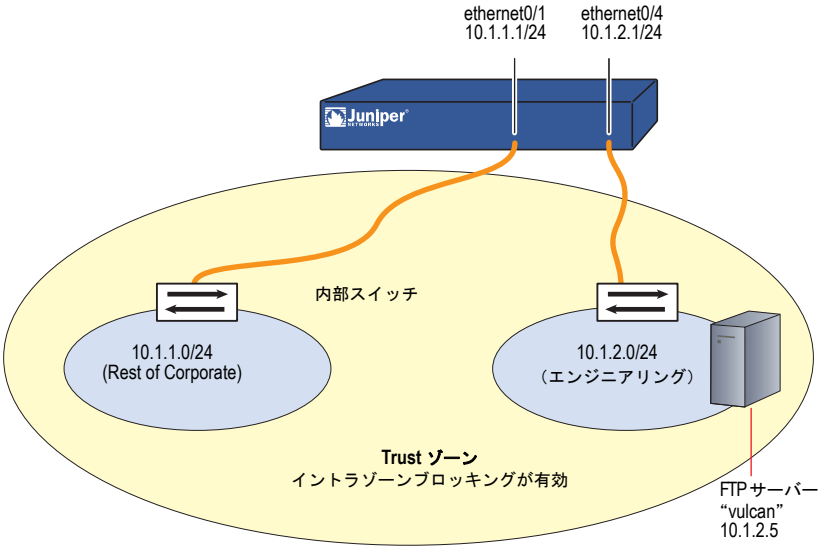
- Trust ゾーンに ethernet0/1 をバインドし、IP アドレス 10.1.1.11/24 を設定
- Trust ゾーンに ethernet0/4 をバインドし、IP アドレス 10.1.2.1/24 を設定

3 番目に、Trust ゾーンにある vulcan という名前の FTP サーバーに対してアドレス (10.1.2.5/32) を作成します。

2 番目と 3 番目の手順を完了すると、ゾーン内ポリシーを作成できます。

注 : エンジニアは 10.1.2.0/24 サブネットにも存在しているので Juniper Networks ファイアウォールを通過して自分専用のサーバーに到達する必要がないため、FTP サーバーに到達するようにエンジニアリング部のポリシーを作成する必要はありません。

図 61: ゾーン内ポリシー否定



WebUI

1. **イントラゾーンブロッキング**
   Network > Zones > Edit (Trust): 次のように入力してから **OK** をクリックします。

   Virtual Router Name: trust-vr
   Block Intra-Zone Traffic: (選択)

2. **Trust ゾーンインターフェース**
   Network > Interfaces > Edit (ethernet0/1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように選択してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet0/4): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.2.1/24
   次のように選択してから **OK** をクリックします。
   Interface Mode: NAT

3. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: vulcan
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.2.5/32
   Zone: Trust

4. **ポリシー**
   Policy > Policies > (From: Trust, To: Trust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Any
   Destination Address:
   Address Book Entry: (選択), vulcan

   > **Multiple** をクリックし、**Negate Following** を選択してから **OK** をクリックして、基本ポリシー構成ページに戻ります。

   Service: FTP
   Action: Permit

CLI

1. **イントラゾーンブロッキング**
   set zone trust block
2. **Trust ゾーンインターフェース**
   set interface ethernet0/1 zone trust
   set interface ethernet0/1 ip 10.1.1.1/24
   set interface ethernet0/1 nat
   set interface ethernet0/4 zone trust
   set interface ethernet0/4 ip 10.1.2.1/24
   set interface ethernet0/4 nat
3. **アドレス**
   set address trust vulcan 10.1.2.5/32
4. **ポリシー**
   set policy from trust to trust any !vulcan ftp permit
   save

ポリシーの変更と使用不可

ポリシーを作成すると、以後いつでもポリシーに戻って変更を加えることができます。WebUI では、変更するポリシーの Configure 列にある **Edit** リンクをクリックします。そのポリシーについて表示されるポリシー構成ページで変更を加えてから、**OK** をクリックします。CLI では、**set policy** コマンドを使用します。

ScreenOS では、ポリシーを使用可能および使用不可にする方法もあります。デフォルトでは、ポリシーは使用可能になっています。使用不可にするには、以下を実行します。

WebUI

Policies: 使用不可にするポリシーの Configure 列にある **Enable** チェックボックスをオフにします。

使用不可になっているポリシーのテキスト行が灰色で表示されます。

CLI

set policy id *id_num* disable
save

注 : 再度ポリシーを使用可能にするには、使用可能にしたいポリシーの Configure 列で **Enable** を選択するか (WebUI)、または **unset policy id** *id_num* **disable** と入力します (CLI)。

ポリシーの検証

ScreenOS には、ポリシーリストのポリシーの順序が有効であることを検証するツールがあります。1 つのポリシーが別のポリシーを覆っているかまたは影（シャドウ）にしている可能性があります。以下の例を考察してみてください。

```
set policy id 1 from trust to untrust any any HTTP permit
set policy id 2 from trust to untrust any dst-A HTTP deny
```

セキュリティデバイスはリストの最上位からポリシールックアップを実行するため、受信したトラフィックと一致するものを見つけると、ポリシーリスト中のそれ以下の部分は調べません。上記の例で、セキュリティデバイスはポリシー 2 に達することは決してありません。なぜならポリシー 1 の宛先アドレス“any”はポリシー 2 のよりも具体的な“dst-A”を含むためです。HTTP パケットが Untrust ゾーンの dst-A にバインドされた Trust ゾーンのアドレスから セキュリティデバイスに達すると、セキュリティデバイスは常にポリシー 1 と一致するものを見つけることになります。

上記の例を修正するには、具体的に示す方が先にくるように、ポリシーの順序を変えるだけですみます。

```
set policy id 2 from trust to untrust any dst-A HTTP deny
set policy id 1 from trust to untrust any any HTTP permit
```

当然のことながら、この例は意図して簡単に基本概念を説明しているものです。何十、何百のポリシーがある場合など、1 つのポリシーが別のポリシーを補完する場合には、単純にはわからないことがあります。ポリシーリストにポリシーのシャドウがあるかどうかをチェックするには、以下の CLI コマンドを使用します。

```
exec policy verify
```

このコマンドを使用すると、シャドウとシャドウされたポリシーを報告します。その後、問題を修正するのは管理者の責任です。

注： ポリシーの「シャドウ」の概念は、ポリシーリストの中で上位にあるポリシーがその下にあるポリシーの前に有効になる状況を表します。ポリシールックアップによる検索では、5 つの部分に分かれたソースの集合、宛先ゾーン、ソースアドレスと宛先アドレス、およびサービスタイプが一致する最初のポリシーが使用されます。そのため、別のポリシーが同じ集合 (または集合のサブセット) に適用される場合、ポリシールックアップはリストの最初のポリシーを使用し、2 番目のポリシーに到達することはありません。

ポリシー検証ツールは、ポリシーを組み合わせて別のポリシーをシャドウしている状況を検出できません。次の例では、ポリシー 3 をシャドウしている単独のポリシーはありませんが、ポリシー 1 と 2 の組み合わせがシャドウしています。

```
set group address trust grp1 add host1
set group address trust grp1 add host2
set policy id 1 from trust to untrust host1 server1 HTTP permit
set policy id 2 from trust to untrust host2 server1 HTTP permit
set policy id 3 from trust to untrust grp1 server1 HTTP deny
```

ポリシーの再順序付け

セキュリティデバイスでは、ファイアウォールを通過しようとするすべてのトラフィックについて、適切なリスト（165 ページの「ポリシーセットリスト」を参照）中の先頭のポリシーから 開始して 下方向に移動しながら、各ポリシーと照らし合わせてチェックします。セキュリティデバイスは、リスト内で最初に一致したポリシーにポリシーで指定されているアクションを適用するため、最も具体的なものから最も汎用的なものへとポリシーを配列する必要があります。(特定のポリシーでは、リスト下部に位置しているそれよりも汎用的なポリシーの適用を排除しませんが、特定のポリシーよりも前に表示される汎用ポリシーは、リスト下部に位置しているそれよりも汎用的なポリシーの適用を排除します。)

デフォルトでは、新たに作成されたポリシーはポリシー群リストの最下位に表示されます。代わりにリストの最上位にポリシーを配置できるオプションもあります。WebUI のポリシー構成ページで、**Position at Top** チェックボックスをオンにします。CLI では、**set policy** コマンド : **set policy top** にキーワード **top** を追加します。

リスト内の異なる位置にポリシーを移動するには、以下いずれかを実行します。

WebUI

WebUI でポリシーを再順序付けするには、以下の 2 つの方法があります。円形矢印をクリックするか、または移動させるポリシーの Configure 列にある単一矢印をクリックします。

円形矢印をクリックする場合、

User Prompt のダイアログボックスが表示されます。

リストの端までポリシーを移動するには、**<-1 >** と入力します。リスト内で上に移動するには、移動したいポリシーの上方にそのポリシーの ID 番号を入力します。

OK をクリックすると、移動が実行されます。

単一矢印をクリックする場合、

Policy Move ページには、移動させるポリシーと、残りのポリシーがあるテーブルが表示されます。

残りのポリシーが表示されているテーブルでは、ポリシーを移動できる場所を指し示す矢印が先頭の列 (Move Location) に表示されます。この矢印の移動先は、ポリシーが移動するリスト内の場所です。矢印をクリックします。

移動したポリシーが新しい場所に置かれ、Policy List ページが再表示されます。

CLI

```
set policy move id_num { before | after } number
save
```

ポリシーの削除

ポリシーの変更と再配置に加えて、ポリシーを削除することもできます。WebUI では、削除したいポリシーの Configure 列にある **Remove** をクリックします。システムメッセージが削除の確認プロンプトを表示したら、**Yes** をクリックします。CLI では、**unset policy** *id_num* コマンドを使用します。

第 7 章

トラフィックシェーピング

本章では、すべてのユーザーのネットワークの品質と可用性を損なうことなく Juniper Networks セキュリティデバイスを使用して限られた帯域幅を管理する様々な方法について説明します。本章のセクションは、以下のようになります。

- 196 ページの「ポリシーレベルでの帯域幅管理」
- 197 ページの「トラフィックシェーピングの設定」
- 200 ページの「サービス優先順位の設定」
- 201 ページの「優先順位キューの設定」
- 205 ページの「ingress ポリシング」
- 206 ページの「仮想インターフェースのトラフィックシェーピング」
- 216 ページの「DSCP マーキングとシェーピング」

トラフィックシェーピングとは、インターフェース上で各ユーザーとアプリケーションにネットワーク帯域幅を適正な量で割り当てることです。帯域幅の適正な量は、保証された QoS (通信品質) において費用効率がよい伝送容量として定義されます。セキュリティデバイスを使用に、ポリシーを作成したり、デバイスを通過するトラフィックの各クラスに適正なレート制御を適用することにより、トラフィックをシェーピングすることができます。

ポリシーレベルでの帯域幅管理

トラフィックを分類するためには、ポリシーを作成し、トラフィックの各クラスに保証帯域幅と最大帯域幅の量、および優先順位を指定します。保証帯域幅と最大帯域幅は厳密にはポリシーベースではありません。egress ゾーンに複数の物理インターフェースがあるため、ポリシーと egress 物理インターフェースの利用可能な帯域幅の両方に基づきます。各インターフェースの物理帯域幅は、すべてのトラフィックシェーピングポリシーの保証帯域幅パラメータに割り当てられます。残された帯域幅がある場合は、他のトラフィックによって共用可能です。すなわち、各ポリシーは保証帯域幅を取得するとともに、優先順位ベースで残った帯域幅があれば（仕様上の最大帯域幅を限度に）その帯域幅を他のポリシーと共用します。

トラフィックシェーピング機能は、すべてのポリシーからのトラフィックに適用されます。特定のポリシーのトラフィックシェーピングをオフにしても、他のポリシーのトラフィックシェーピングがまだオンの場合は、システムはそのポリシーに、以下のパラメータのデフォルトのトラフィックシェーピングポリシーを適用します。

- 保証帯域幅 0
- 無限の最大帯域幅
- 優先順位 7 (最低の優先順位設定)

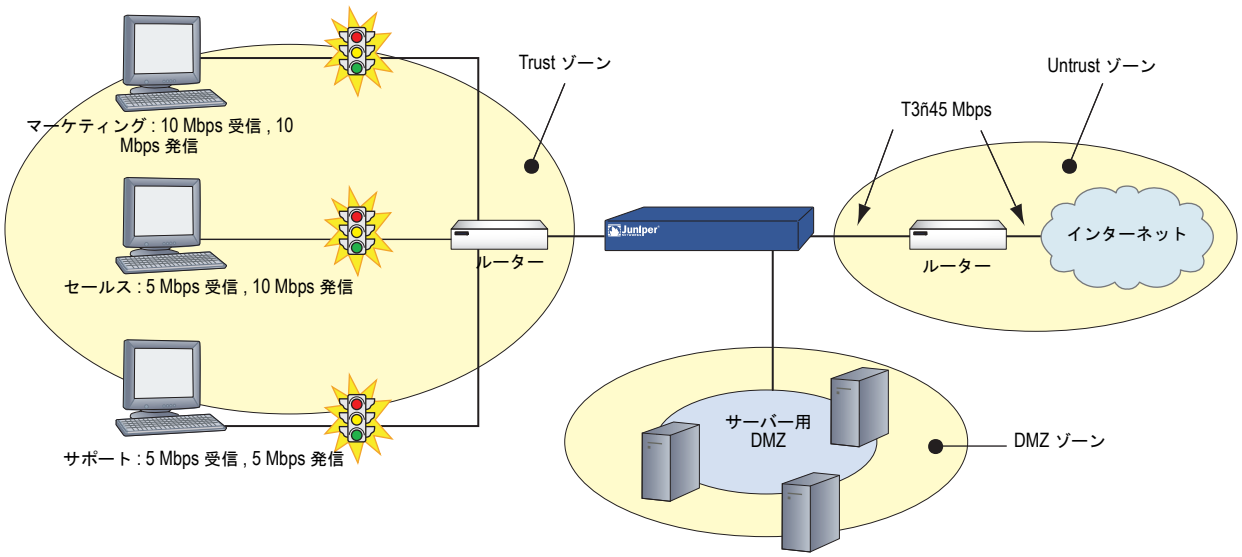
注： DiffServ コードポイントマーキングシステムへの優先順位レベルのマッピングを使用可能にすることができます。DS コードポイントマーキングに関する詳細については、175 ページの「トラフィックシェーピング」を参照してください。

トラフィックシェーピングをオフにしたポリシーにこのデフォルトトラフィックシェーピングポリシーが割り当てられないようにするには、CLI コマンド **set traffic-shaping mode off** を使用してトラフィックシェーピングシステム自体をオフにします。CLI コマンド **set traffic-shaping mode on** を使用して、インターフェース上のシェーピングをオンにします。また、WebUI の **Configuration > Advanced > Traffic Shaping** を実行して、トラフィックシェーピングを自動に設定することもできます。自動に設定すると、システムは、ポリシーで必要な場合にはトラフィックシェーピングをオンにし、必要でない場合にはトラフィックシェーピングをオフにします。

トラフィックシェーピングの設定

この例では、同一のサブネット上にある 3 つのデパートメント間の T3 インターフェース上で帯域幅 45Mbps を分割します。インターフェース ethernet0/1 は、Trust ゾーンにバインドされ、ethernet0/3 は、Untrust ゾーンにバインドされます。

図 62: トラフィックシェーピング



WebUI

1. **インターフェースの帯域幅**
   Network > Interfaces > Edit (ethernet0/1): 次のように入力してから **OK** をクリックします。

   Traffic Bandwidth: 45000

注 : インターフェース上で帯域幅設定が指定されていない場合、セキュリティデバイスは利用可能な物理帯域幅を使用します。

   Network > Interfaces > Edit (ethernet0/3): 次のように入力してから **OK** をクリックします。

   Traffic Bandwidth: 45000

2. **ポリシーの帯域幅**
   Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Name: Marketing Traffic Shaping
   Source Address:
   Address Book Entry: (選択), Marketing
   Destination Address:
   Address Book Entry: (選択), Any
   Service: Any
   Action: Permit
   VPN Tunnel: None

注： VPN トンネルに関連付けるポリシーでは、トラフィックシェーピングも使用可能となります。

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Traffic Shaping: (選択)
Guaranteed Bandwidth: 10000
Maximum Bandwidth: 15000

Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Name: Sales Traffic Shaping Policy
Source Address:
Address Book Entry: (選択), Sales
Destination Address:
Address Book Entry: (選択), Any
Service: Any
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Traffic Shaping: (選択)
Guaranteed Bandwidth: 10000
Maximum Bandwidth: 10000

Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Name: Support Traffic Shaping Policy
Source Address:
Address Book Entry: (選択), Support
Destination Address:
Address Book Entry: (選択), Any
Service: Any
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Traffic Shaping: (選択)
Guaranteed Bandwidth: 5000
Maximum Bandwidth: 10000

Policy > Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Name: Allow Incoming Access to Marketing
Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), Marketing
Service: Any
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Traffic Shaping: (選択)
Guaranteed Bandwidth: 10000
Maximum Bandwidth: 10000

Policy > Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Name: Allow Incoming Access to Sales
Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), Sales
Service: Any
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Traffic Shaping: (選択)
Guaranteed Bandwidth: 5000
Maximum Bandwidth: 10000

Policy > Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Name: Allow Incoming Access to Support
Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), Support
Service: Any
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Traffic Shaping: (選択)
Guaranteed Bandwidth: 5000
Maximum Bandwidth: 5000

CLI

ポリシーによってトラフィックシェーピングを使用可能とするために、以下を実行してください。

1. インターフェースの帯域幅
set interface ethernet0/1 bandwidth 45000
set interface ethernet0/3 bandwidth 45000

注 : インターフェース上で帯域幅設定が指定されていない場合、セキュリティデバイスは利用可能な物理帯域幅を使用します。

---

2. **ポリシーの帯域幅**

```
set policy name ”Marketing Traffic Shaping”rom trust to untrust marketing any any
    permit traffic gbw 10000 priority 0 mbw 15000
set policy name “Sales Traffic Shaping Policy” from trust to untrust sales any any
    permit traffic gbw 10000 priority 0 mbw 10000
set policy name “Support Traffic Shaping Policy” from trust to untrust support any
    any permit traffic gbw 5000 priority 0 mbw 10000
set policy name “Allow Incoming Access to Marketing” from untrust to trust any
    marketing any permit traffic gbw 10000 priority 0 mbw 10000
set policy name “Allow Incoming Access to Sales” from untrust to trust any sales
    any permit traffic gbw 5000 priority 0 mbw 10000
set policy name “Allow Incoming Access to Support” from untrust to trust any
    support any permit traffic gbw 5000 priority 0 mbw 5000
save
```

サービス優先順位の設定

Juniper Networks セキュリティデバイスのトラフィックシェーピング機能を使うと、保証帯域幅に割り当てられていない、または未使用の保証帯域幅上で優先順位キューを実行できます。優先順位キューとは、必要に応じて、重要でないトラフィックの代わりに重要なトラフィックを通過させることで、すべてのユーザーとアプリケーションが利用可能な帯域幅にアクセスできるようにする機能のことです。キューを使うと、セキュリティデバイスは、最大 8 つの異なる優先順位キューでトラフィックをバッファできます。8 つのキュー :

- High priority (最優先)
- 2nd priority (第 2 位優先)
- 3rd priority (第 3 位優先)
- 4th priority (第 4 位優先)
- 5th priority (第 5 位優先)
- 6th priority (第 6 位優先)
- 7th priority (第 7 位優先)
- Low priority (最低優先) (デフォルト)

ポリシーのための優先順位設定は、まだ他のポリシーに保証されていない帯域幅が、最優先事項と優先順位最低事項を基本としてキューされることを意味します。同じ優先順位設定のあるポリシーは、ラウンドロビン方式で帯域幅と競合します。セキュリティデバイスは、まず最初にすべての最優先ポリシーからのトラフィックをすべて処理し、続いて優先順位が次に高いポリシーからのトラフィックをすべて処理します。このようにトラフィック要求は優先順位に従って順次処理されます。トラフィック要求が利用可能な帯域幅を超える場合、最低優先順位トラフィックがドロップします。

注意 : インターフェースのサポートを超える帯域幅を割り当てないように注意してください。ポリシー構成処理により、サポートされていないポリシー構成の作成が妨げられることはありません。競合しているポリシー上の保証帯域幅が、インターフェース上で設定されるトラフィック帯域幅を超える場合、データを失う可能性があります。

保証帯域幅を割り当てない場合、優先順位キューを使用して、ネットワーク上のトラフィックすべてを管理することができます。すなわち、すべての最優先トラフィックは、第 2 位優先トラフィックなどが送られる前に送られます。セキュリティデバイスは、他のすべてのトラフィックが処理された後で低優先トラフィックを処理します。

優先順位キューの設定

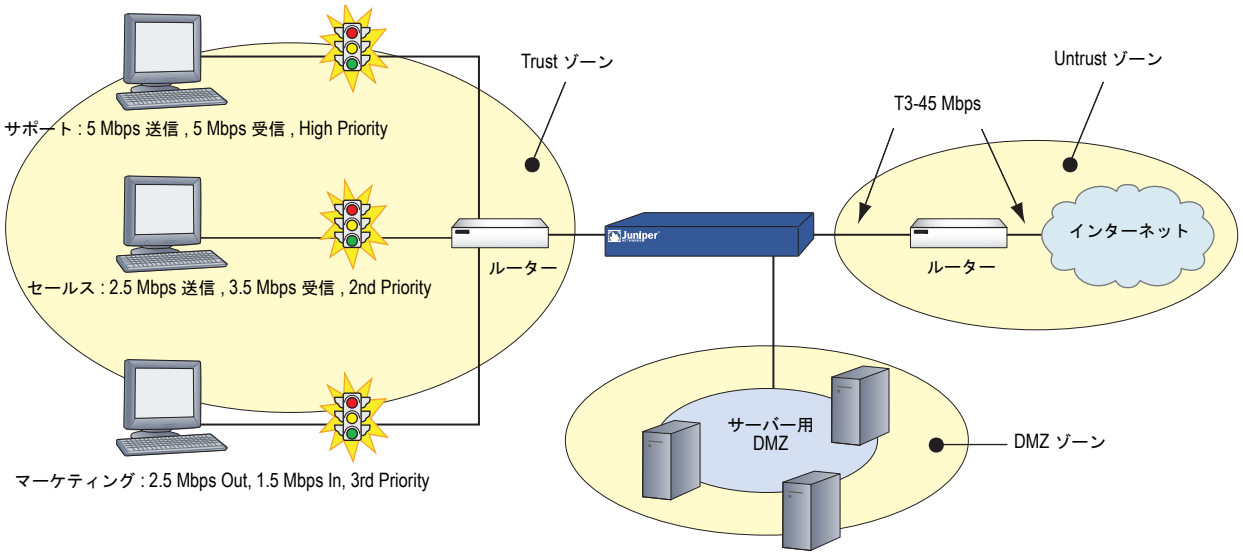
この例では、3 つの部門（サポート、セールス、マーケティング）の保証および最大帯域幅（単位 Mbps）を、表 30 のとおりに構成します。

表 30: 最大帯域幅の構成

	アウトバウンド保証	インバウンド保証	組合せ保証	優先順位
サポート	5	5	10	High
セールス	2.5	3.5	6	2
マーケティング	2.5	1.5	4	3
合計	10	10	20	

3 部門のすべてがファイアウォール経由でトラフィックを同時に送受信する場合、保証ポリシー要求を満たすためにセキュリティデバイスは 20 Mbps の帯域幅を割り当てる必要があります。インターフェース ethernet0/1 は、Trust ゾーンにバインドされ、ethernet0/3 は、Untrust ゾーンにバインドされます。

図 63: 優先順位キュー



WebUI

1. インターフェースの帯域幅

Interfaces > Edit (ethernet0/1): 次のように入力してから **OK** をクリックします。

Traffic Bandwidth: 40000

Interfaces > Edit (ethernet0/3): 次のように入力してから **OK** をクリックします。

Traffic Bandwidth: 40000

2. ポリシーの帯域幅

Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Name: Sup-out
Source Address:
Address Book Entry: (**選択**), Support
Destination Address:
Address Book Entry: (**選択**), Any
Service: Any
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Traffic Shaping: (**選択**)
Guaranteed Bandwidth: 5000
Maximum Bandwidth: 40000
Traffic Priority: High priority
DiffServ Codepoint Marking: (**選択**)

注： 差別化されたサービス (DS) は、優先順位の階層内の場所でトラフィックをタグ (あるいは「マーキング」) するためのシステムです。DS コードポイントマーキングは、ポリシーの ScreenOS 優先順位レベルを IP パケットヘッダーの DS フィールドにあるコードポイントの最初の 3 ビットにマッピングします。DS コードポイントマーキングに関する詳細については、175 ページの「トラフィックシェーピング」を参照してください。

Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Name: Sal-out
Source Address:
Address Book Entry: (**選択**), Sales
Destination Address:
Address Book Entry: (**選択**), Any
Service: Any
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Traffic Shaping: (**選択**)
Guaranteed Bandwidth: 2500
Maximum Bandwidth: 40000
Traffic Priority: 2nd priority
DiffServ Codepoint Marking: Enable

Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Name: Mar-out
Source Address:
Address Book Entry: (**選択**), Marketing
Destination Address:
Address Book Entry: (**選択**), Any
Service: Any
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Traffic Shaping: (**選択**)
Guaranteed Bandwidth: 2500
Maximum Bandwidth: 40000
Traffic Priority: 3rd priority
DiffServ Codepoint Marking: (**選択**)

Policy > Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Name: Sup-in
Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), Support
Service: Any
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Traffic Shaping: (**選択**)
Guaranteed Bandwidth: 5000
Maximum Bandwidth: 40000
Traffic Priority: High priority
DiffServ Codepoint Marking: (**選択**)

Policy > Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Name: Sal-in
Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), Sales
Service: Any
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Traffic Shaping: (**選択**)
Guaranteed Bandwidth: 3500
Maximum Bandwidth: 40000
Traffic Priority: 2nd priority
DiffServ Codepoint Marking: (**選択**)

Policy > Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Name: Mar-in
Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), Marketing
Service: Any
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Traffic Shaping: (**選択**)
Guaranteed Bandwidth: 1500
Maximum Bandwidth: 40000
Traffic Priority: 3rd priority
DiffServ Codepoint Marking: (**選択**)

CLI

1. **インターフェースの帯域幅**
   set interface ethernet0/1 bandwidth 40000
   set interface ethernet0/3 bandwidth 40000

2. **ポリシーの帯域幅**
   set policy name sup-out from trust to untrust support any any permit traffic gbw 5000 priority 0 mbw 40000 enable
   set policy name sal-out from trust to untrust sales any any permit traffic gbw 2500 priority 2 mbw 40000 dscp enable

---

注 : いくつかのデバイスでは、システム全体に渡る環境変数の設定により、明示的に DSCP マーキングを有効にする必要があります。ポリシーで使用する前に、ご使用のデバイスで明示的に DSCP マーキングを有効にする必要があるかどうかはハードウェアのマニュアルを参照してください。必要な場合は、コマンド **set envar ipsec-dscp-mark = yes** を使用して、DSCP マーキングをシステム全体で有効にします。この変数は、WebUI を使って設定できません。システム全体で DSCP マーキングを無効にするには、**unset envar ipsec-dscp-mark** を使用します。

---

set policy name mar-out from trust to untrust marketing any any permit traffic gbw 2500 priority 3 mbw 40000 dscp enable
set policy name sup-in from untrust to trust any support any permit traffic gbw 5000 priority 0 mbw 40000 dscp enable
set policy name sal-in from untrust to trust any sales any permit traffic gbw 3500 priority 2 mbw 40000 dscp enable
set policy name mar-in from untrust to trust any marketing any permit traffic gbw 1500 priority 3 mbw 40000 dscp enable
save

ingress ポリシング

ingress ポリシングは、セキュリティデバイスの ingress 側で行うトラフィック制御です。ingress ポイントでトラフィックのフローを制約することで、帯域幅設定を超過するトラフィックをドロップし、システムリソースを節約します。ingress ポリシングは、インターフェースレベルででも、セキュリティポリシーででも構成できます。

インターフェースでは、最大帯域幅（**mbw** キーワード）を設定することで、ingress ポリシングを構成できます。たとえば、次のコマンドは、ingress インターフェースである Ethernet0/1 の帯域幅を 22 Mbps に制限します。

```
set interface ethernet0/1 bandwidth ingress mbw 22000
```

ethernet0/1 の受信トラフィックでこの帯域幅を超えたものはドロップされます。インターフェースでトラフィックシェーピングを設定している場合は、トラフィックシェーピングモードをオン（**set traffic-shaping mode on**）に設定する必要があります。

ingress ポリシングを特定のアプリケーションに適用する場合には、ポリシーが必要です。次のコマンドは、セキュリティデバイスの ingress 側の FTP 帯域幅を 10 Mbps に制限する、*my_ftp* というポリシーを作成します。

```
set policy my_ftp from untrust to trust any any ftp permit traffic pbw 10000
```

受信 FTP トラフィックで、構成したポリシング帯域幅（**pbw** キーワード）を超過するものはドロップされます。ポリシーの **mbw** を設定することもできますが、ポリシーレベルでは **mbw** はトラフックフローの egress 側でしか適用されません。つまり、構成したレートを超過するトラフックは依然として処理され、egress 側でのみドロップされます（208 ページの図 65 を参照）。ポリシーで **mbw** または **pbw** を構成することができますが、両方を構成することはできません。

仮想インターフェースでの ingress ポリシングの構成と実施は、物理インターフェースの場合と同じですが、唯一、仮想インターフェースでは保証帯域幅（**gbw** キーワード）も構成できる点が異なります（208 ページの「ポリシーレベルのトラフィックシェーピング」を参照）。物理インターフェースでは、保証帯域幅は最大帯域幅と同じです。

注 : トンネルインターフェースでの ingress ポリシングは、暗号化されたパケットが VPN エンジンにより解読されてから実施されます。

仮想インターフェースのトラフィックシェーピング

トラフィックシェーピングのコンテキストでは、*仮想インターフェース*という用語はサブインターフェースおよびトンネルインターフェースのみを指します。つまり、仮想セキュリティインターフェース (VSI) や統合または冗長インターフェースなど、他の種類の仮想インターフェースは含まれません。vsys で作成されたポリシーには、シェーピングパラメータは構成できません。同様に、ユーザー作成の Vsys が所有する（引き継いだ）インターフェースでは、帯域幅はシェーピングできません。詳細については *第 10 部: 仮想 システム* を参照してください。

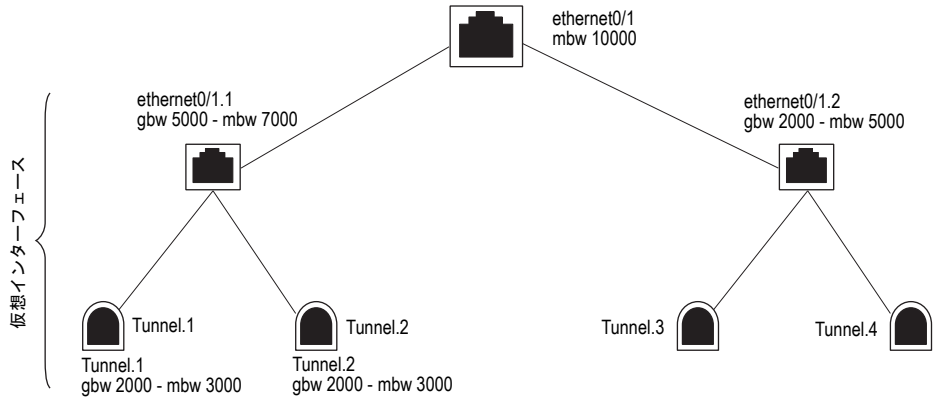
トラフィックシェーピングは、(ingress ポリシングとは異なり）セキュリティデバイスの egress 側でのトラフィック管理に関与します。仮想インターフェースの場合も、物理インターフェースと同様、インターフェースレベルまたはポリシーに帯域幅の値を設定してトラフィックをシェーピングします。

インターフェースレベルのトラフィックシェーピング

インターフェースレベルでのトラフィックシェーピングでは、特定のインターフェースにおけるトラフィックフローの最大量と最小量を制御します。最小帯域幅は、保証帯域幅（**gbw**）の指定によって制御されます。つまり、デバイスに何が起ころうとも、該当するトラフィックにはこの最小レートが保証されます。最大帯域幅（**mbw**）を設定することで、トラフィックが超過することのないレートが確定します。デフォルトでは、物理インターフェースの最大帯域幅はインターフェースの伝送容量になります。したがって物理インターフェースでは保証帯域幅を設定することはできません。

トラフィックシェーピングのコンテキストでは、仮想インターフェースという用語は、物理インターフェースにバインドされているサブインターフェース、およびその延長として、これらのサブインターフェースにバインドされているトンネルインターフェースのことを指します。これらはインターフェースの階層を形成します。物理インターフェースにバインドされたサブインターフェースは、*親*である物理インターフェースの *子*と呼ばれます。したがって、サブインターフェースにバインドされたトンネルインターフェースは、そのサブインターフェースの子になり、物理インターフェースはその *祖父母*になります。206 ページの図 64は、こうした依存関係を示しています。

図 64: インターフェースの階層



仮想インターフェースを操作する際は、インターフェースの階層に関する次のルールに留意してください。

- サブインターフェースに割り当てられた保証帯域幅は、バインド先の物理インターフェースの伝送容量を超過することはできません。たとえば、図 64 では、ethernet0/1.1 と ethernet0/1.2 を合わせた **gbw** は 9000 Kbps で、ethernet0/1 の **mbw** よりも 1000 Kbps 下回っています。一方、これらの 2 つのサブインターフェースの最大帯域幅の合計は、バインド先の物理インターフェースの伝送容量を 2000 Kbps 超えている点に注意してください。このような設定が許容されるのは、**mbw** キーワードがトラフィックを最大レートに制限するためだけに使用されるからですトラフィックがサブインターフェースの最大設定を下回っていれば、同じ物理インターフェースにバインドされている他のどのサブインターフェースもがその帯域幅を利用できます。

- トンネルインターフェースに割り当てられた保証帯域幅は、バインド先のサブインターフェースの保証帯域幅を超過することはできません。

- 直属の親に保証帯域幅が構成されていない場合は、祖父母インターフェースからの帯域幅を使用します。

- すべての子の保証帯域幅の合計が、親の保証帯域幅を超えることはできません。

- 1 つの子の最大帯域幅が、親の最大帯域幅を超えることはできません。

前述のとおり、物理インターフェースに保証帯域幅を設定すことはできません。これは、保証帯域幅がインターフェースのリンク速度である最大帯域幅と同じであるためです。一方、仮想インターフェースでは、egress の **gbw** および **mbw** を構成できます。また、インターフェースレベルの ingress ポリシングである **mbw** も構成することができます。次のコマンドは、Ethernet0/4.1 での最小出力ビットレートとして 1000 Kbps を保証し、最大レートは入出力とも 2000 Kbps を保証します。

```
set interface ethernet0/4.1 bandwidth egress gbw 1000 mbw 2000 ingress mbw
    2000
```

帯域幅は、WebUI の Network > Interfaces > Edit のページで設定します。

帯域幅を設定したら、**get traffic-shaping interface** コマンドを使って、実際の帯域幅がセキュリティデバイスを通過していることを確認します。たとえば、ethernet0/1 から入って ethernet0/3 から出るトラフィックがあるとします。ethernet0/1 に ingress 帯域幅を設定した場合、**get traffic-shaping interface ethernet0/3** コマンドを使うと、デバイス上の実際のスループットが表示されます。

インターフェースでトラフィックシェーピングを設定している場合は、トラフィックシェーピングモードをオン（**set traffic-shaping mode on**）に設定する必要があります。

ポリシーレベルのトラフィックシェーピング

トラフィックをポリシーレベルでシェーピングすると、帯域幅を特定のタイプのトラフィックに割り当てることができます。次のコマンドを使うと、FTP のトラフィックに最低 1Mbps の帯域幅が保証され、また 2 Mbps を越えるトラフィックはすべてドロップされます。

```
set policy from trust to untrust any any ftp permit traffic gbw 1000 pbw 2000
```

このコマンドはポリシング帯域幅（**pbw**）キーワードを使用する点に注意してください。ポリシーで **pbw** または **mbw** を構成することができますが、両方を構成することはできません。**pbw** を使用する利点は、セキュリティデバイスの ingress 側でトラフィックがドロップされるため、スループット処理が軽減されてシステムリソースを節約できることです。（205 ページの「ingress ポリシング」を参照してください。）

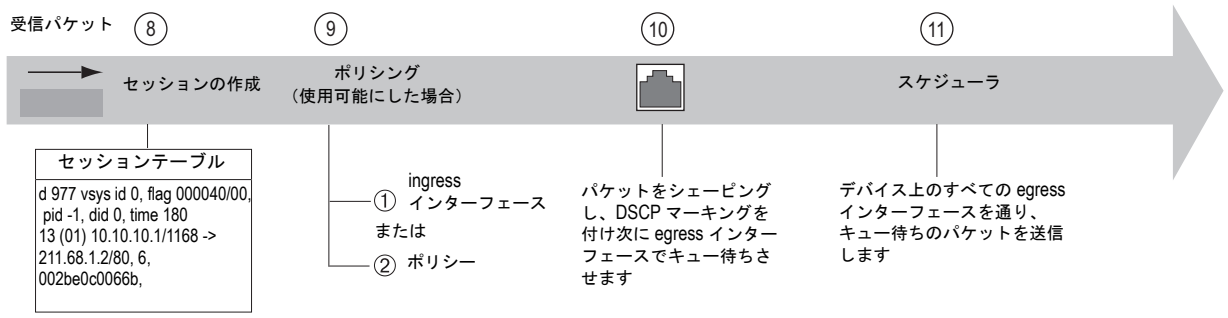
ポリシー作成後に、WebUI の Advanced ボタンをクリックして、トラフィックシェーピングパラメータを構成します。

トラフィックをインターフェースでシェーピングするにはトラフィックシェーピングモードを **on** にする必要がありますが、トラフィックをポリシーでシェーピングする場合はトラフィックシェーピングをオンにする必要はありません。これは、トラフィックシェーピングモードが、デフォルトで **auto** に設定されているためです。セッションがアクティブになり、ポリシールックアップがトラフィックシェーピングを検出すると、ScreenOS がそのセッションのトラフィックシェーピングをオンにします。

パケットフロー

図 65 は、トラフィックシェーピングとポリシングの影響を受けるセキュリティデバイスを通過するパケットフローの一部を示しています（パケットフローの全体図は 11 ページの「パケットフローシーケンス」を参照してください）。**pbw**（インターフェースで構成されている場合は **mbw**）を超過するパケットは手順 9 でドロップされ、手順 10 でシェーピングと DSCP マーキングが実行され、手順 11 で **mbw**（ポリシーで構成の場合）を超過するパケットがドロップされます。

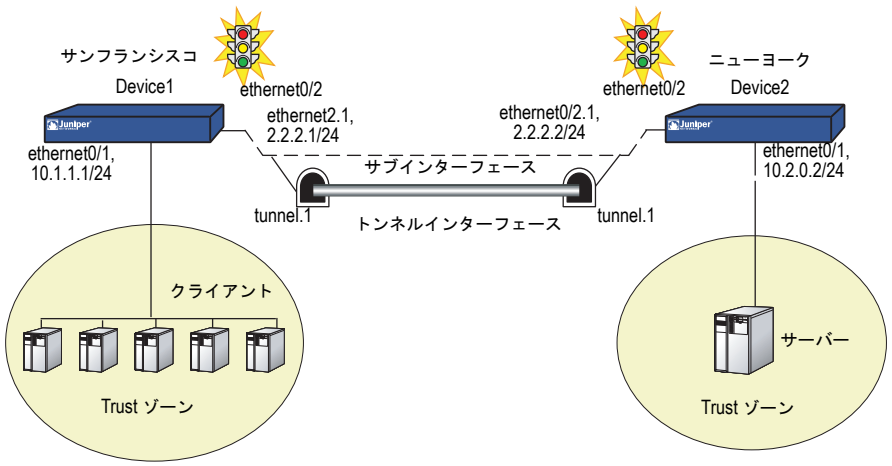
図 65: トラフィックシェーピングパケットフロー



例 : ingress ポリシングのあるルートベースの VPN

次の例では、インターフェースレベルの ingress ポリシングを暗号化トラフックに実施する方法を示します。ingress ポリシングは、サブインターフェース（ethernet0/2.1、最大帯域幅 :1200 Kbps）およびトンネルインターフェース（tunnel.1、最大帯域幅 : 1000 Kbps）の両方で構成されています。サブインターフェースのポリシングレートを、そのサブインターフェースにバインドされているトンネルインターフェースのものよりも高く設定すると、暗号化のオーバーヘッドが可能になります（この例では、サブインターフェースで受信するトラフィックのすべてがトンネルインターフェースに向かうものと仮定としています）。サブインターフェースのポリシングは暗号化パケットに適用され、トンネルインターフェースのポリシングは復号化された内部パケットに適用されます。ethernet0/2.1 の 1200 Kbps を超過する暗号化トラフックはすべてドロップされます。また、tunnel.1 インターフェースの 1000 Kbps を超過する復号化（クリアテキスト）トラフックもすべてドロップされます。

図 66: ルートベース VPN



WebUI（Device1 の構成）

1. **インターフェース**

   Network > Interfaces > Edit (ethernet0/1): 次のように入力してから **OK** をクリックします。

   IP Address/Netmask: 10.1.1.1/24
   Zone: Trust

   Network > Interfaces > Sub-IF > New: 以下を入力して **Apply** をクリックします。

   Interface Name: (選択) ethernet0/2 と 1 を入力
   Zone: Untrust
   IP Address/Netmask: 2.2.2.1/24
   VLAN Tag: 128

   Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

   Tunnel Interface Name: 1
   Zone: Untrust
   Unnumbered (選択) ethernet0/2.1
   Interface: ethernet0/2.1

2. **ルート**
   Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 10.2.0.0/24
   interface (**選択**): Tunnel.1

3. **IKE**
   VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

   Gateway Name: device1_ike
   Security Level: Standard
   Remote Gateway Type:
   Static IP Address: (**選択**), IP Address/Hostname: 2.2.2.2
   事前共有鍵

   Preshared Key: Secret:
   Outgoing Interface: ethernet0/2.1

   VPNs > AutoKey IKE New: 次のように入力してから **OK** をクリックします。

   VPN Name: device1_vpn
   Gateway Name: device1_ike

   > Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

   Bind to: (**選択**) Tunnel Interface, (**選択**) tunnel.1

CLI（Device1 の構成）

1. **インターフェース**
   set interface ethernet0/1 zone trust
   set interface ethernet0/1 ip 10.1.1.1/24
   set interface ethernet0/2.1 tag 128 zone untrust
   set interface tunnel.1 zone trust
   set interface ethernet0/2.1 ip 2.2.2.1/24
   set interface tunnel.1 ip unnumbered interface ethernet0/2.1
   set route 10.2.0.0/24 int tunnel.1

2. **IKE**
   set ike gateway device1_ike address 2.2.2.2 outgoing-interface ethernet0/2.1 preshare sec-level standard
   set vpn device1_vpn gateway 208a_ike sec-level standard
   set vpn device1_vpn bind interface tunnel.1
   save

WebUI（Device2 の構成）

1. **インターフェース**
   Network > Interfaces > Edit (ethernet0/1): 次のように入力してから **OK** をクリックします。

   IP Address/Netmask: 10.2.0.2/24
   Zone: Trust

Network > Interfaces > Sub-IF > New: 以下を入力して **Apply** をクリックします。

Interface Name: (選択) ethernet0/2 と 1 を入力
Zone: Untrust
IP Address/Netmask: 2.2.2.2/24
VLAN Tag: 128

Network > Interfaces > Tunnel IF > New: 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 1
Unnumbered: (選択) ethernet0/2.1
Interface: ethernet0/2.1

2. インターフェースの帯域幅

Network > Interfaces > Edit (ethernet0/2.1): 次のように入力してから **OK** をクリックします。

Traffic Bandwidth, Ingress: 1200

Network > Interfaces > Edit (tunnel.1): 次のように入力してから **OK** をクリックします。

Traffic Bandwidth, Ingress: 1000

3. ルート

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
interface (選択): Tunnel.1

4. IKE

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: device2_ike
Security Level: Standard
Remote Gateway Type:
Static IP Address: (選択), IP Address/Hostname: 2.2.2.2

事前共有鍵

Preshared Key: Secret
Outgoing Interface: ethernet0/2.1

VPNs > AutoKey IKE New: 次のように入力してから **OK** をクリックします。

VPN Name: device2_vpn
Gateway Name: device2_ike

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: (選択) Tunnel Interface, (選択) tunnel.1

5. **ポリシー**
   Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Service: Any
   Action: Permit

   Policy > Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

   Service: Any
   Action: Permit

CLI（Device2 の構成）

1. **インターフェース**
   set interface ethernet0/1 zone trust
   set interface ethernet0/1 ip 10.2.0.2/24
   set interface ethernet0/2.1 tag 128 zone untrust
   set interface ethernet0/2.1 ip 2.2.2.2/24
   set interface tunnel.1 zone untrust
   set interface tunnel.1 ip unnumbered interface ethernet0/2.1
   set route 10.1.1.0/24

2. **インターフェースの帯域幅**
   set interface ethernet0/2.1 bandwidth ingress mbw 1200
   set interface tunnel.1 bandwidth ingress mbw 1000

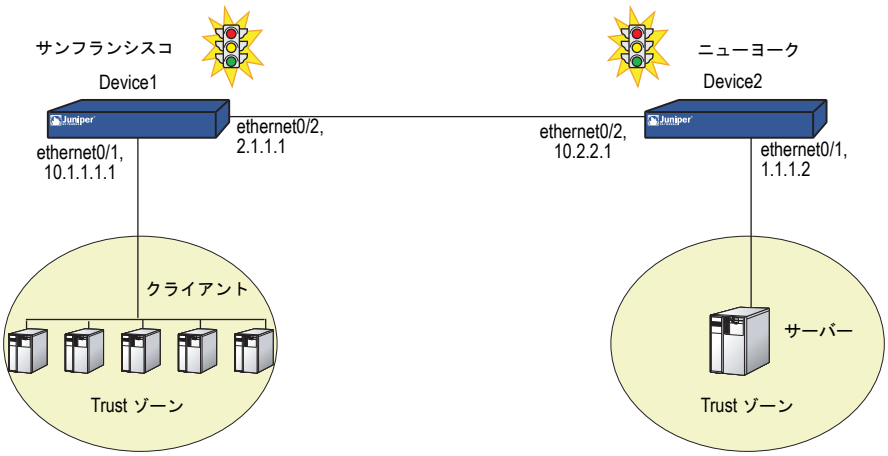
3. **IKE**
   set ike gateway device2_ike address 2.2.2.1 preshare secret sec-level standard
   set vpn device2_vpn gateway 208b_ike sec-level standard
   set vpn device2_vpn bind interface tunnel.1

4. **ポリシー**
   set policy from trust to untrust any any any permit
   set policy from untrust to trust any any any permit
   save

例: ingress ポリシングのあるルートベースの VPN

次の例では、インターフェースレベルとポリシーの両方で ingress ポリシングを実施する方法を示します。*Device1* の ethernet0/1 インターフェースで、ingress の最大帯域幅を 20000 Kbps に設定します。この設定により、*Device1* に接続されているクライアントからの 20000 Kbps を超過するトラフィックは ethernet0/1 インターフェースですべてドロップされます。インターフェースでの ingress ポリシングは、そのインターフェースに達するトラフィックすべてに適用されます。細分性を高めるためには、ingress ポリシングをポリシーレベルで適用します。この例では、Trust ゾーンと Untrust ゾーン の間にポリシーを作成することで、*Device1* のすべての ingress FTP プロトコルトラフィックを制限するポリシーを作成し、ポリシング帯域幅を 5000 Kbps に設定しています。Trust ゾーンから Untrust ゾーンに向かう FTP トラフィックで 5000 Kbps を超過するものはすべてドロップされます。

図 67: ポリシーベース VPN



WebUI（Device1 の構成）

1. インターフェース

Network > Interfaces > Edit (ethernet0/1): 次のように入力してから **OK** をクリックします。

IP Address/Netmask: 10.1.1.1/24
Zone: Trust
Interface Mode: (選択) NAT

Network > Interfaces > Edit (ethernet0/2): 次のように入力してから **OK** をクリックします。

IP Address/Netmask: 2.1.1.1/24
Zone: Untrust
Interface Mode: (選択) Route

2. IKE VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: device2_ike
Security Level: Standard
Remote Gateway Type:
Static IP Address: (選択), IP Address/Hostname: 2.2.2.2

事前共有鍵

Preshared Key: Secret:
Outgoing Interface: ethernet0/2

> Advanced: 次の詳細設定を入力してから **OK** をクリックして基本ゲートウェイ構成ページに戻ります。

フェーズ 1 プロポーザル : pre-g2-3des-sha

VPNs > AutoKey IKE New: 次のように入力してから **OK** をクリックします。

VPN Name: device2_vpn
Gateway Name: device2_ike

3. **インターフェースベースポリシング**
   Network > Interfaces > Edit (ethernet0/1): 次のように入力してから **OK** をクリックします。

   Traffic Bandwidth, Ingress: 20000

4. **ルーティング**
   Network > Routing > Destination > New: 次のように入力してから **OK** をクリックします。

   Network IP Address/Netmask: 10.2.1.0/24
   Interface: (選択) ethernet0/2
   Gateway IP Address: 2.2.2.2

5. **ポリシー**
   Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Name: 1
   Service: FTP
   Action: Tunnel
   Tunnel VPN: (選択), device2_vpn
   Modify matching bidirectional VPN policy: (選択)

   > Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

   Traffic Shaping（選択）Policing Bandwidth: 5000

CLI（Device1 の構成）

1. **インターフェース**
   set interface ethernet0/1 zone trust
   set interface ethernet0/2 zone untrust
   set interface ethernet0/1 ip 10.1.1.1/24
   set interface ethernet0/1 nat
   set interface ethernet0/2 ip 2.1.1.1/24
   set interface ethernet0/1 route

2. **IKE VPN**
   set ike gateway device2_ike address 2.2.2.2 main outgoing interface ethernet0/2 preshare secret proposal pre-g2-3des-sha
   set vpn device2_vpn gateway device2_ike no-replay tunnel idletime 0 sec-level standard

3. **ルーティング**
   set route 10.2.1.0/24 interface ethernet0/2 gateway 2.2.2.2

4. **ポリシー**
   set policy from trust to untrust any any ftp tunnel vpn device2_vpn pair-policy 2 traffic pbw 5000
   set policy from untrust to trust any any ftp tunnel vpn netscreen2_vpn pair-policy 1 traffic pbw 5000

5. **インターフェースベースポリシング**
   set interface ethernet0/1 bandwidth ingress mbw 20000
   save

WebUI（Device2 の構成）

1. インターフェース

Network > Interfaces > Edit (ethernet0/1): 次のように入力してから **OK** をクリックします。

IP Address/Netmask: 1.1.1.1/24
Zone: Trust
Interface Mode: (選択) Route

Network > Interfaces > Edit (ethernet0/2): 次のように入力してから **OK** をクリックします。

IP Address/Netmask: 10.2.2.1/24
Zone: Untrust
Interface Mode: (選択) NAT

2. IKE VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: device1_ike
Security Level: Standard
Remote Gateway Type:
Static IP Address: (選択), IP Address/Hostname: 2.1.1.1

3. 事前共有鍵

Preshared Key: Secret:
Outgoing Interface: ethernet0/2

> Advanced: 次の詳細設定を入力してから **OK** をクリックして基本ゲートウェイ構成ページに戻ります。

Phase 1 Proposal: pre-g2-3des-sha

VPNs > AutoKey IKE New: 次のように入力してから **OK** をクリックします。

VPN Name: device1_vpn
Gateway Name: device1_ike

4. *ルーティング*

Network > Routing > Destination > New: 次のように入力してから **OK** をクリックします。

Network IP Address/Netmask: 10.1.1.0/24
Interface: (選択) ethernet0/2
Gateway IP Address: 1.1.1.1

5. ポリシー

Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Name: 1
Service: FTP
Action: Tunnel
Tunnel VPN: (選択), device1_vpn
Modify matching bidirectional VPN policy: (選択)

CLI（Device2 の構成）

1. **インターフェース**
   set interface ethernet0/1 1.1.1.2/24
   set interface ethernet0/1 route
   set interface ethernet0/2 ip 10.2.2.1/24
   set interface ethernet0/2 nat

2. **IKE VPN**
   set ike gateway device1_ike address 2.1.1.1 main outgoing interface ethernet0/2 preshare secret proposal pre-g2-3des-sha
   set vpn device1_vpn gateway device1_ike no-replay tunnel idletime 0 sec-level standard

3. **ルーティング**
   set route 10.1.1.0/24 interface ethernet0/1 gateway 1.1.1.1

4. **ポリシー**
   set policy id 1 from trust to untrust any any ftp tunnel vpn device1_vpn pair-policy 2
   set policy id 2 from untrust to trust any any ftp tunnel vpn device1_vpn pair-policy 1
   save

ループバックインターフェースを使用したトラフィックシェーピング

ループバックインターフェースでは実際にはトラフィックが送信されないため、トラフィックシェーピングはループバックインターフェースではサポートされません。しかし、データが実際の egress インターフェースに送信される間、ループバックインターフェースがアンカーポイントとして使用されることがよくあります（ソース IP アドレスを導き出すための VPN の場合など）。したがって、VPN でループバックインターフェースを使用するときは、出力インターフェースでトラフィックシェーピングを構成します。ScreenOS は、セッションを実際の出力インターフェースと関連付け（ルーティングテーブルからその関連付けを推定）、ルーティングテーブルが変更されるときに関連付けを動的に更新します。

DSCP マーキングとシェーピング

この章の前の部分で説明したように、差別化されたサービス (DS) は、優先順位の階層内の場所でトラフィックをタグ (あるいは「マーキング」) するためのシステムです。DSCP (Differentiated Services Codepoint: 差別化されたサービスコードポイント) マーキングは、ポリシーの ScreenOS 優先順位レベルを IP パケットヘッダーの DS フィールドにあるコードポイントの最初の 3 ビットにマッピングします。(詳細については、200 ページの「サービス優先順位の設定」を参照してください。)

DSCP マーキングを使用するポリシーでトラフィックをシェーピングすることも、トラフィックシェーピングとは関係なく DSCP マーキングを使用することもできます。トラフィックシェーピングは、トラフィックがセキュリティデバイスでどのように処理されるかを規定するもので、インターフェースレベルまたはポリシーで構成できます。DSCP マーキングは、ポリシーレベルで設定するもので、トラフィックが下流ルーターによってどのように処理されるかを規定します。

注 : いくつかのデバイスでは、システム全体に渡る環境変数の設定により、明示的に DSCP マーキングを有効にする必要があります。ポリシーで使用する前に、ご使用のデバイスで明示的に DSCP マーキングを有効にする必要があるかどうかはハードウェアのマニュアルを参照してください。必要な場合は、コマンド **set envar ipsec-dscp-mark = yes** を使用して、DSCP マーキングをシステム全体で有効にします。この変数は、WebUI を使って設定できません。システム全体で DSCP マーキングを無効にするには、**unset envar ipsec-dscp-mark** を使用します。

ポリシーで DSCP マーキングを指定しながら値が設定されていない場合は、ScreenOS はポリシー優先順位を DSCP システムにある同等の IP の優先順位にマッピングします。この場合、ToS の最初の 3 バイトをその IP 優先順位で上書きします。たとえば、すべてのトラフィックに優先順位 2（0 が最優先）を付けるポリシーを作成し、DSCP マーキングを使用可能にした場合、ScreenOS は、トラフィックを egress インターフェースでレベル 2 のポリシーのキューに入れ、同等の IP の優先順位でマーキングします。次のコマンドは、すべてのトラフィックに優先順位 2 を付け、DSCP マーキングを使用可能にするポリシーを作成します。

```
set policy from trust to untrust any any any permit traffic priority 2 dscp enable
```

しかし、DSCP に、たとえば 46（最優先）の *dscp-byte* **value** を付ける場合も、セキュリティデバイスはトラフィックを egress インターフェースで優先順位 2 のキューに入れますが、ToS の最初の 6 バイトを DSCP 値で上書きします。

```
set policy from trust to untrust any any any permit traffic priority 2 dscp enable
    value 46
```

DSCP マーキングは、すべてのプラットフォームでサポートされ、トラフィックシェーピングでまたは独自に構成されます。表 31 は、DSCP マーキングがポリシーでクリアパケットにどのように作用するかを示しています。図 66 は、DSCP マーキングがポリシーベースの VPN でクリアパケットにどのように作用するかを示し、表 33 は、DSCP マーキングがルートベースの VPN でクリアパケットにどのように作用するかを示しています。

表 31: クリアテキストトラフィックの DSCP マーキング

解説	アクション
ポリシーにマーキングのないクリアパケット。	マーキングなし。
ポリシーにマーキングのあるクリアパケット。	パケットにポリシーベースでマーキング。
ポリシーにマーキングのないマーキング済みパケット。	パケットのマーキングを維持。
ポリシーにマーキングのあるマーキング済みパケット。	パケットのマーキングにポリシーベースで上書き。

表 32: ポリシーベース VPN の DSCP マーキング

解説	アクション
クリアパケットをポリシーにマーキングのないポリシーベース VPN に送信。	マーキングなし。
クリアパケットをポリシーにマーキングのあるポリシーベース VPN に送信。	内部パケットと ESP ヘッダーの両方にポリシーベースでマーキング。

解説	アクション
マーキング済みパケットをポリシーにマーキングのないポリシーベース VPN に送信。	内部パケットのマーキングを ESP ヘッダーにコピー、内部パケットのマーキングは維持。
マーキング済みパケットをポリシーにマーキングのあるポリシーベース VPN に送信。	ポリシーベースで内部パケットのマーキングを上書き、かつ内部パケットのマーキングを ESP ヘッダーにコピー。

表 33: ルートベース VPN の DSCP マーキング

解説	アクション
クリアパケットをポリシーにマーキングのないルートベース VPN に送信。	マーキングなし。
クリアパケットをポリシーにマーキングのあるルートベース VPN に送信。	内部パケットと ESP ヘッダーの両方にポリシーベースでマーキング。
マーキング済みパケットをポリシーにマーキングのないルートベース VPN に送信。	内部パケットのマーキングを ESP ヘッダーにコピー、内部パケットのマーキングは維持。
マーキング済みパケットをポリシーにマーキングのあるルートベース VPN に送信。	ポリシーベースで内部パケットのマーキングを上書き、かつ内部パケットのマーキングを ESP ヘッダーにコピー。

第 8 章
システムパラメータ

本章では、セキュリティアプライアンスの以下の領域に影響を及ぼすシステムパラメータの設定に関する概念を中心に取り上げます。本章のセクションは、以下のようになります。

- 219 ページの「ドメイン名システムサポート」
- 227 ページの「動的ホスト構成プロトコル」
- 246 ページの「Point-to-Point Protocol over Ethernet」
- 254 ページの「ライセンスキー」
- 255 ページの「ライセンスサービスの登録およびアクティブ化」
- 257 ページの「システムクロック」

ドメイン名システムサポート

Juniper Networks セキュリティデバイスは、位置を識別するドメイン名と IP アドレスを使用できる DNS（ドメイン名システム）サポートを実装しています。DNS サーバーは、ドメイン名と関連付けられた IP アドレスのテーブルを保持しています。DNS を使用することによって、ルーティング可能な IP アドレスを使用できるだけではなく、ドメイン名 (www.juniper.net など) による位置の参照もできます。すなわち、www.juniper.net の DNS は 207.17.137.68 になります。DNS 変換は、以下のすべてのプログラムでサポートされています。

- アドレス帳
- Syslog
- Email
- WebTrends
- Websense
- LDAP
- SecurID

- RADIUS
- NetScreen-Security Manager

ドメイン名 / アドレス解決のために DNS を使用する前に、セキュリティデバイスの DNS サーバー（1 次 DNS サーバーと 2 次 DNS サーバー）にアドレスを入力する必要があります。

注： DHCP（動的ホスト構成プロトコル）サーバーとして セキュリティデバイスを使用可能にする場合は（227 ページの「動的ホスト構成プロトコル」を参照）、WebUI の DHCP ページ、または CLI の **set interface** *interface* **dhcp** コマンドで、DNS サーバーの IP アドレスを入力する必要があります。

DNS ルックアップ

セキュリティデバイスは以下のときに、DNS テーブルにあるすべてのエントリを指定 DNS サーバーでチェックして、これらをリフレッシュします。

- HA フェールオーバーが発生した後
- 時間単位でスケジュールされている間隔、および日数単位でスケジュールされている間隔
- NetScreen デバイスで DNS ルックアップを手動で実行する場合
  - WebUI: Network > DNS > Host: **Refresh** をクリックします。
  - CLI: **exec dns refresh**

DNS テーブルを毎日自動でリフレッシュする時間を設定することはすでにできますが、4 ～ 24 時間で間隔を定義することもできます。

注： アドレスや IKE ゲートウェイなど、完全に修飾されたドメイン名（FQDN）を WebUI を介して追加した場合は、**Apply** または **OK** をクリックしたときに、セキュリティデバイスはその名前を解決します。FQDN を参照する CLI コマンドを入力すると、セキュリティデバイスは入力時にその名前を解決しようとします。

セキュリティデバイスが DNS サーバーに接続してドメイン名 /IP アドレスマッピングを解決する場合、デバイス自身の DNS ステータステーブルにドメイン名 /IP アドレスのマッピングのエントリを格納します。以下のリストには、DNS ルックアップに関するいくつかの詳細が記載されています。

- DNS ルックアップが複数のエントリを返した場合は、アドレス帳はすべてのエントリを受け付けます。219 ページにリストされているその他のプログラムは、最初のものだけを受け付けます。
- WebUI の **Refresh** ボタンを使用して、または CLI の **exec dns refresh** コマンドを入力してルックアップがリフレッシュされると、セキュリティデバイスはドメイン名に変更があることを見つけた場合にすべてのポリシーを再インストールします。

- DNS サーバーで失敗した場合、セキュリティデバイスはもう 1 度すべてをルックアップします。
- ルックアップに失敗した場合は、キャッシュテーブルからルックアップを削除します。
- アドレス帳にアドレスを追加する時にドメイン名のルックアップに失敗した場合、セキュリティデバイスは、アドレスの追加には成功したが、DNS 名前ルックアップには失敗したことを知らせるエラーメッセージを表示します。

セキュリティデバイスは、1 日に 1 回新しいルックアップを実行する必要があります。指定した時間にルックアップを実行するようにセキュリティデバイスをスケジュールできます。

WebUI

Network > DNS > Host: 以下を入力して **Apply** をクリックします。

DNS refresh every day at: **チェックボックスを選択して、時間** <hh:mm> **を入力します。**

CLI

set dns host schedule *time_str*
save

DNS 状況テーブル

DNS 状況テーブルは、ルックアップされたすべてのドメイン名、対応する IP アドレス、ルックアップ成功の有無、および各ドメイン名 /IP アドレスが最後に解決された時期を報告します。

表 34: DNS 状況テーブル

名前	IP Address	状況	最後のルックアップ
www.yahoo.com	204.71.200.74 204.71.200.75 204.71.200.67 204.71.200.68	成功	8/13/2000 16:45:33
www.hotbot.com	209.185.151.28 209.185.151.210 216.32.228.18	成功	8/13/2000 16:45:38

DNS 状況テーブルを閲覧するには、以下のいずれかを実行します。

WebUI

Network > DNS > Host > Show DNS Lookup Table

CLI

get dns host report

DNS サーバーとリフレッシュスケジュールの設定

DNS 機能性を実装するには、DNS サーバーの IP アドレス 24.1.64.38 と 24.0.0.3 を セキュリティデバイスに入力し、ホームオフィス内の単一のホストを保護します。セキュリティデバイスは、毎日午後 11:00 に DNS ステータステーブルに格納されている DNS 設定をリフレッシュするようスケジュールされています。

図 68: DNS リフレッシュ



WebUI

Network > DNS > Host: 以下を入力して **Apply** をクリックします。

Primary DNS Server: 24.0.0.3
Secondary DNS Server: 24.1.64.38
DNS Refresh: (選択)
Every Day at: 23:00

CLI

```
set dns host dns1 24.0.0.3
set dns host dns2 24.1.64.38
set dns host schedule 23:00
save
```

DNS リフレッシュ間隔の設定

この例では、DNS テーブルを毎日午前 00:01 から 4 時間ごとにリフレッシュするように セキュリティデバイスを構成します。

WebUI

Network > DNS > Host: 以下を入力して **Apply** をクリックします。

DNS Refresh: (選択)
Every Day at: 00:01
Interval: 4

CLI

```
set dns host schedule 00:01:00 interval 4
save
```

動的ドメイン名システム

動的 DNS（DDNS）とは、登録されたドメイン名の IP アドレスをクライアント側で動的に更新できる機構です。この更新は、ISP 側で PPP や DHCP、XAuth を使用して CPE ルーター（セキュリティデバイスなどの、Web サーバーを保護するデバイス）の IP アドレスを動的に変更する場合に有効です。CPE ルーターの IP アドレスが変更されている場合でも、インターネットからのクライアントはドメイン名を使用して Web サーバーにアクセスすることができます。dyndns.org や ddo.jp などの DDNS サーバーには動的に変更されたアドレスとそのアドレスに関連付けられたドメイン名が含まれます。DDNS サーバーによって、この IP アドレス変更が可能となります。CPE ルーターは DDNS サーバーのアドレスとドメイン名の情報を使用して、定期的または IP アドレス変更のたびに DDNS サーバーを更新します。

DDNS を使用するには、DDNS サーバー上でアカウント (ユーザー名とパスワード) を作成します。DDNS サーバーは、このアカウント情報を使用してクライアントデバイスを設定します。

図 69: 動的 DNS

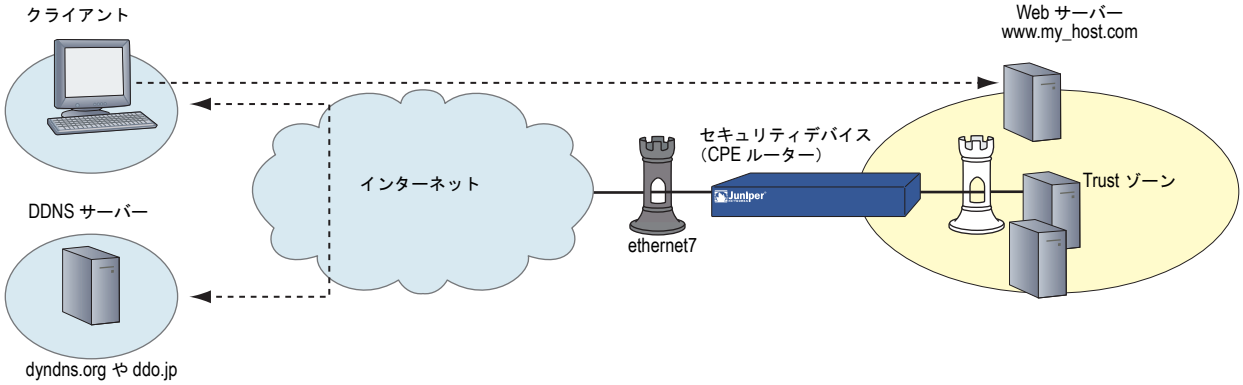


図 69 では、インターフェース ethernet7 の IP アドレスが変更される可能性があります。IP アドレスが変更されても、クライアントはホスト名（www.my_host.com）を使用して dyndns.org サーバー または ddo.jp サーバーのいずれかを経由して保護されている Web サーバーにアクセスできます。この 2 つのサーバーは、セキュリティデバイス上での設定が異なります。

DynDNS サーバー用の DDNS の設定

次の例では、DDNS 動作を有効にするためにセキュリティデバイスを設定します。NetScreen デバイスが dyndns.org サーバーを使用して変更されたアドレスを解決します。このサーバーについては、Host Name 設定を使って保護されているホストを指定し、DNS インターフェース（ethernet7）を明示的にバインドします。デバイスは、ddo.jp サーバーに更新を送信するときに、ホスト名をインターフェースの IP アドレスに関連付けます。

WebUI

Network > DNS > DDNS > New: 次のように入力してから **OK** をクリックします。

ID: 12
サーバー設定
Server Type: dyndns
Server Name: dyndns.org
Refresh Interval: 24
Minimum Update Interval: 15
アカウント設定
Username: swordfish
Password: ad93lvb
Bind to Interface: ethernet7
Host Name: www.my_host.com

注： Minimum Update Interval 設定は、DDNS を更新する最小の時間間隔（分）を指定します。デフォルトは 10 秒で、設定可能範囲は 1 ～ 1440 です。DNS サーバーはまずキャッシュから DDNS エントリをタイムアウトする必要があるため、場合によってはこの最小時間間隔で更新が行われない可能性があります。さらに、Minimum Update Interval 設定値を小さくすると、セキュリティデバイスがユーザーをロックアウトする可能性があります。推奨値は、10 分以上です。

CLI

```
set dns ddns
set dns ddns enable
set dns ddns id 12 server dyndns.org server-type dyndns refresh-interval 24
    minimum-update-interval 15
set dns ddns id 12 src-interface ethernet7 host-name www.my_host.com
set dns ddns id 12 username swordfish password ad93lvb
save
```

DDO サーバー用の DDNS の設定

次の例では、DDNS を動作させるためのセキュリティデバイスを構成します。NetScreen デバイスが ddo.jp サーバーを使用してアドレスを解決します。ddo.jp サーバーでは、設定したホスト名を使用して保護されたホストを指定するのではなく、保護されたホストの FQDN を DDNS エントリのユーザー名として指定します。ユーザー名からホスト名が自動的に生成されます。たとえば、ddo.jp サーバーはユーザー名 my_host を my_host.ddo.jp に変換します。ddo.jp に登録されているドメイン名が、派生された DNS と一致することが必要です。

WebUI

Network > DNS > DDNS > New: 次のように入力してから **OK** をクリックします。

ID: 25
サーバー設定
Server Type: ddo
Server Name: juniper.net
Refresh Interval: 24
Minimum Update Interval: 15
アカウント設定
UserName: My_host
Password: ad93lvb
Bind to Interface: ethernet7

CLI

```
set dns ddns
set dns ddns enable
set dns ddns id 25 server ddo.jp server-type ddo refresh-interval 24
     minimum-update-interval 15
set dns ddns id 25 src-interface ethernet7
set dns ddns id 25 username my_host password ad93lvb
save
```

プロキシ DNS アドレスの分割

プロキシ DNS 機能によって、分割した DNS クエリーをクライアント側で作成できる透過メカニズムが提供されます。この機能ではドメイン名の一部またはすべてに従って、プロキシが DNS クエリーを特定の DNS サーバーに選択的に転送します。この機能は、複数のネットワーク接続を提供する VPN トンネルや PPPoE 仮想リンクが、複数の DNS クエリーを単数のネットワークに転送することが必要な場合に有効です。

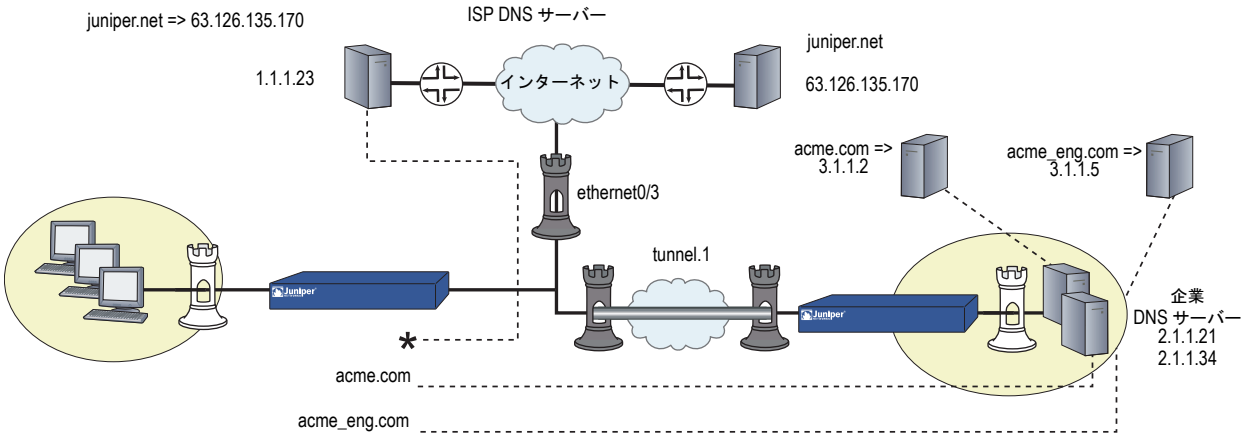
DNS プロキシの利点は次の通りです。

- 通常のドメインルックアップが効率的になります。たとえば、acme.com などの企業ドメインに向けた DNS クエリーは企業の DNS サーバーに排他的に転送し、他のクエリーはすべて ISP DNS サーバーに転送すると、企業サーバーへの負荷が軽減されます。また、企業ドメイン情報がインターネットに漏洩することを防ぐことができます。

- DNS プロキシを使用すると、選択した DNS クエリーをトンネルインターフェース経由で転送して、悪意のあるユーザーにネットワークの内部構成を知られないようにすることができます。たとえば、企業サーバーに向けた DNS クエリーはトンネルインターフェースを通過して、認証や暗号化、再生防止などのセキュリティ機能を使用できます。

以下にあるコマンドを使用すると、DNS クエリーをさまざまなサーバーに選択的に転送するプロキシ DNS エントリが 2 つ作成されます。

図 70: DNS 要求の分割



- ドメイン名 acme.com が含まれている FQDN に関連付けられた任意の DNS クエリーは、トンネルインターフェース tunnel.1 を経由して、IP アドレス 2.1.1.21 にある企業 DNS サーバーに転送されます。

  たとえば、ホスト側で www.acme.com に関連する DNS クエリーを送信すると、デバイス側でその DNS クエリーを DNS サーバーに自動的に転送します。(サーバーがそのクエリーを IP アドレス 3.1.1.2 に解決すると想定します。)

- ドメイン名 acme_engineering.com が含まれている FQDN に関連付けられた任意の DNS クエリーは、トンネルインターフェース tunnel.1 を経由して、IP アドレス 2.1.1.34 にある DNS サーバーに転送されます。

  たとえば、ホスト側で acme_eng.com に関連する DNS クエリーを送信すると、デバイス側でその DNS クエリーを DNS サーバーに転送します。(サーバーがそのクエリーを IP アドレス 3.1.1.5 に解決すると想定します。)

- その他のクエリー (* で表記) はすべて、企業サーバーに転送されません。ethernet0/3 インターフェースを経由して、IP アドレス 1.1.1.23 にある DNS サーバーに転送されます。

  たとえば、ホスト名とドメイン名が www.juniper.net である場合、デバイス側で企業サーバーを自動的に回避してその DNS クエリーを上記の DNS サーバーに自動的に転送します。この DNS サーバーは、IP アドレス 207.17.137.68 への DNS クエリーを解決するとしています。

WebUI

1. **Network > DNS > Proxy: 以下を入力して Apply をクリックします。**
   Initialize DNS Proxy: Enable
   Enable DNS Proxy: Enable

2. **Network > DNS > Proxy > New: 次のように入力してから OK をクリックします。**
   Domain Name: Acme.com
   Outgoing Interface: tunnel.1
   Primary DNS Server: 2.1.1.21

3. **Network > DNS > Proxy > New: 次のように入力してから OK をクリックします。**
   Domain Name: Acme_eng.com
   Outgoing Interface: tunnel.1
   Primary DNS Server: 2.1.1.34

4. **Network > DNS > Proxy > New: 次のように入力してから OK をクリックします。**
   Domain Name: *
   Outgoing Interface: ethernet0/3
   Primary DNS Server: 1.1.1.23

CLI

```
set dns proxy
set dns proxy enable
set interface ethernet0/3 proxy dns
set dns server-select domain acme.com outgoing-interface tunnel.1 primary-server
    2.1.1.21
set dns server-select domain acme_eng.com outgoing-interface tunnel.1
    primary-server 2.1.1.34
set dns server-select domain * outgoing-interface ethernet0/3 primary-server
    1.1.1.23
save
```

動的ホスト構成プロトコル

DHCP (動的ホスト構成プロトコル) は、ネットワーク上のホストに TCP/IP 設定を自動的に割り当てることによって、ネットワーク管理者への要求を軽減するようにデザインされています。(必要に応じて) ネットワーク上のすべてのマシンごとにすべての TCP/IP 設定の割り当て、構成、トラック、変更を行うことを管理者に要求する代わりに、DHCP がすべてを自動的に実行します。さらに、DHCP は重複アドレスが使用されていないことを確認したり、使用されていないアドレスの再割り当てを行ったり、ホストが接続されているサブネットに適切な IP アドレスを自動的に割り当てます。

異なるセキュリティデバイスごとに、表 35 に示す異なる DHCP ロールがサポートされます。

表 35: DHCP ロール

ロール	解説
DHCP クライアント	セキュリティデバイスには、DHCP クライアントの機能を果たすことが可能なものがあり、任意のゾーンの物理インターフェースに動的に割り当てられた IP アドレスを受け取ります。
DHCP サーバー	また、セキュリティデバイスには、DHCP サーバーの機能を果たすことができるデバイスもあり、任意のゾーン内の物理または VLAN インターフェース上の（DHCP クライアントの機能を果たす）ホストに動的 IP アドレスを割り当てます。 **注 :** DHCP サーバーモジュールを使用してゾーン内のワークステーションなどのホストにアドレスを割り当てる一方で、メールサーバーや WINS サーバーなどの他のマシンには固定 IP アドレスを使用することもできます。
DHCP リレーエージェント	また、セキュリティデバイスには、DHCP リレーエージェントの機能を果たすものもあり、DHCP サーバーから DHCP 情報を受け取り、その情報を任意のゾーン内の物理または VLAN インターフェースのホストに中継します。
DHCP クライアント / サーバー / リレーエージェント	セキュリティデバイスによっては、DHCP クライアント、サーバー、リレーエージェントとして同時に機能できるデバイスがあります。ただし、1 つのインターフェースで構成できる DHCP ロールは 1 つだけです。たとえば、DHCP クライアントとサーバーを同じインターフェースで構成することはできません。必要に応じて、DHCP クライアントモジュールを構成して、そのモジュールが受信する TCP/IP 設定を DHCP サーバーモジュールに転送し、DHCP クライアントの機能を果たす Trust ゾーンのホストに TCP 設定を提供するときに使用できます。

DHCP は、ホスト固有の TCP/IP 構成設定を配信するためのプロトコル、および IP アドレスを割り当てるためのメカニズムの 2 つのコンポーネントから構成されています。ホスト固有の TCP/IP 構成設定を配信するためのプロトコルと、IP アドレスを割り当てるための機構です。セキュリティデバイスが DHCP サーバーの機能を果たす場合は、各ホストの起動時にそのホストに以下の TCP/IP 設定を提供します。

- デフォルトのゲートウェイ IP アドレスとネットマスク。デフォルトのゲートウェイ IP アドレスとネットマスク これらの設定を 0.0.0.0/0 のままにすると、DHCP サーバーモジュールは、デフォルト Trust ゾーンインターフェースの IP アドレスおよびサブマスクを自動的に使用します。

注： 複数のインターフェースを Trust ゾーンにバインドできるデバイスでは、デフォルトのインターフェースがそのゾーンにバインドされ、IP アドレスが割り当てられる最初のインターフェースになります。

- 以下のサービスの IP アドレス
  - WINS サーバー (2): WINS (Windows インターネットネーミングサービス) サーバーは、Windows NT ネットワーク環境で使用されている NetBIOS 名を IP ベースのネットワークで使用されている IP アドレスにマッピングします。括弧内の数字は、サポートされているサーバーの数を示しています。
  - NetInfo サーバー (2):NetInfo とは、LAN 内での管理データの配布に使用される Apple ネットワークサービスのことです。
  - NetInfo タグ (1): Apple NetInfo データベースによって使用される識別タグです。
  - DNS サーバー (3): DNS (ドメイン名システム) サーバーは、URL (ユニフォームリソースロケータ) を IP アドレスにマッピングします。
  - SMTP サーバー (1): SMTP (簡易メール転送プロトコル) サーバーは、POP3 サーバーなどの受信メールを格納するメールサーバーに SMTP メッセージを配信します。
  - POP3 サーバー (1): POP3 (ポストオフィスプロトコルバージョン 3) サーバーは、受信メールを格納します。POP3 サーバーは SMTP サーバーと一緒に動作する必要があります。
  - News サーバー (1): ニュースサーバーは、ニュースグループの投稿を受け取って、格納します。

注： セキュリティデバイスが上記のパラメータを転送している DHCP クライアントに、指定 IP アドレスが割り当てられている場合、そのアドレスは DHCP サーバーから受け取ったすべての動的情報より優先されます。

DHCP サーバーの構成

セキュリティデバイスは、任意のゾーンの物理または VLAN インターフェース上で最大で 8 台の DHCP サーバーをサポートできます。DHCP サーバーとして機能する場合は、セキュリティデバイスは以下の 2 つのモードで IP アドレスとサブネットマスクを割り当てます。

- Dynamic mode（動的モード）では、DHCP サーバーの機能を果たすセキュリティデバイスは、ホスト DHCP クライアントに、アドレスプールから IP アドレスを割り当てます（または「リース」します)。IP アドレスは、決められた期間、またはクライアントがアドレスを破棄するまでリースされます。(無制限のリース期間を定義するには 0 を入力します。)
- Reserved mode（予約モード）では、セキュリティデバイスはクライアントがオンラインにするたびに、アドレスプール内から指定 IP アドレスを特定のクライアントに対して排他的に割り当てます。

注 : アドレスプールとは、セキュリティデバイスが DHCP アドレス割り当てを引き出すことができる、同一のサブネット内の IP アドレスの定義範囲のことです。IP アドレスは 255 個までグループ化できます。

DHCP サーバーは、動的および予約 IP アドレスに対して最大で 64 エントリをサポートします。各エントリには、単体の IP アドレスならびに IP アドレスの範囲を含めることができます。

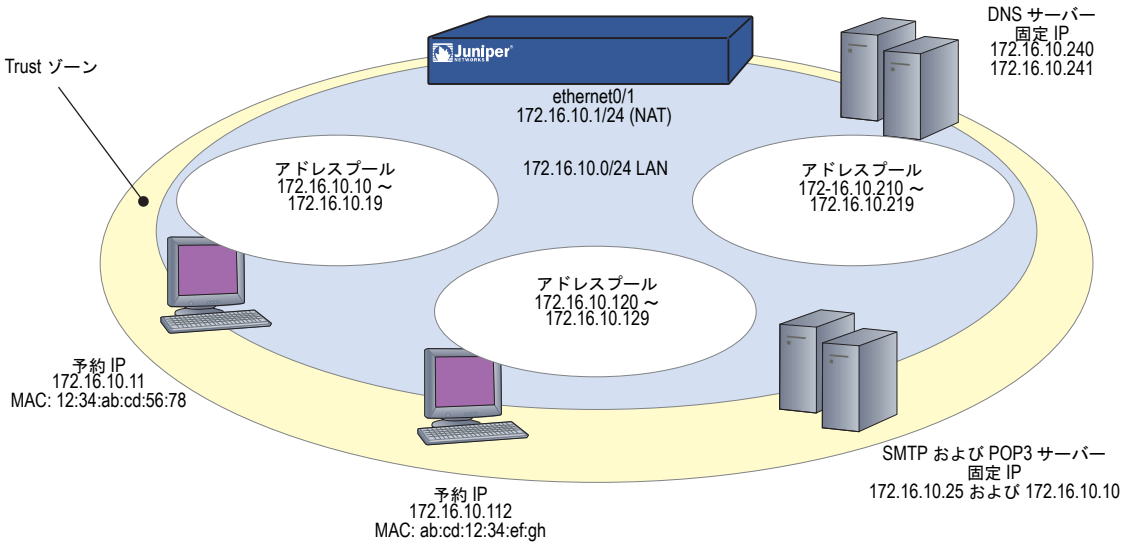
セキュリティデバイスは、DHCP によって割り当てられたすべての IP アドレスをフラッシュメモリーに保存します。そのため、セキュリティデバイスを再起動しても、アドレスの割り当てに影響はありません。

この例では、DHCP を使用して、Trust ゾーン内の 172.16.10.0/24 ネットワークを 3 つの IP アドレスプールに区分します。

- 172.16.10.10 ～ 172.16.10.19
- 172.16.10.120 ～ 172.16.10.129
- 172.16.10.210 ～ 172.16.10.219

DHCP サーバーは、予約 IP アドレスが割り当てられている 2 台のワークステーションと静的 IP アドレスが割り当てられている 4 台のサーバーを除いたすべての IP アドレスを動的に割り当てます。インターフェース ethernet0/1 は Trust ゾーンにバインドされ、IP アドレス 172.16.10.1/24 を割り当てられて NAT モードになっています。ドメイン名は dynamic.com です。

図 71: DHCP サーバーとしてのデバイス



WebUI

1. **アドレス**

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: DNS#1
   Comment: Primary DNS Server
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 172.16.10.240/32
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: DNS#2
   Comment: Secondary DNS Server
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 172.16.10.241/32
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: SMTP
   Comment: SMTP Server
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 172.16.10.25/32
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: POP3
   Comment: POP3 Server
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 172.16.10.110/32
   Zone: Trust

2. **DHCP サーバー**

   Network > DHCP > Edit (ethernet0/1) > DHCP Server: 以下を入力して **Apply** をクリックします。

   Lease: Unlimited (**選択**)
   WINS#1: 0.0.0.0
   DNS#1: 172.16.10.240

注： Gateway フィールドおよび Netmask フィールドを **0.0.0.0** のままにすると、DHCP サーバーモジュールは、ethernet0/1 に設定されている IP アドレスおよびネットマスクをそのクライアントに送信します（この例の場合は、172.16.10.1 と 255.255.255.0）。ただし、TCP/IP 設定が DHCP サーバーモジュールに送信されるように DHCP クライアントモジュールを構成している場合は（243 ページの「TCP/IP 設定の伝播」を参照）、Gateway フィールドおよび Netmask フィールドに手動で **172.16.10.1** および **255.255.255.0** を入力する必要があります。

> Advanced Options: 以下を入力して、**OK** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

WINS#2: 0.0.0.0
DNS#2: 172.16.10.241
DNS#3: 0.0.0.0
SMTP: 172.16.10.25
POP3: 172.16.10.110
NEWS: 0.0.0.0
NetInfo Server #1: 0.0.0.0
NetInfo Server #2: 0.0.0.0
NetInfo Tag: (フィールドに入力しない)
Domain Name: dynamic.com

> Addresses > New: 次のように入力してから **OK** をクリックします。

Dynamic: (選択)
IP Address Start: 172.16.10.10
IP Address End: 172.16.10.19

> Addresses > New: 次のように入力してから **OK** をクリックします。

Dynamic: (選択)
IP Address Start: 172.16.10.120
IP Address End: 172.16.10.129

> Addresses > New: 次のように入力してから **OK** をクリックします。

Dynamic: (選択)
IP Address Start: 172.16.10.210
IP Address End: 172.16.10.219

> Addresses > New: 次のように入力してから **OK** をクリックします。

Reserved: (選択)
IP Address: 172.16.10.11
Ethernet Address: 1234 abcd 5678

> Addresses > New: 次のように入力してから **OK** をクリックします。

Reserved: (選択)
IP Address: 172.16.10.112
Ethernet Address: abcd 1234 efgh

CLI

1. **アドレス**

```
set address trust dns1 172.16.10.240/32 “primary dns server”
set address trust dns2 172.16.10.241/32 “secondary dns server”
set address trust snmp 172.16.10.25/32 “snmp server”
set address trust pop3 172.16.10.110/32 “pop3 server”
```

2. **DHCP サーバー**

```
set interface ethernet0/1 dhcp server option domainname dynamic.com
set interface ethernet0/1 dhcp server option lease 0
set interface ethernet0/1 dhcp server option dns1 172.16.10.240
set interface ethernet0/1 dhcp server option dns2 172.16.10.241
set interface ethernet0/1 dhcp server option smtp 172.16.10.25
set interface ethernet0/1 dhcp server option pop3 172.16.10.110
```

```
set interface ethernet0/1 dhcp server ip 172.16.10.10 to 172.16.10.19
set interface ethernet0/1 dhcp server ip 172.16.10.120 to 172.16.10.129
set interface ethernet0/1 dhcp server ip 172.16.10.210 to 172.16.10.219
set interface ethernet0/1 dhcp server ip 172.16.10.11 mac 1234abcd5678
set interface ethernet0/1 dhcp server ip 172.16.10.112 mac abcd1234efgh
set interface ethernet0/1 dhcp server service
save
```

注： ゲートウェイまたはネットマスクに IP アドレスを設定していない場合、DHCP サーバーモジュールは、そのクライアントを ethernet0/1 の IP アドレスおよびネットマスクに送信します (この例の場合、172.16.10.1 と 255.255.255.0 です)。ただし、TCP/IP 設定が DHCP サーバーモジュールに送信されるように DHCP クライアントモジュールを構成している場合 (243 ページの「TCP/IP 設定の伝播」を参照)、**set interface ethernet0/1 dhcp server option gateway 172.16.10.1** および **set interface ethernet0/1 dhcp server option netmask 255.255.255.0** を手動で設定する必要があります。

DHCP サーバーオプションのカスタマイズ

インターフェースの DHCP サーバーを指定する際には、サーバーを識別したりサーバーが使用する情報を提供したりするオプションを指定する必要があります。たとえば、1 次サーバーや 2 次サーバーの IP アドレスを指定したり、IP アドレスのリース時刻を設定したりすることができます。

以下は RFC 2132、*DHCP Options and BOOTP Vendor Extensions* に記述されている事前定義の DHCP サービスです。

表 36: 事前定義済みサービス

用語	ScreenOS CLI での用語	オプションコード
Subnet Mask	netmask	1
Router Option	gateway	3
Domain Name System (DNS) server	dns1, dns2, dns3	6
Domain Name	domainname	15
NetBIOS over TCP/IP Name Server Option	wins1, wins2	44
IP Address Lease Time	lease	51
SMTP Server Option	smtp	69
POP3 Server Option	pop3	70
NNTP Server Option	news	71
(N/A)	nis1, nis2	112
(N/A)	nistag	113

定義済みサーバーオプションが適切でない状況では、カスタムの DHCP サーバーオプションを定義できます。たとえば、特定の VoIP（音声 IP 化）構成について、定義済みサーバーオプションがサポートしない追加の構成情報を送信する必要があるとします。そのような場合には、カスタムのオプションを適切に定義する必要があります。

以下の例では、DHCP クライアントとして機能する IP 電話の DHCP サーバー定義を作成します。IP 電話が以下のオプションを使用するとします。

- 文字列 Server 4 を含むオプションコード 444
- IP アドレス 1.1.1.1 を含むオプションコード 66
- 整数 2004 を含むオプションコード 160

CLI

1. **アドレス**
   set address trust dns1 172.16.10.240/32 “primary dns server”
   set address trust dns2 172.16.10.241/32 “secondary dns server”

2. **DHCP サーバー**
   set interface ethernet0/1 dhcp server option domainname dynamic.com
   set interface ethernet0/1 dhcp server option lease 0
   set interface ethernet0/1 dhcp server option dns1 172.16.10.240
   set interface ethernet0/1 dhcp server option dns2 172.16.10.241
   set interface ethernet0/1 dhcp server option custom 444 string “Server 4”
   set interface ethernet0/1 dhcp server option custom 66 ip 1.1.1.1
   set interface ethernet0/1 dhcp server option custom 160 integer 2004
   set interface ethernet0/1 dhcp server ip 172.16.10.10 to 172.16.10.19

NSRP クラスタの DHCP サーバーの配置

冗長 NSRP クラスタの 1 次ユニットが DHCP サーバーとして機能している場合は、クラスタ内のすべてのメンバーは、DHCP 構成と IP アドレス割り当てすべてを維持します。フェールオーバー時には、新しい 1 次ユニットがすべての DHCP 割り当てを維持します。ただし、HA 通信が終了すると、クラスタメンバー間の既存の DHCP 割り当ての同期化が損なわれます。同期化が失われた割り当ては、HA 通信を復旧した後で CLI コマンド **set nsrp rto-mirror sync** をクラスタの両方のユニットで使用することによって再び同期化できます。

DHCP サーバー検出

セキュリティデバイスの DHCP サーバーが起動する際に、システムはまずインターフェース上に別の DHCP がすでにあるかどうかをチェックします。ネットワーク上に別の DHCP サーバーを検出した場合、ScreenOS は自動的にローカル DHCP サーバーのプロセス開始を停止します。他の DHCP サーバーを検出するために、デバイスは DHCP 起動要求を 2 秒間隔で送り出します。デバイスが起動要求に対する応答を受信しなかった場合、ローカル DHCP サーバーのプロセスを開始します。

セキュリティデバイスが他の DHCP サーバーから応答を受信した場合、システムは、DHCP サービスがセキュリティデバイスで使用可能であるが、他の DHCP サーバーがネットワーク上に存在するため DHCP サービスが開始されないことを示すメッセージを生成します。ログメッセージには、既存の DHCP サーバーの IP アドレスが含まれます。

インターフェースでの DHCP サーバー検出には、Auto、Enable、Disable の 3 つの動作モードのいずれかを設定できます。Auto モードでは、セキュリティデバイスは常に起動時に DHCP サーバーがすでに存在するかをチェックします。セキュリティ DHCP サーバーを Enable または Disable モードに設定することに

よって、他の DHCP サーバーの検出を行わないようにデバイスを構成することができます。Enable モードでは、DHCP サーバーは常にオンの状態で、デバイスはネットワーク上に DHCP サーバーが存在するかどうかをチェックしません。Disable モードでは、DHCP サーバーは常にオフの状態です。

DHCP サーバー検出の有効化

この例では、ethernet0/1 インターフェース上の DHCP サーバーを設定して、起動前にこのインターフェース上に既存の DHCP サーバーが存在するかどうかをチェックします。

WebUI

Network > DHCP > Edit (ethernet0/1) > DHCP Server: 次のように入力してから **OK** をクリックします。

Server Mode: Auto (**選択**)

CLI

```
set interface ethernet0/1 dhcp server auto
save
```

DHCP サーバー検出の無効化

この例では、ethernet0/1 インターフェース上の DHCP サーバーを設定して、ネットワーク上に DHCP サーバーが存在するかどうかをチェックせずに起動するようにします。

WebUI

Network > DHCP > Edit (ethernet0/1) > DHCP Server: 次のように入力してから **OK** をクリックします。

Server Mode: Enable (**選択**)

CLI

```
set interface ethernet0/1 dhcp server enable
save
```

注 : CLI コマンド **set interface** interface **dhcp server service** を実行すると、DHCP サーバーがアクティブになります。インターフェースの DHCP サーバー検出モードが Auto に設定されている場合、セキュリティデバイス上の DHCP サーバーは、ネットワーク上に既存のサーバーが見つからない場合にのみ開始します。**unset interface** interface **dhcp server service** コマンドは、セキュリティデバイス上の DHCP サーバーを使用不可にし、既存の DHCP 構成を消去します。

DHCP リレーエージェントとしてのセキュリティデバイスの割り当て

セキュリティデバイスは DHCP リレーエージェントの機能を果たす場合、あるインターフェースに直接付いている DHCP クライアントと、別のインターフェース経由でアクセス可能な 1 つ以上の DHCP サーバーに付いている DHCP クライアントとの間で、DHCP 要求と割り当てを転送します。クライアントとサーバーが存在するセキュリティゾーンは、同じであっても、異なっていてもかまいません。

DHCP リレーエージェントは、セキュリティデバイス上の 1 つ以上の物理または VLAN インターフェース上に構成できますが、DHCP リレーエージェントと DHCP サーバーまたはクライアントの機能を同じインターフェース上に構成することはできません。

セキュリティデバイスが DHCP リレーエージェントとして機能する場合は、デバイスのインターフェースはルートモードであるか、またはレイヤー 3 デバイスとして機能する必要があります。たとえば Layer 3 モード（すなわち、IP アドレスをインターフェースに割り当てする場合）では、転送が行われる前に、事前定義されているサービス DHCP-Relay を許可するようにセキュリティポリシー（ゾーン間またはゾーン内）を設定することが必要です。

各 DHCP リレーエージェントには、DHCP サーバーを 3 つまで構成できます。リレーエージェントは、DHCP クライアントからのアドレス要求を、構成されているすべての DHCP サーバーにユニキャストします。リレーエージェントは、すべてのサーバーから受信したすべての DHCP パケットをクライアントに転送します。239 ページの「すべての DHCP パケットの転送」を参照してください。

注 : セキュリティデバイスが DHCP リレーエージェントとして機能する場合は、リモート DHCP サーバーがすべての IP アドレス割り当てを制御するため、セキュリティデバイスは DHCP 割り当て状態レポートを生成しません。

ScreenOS は、DHCP リレーを異なる vsys および VLAN タグ付きサブインターフェースでサポートします。

図 72 は、セキュリティデバイスを DHCP リレーエージェントとして使用した場合のプロセスを示しています。セキュリティ確保のため、DHCP メッセージがアントラステッドネットワークを介して転送される場合は VPN トンネルを通過します。

図 72: DHCP リレーエージェントトラフィック

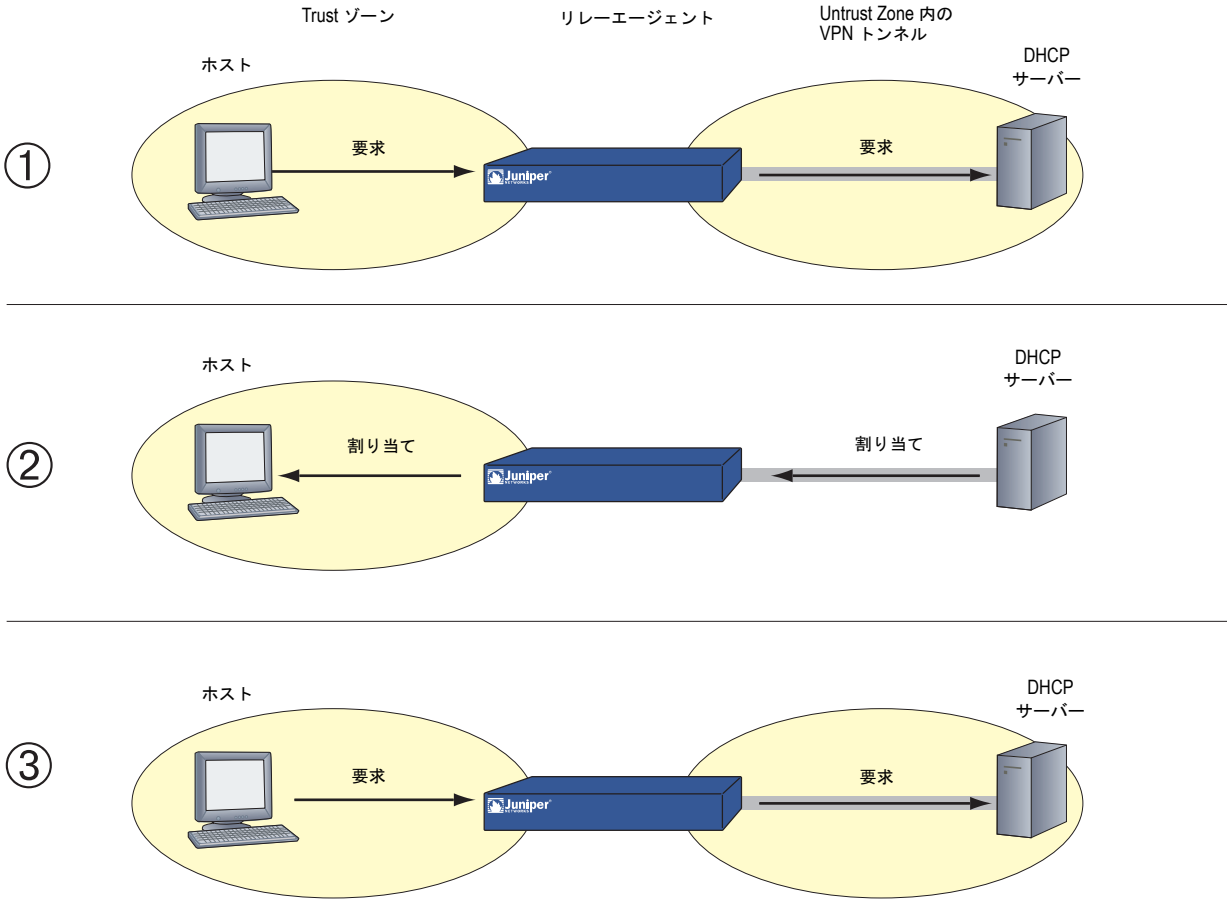
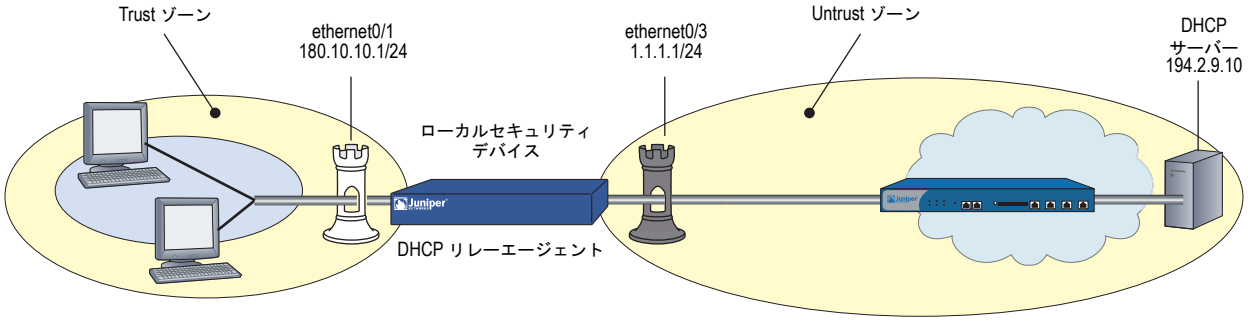


図 73 では、セキュリティデバイスは 194.2.9.10 の DHCP サーバーから DHCP 情報を受け取り、Trust ゾーンのホストに中継します。ホストは DHCP サーバー上で定義されている IP プールから IP アドレスを受け取ります。アドレスの範囲は、180.10.10.2 から 180.10.10.254 までです。DHCP メッセージは、ローカルセキュリティデバイスと、Untrust ゾーンインターフェース IP アドレスが 2.2.2.2/24 であるリモートセキュリティデバイスの背後にある DHCP サーバーとの間の VPN トンネルを通過します。インターフェース ethernet0/1 は Trust ゾーンにバインドされ、IP アドレス 180.10.10.1/24 を割り当てられてルートモードになっています。インターフェース ethernet0/3 は Untrust ゾーンにバインドされ、IP アドレス 1.1.1.1/24 を割り当てられています。セキュリティゾーンはすべて trust-vr ルーティングドメイン内にあります。

図 73: DHCP リレーエージェントとしてのデバイス



WebUI

1. **インターフェース**
   Interfaces > Edit (ethernet0/1): 以下を入力して **Apply** をクリックします。

   Zone: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 180.10.10.1/24

   次のように入力してから **OK** をクリックします。

   Interface Mode: Route

   Interfaces > Edit (ethernet0/3): 次のように入力してから **OK** をクリックします。

   Zone: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: DHCP Server
   IP Address/Domain Name:
   IP/Netmask: (選択), 194.2.9.10/32
   Zone: Untrust

3. **VPN**
   VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

   Gateway Name: dhcp server
   Security Level: Custom
   Remote Gateway Type:
   Static IP: (選択), Address/Hostname: 2.2.2.2
   Outgoing Interface: ethernet0/3

   > Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

   Security Level:
   User Defined: Custom (選択)
   Phase1 Proposal: rsa-g2-3des-sha
   Mode (Initiator): main (ID 保護)

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: to_dhcp
Security Level: Compatible
Remote Gateway:
Predefined: (**選択**), to_dhcp

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Bind to: **なし**

4. **DHCP リレーエージェント**
   Network > DHCP > Edit (ethernet0/1) > DHCP Relay Agent: 以下を入力して **Apply** をクリックします。

   Relay Agent Server IP or Domain Name: 194.2.9.10
   Use Trust Zone Interface as Source IP for VPN: (**選択**)

5. **ルート**
   Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (**選択**)
   Interface: ethernet0/3
   Gateway IP Address: 1.1.1.250

注 : デフォルトゲートウェイに指定された外部ルーターへのルートの設定は、アウトバウンド VPN とネットワークトラフィックの両方に必須です。この例では、セキュリティデバイスはリモートセキュリティデバイスへのルート上の最初のホップとして、カプセル化された VPN トラフィックをこのルーターに送信します。図 73 では、ルーターを通るトンネルという概念として描かれています。

---

6. **ポリシー**
   Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), Any
   Destination Address:
   Address Book Entry: (**選択**), DHCP Server
   Service: DHCP-Relay
   Action: Tunnel
   Tunnel VPN: to_dhcp
   Modify matching outgoing VPN policy: (**選択**)

CLI

1. **インターフェース**
   set interface ethernet0/1 zone trust
   set interface ethernet0/1 ip 180.10.10.1/24
   set interface ethernet0/1 route
   set interface ethernet0/3 zone untrust
   set interface ethernet0/3 ip 1.1.1.1/24

2. **アドレス**
   set address untrust dhcp_server 194.2.9.10/32

3. **VPN**
   set ike gateway “dhcp server” ip 2.2.2.2 main outgoing-interface ethernet0/3
   proposal rsa-g2-3des-sha
   set vpn to_dhcp gateway “dhcp server” proposal g2-esp-3des-sha

4. **DHCP リレーエージェント**
   set interface ethernet0/1 dhcp relay server-name 194.2.9.10
   set interface ethernet0/1 dhcp relay vpn

5. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet0/3 gateway 1.1.1.250

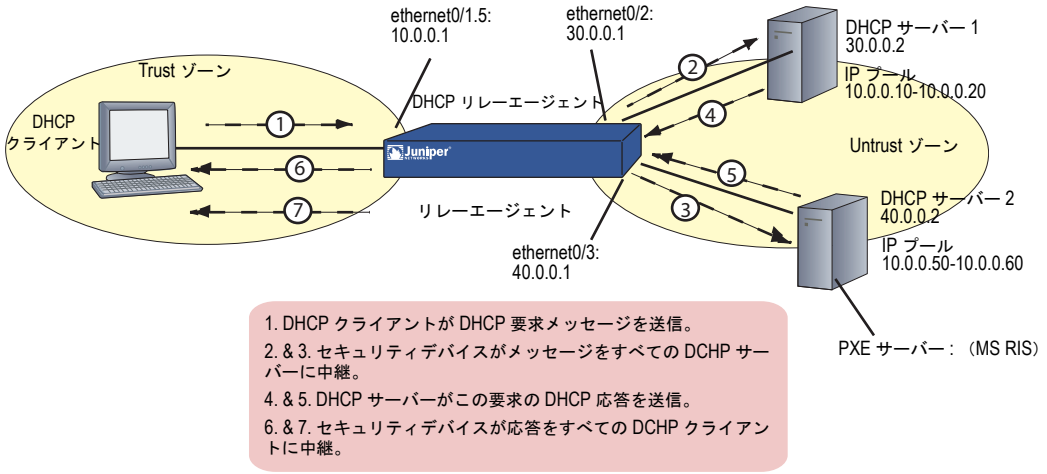
6. **ポリシー**
   set policy from trust to untrust any dhcp_server dhcp-relay tunnel vpn to_dhcp
   set policy from untrust to trust dhcp_server any dhcp-relay tunnel vpn to_dhcp
   save

すべての DHCP パケットの転送

ScreenOS では、セキュリティデバイスが複数のサーバーのすべての DHC 応答を 1 つのクライアントに中継することができます。複数のサーバーがすべて同じデータで応答し、クライアントは最初に受け取った応答だけを処理することが必要な環境があります。または、複数のサーバーがそれぞれ独自のデータで応答し、クライアントは、たとえばプレブート実行環境（Pre-Boot Execution Environment、PXE）などにおいて、個々の応答について適切であれば処理するという環境もあります。

よくある PXE の場合（図 74 を参照）、少なくても 2 つの DHCP サーバーがクライアントにサービスします。これらの DHCP サーバーが DHCP クライアントの要求を受信すると、DHCP サーバー 1 がクライアントに DHCP アドレス情報を提供し、もう 1 つのサーバー、DHCP サーバー 2（MS RIS など）が PXE 情報を提供します。ScreenOS のこのリリースでは、セキュリティデバイスはクライアントにすべての DHCP パケットを転送することができます。

図 74: 複数の DHCP サーバーのすべての DHCP パケットを中継



通常、PXE サーバーは、ディスクを持たない PXE クライアントにディスク無し PC マシンであるブートイメージサーバーを提供します。PXE クライアントに電源が入ると、このクライアントはブロードキャスト DHCP-DISCOVER（要求の一種）を送信します。これは、クライアントが IP とブートイメージパスを要求したことを意味します。多くの場合、2 種類のサーバーが PXE にサービスします。PXE サーバー（Microsoft RIS サーバーなど）と、DHCP サーバーです。両方のサーバーが DISCOVER 要求を受信します。PXE サーバーは、ブートイメージサーバー情報で DISCOVER 要求に応答します。同時に、DHCP サーバーは、IP 割り当て情報で DISCOVER 要求に応答します。2 つのサーバーの応答は両方とも、DHCP クライアント（ディスク無し PC）に転送されます。

Next-Server-IP の構成

セキュリティデバイスは、DHCP サーバーから競合や混同している情報を受け取る場合は、Next-Server-IP フィールドの IP アドレスを使用します。この DHCP 構成パラメータは、ブートストラップ手続きで TFTP サーバーのアドレスとしてこれまで使用されてきました。

たとえば、PXE の例では、最初の DHCP サーバーが IP アドレスをサービスし、2 番目の DHCP サーバーは OS 情報を提供します。Next-Server-IP フィールドには、チェーン内の次のサーバーを指定します。チェーンと各メンバーは、サイトごとに異なります。ただし、通常は DHCP サーバーであり、後続の TFTP サーバーに連鎖しています。チェーンの終端とするには、表 37 が示すように、このフィールドにすべてゼロ（0.0.0.0）を入力するか、またはデバイスのインターフェース IP を指定します。

この Next-Server-IP 情報は、DHCP ヘッダーの siaddr フィールドで返され、数個のブートストラップサーバーをチェーンで繋いで、サーバーごとに特定の機能でサービスさせる場合によく使用されます。siaddr フィールドは、設定されていなければ DHCP サーバーによっては自身の IP アドレスを入力する可能性があるため、使用可能であれば必須です。

表 37: Next-Server-IP の指定

Next Server IP	解説
None（デフォルト）	siaddr = 0.0.0.0（デフォルト）
インターフェース	siaddr = DHCP サーバーにバインドされている IP インターフェース
Option66	siaddr = option66 （ディスク無し PC をサポートするための TFTP サーバーを識別）
入力	siaddr = カスタム IP アドレス

Next-Server-IP がゼロ値ではなく、このサーバーのアドレスと同じでもない場合は、追加のブート情報を持つ、チェーン中の次に続くサーバーのアドレスであるとクライアントに解釈されます。次の例では、Next-Server-IP を Option66 に設定します。

WebUI

Network > DHCP > Edit (DHCP サーバー): 次のいずれかを選択してから **Apply** をクリックします。

Next Server IP: From Option66

CLI

```
set interface ethernet0/1 dhcp server enable
set interface ethernet0/1 dhcp server option custom 66 ip 10.10.10.1
set interface ethernet0/1 dhcp server config next-server-ip option66
save
```

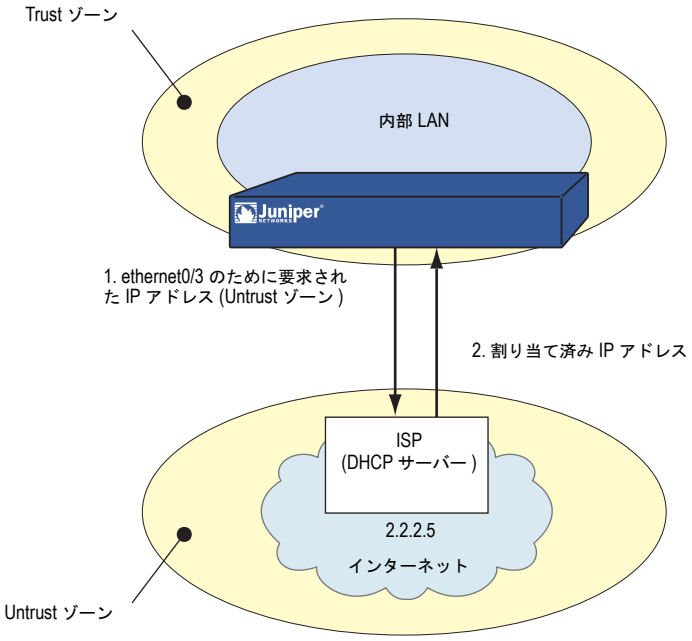
セキュリティデバイスを DHCP クライアントとして使用

セキュリティデバイスが DHCP クライアントの機能を果たしている場合、任意のセキュリティゾーンにある物理インターフェースの DHCP サーバーから動的に IP アドレスを受信します。1 つのセキュリティゾーンにバインドされた複数のインターフェースが存在する場合、各インターフェースが同じネットワークセグメントに接続されていない場合は、各インターフェースに DHCP クライアントを構成できます。同じネットワークセグメントに接続された 2 つのインターフェースに対して 1 つの DHCP クライアントを構成すると、DHCP サーバーによって割り当てられた最初のアドレスが使用されます。（DHCP クライアントが同じ IP アドレスへのアドレス更新を受信しても、IKE は再入力されません。）

注 : セキュリティデバイスによっては DHCP サーバー、DHCP リレーエージェント、または DHCP クライアントとして同時に機能することができます。この場合、1 つのインターフェースに複数の DHCP ロールを構成することはできません。

この例では、Untrust ゾーンにバインドされているインターフェースが IP アドレスを動的に割り当てています。セキュリティデバイスが ISP に IP アドレスを要求すると、IP アドレス、サブネットマスク、ゲートウェイ IP アドレス、およびアドレスのリース期間を受信します。DHCP サーバーの IP アドレスは、2.2.2.5 です。

図 75: DHCP クライアントとしてのデバイス



注： DHCP サービス用のサイトを設定する前に、DSL（ディジタル加入者線）と ISP（インターネットサービスプロバイダ）のアカウントが必要になります。

WebUI

Network > Interfaces > Edit (ethernet0/3): **Obtain IP using DHCP** を選択し、**OK** をクリックします。

注： WebUI から DHCP サーバーの IP アドレスを指定することはできませんが、CLI から指定できます。

CLI

```
set interface ethernet0/3 dhcp client
set interface ethernet0/3 dhcp settings server 2.2.2.5
save
```

TCP/IP 設定の伝播

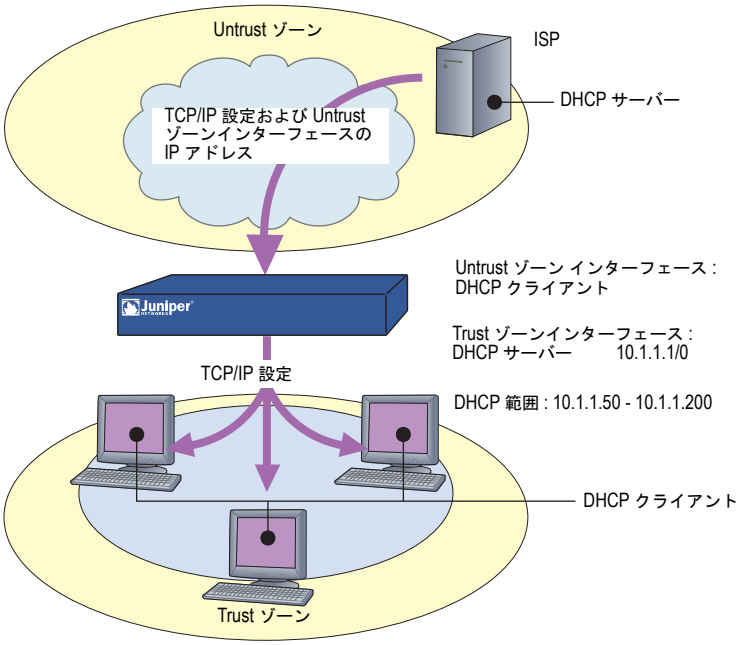
セキュリティデバイスによっては、DHCP（Dynamic Host Control Protocol）クライアントの機能を果たし、任意のセキュリティゾーンにある物理インターフェースの TCP/IP 設定および IP アドレスを外部 DHCP サーバーから受信できます。また、DHCP サーバーの機能を果たし、任意のゾーンにあるクライアントに TCP/IP 設定および IP アドレスを提供できるセキュリティデバイスもあります。セキュリティデバイスが DHCP クライアントと DHCP サーバーの両方の機能を同時に果たす場合、その DHCP クライアントモジュールを介して認識した TCP/IP 設定をデフォルトの DHCP サーバーモジュールに転送できます。

TCP/IP 設定には、デフォルトゲートウェイおよびサブネットマスクの IP アドレス、および以下のサーバーの任意またはすべての IP アドレスが含まれます。

- DNS (3)
- WINS (2)
- NetInfo (2)
- SMTP (1)
- POP3 (1)
- News (1)

図 76 では、セキュリティデバイスは Untrust ゾーンにある DHCP サーバーのクライアントでもあり、Trust ゾーンのクライアントに対する DHCP サーバーでもあります。デバイスは、DHCP クライアントとして受信した TCP/IP 設定を、DHCP サーバーとして Trust ゾーンにあるクライアントに転送します。Untrust ゾーンインターフェースは DHCP クライアントであり、ISP から IP アドレスを動的に受信します。

図 76: DHCP 伝播



set interface *interface* **dhcp-client settings update-dhcpserver** コマンドを使用し、DHCP クライアントモジュールを構成して、そのモジュールが DHCP クライアントから受信するすべての TCP/IP 設定を伝播することができます。また、設定を別の設定に上書きすることもできます。

この例では、セキュリティデバイスを、ethernet0/3 インターフェース上の DCHP クライアントと ethernet0/1 インターフェース上の DHCP サーバーの両方として機能するように構成します。(デフォルト DHCP サーバーは ethernet0/1 インターフェース上にあります。)

セキュリティデバイスは DHCP クライアントとして、211.3.1.6 にある外部 DHCP サーバーから ethernet0/3 インターフェースの IP アドレスおよびその TCP/IP 設定を受信します。セキュリティデバイスの DHCP クライアントモジュールを使用可能にして、受信する TCP/IP 設定を DHCP サーバーモジュールに転送します。

DHCP サーバーモジュールを構成し、DHCP クライアントモジュールから受信する TCP/IP 設定を使用して以下の項目を実行します。

- DNS IP アドレスを Trust ゾーンにある DHCP クライアントに転送する。
- デフォルトのゲートウェイ、ネットマスク、SMTP サーバー、および POP3 サーバー IP アドレスを以下の内容で上書きする。
  - 10.1.1.1 (ethernet0/1 インターフェースの IP アドレス)
  - 255.255.255.0 (ethernet0/1 インターフェースのネットマスク)
  - SMTP: 211.1.8.150
  - POP3: 211.1.8.172

注 : DHCP サーバーが Trust インターフェースですでに使用可能にされていて、定義済みの IP アドレスプールを有する場合（これは一部のプラットフォームではデフォルトの動作）、デフォルトのゲートウェイとネットマスクを変更する前に IP アドレスプールを削除する必要があります。

また、DHCP クライアントモジュールから受信しない以下の TCP/IP 設定を配信するように DHCP サーバーモジュールを構成します。

- Primary WINS server: 10.1.2.42
- Secondary WINS server: 10.1.5.90

最後に、IP プール 10.1.1.50 ～ 10.1.1.200 の IP アドレスを、Trust ゾーンの DHCP クライアントとして機能しているホストに割り当てるように、DHCP サーバーモジュールを構成します。

WebUI

注 : この機能は、CLI からのみ設定できます。

CLI

1. **DHCP クライアント**
```
set interface ethernet0/3 dhcp-client settings server 211.3.1.6
set interface ethernet0/3 dhcp-client settings update-dhcpserver
set interface ethernet0/3 dhcp-client settings autoconfig
set interface ethernet0/3 dhcp-client enable
```
2. **DHCP サーバー**
```
set interface ethernet0/1 dhcp server option gateway 10.1.1.1
set interface ethernet0/1 dhcp server option netmask 255.255.255.0
set interface ethernet0/1 dhcp server option wins1 10.1.2.42
set interface ethernet0/1 dhcp server option wins2 10.1.5.90
set interface ethernet0/1 dhcp server option pop3 211.1.8.172
set interface ethernet0/1 dhcp server option smtp 211.1.8.150
set interface ethernet0/1 dhcp server ip 10.1.1.50 to 10.1.1.200
set interface ethernet0/1 dhcp server service
save
```

仮想システムの DHCP の構成

DHCPScreenOS は、現在、vsys 用の DHCP を完全にサポートします。ある特定の vsys の DHCP リレーを構成し、複数の DHCP サーバーのすべてのパケットを 1 つのクライアントに中継することができます。

仮想システムの DHCP メッセージリレーの設定

ScreenOS では、仮想システム（vsys）内の 1 つまたは複数の DHCP サーバーからクライアントへの DHCP（動的ホスト構成プロトコル）メッセージリレーを構成することができます。DHCP メッセージリレーを仮想システムが使用できるインターフェース上に構成できます。

DHCP サーバー 1 とサーバー 2 がある場合、これらのサーバーと 1 つのクライアントの間に位置するセキュリティデバイスは、異なる送信インターフェース上の各 DHCP サーバーに個別に DHCP 要求を渡します。セキュリティデバイスは受信した各 DHCP 応答を ルート vsys に渡した後に、vsys 内の適切な DHCP クライアントに転送します。

図 77: vsys 内の DHCP リレーサービス



vsys で DHCP を構成するには、以下の手順を実行します。

1. 仮想システムを作成。
2. その vsys の DHCP を有効化。
3. ルートシステムにいる DHCP サーバーが vsys にアクセスできる静的ルートを構成。
4. 仮想システムのセキュリティポリシーを設定。

Point-to-Point Protocol over Ethernet

PPPoE (Point-to-Point Protocol over Ethernet) は通常ダイヤルアップ接続に使用される PPP (Point-to-Point Protocol) を併合し、Ethernet プロトコルによって、あるサイトの複数のユーザーを同顧客の構内の装置に接続することができます。多くのユーザーが同じ物理的接続を使用できる一方で、アクセス制御、ビリング、およびサービスの種類についてはユーザー単位で扱われます。セキュリティデバイスの中には、クライアントによるインターネットアクセスのために PPPoE クライアントをサポートするデバイスがあります。これによって、PPPoE を使用している ISP が運営する DSL や Ethernet Direct、ケーブルネットワークとの互換動作が可能になっています。

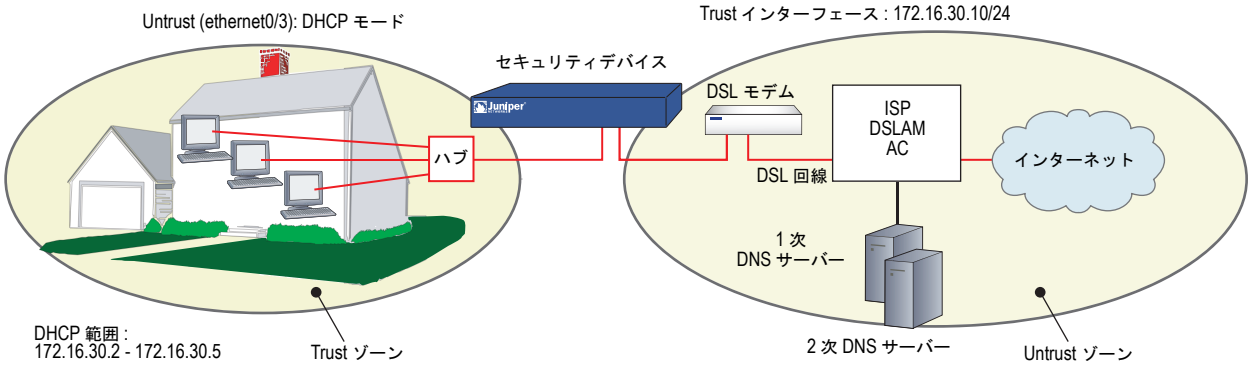
PPPoE をサポートするデバイスでは、任意のまたはすべてのインターフェースで PPPoE クライアントインスタンスを構成できます。特定の PPPoE インスタンスをユーザー名、パスワード、および他のパラメータで構成し、そのインスタンスをあるインターフェースにバインドします。2 つの Ethernet インターフェース（1 次とバックアップ）が Untrust ゾーンにバインドされている場合、どちらかまたは両方のインターフェースを PPPoE に構成することが可能です。

PPPoE の設定

次の例は、PPPoE 接続のための セキュリティデバイスのアントラステッドインターフェースの定義方法、および PPPoE サービスの開始方法を示しています。

この例では、セキュリティデバイスは、Untrust ゾーンインターフェース（ethernet0/3）のために動的に割り当てられた IP アドレスを ISP から受け取り、同時に Trust ゾーン内の 3 台のホストの IP アドレスを動的に割り当てます。この場合では、セキュリティデバイスは PPPoE クライアントとして機能すると同時に DHCP サーバーとしての機能も果たします。Trust ゾーンインターフェースは、NAT モードまたはルートモードのいずれかでなければなりません。この例では NAT モードになっています。

図 78: PPPoE



この PPPoE サービスの例では、サイトを設定する前に以下が必要です。

- デジタル加入者線 (DSL) モデム および回線
- ISP のアカウント
- ユーザー名とパスワード（ISP から取得）

WebUI

1. **インターフェースおよび PPPoE**
   Network > Interfaces > Edit (ethernet0/1): 次のように入力してから **OK** をクリックします。

   Zone: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 172.16.30.10/24

Network > Interfaces > Edit (ethernet0/3): 次のように入力してから **OK** をクリックします。

Zone: Untrust
Obtain IP using PPPoE: (**選択**)
User Name/Password: **ユーザー名 / パスワード**

Network > Interfaces > Edit (ethernet0/3): PPPoE 接続をテストするには、**Connect** をクリックします。

注 : PPPoE 接続開始時に、ISP は Untrust ゾーンインターフェースの IP アドレスおよび DNS （ドメイン名サービス) サーバーの IP アドレスを自動的に提供します。セキュリティデバイスが PPPoE を介して DNS アドレスを受信すると、デフォルトでは、新規の DNS 設定によりローカル設定が上書きされます。ローカル設定が新しい DNS 設定に置き換えられないようにするには、CLI コマンド **unset pppoe dhcp-updateserver** を使用して、この動作を使用不可にできます。

Untrust ゾーンインターフェースに静的 IP アドレスを使用する場合は、DNS サーバーの IP アドレスを取得し、これらの IP アドレスを セキュリティデバイス上と Trust ゾーン内のホスト上で手動で入力する必要があります。

---

2. DHCP サーバー

Network > Interfaces > Edit (ethernet0/1) > DHCP: **DHCP Server** を選択し、**Apply** をクリックします。

Network > Interfaces > Edit (ethernet0/1) > DHCP: 以下を入力して **Apply** をクリックします。

Lease: 1 hour
Gateway: 0.0.0.0
Netmask: 0.0.0.0
DNS#1: 0.0.0.0

> Advanced: 次のように入力してから **Return** をクリックします。

DNS#2: 0.0.0.0
Domain Name: (**何も入力しない**)

Network > Interfaces > DHCP (ethernet0/1) > New Address: 次のように入力してから **OK** をクリックします。

Dynamic: (**選択**)
IP Address Start: 172.16.30.2
IP Address End: 172.16.30.5

3. セキュリティデバイス上での PPPoE の起動

1. DSL モデム、セキュリティデバイス、および 3 台のワークステーションの電源をオフにします。
2. DSL モデムの電源をオンにします。
3. セキュリティデバイスの電源をオンにします。

セキュリティデバイスは ISP への PPPoE 接続を作成し、ISP を介して DNS サーバーの IP アドレスを取得します。

4. インターネットネットワーク上での DHCP の起動
ワークステーションの電源をオンにします。

ワークステーションが DNS サーバーの IP アドレスを自動的に受け取ります。ワークステーションは、TCP/IP 接続を試行する際にワークステーション自身の IP アドレスを取得します。

注 : DHCP を使用して Trust ゾーン内のホストに IP アドレスを割り当てる場合は、セキュリティデバイス側で ISP から受け取った DNS サーバーの IP アドレスをホストに自動的に転送します。

ホストの IP アドレスが DHCP を通して動的に割り当てられない場合は、それぞれのホスト上で DNS サーバーの IP アドレスを手動で入力する必要があります。

Trust ゾーン内のホストが Untrust ゾーンに自動的に作成した TCP/IP 接続はすべて、PPPoE カプセル化プロセスを経ます。

CLI

1. インターフェースおよび PPPoE

```
set interface ethernet0/1 zone trust
set interface ethernet0/1 ip 172.16.30.10/24
set interface ethernet0/3 zone untrust
set pppoe interface ethernet0/3
set pppoe username name_str password pswd_str
```

PPPoE 接続をテストするには、

```
exec pppoe connect
get pppoe
```

2. DHCP サーバー

```
set interface ethernet0/1 dhcp server service
set interface ethernet0/1 dhcp server ip 172.16.30.2 to 172.16.30.5
set interface ethernet0/1 dhcp server option lease 60
save
```

3. セキュリティデバイス上での PPPoE の起動

1. DSL モデム、セキュリティデバイス、および 3 台のワークステーションの電源をオフにします。
2. DSL モデムの電源をオンにします。
3. セキュリティデバイスの電源をオンにします。

4. インターネットネットワーク上での DHCP の起動
ワークステーションの電源をオンにします。

ワークステーションが DNS サーバーの IP アドレスを自動的に受け取ります。ワークステーションは、TCP/IP 接続を試行する際にワークステーション自身の IP アドレスを取得します。

Trust ゾーン内のホストが Untrust ゾーンに自動的に作成した TCP/IP 接続はすべて、PPPoE カプセル化プロセスを経ます。

1 次およびバックアップ Untrust インターフェースに PPPoE を構成する

以下の例では、1 次 (ethernet0/3) とバックアップ (ethernet0/2) の両方の Untrust ゾーンへのインターフェースを PPPoE に構成します。

WebUI

1. **ethernet0/3 インターフェースの PPPoE 構成**
   Network > PPP > PPPoE Profile > New: 次のように入力してから **OK** をクリックします。

   PPPoE instance: eth3-pppoe
   Bound to Interface: ethernet0/3 (選択)
   Username: user1
   Password: 123456
   Authentication: Any (選択)
   Access Concentrator: ac-11

2. **ethernet0/2 インターフェースの PPPoE 構成**
   Network > PPP > PPPoE Profile > New: 次のように入力してから **OK** をクリックします。

   PPPoE instance: eth2-pppoe
   Bound to Interface: ethernet0/2 (選択)
   Username: user2
   Password: 654321
   Authentication: Any (選択)
   Access Concentrator: ac-22

CLI

1. **PPPoE Configuration for ethernet0/3 Interface**
   set pppoe name eth3-pppoe username user1 password 123456
   set pppoe name eth3-pppoe ac ac-11
   set pppoe name eth3-pppoe authentication any
   set pppoe name eth3-pppoe interface ethernet0/3

2. **PPPoE Configuration for ethernet0/2 Interface**
   set pppoe name eth2-pppoe username user2 password 654321
   set pppoe name eth2-pppoe ac ac-22
   set pppoe name eth2-pppoe authentication any
   set pppoe name eth2-pppoe interface ethernet0/2
   save

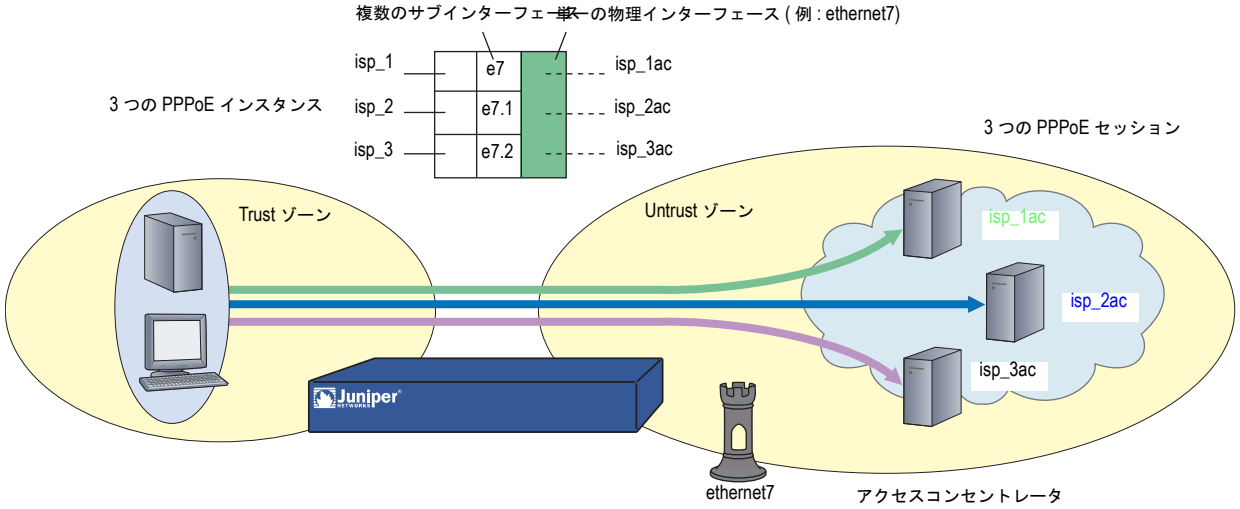
単一インターフェースでの複数の PPPoE セッションの構成

一部のセキュリティデバイスでは、任意の物理インターフェースに対して複数の PPPoE サブインターフェース（それぞれ同じ MAC アドレス）の作成をサポートしています。このサポートによって、ある ISP へのプライベートネットワーク接続を確立しながら、同じ物理インターフェースから別の ISP 経由でインターネット接続が可能になります。これらの接続を異なるユーザー名やドメイン名で確立したり、異なる ISP に同時に接続することができます。

1 物理インターフェース上での PPPoE 同時セッションの最大数は、セキュリティデバイスが許可するサブインターフェース数のみによって制限されます。複数のセッションをサポートするための物理インターフェースの数に関する制限はありません。ユーザー名や静的 IP、アイドルタイムアウト、自動接続およびその他パラメータは、各 PPPoE インスタンスやセッションについて個別に設定することができます。

PPPoE セッションをサポートするには、サブインターフェースをタグなしにする必要があります。タグなしインターフェースでは、(VLAN タグではなく) encap を使ってサブインターフェースの VLAN を識別します。encap はサブインターフェースを PPPoE カプセル化にバインドします。複数のサブインターフェースをホストすることによって、単一の物理インターフェースが複数の PPPoE インスタンスをホストできます。各インスタンスを構成して特定のアクセスコンセントレータ (AC) へ転送すると、ISP などの個々のエンティティ側で単一のインターフェース経由の PPPoE セッションを管理できます。VLAN および VLAN タグの詳細は、“ 第 10 部 : 仮想 システム ” を参照してください。

図 79: 複数のセッションを持つ PPPoE



次の例では、3 つの PPPoE インスタンスを定義して、各インスタンスにアクセスコンセントレータ (AC) を指定してから各インスタンスを起動します。

- Instance isp_1 では、ユーザー名を **user1@domain1**、パスワードを **swordfish**、バインドするインターフェースを ethernet7 にします。AC の名前は **isp_1ac** です。
- Instance isp_2 では、ユーザー名を **user2@domain2**、パスワードを **marlin**、バインドするインターフェースを ethernet7.1 にします。AC の名前は **isp_2ac** です。
- Instance isp_3 では、ユーザー名を **user3@domain3**、パスワードを **trout**、バインドするインターフェースを ethernet7.2 にします。AC の名前は **isp_3ac** です。

WebUI

1. **インターフェースおよびサブインターフェース**
   Network > Interfaces > Edit (ethernet7):

   次のように入力してから **OK** をクリックします。

   Zone Name: Untrust

   Network > Interfaces > New (Sub-IF):

   次のように入力してから **OK** をクリックします。

   Interface Name: ethernet7.1
   Zone Name: Untrust

   Network > Interfaces > New (Sub-IF):

   次のように入力してから **OK** をクリックします。

   Interface Name: ethernet7.2
   Zone Name: Untrust

2. **PPPoE インスタンスおよび AC**
   Network > PPP > PPPoE Profile > New:

   次のように入力してから **OK** をクリックします。

   PPPoE Instance: isp_1
   Enable: Enable
   Bound to Interface: ethernet7
   Username: user1@domain1
   Access Concentrator: isp_1ac

   Network > PPP > PPPoE Profile > New:

   次のように入力してから **OK** をクリックします。

   PPPoE Instance: isp_2
   Enable: Enable
   Bound to Interface: ethernet7.1
   Username: user2@domain2
   Access Concentrator: isp_2ac

   Network > PPP > PPPoE Profile > New:

   次のように入力してから **OK** をクリックします。

   PPPoE Instance: isp_3
   Enable: Enable
   Bound to Interface: ethernet7.2
   Username: user3@domain3
   Access Concentrator: isp_3ac

3. **PPPoE の起動**
   Network > PPP > PPPoE Profile > Connect (for isp_1)

   Network > PPP > PPPoE Profile > Connect (for isp_2)

   Network > PPP > PPPoE Profile > Connect (for isp_3)

CLI

1. **インターフェースおよびサブインターフェース**
   set interface ethernet7 zone untrust
   set interface ethernet7.1 encap pppoe zone untrust
   set interface ethernet7.2 encap pppoe zone untrust

2. **PPPoE インスタンスおよび AC**
   set pppoe name isp_1 username user1@domain1 password swordfish
   set pppoe name isp_1 interface ethernet7
   set pppoe name isp_1 ac isp_1ac
   set pppoe name isp_2 username user2@domain2 password marlin
   set pppoe name isp_2 interface ethernet7.1
   set pppoe name isp_2 ac isp_2ac
   set pppoe name isp_3 username user3@domain3 password trout
   set pppoe name isp_3 interface ethernet7.2
   set pppoe name isp_3 ac isp_3ac
   save

3. **PPPoE の起動**
   exec pppoe name isp_1 connect
   exec pppoe name isp_2 connect
   exec pppoe name isp_3 connect

PPPoE と高可用性

アクティブ / パッシブモードでの PPPoE をサポートする 2 台の セキュリティデバイスは、PPPoE 接続のフェールオーバーを処理できます。接続が開始されると、1 次デバイスが自身の PPPoE 状態をバックアップデバイスと同期します。パッシブ（バックアップ）デバイスは 1 次デバイスと同じ IP アドレスを使用するため、パッシブデバイスが 1 次デバイスとなった場合に新しく PPPoE 接続を確立する必要はありません。そのため、1 次デバイスで障害が発生しても、アクセスコンセントレータとの通信を維持することができます。これは PPPoE インターフェースが VPN 接続をサポートする場合に必要です。フェールオーバー後は同じインターフェース IP を使用して VPN 接続が継続している必要があります。HA 構成の詳細については、“ 第 11 部 : 高可用性 ” を参照してください。

ライセンスキー

ライセンスキーの機能によって、異なるデバイスやシステムイメージにアップグレードせずに、Juniper Networks セキュリティデバイスの機能を拡張することができます。以下のタイプのキーを購入することができます。

- Advanced
- Capacity
- Extended
- Virtualization
- GTP
- Vsys
- IDP

各セキュリティデバイスは、使用可能な標準機能群を組み込んで出荷され、オプション機能のアクティベーション、または既存の機能の拡張をサポートしていることもあります。現在どの機能がアップグレードできるかについては、Juniper Networks の最新のマーケティング文献を参照してください。

ライセンスキーの取得と適用の手順は以下のとおりです。

1. 許可コードとデバイスのシリアルナンバーを集めます。

   許可コード: ご使用のセキュリティデバイスについて、個人または会社が購入されたライセンスキーの生成とアクティベーションに必要なパスキー。注記 : 許可コードはライセンスキーの生成に必要ですが、実際のライセンスキーとは異なります。

   デバイスのシリアルナンバー: ライセンスキーの生成時に、特定のセキュリティデバイスを識別するために Juniper Networks が使用する、固有の 16 文字のコード。シリアルナンバーはデバイスの下部、または背面にあります。また、GUI のデバイス情報セクションを参照したり、CLI の get system コマンドを実行して確認することもできます。

2. http://www.juniper.net/generate_license から Juniper Networks License Management System（LMS）にサインインして、**Firewall/IPSec VPN and Intrusion Prevention** リンクを選択し、システムユーザーインターフェースの指示に従います。

3. Juniper License Management System では、次の 2 つの方法でライセンスキーを提供しています。

   - ご使用のコンピュータにライセンスキーをダウンロードします。
   - ライセンスキーを含む E メールを受信する方法

4. 次のいずれかの方法でライセンスキーをインストールします。

WebUI

Configuration > Update > ScreenOS/Keys > **License Key Update (Features)** を選択 > **Browse** をクリック > ライセンスキーのあるファイルをクリックしてから **Apply** をクリックします。

CLI

exec license-key *key_num*

ライセンスサービスの登録およびアクティブ化

Juniper Networks セキュリティデバイスが、AV（アンチウィルス）パターン、DI（徹底監視）シグネチャ、アンチスパム、または Web フィルタリングに関する定期的なサブスクリプションサービスを受けるには、以下の項目を実行する必要があります。

- サブスクリプションの購入
- サブスクリプションの登録
- サブスクリプションキーの取得

サブスクリプションキーライセンスキーを取得すると、購入した期間、デバイスのサービスがアクティブになります。個別のサービスアクティブ化手続きは、購入したサービスと購入に使用した方法によって異なります。

トライアルサービス

AV、DI、アンチスパム、またはウェブフィルタリングサービスを試用できるように、セキュリティデバイスにはトライアル期間があります。この期間中、デバイスが一時的にサービスを受けることができます。ライセンスサーバーから有効なトライアルライセンスキーを取得するには、CLI コマンド、**exec license-key** update trials を使用します。

- Juniper Networks セキュリティデバイスでは、DI は最初から使用可能にはなっていません。トライアル DI サービスを取得するには、WebUI セッションを開始して、Configuration > Update > ScreenOS/Keys ページの **Retrieve Subscriptions Now** ボタンをクリックする必要があります。これにより、1 度だけ、1 日限りの DI 鍵が提供されます。
- 購入時に AV サービスがデバイスにバンドルされている場合、そのデバイスにはトライアルサービスが事前にインストールされています。このトライアルサービスは 60 日間有効です。
- アンチスパム
- Juniper Networks セキュリティデバイスでは、Web フィタリング は最初から使用可能にはなっていません。この機能にはトライアルサービスがありません。

注意 : サービスの中断を回避するため、サービスを購入したらできるだけ早く Juniper Networks セキュリティデバイスを登録してください。登録することにより、サービス購入の継続が確認されます。

サブスクリプションキーの更新

有効期限のあるソフトウェアがセキュリティデバイスにインストールされている場合は、デバイスはライセンスサーバーに定期的に接続してサブスクリプションキーを読み出します。以下の条件に当てはまる場合、デバイスはライセンスサーバー、すなわち License Management System に接続します。

- 2 か月以内にキーの期限が切れる
- 1 か月以内にキーの期限が切れる
- 2 週間以内にキーの期限が切れる
- キーの期限が切れる
- キーの期限が切れた 30 日後

注 : キーファイルから単一のライセンスキーを削除するには、CLI コマンドの **exec license-key delete** *name_str* を使用します。

既存または新しいデバイスへのアンチウィルス、Web フィルタリング、アンチスパム、徹底監視の追加

AV、Web フィルタリング、アンチスパム、および DI（徹底監視）サブスクリプションを購入して既存の Juniper Networks セキュリティデバイスに追加した場合は、以下の手順に従ってサービスをアクティブにします。

1. サブスクリプションを注文すると、Juniper Networks または許可を受けている VAR から E メールを介して許可コードを受け取ります。このコードは、サブスクリプションの登録に必要な情報を含む可読ドキュメントです。
2. デバイスが登録されたかどうかを確認します。まだ登録されていない場合は、以下のサイトにアクセスしてください。

   http://tools.juniper.net/subreg

3. サブスクリプション許可コードをデバイスに登録します。
4. デバイスにインターネット接続があるかどうかを確認します。
5. デバイスのライセンスキーを取得します。以下のいずれかの方法で行います。
   - WebUI で、Configuration > Update > ScreenOS/Keys ページから **Retrieve Subscriptions Now** ボタンをクリックします。
   - CLI では、以下のコマンドを実行します。

     ```
     exec license-key update
     ```

6. キーをロードしたら、必ずデバイスをリセットしてください。

これで、署名サービスを自動または手動で取得するようにデバイスを構成できます。これらのサービスを受けるようにセキュリティデバイスを構成する方法については、以下のセクションを参照してください。

- **4**-58 ページの「フラグメントの再アセンブリ」
- **4**-62 ページの「ウィルス対策スキャン」
- **4**-98 ページの「Web フィルタリング」

システムクロック

Juniper Networks セキュリティデバイスでは、常に正確な時刻に設定することが重要です。特にデバイスの時刻は、VPN トンネルの設定とスケジュール時間に影響します。まず、デバイスが常に正しい時刻を維持するように、システムクロックを現在の時刻に設定する必要があります。次に、夏時間（DST）オプションを使用可能にして、デバイスが定期的にシステムクロックを更新するときに使用できる NTP（ネットワークタイムプロトコル）サーバーを最高 3 台（1 次を 1 台、バックアップを 2 台）まで構成できます。

日付および時刻

クロックを現在の日付および時刻に設定するには、WebUI または CLI を使用します。WebUI から設定する場合は、以下のとおりにシステムクロックをコンピュータのクロックと同期化します。

1. Configuration > Date/Time: **Sync Clock with Client** ボタンをクリックします。

   コンピュータクロックで DST オプションを有効にしているかどうかを指定するように求めるポップアップメッセージが表示されます。

2. **Yes** をクリックすると、システムクロックが同期化されて夏時間に合わせて調整されます。**No** をクリックすると、夏時間に合わせずにシステムクロックを同期化します。

CLI から設定する場合は、以下のコマンドを使用して日付と時刻を手動で入力します。

```
set clock mm/dd/yyyy hh:mm:ss
```

夏時間

夏時間（DST）は、エネルギーを節約し、明るいうちに仕事や学校での活動をできるように、夏の数か月間公式現地時間を早める、広く用いられているシステムです。

DST の実施は、国によって異なります。したがって、当該国に適用される適切な DST 設定を選ぶことができます。

平日のスケジュール（たとえば 4 月の最初の日曜日)、または特別な日付に DST 調節を繰り返すよう設定できます。さらに、DST 調節を繰り返さないように設定することもできます。その場合には、1 年間だけ DST 設定を調節できます。

タイムゾーン

タイムゾーンの設定では、セキュリティデバイスのローカルタイムが GMT（グリニッジ標準時間）から何時間遅れているか、または何時間進んでいるかを指定します。たとえば、デバイスのローカルタイムゾーンが太平洋標準時間の場合は、GMT から 8 時間遅れています。したがって、クロックを **-8** に設定する必要があります。

WebUI からタイムゾーンを設定する場合

Configuration > Date/Time > Set Time Zone_hours_minutes from GMT

CLI からタイムゾーンを設定する場合

device -> set clock timezone *number*（-12 ～ 12 の数値）

または

device -> set ntp timezone *number*（-12 ～ 12 の数値）

ネットワークタイムプロトコル

セキュリティデバイスの時刻が常に正確になるようにするため、セキュリティデバイスで NTP（ネットワークタイムプロトコル）を使用してインターネットからデバイスのシステムクロックを NTP サーバーのシステムクロックと同期することができます。同期化は手動で行うか、指定した間隔で自動的に実行するようにデバイスを構成することができます。

複数の NTP サーバーの構成

NTP サーバーは 1 台の Juniper Networks セキュリティデバイスにつき最高 3 台（1 次を 1 台、バックアップを 2 台）まで構成できます。システムクロックを自動的に同期化するようにセキュリティデバイスを構成すると、構成した各 NTP サーバーが連続して検索されます。デバイスは常に、1 次 NTP サーバーを最初に検索します。次に、1 次 NTP サーバーの検索が失敗すると、デバイスに構成されているいずれかの NTP サーバーから有効な応答を得られるまで、最初のバックアップ NTP サーバー、次のバックアップ NTP サーバーというように検索を実行します。検索は、更新を終了して失敗のログを記録するまで、各 NTP サーバーで 4 回試行されます。

手動でシステムクロックを同期化する場合、CLI のみが使用できます。このとき、特定の NTP サーバーを 1 つ指定するか、サーバーを 1 台も指定しません。NTP サーバーを指定した場合、そのサーバーだけを検索します。NTP サーバーを指定しなかった場合、そのデバイスに構成されている各 NTP サーバーを連続して検索します。NTP サーバーは、その IP アドレスまたはドメイン名を使用して指定します。

バックアップ NTP サーバーの構成

必要に応じて、個別のインターフェースをソースアドレスとして指定して、デバイスからの NTP 要求を VPN トンネルを介して 1 次 NTP サーバーまたはバックアップサーバーに導くことができます。この機能を実行するには、インターフェースタイプの中でも、ループバックインターフェースを選択できます。

セキュリティデバイスはソースインターフェースから NTP 要求を送信します。NTP サーバーに NTP 要求を送信するときに、暗号化された事前共有鍵を使用することもあります。鍵により認証が行われます。

次の例では、1 次 NTP サーバーと 2 台のバックアップ NTP サーバーにそれぞれ IP アドレスを割り当てて構成します。次に、各サーバーを設定して Trust インターフェースから NTP 要求を送信します。その後、各サーバーに鍵 ID と事前共有鍵を設定します。

WebUI

Configuration > Date/Time: 以下を入力して **Apply** をクリックします。

Primary Server IP/Name: 1.1.1.1
Primary server Key ID: 10
Source interface: Select Trust from the list.
Preshared Key: !2005abc
Backup Server1 IP/Name: 1.1.1.2
Primary server Key ID: 10
Source interface: Select Trust from the list.
Preshared Key: !2005abc
Backup Server2 IP/Name: 1.1.1.3
Primary server Key ID: 10
Source interface: Select Trust from the list.
Preshared Key: !2005abc

CLI

```
set ntp server 1.1.1.1
set ntp server backup1 1.1.1.2
set ntp server backup2 1.1.1.3
set ntp server src-interface trust
set ntp server backup1 src-interface trust
set ntp server backup2 src-interface trust
set ntp server key-id 10 pre-share-key !2005abc
set ntp server backup1 key-id 10 pre-share-key !2005abc
set ntp server backup2 key-id 10 pre-share-key !2005abc
save
```

最大時間調整

自動同期化の場合、最大時間調整値を (秒単位で) 指定できます。最大時間調整値とは、セキュリティデバイスのシステムクロックと NTP サーバーから受信した時刻との許容可能な時間差です。デバイスがクロックを NTP 時刻に合わせて調整するのは、セキュリティデバイスのクロックと NTP サーバー時刻との時間差が、設定されている最大時間調整値内にある場合のみです。たとえば、最大時間調整値が 3 秒で、デバイスシステムクロックの時刻が 4:00:00、NTP サーバーの時刻が 4:00:02 の場合、これらの時間は許容可能であるため、デバイスでクロックを更新できます。時間調整が設定した値より大きい場合、クロックが同期化されずに、デバイスに構成されている最初のバックアップ NTP サーバーの検索を試行します。構成されているすべての NTP サーバーの検索を試行しても有効な応答が得られない場合は、エラーメッセージがイベントログに生成されます。この機能のデフォルト値は 3 秒で、指定可能な範囲は 0 (無制限) ～ 3600 (1 時間) です。

手動でシステムクロックを同期化する場合は、CLI でのみできます。この場合デバイスは最大時間調整値を確認しません。代わりに、デバイスは有効な応答を受信すると、応答を受信した NTP サーバー、時刻調整、および使用された認証メソッドのタイプを通知するメッセージを表示します。また、このメッセージではシステムクロック更新を確認するかキャンセルするかをたずねます。

セキュリティデバイスが有効な応答を得られなかった場合は、タイムアウトメッセージを表示します。このメッセージは、デバイスに構成されているすべての NTP サーバーへの到達に失敗した場合にのみ表示されます。

注： CLI を使用して要求を発行する場合は、キーボードの **Ctrl-C** を押すと現在の要求をキャンセルできます。

NTP および NSRP

NSRP（NetScreen 冗長プロトコル）には、NSRP クラスタメンバーのシステムクロックを同期化するための機構があります。同期化の解決は秒単位ですが、NTP には別の秒単位の解決があります。各クラスタメンバーの時刻は処理の遅延により数秒異なることがあるため、NTP が両方のクラスタメンバーで使用可能になっていて各メンバーがそれぞれのシステムクロックを NTP サーバーから更新できる場合は、NSRP 時間同期化を使用不可にしておくことをお勧めします。NSRP 時間同期化機能を使用不可にするには、**set ntp no-ha-sync** CLI コマンドを入力します。

NTP サーバーへの最大時間調整値の設定

次の例では IP アドレス 1.1.1.1、1.1.1.2、および 1.1.1.3 の NTP サーバーからクロックを 5 分間隔で更新するようにセキュリティデバイスを構成します。また、最大時間調整値は 2 秒に設定しています。

WebUI

Configuration > Date/Time: 以下を入力して **Apply** をクリックします。

Automatically synchronize with an Internet Time Server (NTP): (**選択**)
Update system clock every minutes: 5
Maximum time adjustment seconds: 2
Primary Server IP/Name: 1.1.1.1
Backup Server1 IP/Name: 1.1.1.2
Backup Server2 IP/Name: 1.1.1.3

CLI

```
set clock ntp
set ntp server 1.1.1.1
set ntp server backup1 1.1.1.2
set ntp server backup2 1.1.1.3
set ntp interval 5
set ntp max-adjustment 2
save
```

セキュア NTP サーバー

NTP トラフィックを安全にするには、MD5 ベースのチェックサムを使用して、NTP パケットの認証を提供します。IPSec トンネルを作成する必要はありません。このタイプの認証は、NTP トラフィックの保全性を保証します。外部パーティによるデータ表示は防止できませんが、データの改ざんは防止できます。

NTP トラフィックの認証を使用可能にするには、セキュリティデバイスで構成した各 NTP サーバーに固有の鍵 ID と事前共有鍵を割り当てる必要があります。この鍵 ID と事前共有鍵は、セキュリティデバイスおよび NTP サーバーがデータを認証するときに使用できるチェックサムを作成する際に使用されます。

表 38 は、2 種類の NTP トラフィックの認証を示しています。

表 38: NTP トラフィック認証

タイプ	解説
Required（必須）	これを選択する場合は、セキュリティデバイスは、NTP サーバーに送信するすべてのパケットに認証情報（鍵 ID とチェックサム）を入れて、NTP サーバーから受信するすべての NTP パケットを認証する必要があります。セキュリティデバイスと NTP サーバー間で認証を行う前に、まずセキュリティデバイスと NTP サーバーの管理者で鍵 ID と事前共有鍵を交換する必要があります。これらの交換は手動で行う必要があります。交換方法は、E メールや電話などいくつかの方法があります。
Preferred（優先）	これを選択する場合、セキュリティデバイスはすべての NTP トラフィックの認証を試行して、まず Required モードの場合と同様に動作する必要があります。認証の試行がすべて失敗すると、セキュリティデバイスは認証が選択されていないかのように動作します。この場合、鍵 ID とチェックサムを入れずにパケットを NTP サーバーに送信します。基本的には認証を優先しますが、認証が失敗しても NTP トラフィックは許可されます。

索引

数字

2 次 IP アドレス 51

A

ALGALG
- MS RPC 130
- RTSP 132
- Sun RPC 129
- カスタムサービス 169

ARP 84
ARP、入口 IP アドレス 87

C

CLI、set arp always-on-dest 76, 79

D

DC コードポイントマーキング 196, 202, 216
DHCP 98, 102, 247
- client 227
- HA 233
- PXE など 239
- サーバー 227
- リレーエージェント 227

DiffServ 176, 202, 216
- DC コードポイントマーキングも参照

DIP 101, 143–146
- PAT 144
- グループ ..... 155, ??–157
- 固定ポート 145
- プール 171
- プール、変更 145

DNS 219
- アドレス、分割 226
- サーバー 248
- サーバー、トンネリング 225
- 状況テーブル 221
- ルックアップ 220
- ルックアップ、ドメイン 225

DSL 242, 247

H

HA
- NSRP も参照
- DHCP 233
- インターフェース、仮想 HA 39

I

ICMP サービス 128
- メッセージコード 128
- メッセージタイプ 128

IP アドレス
- 2 次、ルーティング 52
- 2 次 51
- インターフェース、トラッキング 64
- 管理 97
- 公開 47
- ネットワーク ID 48
- 非公開 47
- 非公開アドレス範囲 48
- ポート、定義 106
- ホスト ID 48

IP トラッキング
- vsys 65
- インターフェース、共有 65
- インターフェース、サポートされる 64
- ウェイト 66
- オブジェクトの障害しきい値 66
- 動的オプション 65
- トラフィックの再ルーティング 64–80

IP トラッキング、障害
- 入口インターフェース、オン 78–80
- 出口インターフェース、オン 77–78
- トラックされる IP のしきい値 66

IP プール
- DIP プールを参照

IP アドレス
- L3 セキュリティゾーン 47–48

IP を管理する 97
ISP 225

L

L2TP ポリシー 170

M

MGT インターフェース 38
MIP 12
MIP、インターフェースベースの NAT を使ったゾーン向け 96
MS RPC ALG、定義済み 130

N

NAT モード 94–100
  Untrust ゾーンに向かうトラフィック 81, 96
  インターフェース設定 97
NAT-src、Route モード 100
NetInfo 228
NSRP
  DHCP 233
  DIP グループ 155, 157
  HA セッションバックアップ 174
  NTP 同期化 260
  VSI 38
  冗長インターフェース 37
NTP 258–261
  NSRP 同期化 260
  サーバー 258
  最大時間調整 259
  セキュアサーバー 260
  認証タイプ 261
  複数のサーバー 258

P

PAT 144
PXE 239
PXE サーバー 240

Q

QoS 195

R

RFC
  0792, *インターネット制御メッセージプロトコル* 128
  1918, *Address Allocation for Private Internets* 48
  2326, *Real Time Streaming Protocol (RTSP)* 132, 137
  1349, *1349、インターネットプロトコルスイートのサービスのタイプ* 176
  2474, *2474、IPv4、IPv6 ヘッダーの差別化フィールド（DS フィールド）の定義* 176
  2132, *DHCP Options and BOOTP Vendor Extensions* 232
Route モード 100–103
RSH ALG 129
RTSP ALG
  ステータスコード 135
  定義 132
  パブリックドメイン内のメディアサーバー 139
  プライベートドメイン内のメディアサーバー 137
  要求メソッド 133

S

ScreenOS
  Global ゾーン 28
  概要 1
  仮想システム 10
  機能ゾーン 33
  セキュリティゾーン 2, 28
  セキュリティゾーン、Global 2
  セキュリティゾーン、定義済み 2
  ゾーン ..... 25, ??–33
  トンネルゾーン 29
  パケットフロー ..... 11, ??–13
  ポリシー 3
ScreenOS インターフェース
  サブインターフェース 3
  セキュリティゾーン 3
SCREEN、MGT ゾーン 28
Sun RPC ALG
  定義 129
  呼び出し手順 129

T

trace-route 87
Tunnel インターフェース 39
  定義 39
  ポリシーベース NAT 39

U

URL フィルタリング
  Web フィルタリングを参照

V

VIP 12
VIP、インターフェースベースの NAT を使ったゾーン向け 96
VLAN ゾーン 83
VLAN1
  インターフェースをチェックします 83, 89
  ゾーン 83
VLAN、タグ 3
VPN
  インターフェースベースの NAT で保護されたゾーン向け 96
  トンネルゾーン 29
  ポリシー 170
VR
  VR 間のトラフィック転送 5
  はじめに 4

W

Web フィルタリング 174
WebAuth、事前ポリシー認証手続き 173

あ

アクセスポリシー
　ポリシーを参照
宛先不明のユニキャストの処理方式.....84–89
　ARP.....87–89
　trace-route.....87
　フラッド.....85–86
アドレス
　IP、ホストおよびネットワーク ID.....48
　公開.....47
　定義.....168
　非公開.....48
　ポリシー内.....168
　アドレス帳エントリ.....106–110
アドレスグループ.....108, 168
　エントリ、削除.....110
　オプション.....108
　作成.....109
　編集.....110
アドレス帳
　アドレス
　　削除.....110
　　設定変更.....107
　　追加.....106
　アドレスも参照
　エントリ.....106
　グループ.....108
　グループエントリ、編集.....110
アドレス否定.....188
アプリケーションオプション、ポリシーで.....169
アラーム、しきい値.....174

い

インターネットサービスプロバイダ（ISP）.....225
インターフェース
　DIP.....143
　VLAN1.....83
　VSI.....38
　デフォルト.....49
　2 次 IP アドレス.....51
　HA 機能ゾーン.....38
　IP トラッキング (IP トラッキングを参照)
　L3 セキュリティゾーン.....47
　MGT.....38
　アップ、物理的.....62
　アドレス設定.....47
　インターフェース表を表示する.....43
　インターフェース表、表示.....43
　仮想 HA.....39
　期限ゾーン.....38
　状態の変化.....62
　冗長.....37
　セキュリティゾーンの物理.....36
　接続、監視.....64
　設定変更.....49
　ゾーンにバインドする.....45
　ゾーン、アンバインド.....46
　ダウン、物理的.....62
　統合.....37
　トンネル.....39, 39–43
　ポリシーベース NAT トンネル.....39
　ループバック.....59
インターフェース、監視.....69–75
　セキュリティーゾーン.....75
　ループ.....70

か

カスタムサービス、ルート、vsys.....123
仮想 HA インターフェース.....39
仮想システム.....10
仮想ルーター
　VR を参照

き

キー、ライセンス.....254
機能ゾーンインターフェース.....38
　HA.....38
　管理.....38

く

グラフ、履歴.....174
グループ
　アドレス.....108
　サービス.....140
クロック、システム
　システムクロックも参照

こ

公開アドレス 47
顧客サービス 123

さ

サービス 110
  ICMP 128
    タイムアウトしきい値 125
    定義 168
    ドロップダウンリスト 110
    ポリシー内 168
サービスグループ 140–142
    削除 142
    作成 141
    設定変更 142
サービスグループ (WebUI) 140
サービス購入
    一時サービス 255
    登録およびアクティブ化 255–257
サービスブック
    エントリ、削除（CLI） 125
    エントリ、変更（CLI） 124
サービスブック、サービス
    カスタム 110
    カスタム（CLI） 124
    追加 124
    定義済み 110
サービス、カスタム 123
    ALGALG 169
    vsys 123
サブインターフェース 3
    削除 51
    作成する (ルートシステム) 50

し

システムパラメータ 260
システムクロック 257–261
    クライアントとの同期化 257
    タイムゾーン 258
    日付および時刻 257

す

スケジュール 158, 175

せ

セキュリティゾーン 2
    グローバル 2
    決定、宛先ゾーン 13
    決定、ソースゾーン 11
    定義済み 2
セキュリティゾーン、インターフェース 3
    物理 36

そ

ゾーン 25–33
    Layer 2 83
    VLAN 33, 83
    Global セキュリティ 2
    機能 33
    機能、MGT インターフェース 38
    グローバル 28
    定義 30
    トンネル 29
    編集 31
ゾーン、ScreenOS ..... 25, ??–33
    セキュリティインターフェース 3
    定義済み 2
ゾーン、セキュリティ 2, 28
    インターフェース、監視 75
    インターフェース、物理 36
    グローバル 2
    決定、宛先ゾーン 13
    決定、ソースゾーン 11

た

帯域幅 176
    Priority
      キュー 200
      デフォルト 200
      レベル 201
    管理 196
    最大 176, 196, 201
    最大、無限の 196
    保証 176, 196, 201
タイムゾーン 258
タグ、VLAN 3

と

透過モード
    ARP 以外のトラフィックを遮断 84
    ARP/trace-route 85
    IP 以外のトラフィックを遮断 84
    フラッド 85
    ブロードキャストトラフィック 84
    ユニキャストオプション 85
    ルート 84
..... 82–94
統合インターフェース 37
動的 IP（DIP）プール 145, 171
ドメイン名システム
    DNS を参照
トラフィック
    Priority 176
    カウンティング 174
    シェーピング 195
    ロギング 174

トラフィックシェーピング.....195
サービス優先順位.....200
自動.....196

に

認証
Allow Any.....173
ポリシー.....172
ユーザー.....172
認証ユーザー
WebAuth.....173
事前ポリシー認証.....173
ランタイム認証.....172
ランタイム認証プロセス.....172

ね

ネットマスク.....48, 168
ネットワーク、帯域幅.....195

は

パケットフロー.....11, ??–13

ひ

非公開アドレス.....48
否定、アドレス.....188

ふ

物理インターフェース
論理インターフェース.....36
ブリッジグループ
アンバインド.....46
論理インターフェース.....36

ほ

ポートアドレス変換
PAT を参照

ポリシー 3
ID 168
Deny 169
DIP グループ 155
HA セッションバックアップ 174
L2TP 170
L2TP トンネル 170
NAT-dst 172
NAT-Src 171
permit 169
Reject 169
VPN 170
VPN ダイアルアップユーザーグループ 168
アクション 169
アドレス 168
アドレスグループ 168
アドレス否定 188
アプリケーション、に明示的にリンク 169
カウンティング 174
仮想システム 166
管理 177
機能 161
グローバル 164, 177, 186
警告 174
検証 192
コンポーネントごとの複数の項目 187
サービス 110, 168
サービスグループ 140
サービスブック 110
再順序付け 193
最上位 171, 193
最大制限 109
削除 194
シャドウ 192
種類 163–164
順序 193
使用可能 191
使用不可 191
スケジュール 175
セキュリティゾーン 168
ゾーン内 164, 177, 185
帯域幅の管理 196
地域間 163, 177, 180
徹底監視 (DI) 171
トラフィックシェーピング 175
トラフィックロギング 174
トンネル 169
内部ルール 166
名前 170
認証 172
必要な要素 162
変更 191
編集 191
ポリシーセットリスト 165
ポリシーの内容 187
両方向 VPN 170
ルートシステム 166
ルックアップの順序 165
ポリシーベース NAT、トンネルインターフェース .39

も

モード
NAT、Untrust ゾーンに向かうトラフィック 81
透過 82

ゆ

優先順位キュー 200

ら

ライセンスキー 254
ランタイム認証 172

り

履歴グラフ 174

る

ルートモード
NAT-Src 100
インターフェース設定 101
ループバックインターフェース 59
ルール、ポリシーから派生 166

ろ

ロギング 174

わ

ワイヤレスインターフェース
論理インターフェース 36



概念と用例
ScreenOS リファレンス ガイド

第 3 部 :
管理

リリース 6.0.0、改訂 02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

品番 : 530-017769-01-JP, 改訂 02

Copyright Notice

Copyright © 2007 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

目次

本編について vii

ドキュメントの規則 vii
Web ユーザーインターフェースの規則 vii
コマンドラインインターフェースの規則 viii
ネーミング規則および文字タイプ viii
説明図の規則 ix
技術ドキュメンおよびテクニカルサポート x

第 1 章 管理 1

Web ユーザーインターフェースからの管理 1
WebUI ヘルプ 2
ローカルドライブにヘルプファイルをコピーする 2
WebUI を新しいヘルプ位置にポイントさせる 3
HTTP（ハイパーテキスト転送プロトコル） 3
セッション ID 4
セキュアソケットレイヤー 5
SSL の構成 6
HTTP を SSL に転送する 8
コマンドラインインターフェースからの管理 9
Telnet 9
Telnet 接続を保護する 10
セキュアシェル 11
クライアント要件 12
デバイス上の基本的な SSH 構成 13
認証 14
SSH と Vsys 16
ホスト鍵 16
例 : SSHv1 で PKA を使用して自動ログインする 17
セキュアコピー 18
Serial Console 19
リモートコンソール 20
V.92 モデムポートを使用するリモートコンソール 20
AUX ポートを使用するリモートコンソール 21
モデムポート 22
NetScreen-Security Manager からの管理 22
NSM エージェントと MGT システムの接続の開始 23
NSM エージェントを使用可能、使用不可、設定解除する 24
管理システムのプライマリ サーバーの IP アドレスの設定 25
アラームおよび統計データ レポートの設定 25
構成同期化 26
例 : 構成状態を表示する 26
例 : 構成ハッシュを取得する 27
構成タイムスタンプを取得する 27

管理トラフィックのコントロール 28
MGT および VLAN1 インターフェース 29
例 : MGT インターフェースによる管理 29
例 : VLAN1 インターフェースを介した管理 29
管理インターフェースオプションの設定 30
複数のインターフェースに対して管理 IP を設定する 31
管理レベル 33
ルート管理者 33
読取 / 書込管理者 34
読取専用管理者 34
仮想システム管理者 34
仮想システム読取専用管理者 35
管理ユーザーの定義 35
例 : 読取専用管理者を追加する 35
例 : 管理者を変更する 35
例 : 管理者を削除する 36
例 : ダイアルアップ接続用の管理者アカウントを構成する 36
例 : 管理者のセッションを消去する 37
セキュアな管理トラフィック 37
ポート番号を変更する 38
管理者ログイン名およびパスワードを変更する 39
例 : 管理ユーザーのログイン名およびパスワードを変更する 40
例 : ユーザー自身のパスワードを変更する 40
ルート管理者パスワードの最小文字数を設定する 41
デバイスのデフォルト設定へのリセット 41
管理者アクセスを制限する 42
例 : 管理を 1 つのワークステーションに制限する 42
例 : 管理を特定のサブネットに制限する 42
ルート管理者をコンソールアクセスに制限する 42
管理トラフィックの VPN トンネル 43
ルートベース手動鍵 VPN トンネルを介した管理 44
ポリシーベース手動鍵 VPN トンネルを介した管理 47
パスワードポリシー 51
パスワードポリシーを設定する 51
パスワードポリシーを削除する 52
パスワードポリシーを表示する 52
拒否されたデフォルトの管理者パスワードからの回復 52
ログインバナーの作成 53

第 2 章 セキュリティ デバイスの監視 55

ログ情報の保存 55
イベントログ 57
重大度とキーワードでイベントログを参照する 58
イベントログのソーティングとフィルタリング 59
イベントログのダウンロード 60
例 : イベント ログ全体をダウンロードする 60
例 : クリティカルイベントのイベントログをダウンロードする 60
トラフィックログ 61
トラフィックログの参照 62
例 : トラフィックログのエントリを参照する 62
トラフィックログのソーティングとフィルタリング 63
例 : 時刻でトラフィックログをソーティングする 63
トラフィックログのダウンロード 64
終了の理由フィールドを削除する 64

自己ログ 66
自己ログの参照 67
自己ログのソーティングとフィルタリング 67
例 : 自己ログを時刻でフィルタリングする 67
自己ログのダウンロード 68
リカバリ ログのダウンロード 68
トラフィック警告 69
例 : ポリシーベースの侵入試行を検出する 69
例 : システム妥協通知をする 70
例 : E メール警報を送信する 71
Syslog 72
例 : 複数の Syslog サーバーを使用可能にする 72
WebTrends を通知イベントで有効にする 73
簡易ネットワーク管理プロトコル 74
インプリメンテーションの概要 76
読取 / 書込 SNMP コミュニティを定義する 77
自己開始トラフィックの VPN トンネル 78
例 : ルートベースのトンネルを経由する自己生成のトラフィック 79
例 : ポリシーベースのトンネルを経由する自己生成のトラフィック 86
Screen カウンタを参照する 93

索引 ..... IX-I

本編について

Juniper Networks セキュリティ デバイスは、ローカルやリモートでデバイスを管理するさまざまな方法を提供します。*第 3 部: 管理*には、以下の章が含まれます。

- 第 1 章「管理」は、ローカルおよびリモートの両方で、セキュリティデバイスの管理に利用できる様々な方法について説明します。本章はまた、定義可能な 4 段階のネットワーク管理者のそれぞれに与えられる権限についても説明します。
- 第 2 章「セキュリティ デバイスの監視」は、様々な監視方法について説明すると共に、監視出力を理解する手引きを提供しています。

ドキュメントの規則

このドキュメントは、次のセクションで説明されている規則を使用しています。

- 「Web ユーザーインターフェースの規則」
- 「コマンドラインインターフェースの規則」
- viii ページの「ネーミング規則および文字タイプ」
- ix ページの「説明図の規則」

Web ユーザーインターフェースの規則

WebUI（Web ユーザーインターフェース）では、各作業の操作指示は、操作手順と構成設定値に分かれています。構成設定を入力できる WebUI ページを開くには、画面の左側にあるナビゲーション ツリーのメニュー項目をクリックして、そのページに移動します。先へ進むと、ナビゲーション パスが画面の上部に表示されます。各ページは角括弧で分離されています。

WebUI のパスおよびアドレスを定義するためのパラメータは、以下のとおりです。

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

```
Address Name: addr_1
IP Address/Domain Name:
    IP/Netmask: ( 選択 ), 10.2.2.5/32
Zone: Untrust
```

構成設定のオンラインヘルプを開くには、画面の左上にある疑問符（?）をクリックします。

ナビゲーションツリーにも、Help > Config Guide 構成ページがあり、セキュリティポリシーおよび IPSec (インターネットプロトコルセキュリティ) の構成に役立ちます。ドロップダウンメニューからオプションを選択して、そのページの指示に従います。構成設定のオンラインヘルプを開くには、左上にある **?** 文字をクリックします。

コマンドラインインターフェースの規則

次の規則は、例とテキストにおいて、コマンドラインインターフェース（CLI）コマンドの構文を示すために使用されます。

例においては、次のように使用されます。

- 角括弧 [ ] 内にあるものはすべてオプションです。
- 中括弧 { } 内にあるものはすべて必須です。
- 選択肢が複数ある場合、各選択肢はパイプ (|) で区切られています。例えば、次のように表示されます。

  set interface { ethernet1 | ethernet2 | ethernet3 } manage

- 変数は*斜体*で表示されます。

  set admin user *name1* password *xyz*

テキストにおいては、コマンドは**太字**で、変数は*斜体*で表示されます。

注 : キーワード入力時には、単語を間違いなく識別できる数の文字を入力すれば十分です。**set admin user wheezer j12fmt54** というコマンドを入力する際には、**set adm u whee j12fmt54** と入力するだけで十分です。ただし、本編に記載されたコマンドはすべて本来の形式で記載されています。

ネーミング規則および文字タイプ

ScreenOS はオブジェクトの名前 (アドレス、管理ユーザー、認証サーバー、IKE ゲートウェイ、仮想システム、VPN トンネルおよびゾーンなど、ScreenOS 構成に定義されているもの) に関して、次の規則に従います。

- 名前文字列に 1 つまたは複数のスペースが含まれる場合、文字列全体を二重引用符で囲む必要があります。例えば

  set address trust “local LAN” 10.1.1.0/24

- 二重引用符で囲まれた文字列の先頭または末尾のスペースを取り除きます。たとえば、「 **local LAN** 」は「**local LAN**」となります。
- 連続した複数のスペースは、一つのスペースとして扱われます。
- CLI キーワードの多くはケースセンシティブではありませんが、名前文字列はケースセンシティブです。たとえば、「**local LAN**」は「**local lan**」とは異なります。

ScreenOS は、次の文字タイプをサポートします。

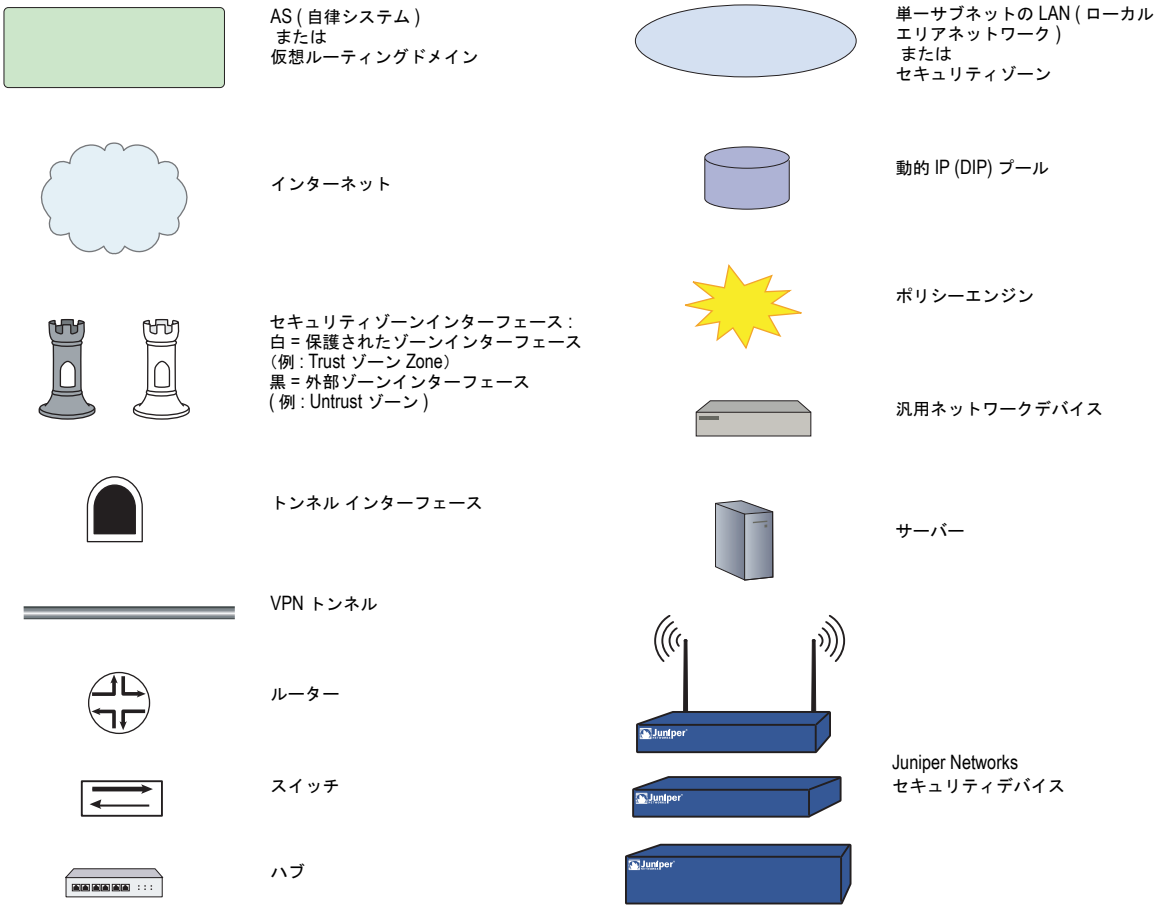
- 1 バイト文字セット (SBCS) およびマルチバイト文字セット (MBCS)。SBCS の例に、ASCII、欧州言語、およびヘブライ語があります。2 バイト文字セット (DBCS) とも呼ばれる MBCS の例に、中国語、韓国語、および日本語があります。
- ASCII 文字の 32（16 進数の 0x20）から 255（0xff)。ただし二重引用符 (") は、スペースを含む名前文字列の先頭と末尾を示す特殊な意味をもつため、例外とします。

注： コンソール接続では、SBCS のみがサポートされます。ご利用のブラウザがサポートする文字セットに応じて、WebUI は SBCS および MBCS の両方をサポートします。

説明図の規則

次の図は、本編を通して説明図に使用されている画像の基本的なものです。

図 1: 説明図の画像



技術ドキュメンおよびテクニカルサポート

Juniper Networks 製品のいずれかの技術ドキュメントを入手するには、www.juniper.net/techpubs/ をご覧ください。

テクニカルサポートについては、http://www.juniper.net/customers/support/ にある Case Manager を使って事例サポートを開くか、1-888-314-JTAC (米国内) か 1-408-745-9500 (その他の国) までお問い合わせください。

本書に間違いや欠落があった場合は、techpubs-comments@juniper.net までお知らせください。

第 1 章
管理

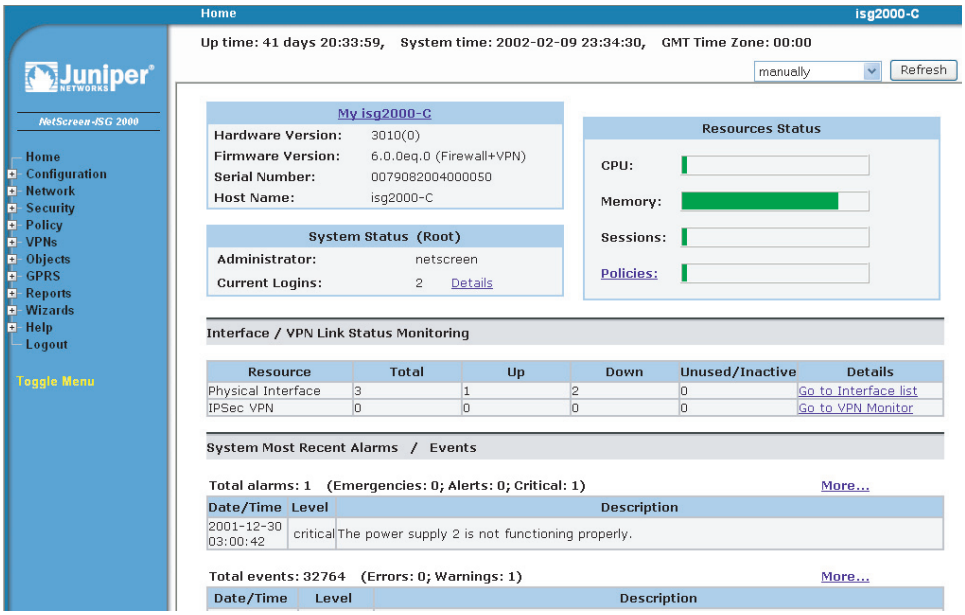
本章では、管理方法、ツール、管理トラフィックの安全性を確保する方法、管理ユーザーに割り当てることのできる管理者特権レベルについて説明します。本章のセクションは、以下のようになります。

- 1 ページの「Web ユーザーインターフェースからの管理」
- 9 ページの「コマンドラインインターフェースからの管理」
- 22 ページの「NetScreen-Security Manager からの管理」
- 28 ページの「管理トラフィックのコントロール」
- 33 ページの「管理レベル」
- 35 ページの「管理ユーザーの定義」
- 37 ページの「セキュアな管理トラフィック」
- 51 ページの「パスワードポリシー」
- 53 ページの「ログインバナーの作成」

Web ユーザーインターフェースからの管理

WebUI（Web ユーザー インターフェース）を使用して、Juniper Networks セキュリティ デバイスを構成および管理することができます。図 2 は、WebUI ウィンドウを示しています。左ペインにはナビゲーション メニューが示され、右ペインにはナビゲーション ウィンドウが表示されます。

図 2: WebUI



WebUI を使用するには、以下のアプリケーションと接続が必要です。

- Netscape Communicator (バージョン 4.7 あるいはそれ以降) または Microsoft Internet Explorer (バージョン 5.5 あるいはそれ以降)
- セキュリティデバイスへの TCP/IP ネットワーク接続

WebUI ヘルプ

WebUI のヘルプファイルは http://help.juniper.net/help/english/*screenos_version*（例えば、http://help.juniper.net/help/english/5.3）から参照できます。

また、ヘルプファイルを再配置するオプションもあります。ローカルで保存する場合、WebUI を管理者のワークステーションまたはローカルネットワークのセキュアなサーバーにポイントします。Internet アクセスができない場合には、ヘルプファイルをローカルで保存することで、通常できないアクセスを行うことができます。

ローカルドライブにヘルプファイルをコピーする

ヘルプファイルは、ドキュメンテーション CD で提供されています。WebUI を変更して、ローカル CD ドライブにある CD のヘルプファイルをポイントさせることもできます。また、CD のファイルをローカル ネットワークのサーバーやワークステーションの別ドライブにコピーして、その位置からヘルプ ファイルを呼び出すように WebUI を構成することもできます。

注： ドキュメンテーション CD から直接ヘルプファイルを起動したい場合には、この手順を省略することができます。3 ページの「WebUI を新しいヘルプ位置にポイントさせる」へ進みます。

1. ドキュメンテーション CD をワークステーションの CD ドライブに挿入します。
2. その CD ドライブに移動して、**help** ディレクトリをコピーします。
3. ヘルプのディレクトリを保存する場所に移動して、そこにヘルプのディレクトリを貼り付けます。

WebUI を新しいヘルプ位置にポイントさせる

ここで、ヘルプディレクトリの新しい位置にポイントするために、WebUI を指定変更する必要があります。デフォルト URL を、新規パスが以下のようになるようにします。*path* は管理者のワークステーションからのヘルプディレクトリの特定パスです。

1. Configuration > Admin > Management: Help Link Path フィールドで、デフォルト URL を置き換えます。

   http://help.juniper.net/help/english/*screenos_version*

   以下のように変更します。

   （ローカルドライブでは）file://*path*.../help

   または

   （ローカルサーバーでは）http://*server_name*.../*path*/help

2. **Apply** をクリックします。

   WebUI の右上隅にある **help** のリンクをクリックすると、デバイスはヘルプファイルを見つけるために、Help Link Path フィールドに指定された新しいパスを使用します。

HTTP（ハイパーテキスト転送プロトコル）

標準ブラウザで HTTP（ハイパーテキスト転送プロトコル）を使い、ネットワークセキュリティ構成をリモートでアクセス、監視、コントロールできます。

HTTP 管理トラフィックは、VPN (仮想プライベートネットワーク) トンネルまたは SSL (セキュアソケットレイヤー) プロトコルによりカプセル化することで保護することができます。また、ネットワークユーザートラフィックから管理トラフィックを完全に切り離すことでも保護することができます。セキュリティデバイス モデルによっては、すべての管理トラフィックを MGT インターフェース（一部のセキュリティ デバイスで利用可能）により実行するか、またはインターフェースを MGT ゾーンにバインドして、管理トラフィック専用にすることができるものがあります。

注 : 詳細については、5 ページの「セキュアソケットレイヤー」、43 ページの「管理トラフィックの VPN トンネル」、および 29 ページの「MGT および VLAN1 インターフェース」を参照してください。

セッション ID

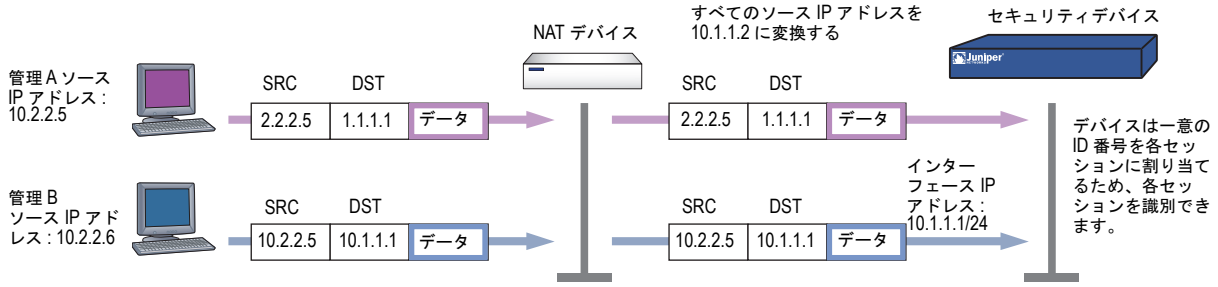
セキュリティデバイスは、一意のセッション ID を各 HTTP 管理セッションに割り当てます。仮想システム（vsys）をサポートするセキュリティデバイスの場合も、この ID はすべてのシステム（root と vsys）でグローバルに一意となります。

各セッション ID は、擬似乱数で生成された 5 つの数を組み合わせた 39 バイトの数です。この ID は乱数によって生成されるため（単純に数を増分する方法とは異なり）、実質的に推測が不可能となります。さらに、この無作為性に加えて ID が前述の長さをもつため、2 つの同時管理セッションに対して同じ ID が偶然に複写される可能性も、極端に低くなります。

管理者がセッション ID を利用して得られる利点に、以下の 2 点があります。

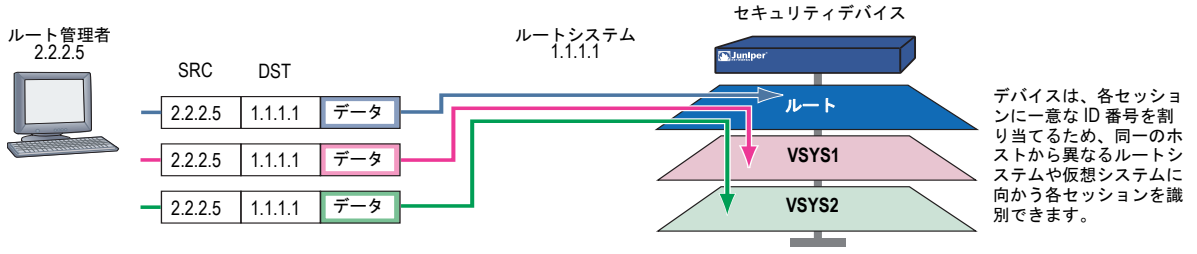
- 図 3 は、セキュリティ デバイスが、すべてのアウトバウンド パケットに同じソース IP アドレスを割り当てる NAT デバイスを介した、複数の管理者からの同時セッションをどのように区別するかを示しています。

図 3: NAT デバイスを使用したセッション ID



- 図 4 は、セキュリティ デバイスが、同じソース IP アドレスからルート システムへ向かう同時ルートレベル管理セッション、およびルート システムから異なる仮想システムへ向かう同時ルートレベル管理セッションをどのように識別するかを示しています。

図 4: ソース IP アドレスを使用したセッション ID



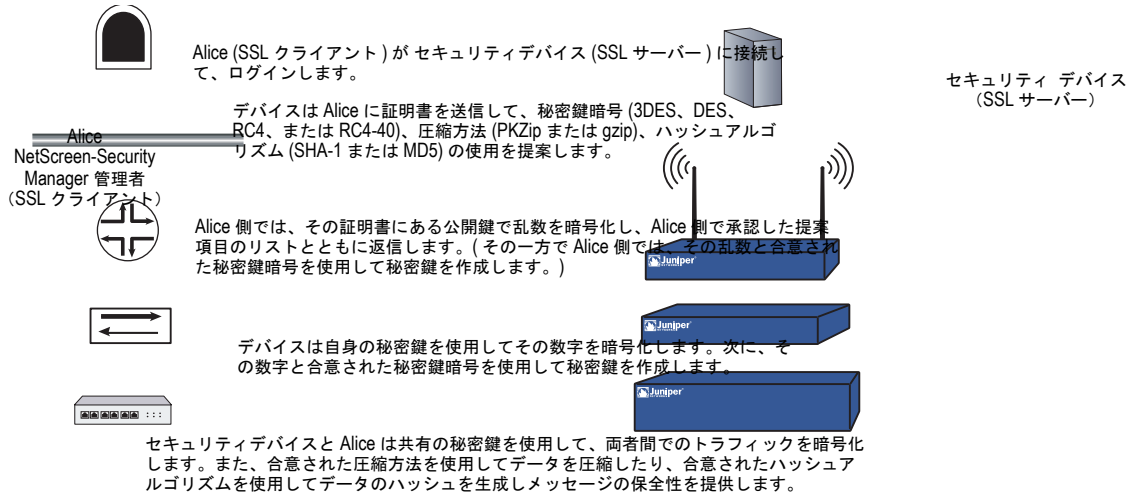
セキュアソケットレイヤー

SSL（セキュア ソケット レイヤー）は、TCP/IP ネットワークで通信する、Web クライアントと Web サーバーの間のセキュアな接続を提供するプロトコルのセットです。SSL は、サーバーとクライアントが互いを認証して、暗号化方式をネゴシエートできるようにする SSLHP (SSL ハンドシェイクプロトコル) および HTTP のような上位レベルのプロトコルに対して、基本セキュリティサービスを提供する SSLRP (SSL レコードプロトコル) によって構成されます。これらの 2 つのプロトコルは、以下の OSI（開放型システム間相互接続）モデルにおける 2 つのレイヤーで動作します。

- アプリケーション レイヤー（レイヤー 7）における SSLHP
- プレゼンテーション レイヤー（レイヤー 6）における SSLRP

SSL はアプリケーションプロトコルから独立して、セキュアサービスを提供するために TCP を使用します（図 5 を参照）。SSL は証明書を使用して、まずサーバーのみかサーバーとクライアントの両方を認証した後に、セッションの間に送信されるトラフィックを暗号化します。ScreenOS は、サーバー（セキュリティデバイス）の認証のみをサポートし、クライアント（SSL を介してセキュリティデバイスに接続する管理者）の認証はサポートしません。

図 5: SSL クライアントからサーバー



Juniper Networks セキュリティ デバイスは、HTTP（デフォルトのポートは 80）を使用した管理トラフィックを SSL（デフォルトのポートは 443）へ転送します。SSL のデフォルト証明書は、自動的に作成される自己署名証明書ですが、必要に応じて後で異なる証明書を使用できます。SSL が PKI 鍵 / 証明書管理と統合されているため、SSL 証明書をリスト中の証明書から選択することができます。また、IPSec VPN についても同じ証明書を使用することもできます。

注 : HTTP 管理トラフィックを SSL に転送する詳細については、8 ページの「HTTP を SSL に転送する」を参照してください。自己署名証明書については、**5**-36 ページの「自己署名証明書」を参照してください。証明書の入手方法に関しては、**5**-24 ページの「証明書および CRL」を参照してください。

SSL の ScreenOS 実装によって、以下の機能、互換性、保全性が提供されます。

- SSL サーバー認証（SSL のサーバーとクライアント認証ではありません）。つまり、セキュリティ デバイスは SSL を介して接続する管理者に対して自身を認証することはできますが、その管理者は SSL を使用してデバイスに対して自身を認証することはできません。
- SSL バージョン 3 互換性 (バージョン 2 とは互換性はありません)
- Netscape Communicator 4.7x 以降および Internet Explorer 5.x 以降との互換性
- PKI（公開鍵インフラストラクチャ）鍵管理の統合（19 ページの「公開鍵暗号化」を参照。）
- SSL に対する以下の暗号化アルゴリズムをサポートします。
  - 40 ビット鍵の RC4-40
  - 128 ビット鍵の RC4
  - DES: 56 ビット鍵のデータ暗号化標準化規格
  - 3DES: 168 ビット鍵のトリプル DES
- SSL に対して VPN の場合と同じ以下の認証アルゴリズムをサポートします。
  - 128 ビット鍵の MD5 (メッセージダイジェストバージョン 5)
  - 160 ビット鍵の SHA-1 (セキュアハッシュアルゴリズムバージョン 1)

注： RC4 アルゴリズムは常に MD5 と、DES および 3DES は SHA-1 とペアになります。

SSL の構成

SSL を設定する基本手順は以下のとおりです。

1. 最初の起動中にセキュリティ デバイスが自動的に作成する自己署名証明書を使用する方法、別の自己署名証明書を作成する方法、CA 署名証明書を取得してデバイスにロードする方法のいずれかを行います。

注 : 許可される暗号強度およびブラウザがサポートする暗号を確認するためブラウザをチェックしてください（セキュリティ デバイスとブラウザはともに、SSL に使用する暗号と同じ種類とサイズの暗号をサポートする必要があります)。Internet Explorer 5x の場合は、**Help**、**About Internet Explorer** の順にクリックし、「暗号強度」の箇所で確認します。高度暗号化パックを入手するには、**Update Information** をクリックしてください。Netscape Communicator の場合は、**Help**、**About Communicator** を順にクリックして、RSA の項目で確認します。SSL 構成の設定を変更するには、**Security Info**、**Navigator**、**Configure SSL v3** の順にクリックしてください。

詳細情報は、**5**-36 ページの「自己署名証明書」を参照してください。証明書の要求とロードに関する詳細については、**5**-24 ページの「証明書および CRL」を参照してください。

2. SSL 管理を使用可能にします。

注 : SSL はデフォルトでは使用可能になっています。

WebUI

Configuration > Admin > Management: 以下を入力して **Apply** をクリックします。

SSL: (選択)
Port: デフォルトのポート番号 (443) を使用するか、別の番号に変更します。
Certificate: 使用する証明書をドロップダウンリストから選択します。
Cipher: 使用する暗号をドロップダウンリストから選択します。

注 : SSL ポート番号を変更する場合、管理者側ではブラウザで URL を入力する際にデフォルト以外の番号を指定する必要があります。

CLI

```
set ssl port num
set ssl cert id_num
set ssl encrypt { { 3des | des } sha-1 | { rc4 | rc4-40 } | md5 }
set ssl enable
save
```

注 : 証明書の ID 番号を知るには、以下のコマンドを入力します。
get pki x509 list cert.

3. セキュリティ デバイスの管理に使用しているインターフェースで、SSL 管理を許可するように構成します。

WebUI

Network > Interfaces > Edit (管理するインターフェースについて): SSL 管理サービスのチェックボックスを選択し、**OK** をクリックします。

CLI

set interface *interface* manage ssl
save

4. SSL ポートを介して、セキュリティ デバイスに接続します。つまり、表示されるセキュリティデバイスの管理用の IP アドレスをブラウザの URL フィールドに入力するときには、「**http**」を「**https**」に変更し、IP アドレスに続いて、コロンと HTTPS（SSL）ポート番号（ポート番号をデフォルトから変更した場合）を入力します（例えば、次のように表示されます。

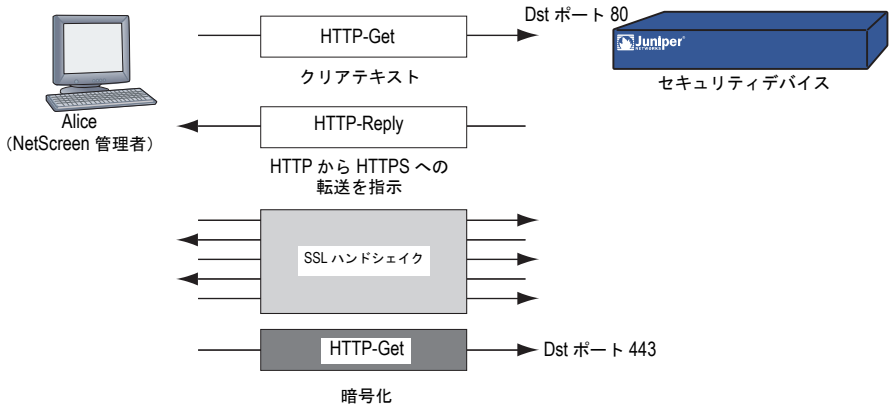
   https://123.45.67.89:1443.

HTTP を SSL に転送する

セキュリティ デバイスは、HTTP（デフォルトのポートは 80）を使用した管理トラフィックを SSL（デフォルトのポートは 443）へ転送できます（図 6 を参照）。

セキュリティデバイスは、SSL ハンドシェイク処理中に Alice にデバイスの証明書を送信します。Alice 側では、その証明書にある公開鍵で乱数を暗号化し、デバイスに返信します。バイスは自身の秘密鍵を使用してその数字を暗号化します。双方の参加者は、共有の乱数とネゴシエートされた秘密鍵暗号 (3DES、DES、RC4、または RC4-40) を使用して、共有秘密鍵を作成します。共有秘密鍵は、両者間でのトラフィック暗号化に使用されます。また、合意された圧縮方法 (PKZip または gzip) を使用してデータを圧縮したり、合意されたハッシュアルゴリズム (SHA-1 または MD5) を使用してデータのハッシュを生成しメッセージの保全性を提供します。

図 6: HTTP を SSL に転送する



リダイレクトを使用可能にして、デフォルトで自動作成されている SSL の自己署名証明書を使用するには、次のいずれかを実行します。

WebUI

Configuration > Admin > Management: 以下を入力して **Apply** をクリックします。

Redirect HTTP to HTTPS: (選択)
Certificate: Default – System Self-Signed Cert

CLI

set admin http redirect
save

注 : デフォルトでは、セキュリティ デバイスが SSL を適用した自己署名証明書を自動作成するため、CLI コマンドは入力する必要はありません。別の SSL 証明書がすでに割り当てられておりデフォルトの証明書を代わりに使用することになった場合には、すでに割り当てている証明書の割り当てを解除する必要があります。その際にはコマンド **unset ssl cert** *id_num* を使用します。ここで、*id_num* は前に割り当てられた証明書の ID 番号です。

HTTP では SSL で提供されるセキュリティは提供されませんが、セキュリティ デバイスを設定して HTTP トラフィックのリダイレクトを止めることができます。HTTP から SSL へのリダイレクトを使用不可にするには、Redirect HTTP to HTTPS オプション（WebUI）をオフにするか、**unset admin http redirect** コマンド（CLI）を入力します。

コマンドラインインターフェースからの管理

上級の管理者は、CLI（コマンドラインインターフェース）を使用することによって、さらに詳細な管理を行うことができます。CLI を使用してセキュリティ デバイスを構成する場合は、VT100 端末をエミュレートする任意のソフトウェアが使用できます。端末エミュレータでは、セキュリティ デバイスを、Windows、UNIX、Macintosh のオペレーティング システムのコンソールから構成することができます。CLI からのリモート管理には、Telnet もしくは SSH (セキュアシェル) を使うことができます。コンソール ポートからの直接接続には、HyperTerminal が使用できます。

注 : すべての ScreenOS CLI コマンドの一覧については、*ScreenOS CLI Reference Guide: IPv4 Command Descriptions* を参照してください。

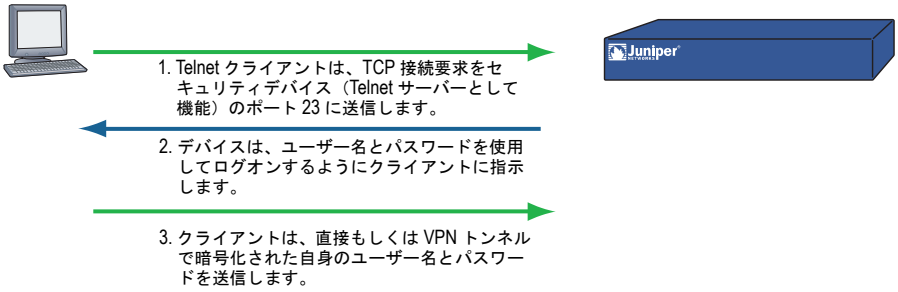
Telnet

Telnet は、TCP/IP ネットワーク上のネットワークデバイスを接続し、リモートで構成するためにクライアント / サーバーの関係を使うログインおよびターミナル エミュレーションプロトコルです。管理者は、管理ワークステーション上で Telnet クライアント プログラムを起動し、セキュリティ デバイス上の Telnet サーバー プログラムへの接続を行います。ログオンすると、管理者はセキュリティ デバイス上の Telnet プログラムに送られる CLI コマンドを発行し、直接接続により操作しているかのように効率的にデバイスを構成できます。セキュリティデバイスを管理するために Telnet を使用するには、以下のアプリケーションおよび接続が必要となります。

- 管理者ワークステーション上の Telnet ソフトウェア
- セキュリティ デバイスへのイーサネット接続

図 7 は、Telnet 接続を確立するための設定手順を表しています。

図 7: Telnet 接続の確立



非認証ユーザーがデバイスにログインする可能性を最小限にするために、ログイン試行での失敗を許可する回数を制限し、その回数を超えるとセキュリティ デバイスが Telnet セッションを終了するように設定することもできます。またこの制限によって、自動ディクショナリ攻撃などの特定タイプの攻撃から保護することもできます。

デフォルトでは、デバイスはログイン試行の失敗を 3 回まで許可し、それまでは Telnet セッションを終了させません。この回数を変更するには、以下のコマンドを入力します。

set admin access attempts *number*

注： この制限を設定するには、CLI を使用する必要があります。

Telnet 接続を保護する

Telnet トラフィックは、ネットワークユーザートラフィックから完全に切り離すことによって保護できます。セキュリティ デバイス モデルによっては、MGT インターフェースからすべての管理トラフィックを実行できるものや、インターフェース（DMZ など）を管理トラフィック専用にできるものもあります。

さらに、管理ユーザーが Telnet を介してセキュリティデバイスを管理する際に、保護された接続を使用することを保証するために、そうしたユーザーが VPN（仮想プライベートネットワーク）トンネルを経由しないと Telnet を利用できないように強制することもできます。この制限を設定すると、VPN トンネルを介さずに Telnet を利用しようとしても、デバイスによってアクセスが拒否されます。

注： VPN トンネルに関しては、*第 5 部: 仮想プライベート ネットワーク* を参照してください。

VPN を介して Telnet アクセスを制限するには、以下のコマンドを入力します。

```
set admin telnet access tunnel
```

注： この制限を設定するには、CLI を使用する必要があります。

セキュアシェル

Juniper Networks セキュリティデバイスに組み込まれた SSH（セキュアシェル）サーバーは、管理者がデバイスを SSH 対応のアプリケーションを利用してセキュアにリモートで管理できる方法を提供します。SSH で、安全にコマンドシェルをリモートで開いてコマンドを実行することができます。SSH は、IP または DNS スプーフィング攻撃、およびパスワードやデータの傍受を防ぎます。

デバイス上で、SSHv1（SSH バージョン 1）または SSHv2（SSH バージョン 2）サーバーのいずれかを選択して実行できます。SSHv2 は SSHv1 よりもよりセキュアであるとされており、現在では IETF 規格として開発されています。しかし、SSHv1 は広範囲に配備され、一般的に使用されています。SSHv1 と SSHv2 は互いに互換性がないことに注意が必要です。つまり、SSHv1 クライアントを使用してセキュリティ デバイス上の SSHv2 サーバーへは接続できず、またその逆方向の接続もできません。クライアントコンソールまたは端末アプリケーションでは、サーバーと同じ SSH バージョンを実行することが必要です。図 8 は、SSH トラフィック フローを表しています。

図 8: SSH トラフィック フロー

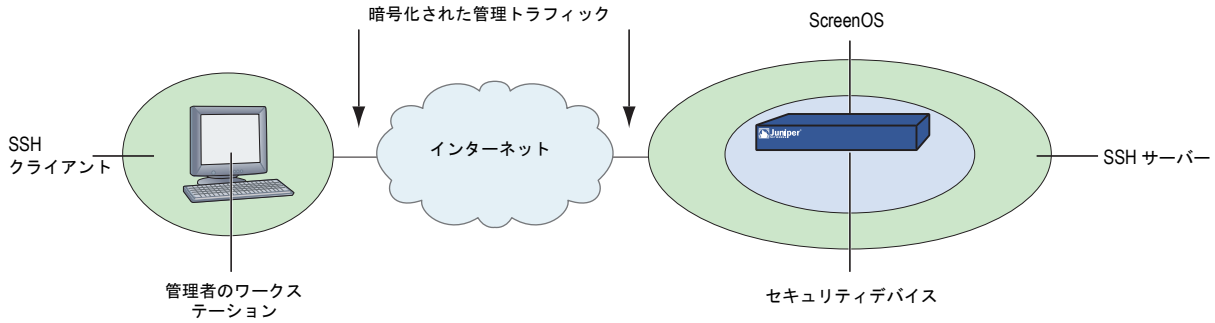
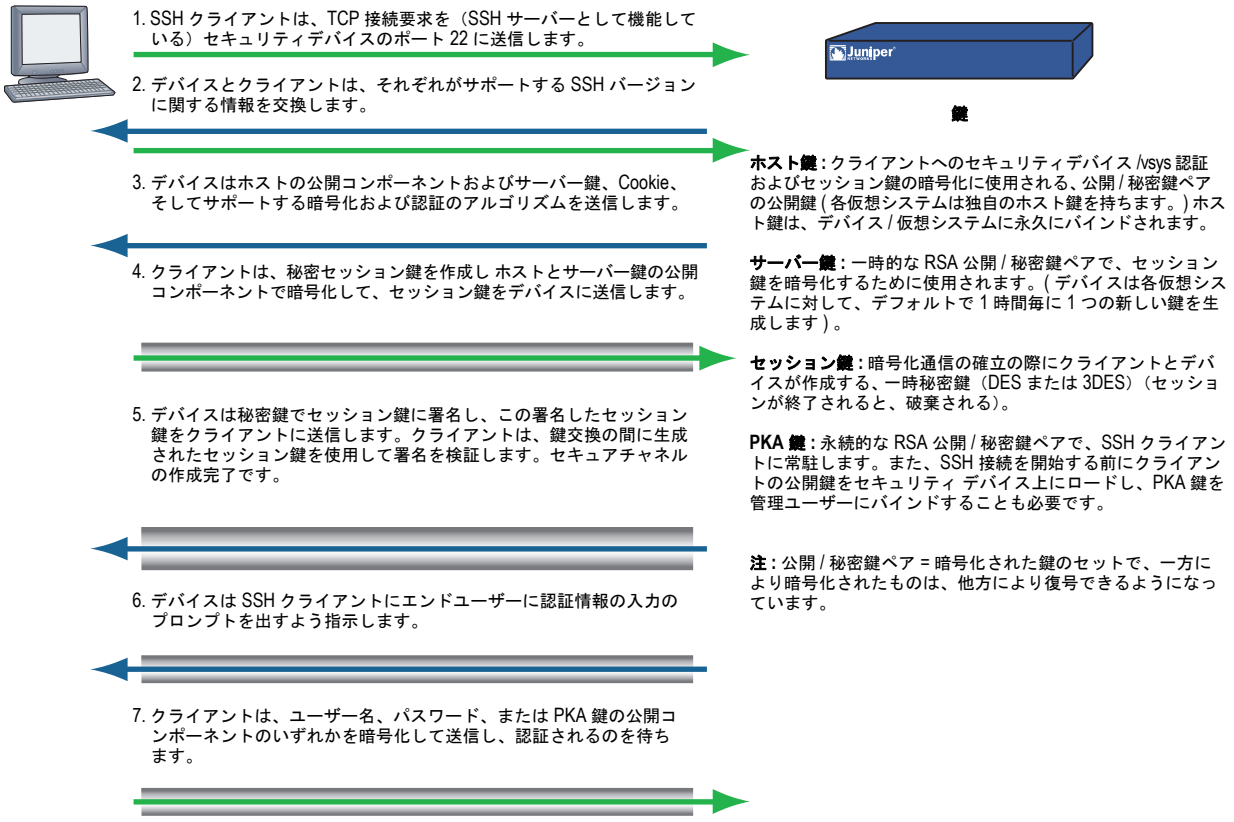


図 9 は、基本的な SSH 接続手順を表しています。

図 9: SSH 接続



1 回につき最大で 5 つの SSH セッションが、Juniper Networks セキュリティ デバイスに許可されます。

クライアント要件

11 ページの「セキュアシェル」、で説明したように、クライアントアプリケーションはセキュリティ デバイス上のサーバーと同じ SSH バージョンを実行する必要があります。SSHv2 クライアントは、公開鍵デバイス認証に対して、Diffie-Hellman の鍵交換アルゴリズムおよびデジタル署名アルゴリズム (DSA) を要求するように構成する必要があります。SSHv1 クライアントは、公開鍵デバイス認証に対して RSA を要求するように構成する必要があります。

デバイス上の基本的な SSH 構成

Juniper Networks セキュリティ デバイス上で SSH を構成する基本的な手順を以下に説明します。

1. SSH に対してパスワードまたは公開鍵認証 (PKA) を使用するかどうかを決定します。PKA を使用する場合は、PKA 鍵を管理にバインドしないと SSH 接続は確立できません。パスワードまたは PKA の使用の詳細については、14 ページの「認証」を参照してください。

2. セキュリティ デバイスを使用可能にするために、どのバージョンの SSH が必要かを確認します。(クライアント アプリケーションおよびデバイスの SSH サーバーは、同じ SSH バージョンを実行する必要があることに注意が必要です。) 以前の ScreenOS バージョンでデバイスの SSH を使用可能にした場合は、ここで SSH を使用可能にすると SSHv1 が起動します。アクティブでありながらデバイス上で使用可能でない SSH のバージョンを調べるには、CLI **get ssh** コマンドを入力します。

   ```
   device> get ssh
   SSH V1 is active
   SSH is not enabled
   SSH is not ready for connections
   Maximum sessions: 8
   Active sessions: 0
   ```

   前述の出力では、SSHv1 はアクティブで、SSH を使用可能にすると動作します。他の SSH バージョンを使用する場合は、以前のバージョンで作成されたすべての鍵が削除されることを確認してください。たとえば、SSHv1 鍵を消去して SSHv2 を使用するには、以下の CLI コマンドを入力します。

   ```
   device> delete ssh device all
   ```

   以下のメッセージが表示されます。

   ```
   SSH disabled for vsys: 1
   PKA key deleted from device: 0
   PKA key deleted from device: 1
   Execute the "Set ssh version v2" command to activate SSH v2 for the device
   ```

   SSHv2 を使用するには、以下の CLI コマンドを入力します。

   ```
   device-> set ssh version v2
   ```

注 : SSH バージョンを設定しても、セキュリティ デバイス上の SSH は使用可能になりません。

3. SSH クライアント接続にポート 22 (デフォルトのポート) を使用するのを避ける場合は、ート番号を 1024 から 32767 の間で指定できます。

注 : WebUI を使用してポート番号を変更し、Configuration > Admin > Management ページで SSHv2 および SCP を使用可能にすることもできます。

```
device-> set admin ssh port 1024
```

4. ルートシステムまたは仮想システムに対して SSH を使用可能にします。仮想システム毎に SSH を使用可能にし使用する方法についての詳しい内容は、16 ページの「SSH と Vsys」を参照してください。

   ルートシステムに対して SSH を使用可能にします。

   ```
   device-> set ssh enable
   ```

   仮想システムに対して SSH を使用可能にするには、まず仮想システムを入力してから SSH を使用可能にします。

   ```
   device-> set vsys v1
   device(v1)-> set ssh enable
   ```

5. SSH クライアントの接続を行うインターフェースで SSH を使用可能にします。

   ```
   device-> set interface manage ssh
   ```

6. セキュリティ デバイスで生成されたホスト鍵を SSH クライアントへ配送します。詳細は 16 ページの「ホスト鍵」を参照してください。

認証

管理者は、以下の 2 つの認証方式のいずれかを使用して、Juniper Networks セキュリティ デバイスに SSH で接続できます。

- **パスワード認証 :** この方法は､セキュリティ デバイスを構成もしくは監視する必要がある管理者が使用します。SSH クライアントは、デバイスへの SSH 接続を開始します。SCS 管理容易性が接続要求を受け取るインターフェースで使用可能になっている場合は、デバイスは、SSH クライアントに合図を送り、ユーザーにユーザー名とパスワードの入力のプロンプトを出すよう指示します。SSH クライアントがこの情報を受け取ると、デバイスに送信します。そしてデバイスは、この情報と管理ユーザーのアカウントにあるユーザー名およびパスワードを比較します。それらが一致すれば、デバイスはユーザーを認証します。一致しなければ、デバイスは接続要求を拒否します。

- **公開鍵認証 (PKA):** この方法によって、パスワード認証方法のセキュリティが強化され、自動化スクリプトを実行することができます。基本的に SSH クライアントは、ユーザー名とパスワードの代わりに、ユーザー名と公開 / 秘密鍵ペアの公開鍵の構成要素を送信します。デバイスは、その公開鍵の構成要素と管理者にバインドできる 4 つの公開鍵を比較します。1 組の鍵が一致すれば、デバイスはユーザーを認証します。一致する鍵の組み合わせがなければ、デバイスは接続要求を拒否します。

注 : 認証アルゴリズムは、SSHv1 に対しては RSA、SSHv2 に対しては DSA がサポートされています。

どちらの認証方法でも、SSH クライアントがログオンする前に、セキュアな接続を確立することが必要です。SSH クライアントがデバイスで SSH 接続を確立した後で、クライアントはユーザー名とパスワードか、ユーザー名と公開鍵のいずれかで自身を認証する必要があります。

パスワード認証および PKA の両方は、デバイスの管理ユーザー アカウントを作成すること、および SSH 接続経由でデバイスを管理するインターフェースの SSH の管理容易性を使用可能にすることを必要とします。(管理ユーザーアカウントの作成の詳細については、35 ページの「管理ユーザーの定義」を参照してください)。パスワード認証方法は、SSH クライアントのさらなる設定を必要としません。

一方、PKA の準備には、まず以下の作業を行う必要があります。

1. SSH クライアントで、鍵生成プログラムを使用して公開および秘密鍵ペアを生成します。(鍵ペアは、SSHv1 に対しては RSA、SSHv2 に対しては DSA のいずれかです。詳細については、SSH クライアントアプリケーションのドキュメントを参照してください)。

注 : PKA を自動ログインのために、SSH クライアントにエージェントもロードして、PKA 公開 / 秘密鍵ペアの秘密鍵コンポーネントを復号し、復号化したバージョンの秘密鍵をメモリーに記憶させておく必要があります。

---

2. 公開鍵を、ローカルの SSH ディレクトリから TFTP サーバーに移動して、TFTP プログラムを起動します。

注 : 公開鍵ファイルの内容を、CLI コマンドの **set ssh pka-rsa** [**username** *name_str*] **key** *key_str*（SSHv1 の場合）、または **set ssh pka-dsa** [**user-name** *name_str*] **key** *key_str*（SSHv2 の場合）に直接貼り付けることもできます。貼り付ける場所は、変数 *key_str* で示される箇所、または WebUI の Key フィールドの中です（Configuration > Admin > Administrators > SSH PKA）。ただし、CLI および WebUI にはサイズ制限があり、公開鍵サイズは 512 ビットを超えることはできません。TFTP を介して鍵をロードする場合は、この制限はありません。

---

3. CLI を介して構成を行えるように、デバイスにログオンします。

4. TFTP サーバーからデバイスへ公開鍵をロードするために、以下の CLI コマンドのいずれか 1 つを入力します。

   SSHv1 の場合 :

   exec ssh tftp pka-rsa [**username** *name*] **file-name** *name_str* **ip-addr** *tftp_ip_addr*

   SSHv2 の場合 :

   exec ssh tftp pka-dsa [**user-name** *name*] **file-name** *name_str* **ip-addr** *tftp_ip_addr*

   username または **user-name** オプションは、ルート管理者が RSA 鍵を別の管理に関連付けることができるように、ルート管理者のみが使用可能です。ルート管理者もしくは読取 / 書込管理者として、ユーザー名なしでコマンドを入力する場合には、デバイスは、鍵をユーザー自身の管理アカウントに関連付けます。つまり鍵はコマンドを入力する管理者にバインドされます。

注： セキュリティ デバイスは、各管理ユーザーに対して最大で 4 つの PKA 公開鍵をサポートします。

管理者が SSH 管理容易性が使用可能になっているインターフェースで SSH を介してログオンを試みた場合、デバイスは、まず公開鍵がその管理者にバインドされているかどうかをチェックします。その場合、デバイスは PKA を使用して管理者を認証します。公開鍵が管理者にバインドされていない場合、デバイスは、ユーザー名とパスワード入力のプロンプトを出します。(**set admin ssh password disable username** *name_str* コマンドを使用すると、管理者に PKA 方式のみを強制することができます。) 管理者が使う認証方法にかかわらず、自身のアカウントを最初に定義する時点では、パスワードを含めなければなりません。これは、後でこのユーザーに公開鍵をバインドするときに、パスワードが必要なくなる場合であっても必要です。

SSH と Vsys

仮想システムをサポートするセキュリティ デバイスに対しては、仮想システム毎に SSH を使用可能にして構成できます。各仮想システムは独自のホスト鍵（16 ページの「ホスト鍵」）を持ち、システムの管理の PKA 鍵を維持して管理します。

SSH セッションの最大数は、2 ～ 24 の間で、プラットフォームによって大きく異なる制限であることに注意が必要です。最大数の SSH クライアントが既にデバイスにログインしている場合は、他の SSH クライアントは SSH サーバーにログインできません。ルートシステムと仮想システムは、同じ SSH ポート番号を共有します。つまり、SSH ポートをデフォルトのポート 22 から変更すると、すべての仮想システムに対しても同様にポートが変更されます。

注： ひとつのデバイスに多くの仮想システムを実装する際、多くの、あるいはすべての vsys 管理者が SSH を使用している場合、PKI オブジェクトに予約されている容量がいっぱいになってしまうことがあります。

ホスト鍵

ホスト鍵によって、セキュリティ デバイスは SSH クライアントに対して自身を識別します。仮想システム（vsys）をサポートするデバイスでは、各仮想システムは独自のホスト鍵を持ちます。SSH が最初に仮想システム（仮想システムをサポートするデバイスに対する）またはデバイスで使用可能にされると、仮想システムまたはデバイスに固有のホスト鍵が生成されます。このホスト鍵は永続的に仮想システムまたはデバイスにバインドされ、SSH が使用可能にされた後に再度使用可能にされた場合も、同じホスト鍵が使用されます。

デバイスのホスト鍵は、以下の 2 つの方法のいずれかによって、SSH クライアントへ配信される必要があります。

- 手動 - ルートまたは vsys 管理者がホスト鍵をクライアント管理ユーザーへ、電子メール、電話などで送付します。受信した管理者は、ホスト鍵を適切な SSH クライアント システム の SSH ファイルに格納します (ファイルの保存場所とフォーマットは、SSH クライアントアプリケーションが決定します) 。
- 自動 - SSH クライアントがデバイスに接続すると、SSH サーバーはホスト鍵の暗合化されていない公開コンポーネントをクライアントに送信します。SSH クライアントはローカル ホスト鍵を検索し、受信したホスト鍵がデバ

イスのアドレスへマッピングされているかどうか確認します。ホスト鍵が未知の（クライアントのホスト鍵データベースにデバイス アドレスへのマッピングが存在しない）場合でも、管理ユーザーはホスト鍵を承認するかどうか決定できることがあります。そうでない場合、接続は終了します。(未知のホスト鍵の承認に関しては、該当する SSH クライアントのドキュメントを参照してください。)

SSH クライアントが正しいホスト鍵を受信したことを確認するために、クライアントシステムの管理ユーザーは、受信したホスト鍵の SHA ハッシュを生成できます。その後に、クライアント管理ユーザーは、この SHA ハッシュとデバイスのホスト鍵の SHA ハッシュとを比較できます。デバイス上では、CLI コマンド **get ssh host-key** を実行することにより、ホスト鍵の SHA ハッシュを表示させることができます。

例 : SSHv1 で PKA を使用して自動ログインする

この例では、ルート管理者は、自動スクリプトを実行するリモートホストに対して、SSHv1 公開キー認証 (PKA) を設定します。このリモート ホストがデバイスにアクセスする唯一の目的は、構成ファイルを毎晩ダウンロードするためです。認証が自動化されているため、SSH クライアントがデバイスにログオンする際に、人が関与する必要はありません。

cfg という管理ユーザー アカウントを定義し、パスワード **cfg** および読取 / 書込特権を与えます。Untrust ゾーンにバインドするインターフェース ethernet1 の SCS 管理容易性を使用可能にします。

すでに、RSA 公開 / 秘密鍵ペアを生成するために、SSH クライアントの鍵生成プログラムを利用し、公開鍵ファイル（ファイル名“idnt_cfg.pub”）を TFTP サーバーのディレクトリに移動し、TFTP プログラムを起動しているとします。TFTP サーバーの IP アドレスは 10.1.1.5 です。

WebUI

Configuration > Admin > Administrators > New: 次のように入力してから **OK** をクリックします。

Name: cfg
New Password: cfg
Confirm Password: cfg
Privileges: Read-Write (**選択**)
SSH Password Authentication: (**選択**)

Network > Interfaces > Edit (ethernet1): Service Options で **SSH** を選択してから、**OK** をクリックします。

注 : TFTP サーバーからは **exec ssh** コマンドを介して、SSH の公開鍵ファイルをロードするしかできません。

CLI

```
set admin user cfg password cfg privilege all
set interface ethernet1 manage ssh
exec ssh tftp pka-rsa username cfg file-name idnt_cfg.pub ip-addr 10.1.1.5
save
```

セキュアコピー

SCP（セキュア コピー）によって、リモート クライアントは SSH プロトコルを使用して セキュリティ デバイスとファイルを受け渡しができるようになります。(SSH プロトコルは、SCP 接続における認証、暗号化、およびデータ保全性の確保を可能にします。) デバイスは SCP サーバーとして機能し、リモート ホストの SCP クライアントからの接続を承認します。

SCP を利用するには、ファイル転送が始まる前にリモートクライアントが認証されることが必要です。SCP 認証は、SSH クライアントの認証に使用するのと全く同じ方法です。SCP クライアントは、パスワードまたは PKA 鍵のいずれかを使用して認証を受けることができます。SCP クライアントが認証されると、1 つまたは複数のファイルがデバイスへ、そしてデバイスから転送できます。SCP クライアントアプリケーションは、コピー元ファイル名およびコピー先ファイル名を指定する的確な方法を決定します (SCP クライアントアプリケーションのドキュメントを参照してください)。

SCP はデバイス上でデフォルトで使用不能になっています。SCP を使用可能にするには、SSH も同時に使用可能にする必要あります。

WebUI

Configuration > Admin > Management: 以下を選択して **Apply** をクリックします。

Enable SSH: (選択)
Enable SCP: (選択)

CLI

```
set ssh enable
set scp enable
save
```

以下の例は、構成ファイルをデバイス（管理者名は “juniper” で IP アドレスは 10.1.1.1）のフラッシュメモリーからクライアントシステムのファイル “ns_sys_config_backup” にコピーする SCP クライアントコマンドです。

```
scp juniper@10.1.1.1: ns_sys_config ns_sys_config_backup
```

ScreenOS イメージをデバイスにコピーしたり、デバイスからコピーしたりすることもできます。管理者のログイン名が “juniper” で、デバイスの IP アドレスが 10.1.1.1 とすると、“ns.5.1.0r1” という名前のイメージを SCP クライアントからデバイスに保存するには、次のコマンドを入力します。

```
scp ns.5.1.0r1 juniper@10.1.1.1: image
```

次に、**reset** コマンドを入力すると、セキュリティ デバイスを再起動して新規 ScreenOS イメージを実行します。

ScreenOS イメージをデバイスから SCP クライアントにコピーして保存したイメージに “current_image_backup” という名前を付けるには、次の SCP クライアントコマンドを入力します。

```
scp juniper@10.1.1.1: image current_image_backup
```

管理者名、デバイス IP アドレス、コピー元ファイル、およびコピー先ファイルを指定する方法については、SCP クライアントアプリケーションのドキュメントで確認する必要があります。

シリアルコンソール

コンソールポートを経由する管理者のワークステーションからセキュリティデバイスへの直接シリアル接続により、セキュリティデバイスを管理できます。直接接続は常に可能であるとは限りませんが、セキュリティ デバイスが安全な場所にある場合は、これが最も安全なデバイスの管理方法です。

注 : 認証されていないユーザーがルート管理者としてリモートでログインするのを防ぐために、ルート管理者がコンソールを介さないとデバイスにログインできないように強制することもできます。この制限についてのさらに詳しい内容は、42 ページの「ルート管理者をコンソールアクセスに制限する」を参照してください。

シリアル接続を行うには、Juniper Networks セキュリティ デバイス モデルに応じて、以下のケーブルのいずれか 1 つが必要となります。

- DB-9 メス - DB-25 オス ストレートシリアルケーブル
- DB-9 メス - DB-9 オス ストレートシリアルケーブル
- DB-9 メス - MiniDIN-8 オス シリアルケーブル
- DB-9 メス - RJ-45 〜 RJ-45 ストレート イーサネット ケーブルを備えた RJ-45 アダプタ

管理ワークステーションには、HyperTerminal ソフトウェア（もしくは、別の VT100 端末エミュレータ）が必要で、その HyperTerminal のポート設定は以下のように構成されます。

- シリアル通信 9600 bps
- 8 ビット
- パリティーなし
- ストップビット 1
- フローコントロールなし

注 : HyperTerminal を使用する際の詳細については、*ScreenOS CLI Reference Guide IPv4: IPv4 Command Descriptions* またはデバイスのドキュメントを参照してください。

リモートコンソール

ダイヤルすることにより、セキュリティデバイス上のコンソールインターフェースにリモートでアクセスできます。コンソールへダイヤルするには、以下の 2 つの方法があります。

- V.92 モデムポートを使用するリモートコンソール
- AUX ポートを使用するリモートコンソール

V.92 モデムポートを使用するリモートコンソール

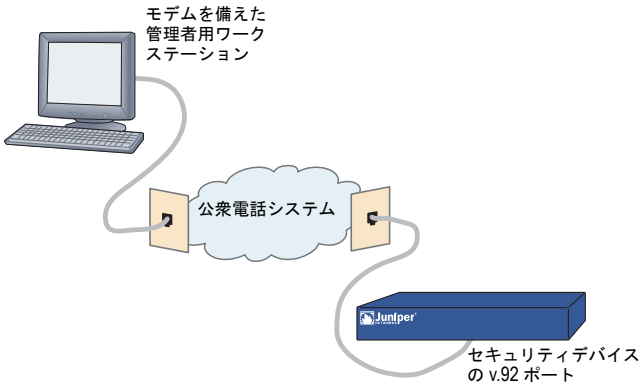
ポートへダイヤルしコンソールインターフェースへアクセスすることにより、v.92 モデムポートを備えたセキュリティデバイスをリモートで管理できます。リモートコンソールを使用するには、電話回線にデバイスの v.92 モデムポートを接続し、モデムを備えたリモートのコンピュータを使用して、デバイスにダイヤルします。コンソールセッションを確立するには、HyperTerminal のようなターミナルプログラムを使用します。

リモートコンソール接続を使用するには、最初に次の CLI コマンドでリモート管理を有効にしなければなりません。

```
set interface serialx/0 modem aux enable
save
```

図 10 は、リモートコンソール管理のためデバイスを接続する方法を示します。

図 10: リモートコンソール管理の接続



管理ワークステーションには、HyperTerminal ソフトウェア（もしくは、別の VT100 端末エミュレータ）が必要で、その HyperTerminal のポート設定は以下のように構成されます。

- シリアル通信 9600 bps
- 8 ビット
- パリティーなし
- ストップビット 1
- フローコントロールなし

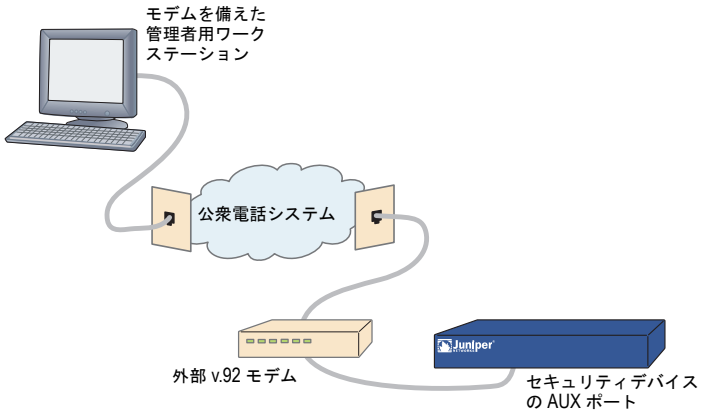
注 : HyperTerminal を使用する際の詳細については、*ScreenOS CLI Reference Guide IPv4: IPv4 Command Descriptions* またはデバイスのドキュメントを参照してください。

AUX ポートを使用するリモートコンソール

ポートに接続されたモデムへダイヤルしコンソールインターフェースへアクセスすることにより、AUX ポートを備えたセキュリティデバイスをリモートで管理できます。リモートコンソールを使用するには、外部モデムを使用して、電話回線にデバイスの AUX ポートを接続し、モデムを備えたリモートのコンピュータを使用して、デバイスにダイヤルします。コンソールセッションを確立するには、HyperTerminal のようなターミナルプログラムを使用します。

図 10 は、リモートコンソール管理のためデバイスを接続する方法を示します。

図 11: リモートコンソール管理の接続



管理ワークステーションには、HyperTerminal ソフトウェア（もしくは、別の VT100 端末エミュレータ）が必要で、その HyperTerminal のポート設定は以下のように構成されます。

- シリアル通信 9600 bps
- 8 ビット
- パリティーなし
- ストップビット 1
- フローコントロールなし

注 : HyperTerminal を使用する際の詳細については、*ScreenOS CLI Reference Guide IPv4: IPv4 Command Descriptions* またはデバイスのドキュメントを参照してください。

モデムポート

管理者のワークステーションをデバイスのモデム ポートに接続することによって、セキュリティ デバイスを管理することもできます。モデムポートはコンソールポートと同じように機能しますが、モデムポートのパラメータを指定できない点や、この接続を画像のアップロードに使用できない点が異なります。

認証されていないユーザーが、コンソールまたはモデムポートへの直接接続を介してデバイスを管理するのを防ぐために、以下のコマンドを入力して両方のポートを使用不可能にすることができます。

```
set console disable
set console aux disable
```

NetScreen-Security Manager からの管理

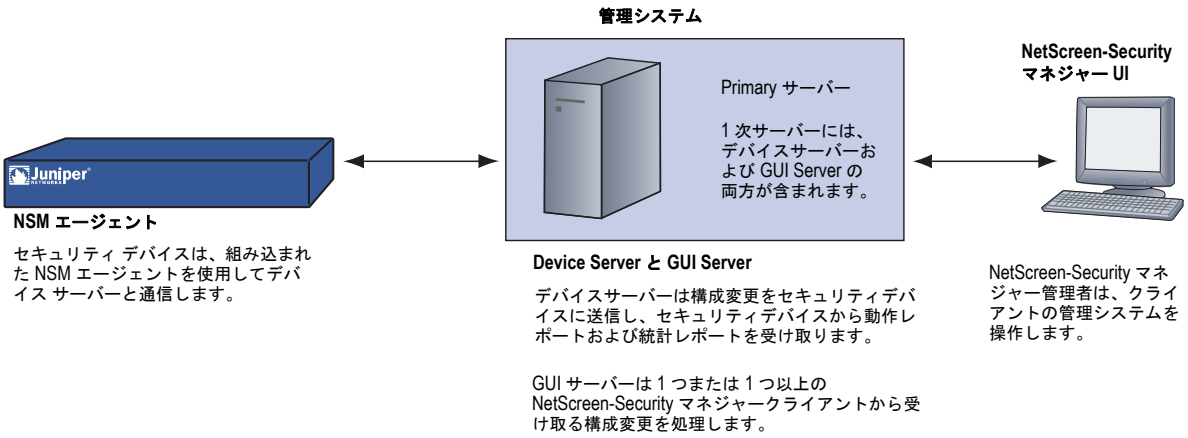
NetScreen-Security Manager は、Juniper Networks の企業向けの管理ソフトウェアアプリケーションです。NetScreen-Security Manager により、複数の Juniper Networks セキュリティデバイスを、LAN（ローカルエリアネットワーク）環境または WAN (ワイドエリアネットワーク) 環境にて構成および監視することができます。NetScreen-Security Manager UI (ユーザー インターフェース) によって、管理者は中央から複数のデバイスを配置、構成、および管理することが可能になります。

NetScreen-Security Manager は 3 つのコンポーネントを使用して、セキュリティデバイスとのリモート通信を可能にします。

- *NetScreen-Security Manager UI (ユーザー インターフェース)* は、NetScreen-Security Manager 管理システムから、ネットワーク上のデータにアクセスしそれらを構成するために使用される Java ベースのソフトウェア アプリケーションです。UI から、ネットワークを参照、構成、および管理できます。
- *管理システム*は外部ホストに存在するサービスのセットです。これらのサービスは、デバイスと NetScreen-Security Manager UI との間で交換されたデバイス管理情報の処理、追跡、および記録を行います。管理システムは 2 つの要素から構成されています。
  - *GUI サーバー* は、UI からの要求やコマンドを受け取り、それらに応答します。また、ネットワークの管理に必要なシステム リソースと構成データを管理します。さらに、管理対象のセキュリティ デバイス、管理者、および構成に関する情報のローカル データ ストアを保持しています。
  - *デバイス サーバー* は、それぞれのネットワーク デバイスによって生成されたすべてのデータの収集点となります。このデータ（主にトラフィック ログ）はローカル データ ストアに格納されます。
  - *NSM エージェント* は、管理される各セキュリティ デバイス上に存在するサービスです。NSM エージェントは外部の管理システムから構成パラメータを受け取って ScreenOS に転送します。NSM エージェントはさらに、各デバイスを監視して管理システムにレポートを伝送します。NSM エージェントを使用すると、セキュリティ デバイスと NetScreen-Security Manager 間で、署名パッケージ、証明書、ライセンスをダウンロードできます。

図 12 は、NetScreen-Security Manager UI がどのように NSM エージェントと通信するかを表しています。

図 12: NSM エージェントが有効なセキュリティデバイス



これらまたはその他の Security Manager コンポーネントの詳細については、*NetScreen-Security Manager 2004 Administrator's Guide* を参照してください。

NSM エージェントと MGT システムの接続の開始

NetScreen-Security Manager がセキュリティ デバイスにアクセスし管理するには、まず NSM エージェント（デバイス上に存在する）と管理システム（外部ホスト上に存在する）との間の通信を開始することが必要です。初期設定を行うには、セキュリティ デバイスの現在の可用性に応じて、異なる 2 つのサイトに最大 2 人のユーザーが必要となることがあります。これらのユーザーには、クライアント ホストで NetScreen-Security Manager UI を使用する NetScreen-Security Manager 管理者、およびコンソール セッションを介してセキュリティ デバイス上で CLI コマンドを実行するオンサイト ユーザーを含めることもできます。初期化を行うケースとして、以下のものが考えられます。

- *ケース 1:* デバイスの IP アドレスが周知で、ネットワークインフラ全体でアクセスができる。

  この場合は、NetScreen-Security Manager 管理者はクライアント ホストで NetScreen-Security Manager UI を使用してデバイスを追加します。(オンサイトユーザーは不要です。) デバイスは自動的に管理システムに再度接続し、そこに存在する NetScreen-Security Manager データベースに構成情報を送信する準備をします。

- *ケース 2:* IP アドレスにアクセスできない。

  この場合は、両方のユーザーが初期化作業を行います。管理者は NetScreen-Security Manager UI を介してデバイスを追加します。また、管理者はオンサイトユーザーに必要な CLI コマンドを特定してユーザーに配信し、以下にユーザーがそのコマンドをコンソールを介して実行します。デバイスは自動的に管理システムに再度接続し、NetScreen-Security Manager データベースに構成情報を送信する準備をします。

- *ケース 3:* デバイスが新しいため、デフォルト設定が残っている。

  この場合は、両方のユーザーが初期化作業を行います。オンサイト ユーザーは、NetScreen-Security Manager 管理者が生成する *Configlet* と呼ばれる暗号化された構成スクリプトを使用できます。その手順は以下のとおりです。

  1. 管理者は、NetScreen-Security Manager UI の Add Device ウィザードを使用して、デバイス プラットフォームおよび ScreenOS バージョンを選択します。
  2. 管理者はデバイスを編集して目的の構成を入力します。
  3. 管理者はデバイスを起動します。
  4. 管理者は、Configlet ファイル (または、ケース 2 と同様に、必要な CLI コマンド) を生成してオンサイトユーザーに配信します。
  5. オンサイトユーザーは Configlet (または CLI コマンド) を実行します。

デバイスの追加の詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。

NSM エージェントを使用可能、使用不可、設定解除する

セキュリティ デバイスが管理システムと通信できるようにするには、まずデバイスに存在する NSM（NetScreen-Management System）エージェントを使用可能にする必要があります。

NetScreen-Security Manager を設定解除するには、**unset nsmgmt all** コマンドを使用します。このコマンドを使用すると、NSM エージェントをデフォルトの初期設定に戻して、NetScreen-Security Manager に接続していない状態となります。NetScreen-Security Manager の設定を再構成する場合に **unset nsmgmt all** コマンドを使用します。

セキュリティ デバイス上の NSM エージェントを使用可能にするには、以下のいずれかを実行します。

WebUI

Configuration > Admin > NSM: **Enable Communication with NetScreen Security Manager (NSM)** を選択して **Apply** をクリックします。

CLI

```
set nsmgt enable
save
```

セキュリティ デバイス上の NSM エージェントを使用不可にするには、以下のいずれかを実行します。

WebUI

Configuration > Admin > NSM: **Enable Communication with NetScreen Security Manager (NSM)** を選択解除して **Apply** をクリックします。

CLI

```
unset nsmgt enable
save
```

管理システムのプライマリ サーバーの IP アドレスの設定

NSM エージェントが外部の管理システム サーバーを識別するのに利用する IP アドレスは、構成可能なパラメータです。

以下の例では、Primary サーバーの IP アドレスを 1.1.1.100 に設定します。

WebUI

Configuration > Admin > NSM: 以下を入力して **Apply** をクリックします。

Primary IP Address/Name: 1.1.1.100

CLI

```
set nsmgmt server primary 1.1.1.100
save
```

アラームおよび統計データ レポートの設定

NSM エージェントはデバイスイベントを監視して管理システムにレポートを伝送します。これによって、NetScreen-Security Manager 管理者は NetScreen-Security Manager UI からイベントを見ることが可能になります。

NSM エージェントが追跡したイベントのカテゴリは以下のようになります。

- *Alarms* は、詳細な検査で検出される攻撃を含めて、危険性のある攻撃やトラフィック異常をレポートします。
- *Log events* はデバイスの構成の変更から、サーバー上で発生する重要度の低い変更までをレポートします。
- *Protocol distribution* イベントは、以下のプロトコルが生成したメッセージをレポートします。
  - 認証ヘッダー (AH)
  - セキュリティペイロードのカプセル化 (ESP)
  - 汎用ルーティングのカプセル化 (GRE)
  - インターネット制御メッセージプロトコル (ICMP)
  - OSPF (オープン最短パスファースト)
  - TCP（伝送制御プロトコル）
  - ユーザーデータグラムプロトコル (UDP)
- *Statistics* メッセージは、以下の統計情報をレポートします。
  - 攻撃統計データ
  - イーサネット統計データ
  - トラフィックフロー統計データ
  - ポリシー統計データ

以下の例では、すべてのアラームおよび統計データメッセージの Management System への伝送を可能にします。

WebUI

Configuration > Admin > NSM: 以下を入力して **Apply** をクリックします。

Attack Statistics: (選択)
Policy Statistics: (選択)
Attack Alarms: (選択)
Traffic Alarms: (選択)
Flow Statistics: (選択)
Ethernet Statistics: (選択)
Deep Inspection Alarms: (選択)
Event Alarms: (選択)

CLI

```
set nsmgmt report statistics attack enable
set nsmgmt report statistics policy enable
set nsmgmt report alarm attack enable
set nsmgmt report alarm traffic enable
set nsmgmt report statistics flow enable
set nsmgmt report statistics ethernet enable
set nsmgmt report alarm idp enable
set nsmgmt report alarm other enable
save
```

構成同期化

ScreenOS の構成が最後に NetScreen-Security Manager で同期化された構成から変更されている場合、セキュリティ デバイス側から NetScreen-Security Manager 管理者に構成の変更を通知します。たとえば、デバイスの管理者がコンソール、Telnet、SSH、または Web UI を使用してセキュリティ デバイスの構成が変更されると、デバイスがメッセージを送信します。NetScreen-Security Manager 以外のアプリケーションで構成を変更すると、構成が非同期になります。NetScreen-Security Manager を正しく動作させるには、NetScreen-Security Manage の構成ファイルはセキュリティ デバイスの構成ファイルと同期する必要があります。NetScreen-Security Manager に構成ファイルをインポートすると、同期化が実行されます。インポートデバイスの詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。

以下の例では、構成状態を表示するために使用するコマンドを説明します。

例 : 構成状態を表示する

以下の例では、セキュリティ デバイスの構成同期化状態を表示します。

WebUI

注 : 実行している構成状態を取得するには、CLI を使用する必要があります。

CLI

```
get config nsmgmt-dirty
```

注 : *NetScreen-Security Manager 以外のアプリケーションが構成ファイルを変更しなかった場合には、コマンドは空白を返します。それ以外の場合は、"Yes" が返されます。*

例 : 構成ハッシュを取得する

NetScreen-Security Manager は構成ハッシュを使用して、セキュリティ デバイスの構成同期化を確認できます。以下の例では、特定の仮想システムについて実行中の構成ハッシュを取得します。

WebUI

注 : 実行している構成ハッシュを取得するには、CLI を使用する必要があります。

CLI

```
device-> enter vsys vsys1
device(vsys1)-> get config hash
a26a16cd6b8ef40dc79d5b2ec9e1ab4f
device(vsys1)->
device(vsys1)-> exit
```

構成タイムスタンプを取得する

セキュリティ デバイスによって、running-config と saved-config の 2 つの構成タイムスタンプが提供されます。running-config タイムスタンプは、各仮想システムについて最後に set または unset のコマンドが実行されたタイムスタンプです。saved-config タイムスタンプは、デバイス構成が最後に保存されたタイムスタンプです。

以下の例では、セキュリティ デバイス側で、仮想システム vsys1 について最後に実行および保存された構成タイムスタンプを取得します。

WebUI

注 : 実行中および保存された構成タイムスタンプを取得するには、CLI を使用する必要があります。

CLI

```
get config timestamp vsys vsys1
get config saved timestamp
```

注 : コマンドから **vsys vsys_name** を省くと、セキュリティ デバイスはルート システムの構成タイムスタンプを取得します。タイムスタンプが使用不可である場合には、“unknown” メッセージが表示されます。

管理トラフィックのコントロール

ScreenOS によって、セキュリティ デバイスの構成と管理のための以下のオプションの利用が可能になります。

- **WebUI:** このオプションを選択することで、インターフェースは、WebUI（Web ユーザー インターフェース）を通じて管理用 HTTP トラフィックを受信できます。
- **Telnet:** インターネットなどの TCP/IP ネットワークの端末エミュレーション プログラム。Telnet はネットワークデバイスをリモートでコントロールする一般的な方法です。このオプションを選択すると、Telnet 管理容易性が使用可能になります。
- **SSH:** SSH（セキュア コマンド シェル）を使用して、イーサネット接続またはダイヤルイン モデムからセキュリティ デバイスを管理することができます。SSH プロトコルのバージョン 1.5 と互換性のある SSH クライアントが必要です。これらのクライアントは、Windows 95 およびそれ以降、Windows NT、Linux、および UNIX で利用できます。セキュリティ デバイスは、組み込みの SSH サーバーを介して、デバイス構成と管理サービスを提供する SSH クライアントと通信します。このオプションを選択すると、SSH 管理容易性が使用可能になります。
- **SNMP:** セキュリティ デバイスは、SNMPv1 と SNMPv2c の両方、および RFC-1213 で定義される、関連するすべての MIB II（管理情報ベース II）グループをサポートします。このオプションを選択すると、SNMP 管理容易性が使用可能になります。
- **SSL:** このオプションを選択することで、インターフェースに WebUI を通じたセキュリティ デバイス の安全な管理のための HTTP トラフィックを受信することができます。
- **NetScreen-Security Manager:** このオプションを選択することで、NetScreen-Security Manager トラフィックをインターフェースで受信できます。
- **Ping:** このオプションを選択することで、セキュリティデバイスは、特定 IP アドレスがネットワーク上でアクセス可能かどうかを確認する ICMP エコー要求に応答することが可能になります。
- **Ident-Reset:** メールや FTP などのサービスは、識別要求を送信します。確認通知が受信できない場合は、要求を再度送信します。要求の処理中には、ユーザーアクセスはありません。Ident-reset オプションを使用可能にすると、セキュリティ デバイスは IDENT 要求に対する応答として TCP リセット通知をポート 113 に送信し、未確認の識別要求によってブロックされているアクセスを回復させます。

これらのオプションを使用するには、セキュリティと管理上のニーズに応じて、1 つまたは複数のインターフェース上で使用可能にします。

MGT および VLAN1 インターフェース

一部の Juniper Networks セキュリティ デバイスは、管理トラフィック専用となる物理インターフェース、つまり MGT（管理）インターフェースも持っています。NetScreen デバイスを NAT もしくはルートモードで動作中に、このインターフェースを管理トラフィックに使用します。

Transparent モードでは、すべてのセキュリティ デバイスを論理的なインターフェース VLAN1 を介して管理するように設定できます。管理トラフィックが VLAN1 インターフェースにアクセスできるようにするには、管理トラフィックが VLAN1 に到達する際に通過する VLAN1 および Layer 2 ゾーン (V1-Trust、V1-Untrust、V1-DMZ、ユーザー定義の Layer 2 ゾーン) で、目的の管理オプションを使用可能にする必要があります。

セキュリティレベルを最高に保つために、管理トラフィックを VLAN1 または MGT インターフェースに、そしてユーザートラフィックをセキュリティゾーンインターフェース限定することを推奨します。管理トラフィックをネットワークユーザー トラフィックから分離すると、管理セキュリティが大幅に強化され、一貫した管理帯域幅が保証されます。

例 : MGT インターフェースによる管理

この例では、MGT インターフェースの IP アドレスを 10.1.1.2/24 に設定し、MGT インターフェースが Web および SSH 管理トラフィックを受信できるようにします。

WebUI

Network > Interfaces > Edit (mgt): 次のように入力してから **OK** をクリックします。

IP Address/Netmask: 10.1.1.2/24
Management Services: WebUI, SSH: (選択)

CLI

```
set interface mgt ip 10.1.1.2/24
set interface mgt manage web
set interface mgt manage ssh
save
```

例 : VLAN1 インターフェースを介した管理

この例では、VLAN1 インターフェースの IP アドレスを 10.1.1.1/24 に設定し、VLAN1 インターフェースが V1-Trust ゾーンを介して Telnet および Web 管理トラフィックを受信できるようにします。

WebUI

Network > Interfaces > Edit (VLAN1): 次のように入力してから **OK** をクリックします。

IP Address/Netmask: 10.1.1.1/24
Management Services: WebUI, Telnet: (選択)

Network > Zones > Edit (V1-Trust): 次のように選択してから **OK** をクリックします。

Management Services: WebUI, Telnet: (選択)

CLI

```
set interface vlan1 ip 10.1.1.1/24
set interface vlan1 manage web
set interface vlan1 manage telnet
set zone v1-trust manage web
set zone v1-trust manage telnet
save
```

管理インターフェースオプションの設定

ネットワーク トラフィックに対して、物理的な MGT インターフェースを除く複数の物理インターフェースを持つセキュリティ デバイスでは、1 つの物理インターフェースを管理専用とし、管理トラフィックを完全にネットワーク ユーザー トラフィックから切り離すこともできます。たとえば、ローカル管理は Trust ゾーンにバインドされたインターフェースを介し、リモート管理は Untrust ゾーンにバインドされたインターフェースを介しデバイスにアクセスするようにできます。

この例では、ethernet1 を Trust ゾーンに、ethernet3 を Untrust ゾーンにバインドします。ethernet1 に IP アドレス 10.1.1.1/24 を割り当てて、管理 IP アドレス 10.1.1.2 を与えます。(管理 IP アドレスは、セキュリティゾーンインターフェース IP アドレスと同じサブネット内にする必要があります。また、ethernet1 は Web トラフィックや Telnet トラフィックを受信することもできます。次に、ethernet3 に IP アドレス 1.1.1.1/24 を割り当てて、ethernet3 に送信されるすべての管理トラフィックをブロックします。

WebUI

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

```
Zone Name: Trust
Static IP: ( ある場合は選択する )
IP Address/Netmask: 10.1.1.1/24
        Manage IP: 10.1.1.2
Management Services:
        WebUI: ( 選択 )
        SNMP: ( オフ )
        Telnet: ( 選択 )
        SSL: ( オフ )
        SSH: ( オフ )
```

次のように入力してから **OK** をクリックします。

```
Interface Mode: NAT
Network > Interfaces > Edit (ethernet3):
```

次のように入力してから **OK** をクリックします。

```
Zone Name: Untrust
Static IP: ( ある場合は選択する )
IP Address/Netmask: 1.1.1.1/24
Management Services:
  WebUI: ( オフ )
  SNMP: ( オフ )
  Telnet: ( オフ )
  SSL: ( オフ )
  SSH: ( オフ )
```

CLI

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 manage-ip 10.1.1.2
set interface ethernet1 manage web
unset interface ethernet1 manage snmp
set interface ethernet1 manage telnet
unset interface ethernet1 manage ssl
unset interface ethernet1 manage ssh
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
save
```

注 : Trust ゾーンと V1-Trust ゾーン以外のセキュリティゾーンにインターフェースをバインドする場合、デフォルトではすべての管理オプションが使用不可になっています。したがって、ここでは ethernet3 の管理オプションを使用不可にする必要はありません。

複数のインターフェースに対して管理 IP を設定する

セキュリティ ゾーンにバインドされる物理インターフェース、冗長インターフェース、統合インターフェース、またはサブインターフェースは、少なくとも 2 つの IP アドレスを持つことができます。

- ネットワークに接続するインターフェース IP アドレス
- 管理トラフィックを受信するための論理管理 IP アドレス

セキュリティ デバイスが HA（高可用性）に関しての冗長グループ内でバックアップ ユニットである場合は、その管理 IP アドレス（複数可）を通じてユニットにアクセスし構成することができます。

注 : 管理 IP アドレスは、VLAN1 アドレスと以下の 2 点で異なります。

セキュリティデバイスが透過モードの時は、VLAN1 IP アドレスは VPN トンネルの端点になることができますが、管理 IP アドレスではできません。

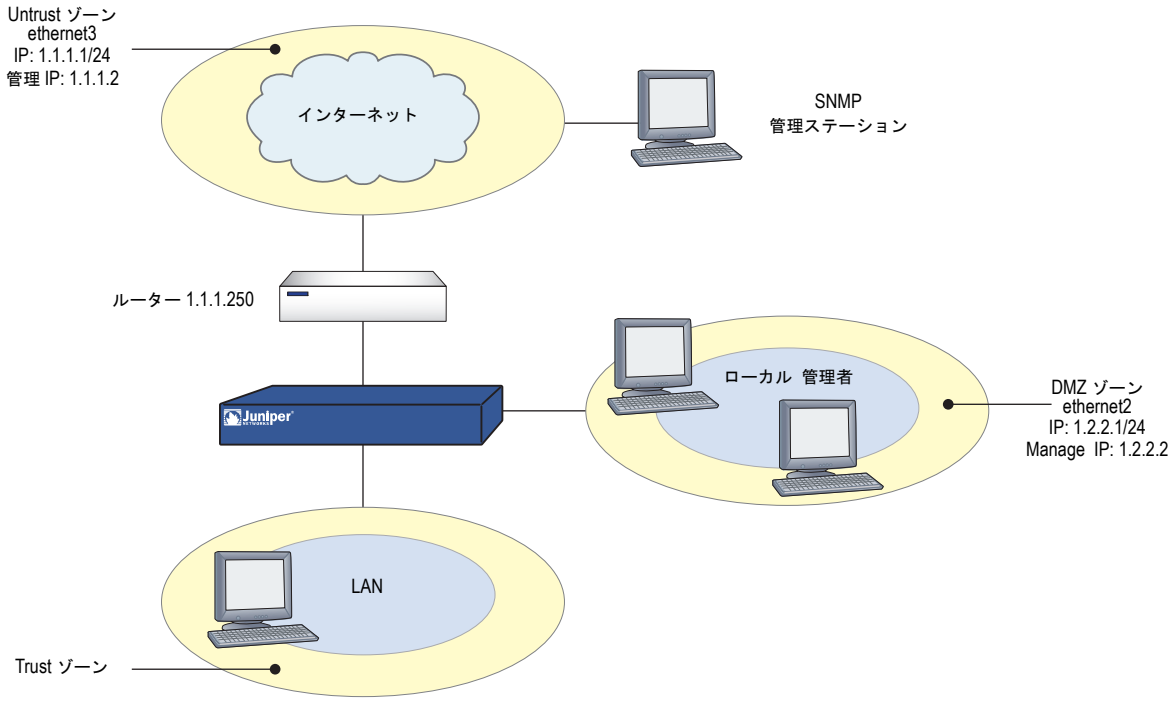
複数の管理 IP アドレスを、ネットワークインターフェースごとに 1 つずつ定義することができますが、VLAN1 IP アドレスは、システム全体に 1 つだけしか定義できません。

WebUI のインターフェース構成ページで Manageable オプションを選択した場合は、そのインターフェースに関連付けられたインターフェース IP アドレスまたは管理 IP アドレスのいずれかを介して、セキュリティ デバイスを管理できます。

32 ページの図 13 では、ethernet2 を DMZ ゾーンに、ethernet3 を Untrust ゾーンにバインドします。特定の管理トラフィックのためのアクセスを提供するようオプションを設定します。DMZ ゾーンのローカル管理者グループのために ethernet2 に HTTP アクセスと Telnet アクセスを、リモートサイトからの中央デバイスモニターのために ethernet3 に SNMP アクセスをそれぞれ許可します。

ethernet2 と、ethernet3 は、それぞれ管理トラフィックが送信される管理 IP アドレスを持っています。さらに、ethernet3 を使用して 1.1.1.250 にある外部ルーターに到するために、自己生成 SNMP トラフィックを誘導するルートを設定する必要があります。

図 13: 複数のインターフェースに対して管理 IP を設定する



WebUI

Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

Zone Name: DMZ
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.2.2.1/24
Manage IP: 1.2.2.2
Management Services:
WebUI: (選択)
Telnet: (選択)

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24
Manage IP: 1.1.1.2
Management Services:
SNMP: (選択)

CLI

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 1.2.2.1/24
set interface ethernet2 manage-ip 1.2.2.2
set interface ethernet2 manage web
set interface ethernet2 manage telnet
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 manage-ip 1.1.1.2
set interface ethernet3 manage snmp
save
```

管理レベル

Juniper Networks セキュリティ デバイスは複数の管理ユーザーをサポートします。管理者によって、構成が変更される場合には、セキュリティ デバイスは以下の情報をログに記録します。

- 変更を行った管理者の名前
- 変更前の IP アドレス
- 変更時刻

管理ユーザーにはいくつかのレベルがあります。Juniper Networks セキュリティ デバイスのモデルによって、利用できるレベルが異なる場合があります。以降のセクションには、すべての管理レベルおよび各レベルの権限がリスト表示されています。これらの権限には、管理者が有効なユーザー名とパスワードでログインした後、その管理者のみアクセスできます。

ルート管理者

ルート管理者は、すべての管理権限を持っています。各セキュリティ デバイスのルート管理者は 1 名のみです。ルート管理者は、以下の権限を持ちます。

- セキュリティ デバイスのルートシステムの管理
- 他の管理者の追加、削除および管理
- 仮想システムの確立と管理、およびそれらに対する物理的・論理的インターフェースの割り当て
- 仮想ルーター (VR) の作成、削除および管理
- セキュリティゾーンの追加、削除および管
- インターフェースをセキュリティゾーンに割り当て
- 初期化の実行
- デバイスを FIPS モードに設定
- デバイスをデフォルト設定にリセット

- ファームウェアの更新
- 構成ファイルのロード
- 特定の管理者またはすべてのアクティブ管理者の全アクティブセッションをクリア

読取 / 書込管理者

読取 / 書込管理者は、ルート管理者と同じ権限を持っていますが、他の管理ユーザーを作成、変更、または削除することはできません。読取 / 書込管理者は、以下の権限を持ちます。

- 仮想システムの作成、および仮想システム管理者の各システムへの割り当て
- 任意の仮想システムの監視
- 統計の監視 (この権限は仮想システム管理者には委譲できません)

読取専用管理者

読取専用管理者は、WebUI を使った参照のみの権限を持ち、CLI コマンドの **get** および **ping** のみを発行できます。読取専用管理者は、以下の権限を持ちます。

- ルートシステムにおける読取専用権限。**enter**、**exit**、**get**、**ping**
- 仮想システムにおける読取専用権限

仮想システム管理者

セキュリティ デバイスには、仮想システムをサポートするものがあります。各 vsys (仮想システム) は、独立したセキュリティドメインで、その vsys のみに適用される権限を持った仮想システム管理者により管理されます。仮想システム管理者は、CLI もしくは WebUI を通じて独立して仮想システムを管理します。各 vsys では、仮想システム管理者は以下の権限を持ちます。

- 認証、IKE、L2TP、XAuth、および手動鍵ユーザーの作成および編集
- サービスの作成と編集
- ポリシーの作成と編集
- アドレスの作成と編集
- VPN の作成と編集
- 仮想システム管理者のログインパスワードの変更
- セキュリティゾーンの作成と管理
- 仮想システム読取専用管理者の追加と削除

仮想システム読取専用管理者

仮想システム読取専用管理者は、読取専用管理者と同じ権限を持ちますが、特定の仮想システム内でのみ行使できます。仮想システム読取専用管理者は、WebUI による特定の vsys についての参照権限を持ち、その vsys 内で、**enter**、**exit**、**get**、および **ping** CLI コマンドを発行できます。

注 : 仮想システムの詳細は、**10**-1 ページの「仮想システム」を参照してください。

管理ユーザーの定義

ルート管理者とは、管理ユーザーの作成、変更、および削除を行える唯一の管理者です。以下の例では、ルート管理者が手順を実行する必要があります。

例 : 読取専用管理者を追加する

この例では、ルート管理者は、Roger という名前で 2bd21wG7 のパスワードを持つ読取管理者を追加します。

WebUI

Configuration > Admin > Administrators > New: 次のように入力してから **OK** をクリックします。

Name: Roger
New Password: 2bd21wG7
Confirm New Password: 2bd21wG7
Privileges: Read-Only (選択)

注 : パスワードは最大 31 文字でケースセンシティブです。

CLI

```
set admin user Roger password 2bd21wG7 privilege read-only
save
```

例 : 管理者を変更する

この例では、ルート管理者は、Roger の権限を読取専用から読取 / 書込に変更します。

WebUI

Configuration > Admin > Administrators > Edit (Roger): 次のように入力してから **OK** をクリックします。

Name: Roger
New Password: 2bd21wG7
Confirm New Password: 2bd21wG7
Privileges: Read-Write (選択)

CLI

```
unset admin user Roger
set admin user Roger password 2bd21wG7 privilege all
save
```

例: 管理者を削除する

この例では、ルート管理者は管理ユーザーの Roger を削除します。

WebUI

Configuration > Admin > Administrators: Roger の Configure コラムの **Remove** をクリックします。

CLI

```
unset admin user Roger
save
```

例: ダイアルアップ接続用の管理者アカウントを構成する

デバイスには、アウトバウンドのダイアルアップ障害回復の状況において、モデム接続をサポートするものがあります。trustee アカウントは、インターフェース、モデム、またはインターフェースとモデムの両方に対応するように設定できます。このセクションでは、2 種類のトラスティ（trustee）について説明しています。

- インターフェース トラスティ

  インターフェース トラスティは、WebUI へのアクセスのみが許可されており、プライマリ Untrust インターフェースのシグナリング手法と IP アドレス割り当てに制限されています。

  ADSL インターフェースを持つデバイスでは、インターフェース トラスティが次の特性を制御します。

  - レイヤー 1 の特性 : VPI/VCI、複合モード、RFC1483 bridged/routed
  - レイヤー 2 シグナリング手法（PPPoE または PPPoA、およびそれらのパラメータ）
  - IP アドレス割り当て手法（管理者によって静的に定義されるか、PPPoE または PPPoA を通じて回線から動的に取得される）。

  イーサネット インターフェースのみを持つデバイスでは、インターフェース トラスティが、インターフェース IP アドレスをどのように割り当てるかを制御できます（管理者によって静的に定義されるか、または DHCP や PPPoE を通じて回線から動的に取得される）。

- モデム トラスティ

  モデム トラスティは、WebUI へのアクセスのみを持ち、シリアル インターフェースのモデム設定と ISP 設定に制限されています。モデム トラスティは、特定のニーズを満たすために、モデム定義を作成、変更、および削除できます。また、ISP1 および ISP2 の設定を作成、変更、削除することができます。モデム トラスティは、ISP3 および ISP4 の構成を参照し、定義された ISP または電話番号への接続をテストできます。

get admin user コマンドを実行することで、すべての管理者アカウントを表示できます。また、**get admin user trustee** コマンドを実行すると、トラスティ アカウントだけを表示できます。

次の例では、Richard Brockie の読取 / 書込モデム トラスティ アカウントを構成します。ユーザー名を *rbrockie*、パスワードを *!23fb* に設定します。

WebUI

Configuration > Admin > Administrators

CLI

```
set admin user rbrockie password !23fb privilege all
set admin user rbrockie trustee modem
```

例 : 管理者のセッションを消去する

この例では、ルート管理者は管理ユーザー Roger のすべてのアクティブなセッションを終了します。以下のコマンドを実行すると、セキュリティ デバイスはすべてのアクティブ セッションを終了し、Roger をシステムから自動的にログオフさせます。

WebUI

注 : CLI を使用して管理者のセッションをクリアする必要があります。

CLI

```
clear admin name Roger
save
```

セキュアな管理トラフィック

設定中のセキュリティ デバイスを保護するためには、以下の手順を実行します。

1. WebUI で、管理ポートを変更します。

   38 ページの「ポート番号を変更する」を参照。

2. 管理アクセス用のユーザー名およびパスワードを変更します。

   39 ページの「管理者ログイン名およびパスワードを変更する」を参照。

3. 管理ユーザーの管理クライアント IP アドレスを定義します。

   42 ページの「管理者アクセスを制限する」を参照。

4. 不要なインターフェース管理サービスオプションをオフにします。

   28 ページの「管理トラフィックのコントロール」を参照。

5. 不審な人物による要求にこたえてネットワークの情報を漏らす、インターフェースの ping および ident-reset サービスオプションを使用不可能にします。

WebUI

Network > Interfaces > Edit (編集するインターフェース): 以下のサービスオプションを使用不可能にして、**OK** をクリックします。

Ping: このオプションを選択することで、セキュリティデバイスは、特定 IP アドレスがネットワーク上でアクセス可能かどうかを確認する ICMP エコー要求もしくは “ping” に応答することが可能になります。

Ident-Reset: メールや FTP などのサービスが、識別要求を送信して、確認を受信できない場合には、その要求が再度送信されます。要求が処理中であれば、ユーザーアクセスは使用不可能になっています。Ident-Reset のチェックボックスが使用可能になっていれば、セキュリティ デバイスは自動的にユーザー アクセスを復旧します。

CLI

```
unset interface interface manage ping
unset interface interface manage ident-reset
```

ポート番号を変更する

セキュリティ デバイスが HTTP 管理トラフィックを待ち受けるポート番号を変更することで、セキュリティが向上します。デフォルト設定は HTTP トラフィックの標準ポート番号の、ポート 80 です。ポート番号を変更した場合は、次にセキュリティ デバイスと通信を行うときに、ブラウザの URL フィールドに新しいポート番号を入力します。(以下の例では、管理者は http://188.30.12.2:15522 と入力してください。) 。

この例では、Trust ゾーンにバインドされたインターフェースの IP アドレスは 10.1.1.1/24 です。このインターフェースの WebUI を介してセキュリティ デバイスを管理するには、HTTP を使う必要があります。HTTP 接続のセキュリティを強化するためには、HTTP ポート番号を 80 (デフォルト) から 15522 に変更します。

WebUI

Configuration > Admin > Management: HTTP Port フィールドに **15522** を入力してから、**Apply** をクリックします。

CLI

```
set admin port 15522
save
```

管理者ログイン名およびパスワードを変更する

デフォルトでは、セキュリティ デバイスの初期ログイン名は **netscreen** になっています。初期パスワードも **netscreen** です。これについては広く公表されているため、Juniper Networks ではログイン名とパスワードをただちに変更することを推奨します。ログイン名もパスワードも、大文字小文字が区別されます。「?」および「”」を除いて、キーボードから入力できるすべての文字が使用できます。新しい管理ログイン名とパスワードを安全な方法で記録してください。



警告 : 新しいパスワードをかならず記録しておいてください。パスワードを忘れた場合は、セキュリティ デバイスをデフォルト設定にリセットする必要があるため、すべての構成が失われます。詳細については、41 ページの「デバイスのデフォルト設定へのリセット」を参照してください。

セキュリティ デバイスの管理ユーザーは、内部データベースまたは外部認証サーバーを使用して認証されます。管理ユーザーがセキュリティ デバイスにログオンする際の認証では、まずローカルの内部データベースがチェックされます。項目が見つからない場合には、外部認証サーバーに接続されていれば、外部認証サーバーデータベースでマッチングエントリを検索します。管理ユーザーが外部認証サーバーへのログオンに成功すれば、セキュリティ デバイスは管理者のログイン状況をローカルで記憶します。

注 : Juniper Networks は、管理ユーザー認証用に RADIUS、SecurID、および LDAP サーバーをサポートします。(詳細は、**9**-2 ページの「管理ユーザー」を参照してください。)) ルート管理者のアカウントは、ローカルデータベースに保存されなければなりませんが、ルートレベル読取 / 書込管理ユーザーとルートレベル読取専用管理ユーザーは、外部認証サーバーに保存することができます。ルートレベルおよび vsys レベル管理ユーザーを外部認証サーバーに保存して、権限を検索するには、サーバーは RADIUS であり、netscreen.dct file をサーバーにロードしておく必要があります。

管理ユーザーレベルの詳細については、33 ページの「管理レベル」を参照してください。外部認証サーバーに関する詳細については、**9**-15 ページの「外部認証サーバー」を参照してください。

ルート管理者がユーザー名、パスワード、または権限など、管理ユーザー プロファイルの何らかの属性を変更した場合は、その管理者が現在開いている管理セッションは自動的に終了します。ルート管理者が、自身の属性を変更するか、ルートレベル読取 / 書込管理者または仮想システム読取 / 書込管理者が、自身のパスワードを変更した場合は、変更を行ったセッションを除き、そのユーザーが現在開いているすべての管理セッションが終了します。

注 : WebUI を使った HTTP もしくは HTTPS セッションの振る舞いは異なります。HTTP は持続接続をサポートしていないため、自身のユーザープロファイルに対して変更を行うと、自動的にログアウトし、オープンセッションはすべて終了します。

例 : 管理ユーザーのログイン名およびパスワードを変更する

この例では、ルート管理者は読取 / 書込管理者のログイン名を「John」から「Smith」に、パスワードを xL7s62a1 から 3MAb99j2 に変更します。

注 : ディクショナリ攻撃により推測または明らかにされる恐れのある実際的な単語をパスワードに使う代わりに、英数字からなるランダムに見える文字列を使うことができます。そのような文字列で簡単に覚えられるものを作成するには、文章を作って各単語の最初の一文字を使います。たとえば、“Charles will be 6 years old on November 21”は、“Cwb6yooN21”になります。

詳細は、33 ページの「管理レベル」を参照してください。

WebUI

Configuration > Admin > Administrators > Edit (John): 次のように入力してから **OK** をクリックします。

```
Name: Smith
New Password: 3MAb99j2
Confirm New Password: 3MAb99j2
```

CLI

```
unset admin user John
set admin user Smith password 3MAb99j2 privilege all
save
```

例 : ユーザー自身のパスワードを変更する

読取 / 書込権限を持つ管理ユーザーは、自身の管理パスワードを変更できますが、ログイン名を変更することはできません。この例では、読取 / 書込権限を持ちログイン名“Smith”を使用する管理者が、自身のパスワードを 3MAb99j2 から ru494Vq5 に変更します。

WebUI

Configuration > Admin > Administrators > Edit (最初の項目): 次のように入力してから **OK** をクリックします。

```
Name: Smith
New Password: ru494Vq5
Confirm New Password: ru494Vq5
```

CLI

```
set admin password ru494Vq5
save
```

ルート管理者パスワードの最小文字数を設定する

企業によっては、誰か 1 人がルート管理者として最初にデバイスを構成した後に、他の人がそのルート管理者の任務を引き継いでデバイスを管理することもあります。引き継いだルート管理者が、容易に複合化できるような短いパスワードを使用するのを防ぐために、最初のルート管理者は、ルート管理者のパスワードに必要な最低文字数を、1 から 31 までの任意の数に設定できます。

最小パスワード文字数を設定できるのはルート管理者のみで、さらにそのルート管理者自身のパスワードが、これから設定する最小文字数要件を満たしている場合だけです。それ以外の場合は、セキュリティ デバイスがエラーメッセージを表示します。

ルート管理者のパスワードの最小文字数を指定するには、以下のコマンドを使用します。

set admin password restrict length *number*

注 : この制限を設定するには、CLI を使用する必要があります。

デバイスのデフォルト設定へのリセット

管理者パスワードが失われた場合には、以下の手順に従ってセキュリティ デバイスをデフォルト設定にリセットすることができます。構成は失われますが、デバイスへのアクセスは回復します。この操作を行うには、コンソール接続を確立する必要があります。コンソール接続の確立については、*ScreenOS CLI Reference Guide IPv4 Command Descriptions* およびデバイスのドキュメントに詳しく説明されています。

注 : デフォルトで、デバイスリカバリ機能は使用可能になっています。**unset admin device-reset** コマンドを入力することで、この機能を使用不能にすることができます。また、セキュリティ デバイスが FIPS モードの場合は、リカバリ機能は自動的に使用不能になります。

---

1. ログイン プロンプトで、デバイスのシリアル番号を入力します。
2. パスワード プロンプトで、シリアル番号をもう一度入力します。

   以下のメッセージが表示されます。

   !!!! Lost Password Reset !!!! You have initiated a command to reset the device to factory defaults, clearing all current configuration, keys and settings. Would you like to continue? y/n

3. Press the **y** key.

   以下のメッセージが表示されます。

   !! Reconfirm Lost Password Reset !! If you continue, the entire configuration of the device will be erased. In addition, a permanent counter will be incremented to signify that this device has been reset. This is your last chance to cancel this command. If you proceed, the device will return to factory default configuration, which is: System IP: 192.168.1.1; username: netscreen; password: netscreen. Would you like to continue? y/n

4. **y** を押してデバイスをリセットします。これで、デフォルトのユーザー名およびパスワードとして **netscreen** を使用してログインできます。

管理者アクセスを制限する

セキュリティ デバイスを 1 つのサブネット内の複数のアドレスから管理することができます。デフォルトでは、Trusted インターフェース上のホストならどれでも、セキュリティ デバイスを管理できます。この機能を特定のワークステーションに制限するためには、管理クライアントの IP アドレスを設定する必要があります。

例 : 管理を 1 つのワークステーションに制限する

この例では、IP アドレス 172.16.40.42 を持つワークステーションの管理者が、セキュリティ デバイスを管理するように指定された唯一の管理者です。

WebUI

Configuration > Admin > Permitted IPs: 次のように入力してから **Add** をクリックします。

IP Address/Netmask: 172.16.40.42/32

CLI

```
set admin manager-ip 172.16.40.42/32
save
```

例 : 管理を特定のサブネットに制限する

この例では、サブネット 172.16.40.0/24 上の管理者のみがセキュリティ デバイスを管理するように指定します。

WebUI

Configuration > Admin > Permitted IPs: 次のように入力してから **Add** をクリックします。

IP Address/Netmask: 172.16.40.0/24

CLI

```
set admin manager-ip 172.16.40.0 255.255.255.0
save
```

ルート管理者をコンソールアクセスに制限する

ルート管理者がコンソールのみを介してセキュリティ デバイスにログインするように制限することもできます。この制限によってルート管理者は、ログインするデバイスへ物理的にアクセスすることが必要となり、非認証ユーザーがルート管理者としてリモートでログインすることを防止します。この制限を設定した後は、誰かが WebUI、Telnet、または SSH などの他の方法でルート管理者としてログインしようとしても、そしてこれらの管理オプションが進入インターフェースで使用可能になっていても、デバイスはアクセスを拒否します。

ルート管理者のアクセスをコンソールのみに制限するには、以下のコマンドを入力します。

set admin root access console

注 : この制限を設定するには、CLI を使用する必要があります。

管理トラフィックの VPN トンネル

VPN（仮想プライベート ネットワーク）トンネルを使用することにより、動的に割り当てられた IP アドレスまたは固定 IP アドレスのどちらかからのセキュリティ デバイスのリモート管理を保護することができます。また、NetScreen-Security Manager、HTTP、Telnet、SSH などのあらゆるトラフィックを保護することができます （VPN トンネルを作成して、NetScreen-Security Manager レポート、syslog レポート、または SNMP トラップなどの自己起動のトラフィックを保護する方法については、78 ページの「自己開始トラフィックの VPN トンネル」を参照してください）。

Juniper Networks セキュリティ デバイスは、2 種類の VPN トンネル構成をサポートしています。

- **ルーティングベース VPN**: セキュリティ デバイスはルートテーブルのエントリを使用してトラフィックをトンネル インターフェースに導きます。トンネル インターフェースは VPN トンネルにバインドされています。
- **ポリシーベース VPN**: セキュリティ デバイスは、ポリシーで具体的に参照された VPN トンネル名を使用してトラフィックが VPN トンネルを経由するようにします。

各 VPN トンネル構成タイプに対して、以下の 3 つのタイプの VPN トンネルがあります。

- **手動鍵** : トンネルの両端で、SA (セキュリティアソシエーション) を定義する 3 つの要素を手動で設定します。3 つの要素とは、SPI (セキュリティパラメータインデックス)、暗号化鍵、認証鍵です。また、これら SA の要素を変更する場合には、トンネルの両端で手動でその設定を変更する必要があります。
- **AutoKey IKE と事前共有鍵** : 1 つまたは 2 つの事前共有（認証用と暗号化用）は、シード値として機能します。それらを用い、IKE プロトコルはトンネルの両端で対称鍵を生成します。つまり同じ鍵が暗号化と復号に使用されます。また、これらの鍵は、あらかじめ設定された間隔で、自動的に再生成されます。
- **AutoKey IKE と証明書**: PKI (公開鍵暗号基盤) では、デジタル証明書 (認証用) と RSA 公開 / 秘密鍵ペア (暗号化用) を使用します。また、暗号化鍵は非対称あり、ペアの 1 つの鍵は暗号化に、もう 1 つは復号に使用されます。

注 : VPN トンネルの詳細については、*第 5 部 : 仮想プライベート ネットワーク*を参照してください。NetScreen-Remote の詳細については、*NetScreen-Remote VPN Client Administrator Guide* を参照してください。

ポリシーベース VPN 構成を使用する場合は、アドレス帳を作成し、出力インターフェースがバインドされていない任意のゾーンに存在するインターフェースの IP アドレスを入力する必要があります。そうすると、VPN トンネルを参照するポリシーのソースアドレスとして、その IP アドレスを使用できます。また、このアドレスはリモート IPSec ピアの終端エンティティアドレスとしても機能します。ルートベース VPN 構成を使用している場合は、このようなアドレス帳入力は不要です。

ルートベース手動鍵 VPN トンネルを介した管理

図 14 の例では、ルートベース手動鍵 VPN トンネルをセットアップし、管理トラフィックの機密性を強化する方法を表しています。このトンネルは、管理者のワークステーション 10.1.1.56 を使用する NetScreen-Remote VPN クライアントから ethernet 1 (10.1.1.1/24) まで続きます。管理者のワークステーションとイーサネット 1 はともに、Trust ゾーンにあります。トンネルの名前は“tunnel-adm”とします。番号なしのトンネルインターフェースを作成して tunnel.1 という名前を付け、Trust ゾーンと VPN トンネル “tunnel-adm”にバインドします。

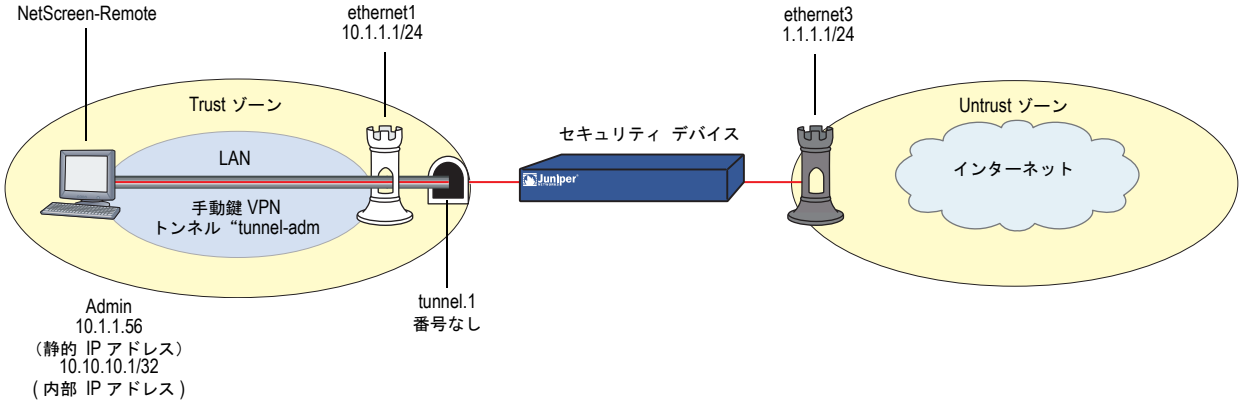
セキュリティ デバイスは、ピア ゲートウェイのアドレス 10.1.1.56 ではなく、NetScreen-Remote クライアント（10.10.10.1）で構成した内部 IP アドレスを宛先アドレスとして定義します。tunnel.1 を経由して 10.10.10.1/32 に到達するルートを定義します。以下の理由により、ポリシーは不要です。

- VPN トンネルは、セキュリティ デバイスを通って他のセキュリティ ゾーンに向かう管理トラフィックは保護せず、セキュリティ デバイスで終了する管理トラフィックを保護します。
- これはルートベース VPN であるため、ルートルックアップが該当する VPN トンネルにバインドされたトンネルインターフェースに宛先アドレスをリンクします。

注： この例を 47 ページの「ポリシーベース手動鍵 VPN トンネルを介した管理」と比べてみてください。

NetScreen-Remote は、リモート ゲートウェイの 10.1.1.1 ではなく、ethernet3 の IP アドレス 1.1.1.1 を宛先アドレスとして使用します。NetScreen-Remote 構成は、リモートパーティ ID タイプを “IP address”、プロトコルを “All”に指定します。

図 14: ルートベース手動鍵 VPN トンネルを介した管理



WebUI

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): Trust (trust-vr)
Unnumbered: (選択)
Interface: ethernet1(trust-vr)

注 : 番号のないトンネルインターフェースは、特定のセキュリティゾーンインターフェースの IP アドレスを借用します。

---

2. VPN

VPNs > Manual Key > New: 次のように入力してから **OK** をクリックします。

VPN Tunnel Name: tunnel-adm
Gateway IP: 10.1.1.56
Security Index (HEX Number): 5555 (ローカル) 5555 (リモート)
Outgoing Interface: ethernet1
ESP-CBC: (選択)
Encryption Algorithm: DES-CBC
Generate Key by Password: netscreen1
Authentication Algorithm: MD5
Generate Key by Password: netscreen2

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Bind to Tunnel Interface: (選択), Tunnel.1

注 : NetScreen-Remote プロセスは他の Juniper Networks 製品と異なった方法でパスワードを処理して鍵を作成するため、トンネルを構成した後で以下の手順に従ってください。(1) Manual Key Configuration ダイアログボックスに戻ります (tunnel-adm の Configure コラムにある **Edit** をクリックします)。(2) 生成された 16 進鍵をコピーします。(3) NetScreen-Remote 側でトンネルを作成する際に、その 16 進鍵を使用します。

---

3. ルート
Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.10.10.1/32
Gateway: (**選択**)
Interface: Tunnel.1
Gateway IP Address: 0.0.0.0

CLI

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface ethernet1
```

注 : 番号のないトンネルインターフェースは、特定のセキュリティゾーンインターフェースの IP アドレスを借用します。

2. VPN

```
set vpn tunnel-adm manual 5555 5555 gateway 10.1.1.56 outgoing ethernet1 esp
    des password netscreen1 auth md5 password netscreen2
set vpn tunnel-adm bind interface tunnel.1
```

注 : NetScreen-Remote プロセスは他の Juniper Networks 製品と異なった方法でパスワードを処理して鍵を作成するため、トンネルを構成した後で以下の手順に従ってください。(1) **get vpn admin-tun** コマンドを入力します。(2) “netscreen1” と “netscreen2” が作成した 16 進鍵をコピーします。(3) トンネルの NetScreen-Remote 側を構成するときに、これらの 16 進鍵を使用します。

3. ルート

```
set vrouter trust-vr route 10.10.10.1/32 interface tunnel.1
save
```

NetScreen-Remote セキュリティポリシーエディタ

1. **Options > Global Policy Settings** をクリックし、Allow to Specify Internal Network Address チェックボックスを選択します。
2. **Options > Secure > Specified Connections** をクリックします。
3. **Add a new connection** をクリックし、表示された新しい接続アイコンの横に **Admin** と入力します。
4. 接続オプションを次のように構成します。

Connection Security: Secure
Remote Party Identity and Addressing:
ID Type: IP Address, 1.1.1.1
Protocol: All
Connect using Secure Gateway Tunnel: (**選択**)
ID Type: IP Address, 10.1.1.1

5. UNIX アイコンの左にある 「+」シンボルをクリックして接続ポリシーを拡張します。

6. **My Identity** をクリックし、Select Certificate ドロップダウンリストで **None** を選択し、Internal Network IP Address に **10.10.10.1** を入力します。

7. **Security Policy** をクリックし、**Use Manual Keys** を選択します。

8. Security Policy アイコンの左にある“+”記号をクリックしてから、Key Exchange（Phase 2）の左にある“+”記号をクリックし、さらにポリシーを展開します。

9. **Proposal 1** をクリックして、以下の IPSec プロトコルを選択します。

   Encapsulation Protocol (ESP): (**選択**)
   Encrypt Alg: DES
   Hash Alg: MD5
   Encapsulation: Tunnel

10. **Inbound Keys** をクリックして、Security Parameters Index フィールドに **5555** を入力します。

11. **Enter Key** をクリックし、以下のように入力してから、**OK** をクリックします。

    Choose key format: Binary
    ESP Encryption Key: dccbee96c7e546bc
    ESP Authentication Key: dccbe9e6c7e546bcb0b667794ab7290c

注 : この 2 つの鍵は、セキュリティ デバイスの構成後にコピーした鍵です。

12. **Outbound Keys** をクリックして、Security Parameters Index フィールドに **5555** を入力します。

13. **Enter Key** をクリックし、以下のように入力してから、**OK** をクリックします。

    Choose key format: Binary
    ESP Encryption Key: dccbee96c7e546bc
    ESP Authentication Key: dccbe9e6c7e546bcb0b667794ab7290c

14. **Save** をクリックします。

ポリシーベース手動鍵 VPN トンネルを介した管理

図 15 の例では、ポリシーベース手動鍵 VPN トンネルをセットアップし、管理トラフィックの機密性を強化する方法を表しています。このトンネルは、管理者のワークステーション 10.1.1.56 を使用する NetScreen-Remote VPN クライアントから ethernet 1 (10.1.1.1/24) まで続きます。管理者のワークステーションと ethernet1 はともに、Trust ゾーンにあります。トンネルに“tunnel-adm”という名前を指定し、Trust ゾーンにバインドします。

セキュリティ デバイスは、ピア ゲートウェイのアドレス 10.1.1.56 ではなく、NetScreen-Remote（10.10.10.1）で構成した内部 IP アドレスを宛先アドレスとして使用します。Trust ゾーンアドレスブックエントリを 10.10.10.1/32 を指定し、Untrust ゾーンアドレスブックエントリを ethernet3 の IP アドレスを指定して定義します。ethernet3 インターフェースのアドレスは 1.1.1.1/24 ですが、作成するアドレスには 32 ビットの次のネットマスクを設定しています。1.1.1.1/32.

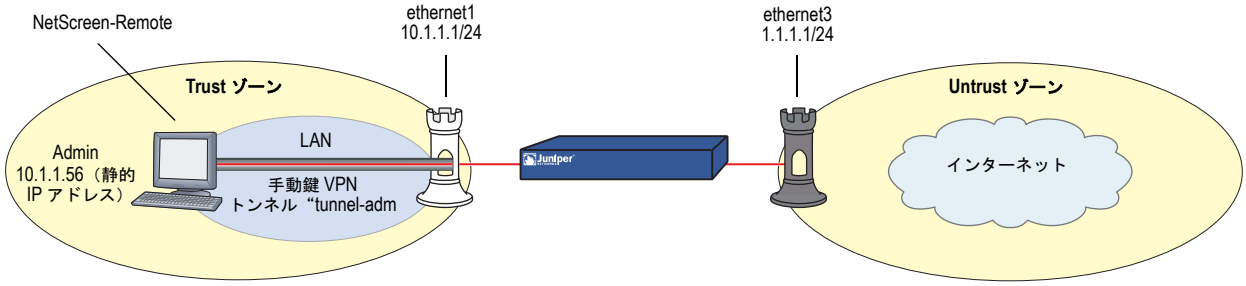
1.1.1.1/32. このアドレスと管理者ワークステーションの内部アドレスを、トンネル“tunnel-adm”を参照して作成するポリシーで使用します。これはポリシーベース VPN であり、ポリシールックアップ（ルートルックアップではない）が該当する VPN チャンネルの宛先アドレスにリンクすることを意味するため、ポリシーは必要です。

ethernet.1 を経由して 10.10.10.1/32 に到達するルートも定義します。

注： この例を 44 ページの「ルートベース手動鍵 VPN トンネルを介した管理」と比べてみてください。

NetScreen-Remote は、リモート ゲートウェイの 10.1.1.1 ではなく、IP アドレス 1.1.1.1 を宛先アドレスとして使用します。NetScreen-Remote トンネル構成は、リモートパーティ ID タイプを “IP addres”、プロトコルを “All”に指定します。

図 15: ポリシーベース手動鍵 VPN トンネルを介した管理



WebUI

1. **インターフェース**

   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24

   次のように選択してから **OK** をクリックします。

   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. **アドレス**

   Policy > Policy Elements > Addresses > Lists > New: 次のように入力してから **OK** をクリックします。

   Address Name: Untrust-IF
   IP Address/Domain Name:
   IP/Netmask: (選択), 1.1.1.1/32
   Zone: Untrust

Policy > Policy Elements > Addresses > Lists > New: 次のように入力してから **OK** をクリックします。

Address Name: admin
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.10.10.1/32
Zone: Trust

3. **VPN**

VPNs > Manual Key > New: 次のように入力してから **OK** をクリックします。

VPN Tunnel Name: tunnel-adm
Gateway IP: 10.1.1.56
Security Index (HEX Number): 5555 (**ローカル**) 5555 (**リモート**)
Outgoing Interface: ethernet1
ESP-CBC: (**選択**)
Encryption Algorithm: DES-CBC
Generate Key by Password: netscreen1
Authentication Algorithm: MD5
Generate Key by Password: netscreen2

注 : NetScreen-Remote プロセスは他の Juniper Networks 製品と異なった方法でパスワードを処理して鍵を作成するため、トンネルを構成した後で以下の手順に従ってください。(1) Manual Key Configuration ダイアログボックスに戻ります (Tunnel-adm の Configure コラムにある **Edit** をクリックします)。(2) 生成された 16 進鍵をコピーします。(3) NetScreen-Remote 側でトンネルを作成する際に、その 16 進鍵を使用します。

4. **ルート**

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.10.10.1/32
Gateway: (**選択**)
Interface: ethernet1
Gateway IP Address: 0.0.0.0

5. **ポリシー**

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), admin
Destination Address:
Address Book Entry: (**選択**), Untrust-IF
Service: Any
Action: Tunnel
Tunnel:
VPN: tunnel-adm
Modify matching bidirectional VPN policy: (**選択**)
Position at Top: (**選択**)

CLI

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **アドレス**
   set address trust admin 10.10.10.1/32
   set address untrust Untrust-IF 1.1.1.1/32

3. **VPN**
   set vpn tunnel-adm manual 5555 5555 gateway 10.1.1.56 outgoing ethernet1 esp des password netscreen1 auth md5 password netscreen2

注 : NetScreen-Remote プロセスは他の Juniper Networks 製品と異なった方法でパスワードを処理して鍵を作成するため、トンネルを構成した後で以下の手順に従ってください。(1) **get vpn admin-tun** コマンドを入力します。(2) “netscreen1” と “netscreen2” が作成した 16 進鍵をコピーします。(3) トンネルの NetScreen-Remote 側を構成するときに、これらの 16 進鍵を使用します。

---

4. **ルート**
   set vrouter trust-vr route 10.10.10.1/32 interface ethernet1

5. **ポリシー**
   set policy top from trust to untrust admin Untrust-IF any tunnel vpn tunnel-adm
   set policy top from untrust to trust Untrust-IF admin any tunnel vpn tunnel-adm
   save

NetScreen-Remote セキュリティポリシーエディタ

1. **Options > Secure > Specified Connections** をクリックします。

2. **Add a new connection** をクリックし、表示された新しい接続アイコンの横に **Admin** と入力します。

3. 接続オプションを次のように構成します。

   Connection Security: Secure
   Remote Party Identity and Addressing:
   ID Type: IP Address, 1.1.1.1
   Protocol: All
   Connect using Secure Gateway Tunnel: (**選択**)
   ID Type: IP Address, 10.1.1.1

4. UNIX アイコンの左にある 「+」シンボルをクリックして接続ポリシーを拡張します。

5. **My Identity** をクリックし、**Select Certificate** ドロップダウンリストで **None** を選択します。

6. **Security Policy** をクリックし、**Use Manual Keys** を選択します。

7. Security Policy アイコンの左にある + シンボルをクリックしてから、Key Exchange (Phase 2) の左にある + シンボルをクリックし、さらにポリシーを拡張します。

8. **Proposal 1** をクリックして、以下の IPSec プロトコルを選択します。

   Encapsulation Protocol (ESP): (**選択**)
   Encrypt Alg: DES
   Hash Alg: MD5
   Encapsulation: Tunnel

9. **Inbound Keys** をクリックして、Security Parameters Index フィールドに **5555** を入力します。

10. **Enter Key** をクリックし、以下のように入力してから、**OK** をクリックします。

    Choose key format: Binary
    ESP Encryption Key: dccbee96c7e546bc
    ESP Authentication Key: dccbe9e6c7e546bcb0b667794ab7290c

注 : この 2 つの鍵は、セキュリティ デバイスの構成後にコピーした鍵です。

11. **Outbound Keys** をクリックして、Security Parameters Index フィールドに **5555** を入力します。

12. **Enter Key** をクリックし、以下のように入力してから、**OK** をクリックします。

    Choose key format: Binary
    ESP Encryption Key: dccbee96c7e546bc
    ESP Authentication Key: dccbe9e6c7e546bcb0b667794ab7290c

13. **Save** をクリックします。

パスワードポリシー

パスワードポリシー機能により、管理者（admin）および認証済み（auth）ユーザーパスワードの最小長と複雑さのスキームを実行します。パスワードポリシー機能は、ローカルデータベースでの使用を意図しており、したがって、パスワードポリシーの集中施行を提供するのに、Windows ディレクトリまたは RADIUS が利用できない環境で役立ちます。

パスワードポリシーを設定する

admin と auth のパスワードが、次の 1 つあるいは両方を満たすことを要求するパスワードポリシーを作成できます。

- 最小長
- 複雑さ

パスワード最小長の範囲は 1 ～ 32 文字です。以下のコマンドを使用して、admin パスワードの最小長が 8 文字であることが必要なパスワードポリシーを作成します。

```
set password-policy user-type admin minimum-length 8
```

パスワードの複雑さとは、たとえば、AAbb12@# のように、パスワードが、少なくとも 2 つの大文字、2 つの小文字、2 つの英数字および 2 つの非英数字文字を含んでいなければならないことを意味します。パスワードが複雑さを含むことを要求するには、複雑さを 1 に設定します。複雑さの要求を解除するには、複雑さを 0 に設定します。以下のコマンドを使用して、auth パスワードが複雑さを含むことを必要とするパスワードポリシーを作成します。

```
set password-policy user-type auth complexity 1
```

次の例では、admin と auth のアカウント用の、複雑さおよび最小長が 8 文字であることを必要とする、パスワードポリシーを作成します :

CLI

```
set password-policy user-type admin minimum-length 8
set password-policy user-type admin complexity 1
set password-policy user-type auth minimum-length 8
set password-policy user-type auth complexity 1
save
```

注 : パスワードポリシーは、コマンドラインインターフェース（CLI）からしか設定できません。

パスワードポリシーを削除する

unset password-policy コマンドを使用して、パスワードポリシーを削除します。パスワードポリシーを削除すると、そのアカウントのパスワード要件はデフォルトの設定に戻ります。次の例では、auth パスワードの最小長要件を削除します。

CLI

```
unset password-policy user-type auth minimum-length
```

パスワードポリシーを表示する

get password-policy コマンドを使用して、admin と auth ユーザーのパスワードポリシーを表示します。

拒否されたデフォルトの管理者パスワードからの回復

パスワードポリシーを設定したデバイスで、ルート admin アカウントを削除（解除）すると、ログオフ前に新規の admin パスワードを設定する必要があるかもしれません。これは、ルート admin アカウントを削除すると、ScreenOS がデフォルトのパスワード（*netscreen*）に戻るためです。複雑さ、または最小長が 9 文字を超えることを必要とするパスワードポリシーを設定している場合、次のログイン試行は失敗します。この場合は、デバイスへのアクセスを獲得するため初期化手順を使用します。詳細は、ご使用のプラットフォームのユーザーガイドを参照してください。

次の例では、**admin2005** という名前の管理者アカウントを削除して、現在のパスワードポリシーを表示します。示されているように、このポリシーは、パスワードが、最小長が 8 文字で、（少なくとも 2 つの大文字、2 つの小文字、2 つの英数字および 2 つの非英数字文字を含む）複雑さを利用したものでなければならないと指定しています。次に、**admin2006** という名前の新しい管理者アカウントを作成し、パスワードポリシーの最小長および複雑さの要件を満たすパスワードをそのアカウントに設定します。

CLI

```
unset admin admin2005
get password-policy

user-type: admin
password minimum length: 8
password complexity scheme: 1

user-type: auth
password minimum length: 8
password complexity scheme: 1

set admin admin2006 password AAbb12@#
save
```

注 : 管理者アカウントは、コマンドラインインターフェース（CLI）からしか設定できません。

ログインバナーの作成

ログインバナーのサイズは、4 キロバイトまで拡大できます。これにより、管理者および認証済みユーザーが、セキュリティデバイスおよびデバイスの背後の保護されたリソースにログインする前に表示される、使用条件のステートメントを表示するスペースができます。ログインバナーは、セキュリティデバイスで作成しそこに格納するクリアテキスト ASCII ファイルです。ファイル名は usrterms.txt としなければなりません。デバイスの再起動により、このバナーが有効になります。バナーファイルが 4 キロバイトより大きければ、セキュリティデバイスはそのファイルを受け付けません。CLI と WebUI によって入力された既存のバナーを使用し続けます。

有効になると、このログインバナーは、ルートデバイスとすべての仮想システム（vsys）によって大域的に使用されます。vsys 間または vsys 内では、異なったバナーを使用したりカスタマイズしたりできません。ログインバナーは、個々に定義された管理アクセスバナーおよびファイアウォール認証バナーより優先的に使用されます。ユーザー名とパスワードを入力したら、ユーザーは Login ボタンをクリックします。Enter キーを押しても、デバイスにログインできません。

SCP ユーティリティを使用して、セキュリティデバイスにバナーファイルを安全にコピーします。次のコマンドを使って、ユーザー名 netscreen の管理者は、バナーファイル my_large_banner.txt を IP アドレス 1.1.1.2 にあるセキュリティデバイスにコピーします。バナーファイルは、セキュリティデバイスに usrterms.txt という名前で保存する必要があります。

```
linux: ~#scp my_large_banner.txt netscreen@1.1.1.2: usrterms.txt
```

新しいバナーを有効にするには、デバイスを再起動します。バナーファイルを変更するには、新しいファイルを作成し、既存のファイルを新しいファイルで上書きします。

バナーを削除するには、セキュリティデバイスで次のコマンドを発行します。

```
device-> delete file usrterms.txt
```

デバイスを再起動した後、ログインバナー機能が無効になります。

第 2 章

セキュリティ デバイスの監視

本章では、Juniper Networks セキュリティ デバイスの監視に関する下記の項目について説明します。

- 55 ページの「ログ情報の保存」
- 57 ページの「イベントログ」
- 61 ページの「トラフィックログ」
- 66 ページの「自己ログ」
- 68 ページの「リカバリ ログのダウンロード」
- 69 ページの「トラフィック警告」
- 72 ページの「Syslog」
- 74 ページの「簡易ネットワーク管理プロトコル」
- 78 ページの「自己開始トラフィックの VPN トンネル」
- 93 ページの「Screen カウンタを参照する」

ログ情報の保存

すべての Juniper Networks セキュリティ デバイスでは、イベント ログおよびトラフィック ログのデータを内部（フラッシュ ストレージ）そして外部（多くの位置）に保存できます。ログ情報を内部に保存するのは便利ですが、デバイスのメモリーの量に制限されます。内部の保存スペースが完全に消費されると、セキュリティ デバイスは最も古いログ エントリを最新のログ エントリで上書きし始めます。ログされた情報を保存する前にこの FIFO (ファーストインファーストアウト) 機構が発生すると、データを失うことがあります。このようなデータ紛失を軽減するため、外部の syslog サーバーまたは WebTrends サーバー、あるいは NetScreen-Global PRO データベースにイベントおよびトラフィックのログを保存することができます。セキュリティ デバイスは 1 秒ごとに新しいイベント ログやトラフィック ログのエントリを外部の記憶位置に送信します。

ログされたデータを保存できる場所を以下のリストに示します。

- **コンソール :** コンソールを使用してセキュリティ デバイスのトラブルシューティングを行うときに、ログ エントリがすべて表示される保存先です。または、コンソールの使用時にアラームが稼働した場合、コンソールにアラームメッセージ (重要、警報、緊急) だけが直ちに表示されるように選択することもできます。

- **内部 :** 一定の数のログ エントリを保存することができます。

- **Email:** イベントおよびトラフィックのログをリモート管理者に送信するための方法です。

- **SNMP:** SNMP のトラップ伝送のほか、セキュリティ デバイスでイベント ログから SNMP コミュニティにアラーム メッセージ（Critical [クリティカル]、Alert [警報]、Emergency [緊急]）を送信することもできます。

- **Syslog:** セキュリティ デバイスが内部に保存できるすべてのイベント ログおよびトラフィック ログのエントリは、syslog サーバーにも送信できます。Syslog サーバーはセキュリティ デバイス上の内部フラッシュ ストレージよりもかなり容量が大きいため、データを syslog サーバーに送信すれば、ログ エントリが内部記憶スペースの上限を超える場合に生じるデータ紛失を軽減することができます。Syslog は警報レベルと緊急レベルのイベントを指定したセキュリティ機能に保存し、他の全イベント (トラフィックデータを含む) を指定した機能に保存します。

- **WebTrends:** テキストベースのツールである syslog よりもグラフィカルな形式で、重要、警報、緊急レベルのイベントに関するログデータを参照することができます。

- **CompactFlash (PCMCIA):** CompactFlash カードにデータを保存することができます。

- **USB:** USB フラッシュドライブにデータを保存することができます。ログの宛先に USB を設定すると、システムは、USB フラッシュドライブのファイルへログメッセージを送ります。ログファイルの名前は *hostname_date*.evt_log となります。ここで、*hostname* は起動時のシステムのホスト名、*date* はデバイスが最後に起動された日付になります。USB へのロギングはデフォルトでは無効になっています。**set log usb enable** CLI コマンドを使用して、USB ロギングを有効にします。

set log... destination... コマンドを使用して、すべてのログ宛先の重大度レベルを設定します。次の例では、レベルが Critical 以上のすべてのシステムモジュールメッセージを USB フラッシュドライブにロギングします。

```
set log module system level critical destination usb
```

イベントログ

ScreenOS では管理者が生成した構成の変更、および動作時の挙動や攻撃に関する自己生成のメッセージやアラームなど、システム イベントを監視するためのイベント ログを提供しています。セキュリティ デバイスでは、システム イベントは以下の重大度レベルに分類されます。

- **Emergency (緊急):** SYN 攻撃、ティアドロップ攻撃、Ping of Death 攻撃などに関するメッセージを生成します。これらの攻撃に関するさらに詳細な情報は、*第 4 部 : 攻撃の検出と防衛機能*を参照してください。
- **Alert (警報):** 即時の対応が必要な状態に関するメッセージ。たとえばファイアウォール攻撃やライセンスキーの失効など。
- **Critical (クリティカル):** デバイスの機能に影響を及ぼす可能性の高い状態に関するメッセージ。たとえば高可用性 (HA) 状況変化など。
- **Error (エラー):** デバイスの機能に影響を及ぼす可能性の高いエラー状態に関するメッセージ。たとえばアンチウィルススキャンの障害や SSH サーバーとの通信障害など。
- **Warning:** デバイスの機能に影響を及ぼす可能性がある状態に関するメッセージ。たとえば E メールサーバーへの接続障害または認証の障害、タイムアウト、および成功など。
- **Notification:** 通常のイベントに関するメッセージ。たとえば管理者によって行われる構成の変更。
- **Information (情報):** システム操作に関する一般情報を提供するメッセージです。
- **Debugging (デバッギング):** デバッギング目的に使用する詳細情報を提供するメッセージです。

イベントログには、各システムイベントの日付、時刻、レベルおよび説明が表示されます。WebUI または CLI を使用して、セキュリティ デバイスのフラッシュストレージに保存されている各カテゴリのシステム イベントを表示することができます。また、ファイルを指定した場所で開くか、あるいは保存して、ASCII テキストエディタ (メモ帳やワードパッドなど) でファイルを表示することもできます。代わりに、外部記憶スペースに送信することもできます (55 ページの「ログ情報の保存」を参照)。

注 : イベントログに表示されるメッセージの詳細は、*NetScreen Message Log Reference Guide* を参照してください。

重大度とキーワードでイベントログを参照する

CLI または WebUI を使用するとデバイスに保存されたイベントログを参照できます。WebUI と CLI の両方で、ログエントリを重大度別に表示しキーワードによりイベントログを検索することができます。

イベントログを重大度別に参照するには、以下のいずれかの方法をとってください。

WebUI

Reports > System Log > Event: Log Level ドロップダウンリストから、重大度を選択します。

CLI

get event level { emergency | alert | critical | error | warning | notification | information | debugging }

イベントログをキーワードで検索するには、以下のいずれかを行います。

WebUI

Reports > System Log > Event: 検索フィールドに単語またはフレーズを 15 文字以内で入力し、**Search** をクリックします。

CLI

get event include *word_string*

この例では重大度 "Warning" でイベントログのエントリを表示し、キーワード AV を検索します。

WebUI

Reports > System Log > Event:

Log Level: Warning (選択)

Search: **AV** を入力して、**Search** をクリックします。

CLI

get event level warning include av

日付	時刻	モジュールレベル	レベル	Type	説明
2003-05-16	15:56:20	system warn	00547	AV	scanman が削除されました。
2003-05-16	09:45:52	system warn	00547	AV	test1 が削除されました。
Total entries matched = 2					

イベントログのソーティングとフィルタリング

さらに、以下の基準に基づき、CLI を使用してイベントログのソートやフィルタを行うことができます。

- **ソースまたは宛先 IP アドレス :** ソース IP アドレスや宛先 IP アドレスは、認証、ランド攻撃や Ping フラッド攻撃など、特定のイベントにだけ含まれています。イベントログをソース IP アドレスや宛先 IP アドレスでソートすると、ソース IP アドレスや宛先 IP アドレスが含まれたイベントログだけがソートおよび表示されます。ソース IP アドレスや宛先 IP アドレスが含まれないイベントログは無視されます。認証ログメッセージには、ユーザーの IP アドレスが含まれます。

  ソース IP アドレスや宛先 IP アドレス、またはアドレスの範囲を指定してイベント ログをフィルタすると、指定されたソース IP アドレスや宛先 IP アドレス、またはアドレスの範囲のログ エントリが表示されます。

- **日付 :** 日付のみ、または日付と時刻でイベントログをソートできます。日付と時刻でログエントリをソートすると、ログエントリが日時に従って降順でリストされます。

  開始日と終了日、または日付の範囲を指定してイベントログのエントリをフィルタすることもできます。開始日を指定すると、開始日より後の日時のタイムスタンプが付いたログエントリが表示されます。終了日を指定すると、終了日より前の日時のタイムスタンプが付いたログエントリが表示されます。

- **時刻 :** 時刻でログをソートすると、ログエントリは日付に関係なく時刻に従って降順で表示されます。開始時刻を指定すると、日付に関係なく指定した開始時刻より後のタイムスタンプが付いたログエントリが表示されます。終了時刻を指定すると、日付に関係なく指定した終了時刻より前のタイムスタンプが付いたログエントリが表示されます。開始時刻と終了時刻の両方を指定すると、指定した期間内のタイムスタンプが付いたログエントリが表示されます。

- **メッセージタイプ ID 番号:** 特定のメッセージ タイプ ID 番号のイベント ログのエントリを表示したり、指定した範囲内のメッセージ タイプ ID 番号のログ エントリを表示したりできます。指定したメッセージタイプ ID 番号のログエントリが日時に従って降順で表示されます。

この例では、10.100.0.0 から 10.200.0.0 の範囲内のソース IP アドレスを含むイベントログのエントリを表示します。ログエントリはまた、ソース IP アドレスによってソートされます。

WebUI

注 : CLI を使用して、イベントログをアドレスエントリでソートする必要があります。

CLI

```
get event sort-by src-ip 10.100.0.0-10.200.0.0
```

イベントログのダウンロード

イベントログを指定した場所で開くか、あるいは保存して、ASCII テキストエディタ (メモ帳やワードパッドなど) でファイルを参照することもできます。代わりに、ログエントリを外部記憶スペースに送信することもできます (55 ページの「ログ情報の保存」を参照)。WebUI を使用してイベントログ全体をダウンロードできます。CLI を使用してイベントログを重大度別にダウンロードできます。

例 : イベント ログ全体をダウンロードする

この例では、イベントログをローカルディレクトリにダウンロードします。WebUI を使用して *C:\netscreen\logs* にダウンロードします。CLI を使用して、IP アドレス 10.1.1.5 にある TFTP サーバーのルートディレクトリにダウンロードします。ファイルには、"evnt07-02.txt" という名前をつけます。

WebUI

1. Reports > System Log > Event: **Save** をクリックします。

   File Download ダイアログボックスが、(ASCII エディタを使って) ファイルを開くか、ディスクに保存するようにプロンプトを出します。

2. **Save** オプションを選択して **OK** をクリックします。

   ファイルダウンロード ダイアログボックスが、ディレクトリを選択するようプロンプトを出します。

3. **C:\netscreen\logs** を指定し、ファイルに *evnt07-02.txt* と名前をつけ、**Save** をクリックします。

CLI

```
get event > tftp 10.1.1.5 evnt07-02.txt
```

例 : クリティカルイベントのイベントログをダウンロードする

この例では、イベント ログに入力された Critical（クリティカル）イベントを、IP アドレス 10.1.1.5 の TFTP サーバーのルート ディレクトリにダウンロードします。ファイルには、*crt_evnt07-02.txt* という名前をつけます。

WebUI

注 : CLI を使用して、重大度別にエントリをダウンロードする必要があります。

CLI

```
get event level critical > tftp 10.1.1.5 crt_evnt07-02.txt
```

トラフィックログ

Juniper Networks セキュリティ デバイスでは事前のポリシー構成に基づいて、許可または拒否されたトラフィックを監視および記録できます。構成した各ポリシーに対してロギングオプションを使用可能にできます。トラフィックを許可するポリシーのロギングオプションを使用可能にすると、そのポリシーで許可されたトラフィックが記録されます。トラフィックを拒否するポリシーのロギングオプションを使用可能にすると、デバイスの通過を試みたもののこのポリシーのために落とされたトラフィックが記録されます。

トラフィックログは、各セッションについて以下のエレメントを記録します。

- 接続開始の日時
- 継続期間
- ソースアドレスおよびポート番号
- 変換されたソースアドレスおよびポート番号
- 宛先アドレスおよびポート番号
- セッション継続時間
- セッションに使用されるサービス

セキュリティ デバイスが受信するすべてのトラフィックをログするためには、すべてのポリシーのロギング オプションを使用可能にする必要があります。特定のトラフィックをログするには、そのトラフィックに適用されるポリシーだけにロギングを使用可能します。ポリシーのロギングオプションを使用可能にするには、以下のいずれかを実行します。

WebUI

Policies > (From: *src_zone*, To: *dst_zone*) New: **Logging** を選択してから、**OK** をクリックします。

CLI

set policy from *src_zone* to *dst_zone src_addr dst_addr service action* log

ポリシーのトラフィックのロギングのほか、ポリシーが適用される全ネットワークトラフィックのバイト数のカウントを管理できます。カウンティングのオプションを使用可能にすると、トラフィックログのエントリを参照するときに以下の情報が含まれます。

- ソースから宛先へ転送されたバイト数
- 宛先からソースへ転送されたバイト数

ポリシーのカウンティングを使用可能にするには、WebUI または CLI のいずれかを使用します。

WebUI

Policies > (From: *src_zone*, To: *dst_zone*) New > Advanced: **Counting** を選択し、**Return** をクリックし、**OK** をクリックします。

CLI

set policy from *src_zone* to *dst_zone src_addr dst_addr service action* log count

トラフィックログの参照

WebUI または CLI を使って、セキュリティデバイス上のフラッシュストレージ内に保存されているトラフィックログのエントリを表示できます。

WebUI

Policies > Logging (ポリシー ID *番号*)

または

Reports > Policies > Logging (ポリシー ID *番号*)

CLI

get log traffic policy *number*

例 : トラフィックログのエントリを参照する

この例では、事前にロギングを使用可能にした ID 番号 3 のポリシーのトラフィックログの詳細を表示します。

WebUI

Policies: ID 番号 3 のポリシーの Logging アイコンをクリックします。

以下の情報が表示されます。

- 日付 / 時刻 : 2003-01-09 21:33:43
- 継続期間 : 1800 sec.
- ソース IP アドレス / ポート : 1.1.1.1:1046
- 宛先 IP アドレス / ポート : 10.1.1.5:80
- Service: HTTP
- 終了の理由 : エージアウト
- 変換ソースアドレス / ポート : 1.1.1.1:1046
- 変換宛先 IP アドレス / ポート : 10.1.1.5:80
- ポリシー ID 番号 : 3

CLI

get log traffic policy 3

トラフィックログのソーティングとフィルタリング

イベントログと同じように、CLI を使用してトラフィックログを表示すると、以下の基準に従ってログエントリをソートまたはフィルタできます。

- **ソースまたは宛先 IP アドレス** : ソース IP アドレスや宛先 IP アドレスでトラフィックログをソートできます。ソース IP アドレスや宛先 IP アドレス、またはアドレスの範囲を指定してトラフィック ログをフィルタすることもできます。

- **日付** : 日付のみ、または日付と時刻でトラフィックログをソートできます。ログエントリが日時に従って降順でリストされます。

  開始日と終了日、または日付の範囲を指定してイベントログのエントリをフィルタすることもできます。開始日を指定すると、開始日より後の日時のタイムスタンプが付いたログエントリが表示されます。終了日を指定すると、終了日より前の日時のタイムスタンプが付いたログエントリが表示されます。

- **時刻** : 時刻でトラフィックログをソートすると、ログエントリは日付に関係なく時刻に従って降順で表示されます。開始時刻を指定すると、日付に関係なく指定した開始時刻より後のタイムスタンプが付いたログエントリが表示されます。終了時刻を指定すると、日付に関係なく指定した終了時刻より前のタイムスタンプが付いたログエントリが表示されます。開始時刻と終了時刻の両方を指定すると、指定した期間内のタイムスタンプが付いたログエントリが表示されます。

例 : 時刻でトラフィックログをソーティングする

この例では、午前 1:00 より後のタイムスタンプで時刻順にソートされたトラフィックログが表示されます。

WebUI

注 : トラフィックログを時刻でソートする機能は、CLI からでのみ使用できます。

CLI

get log traffic sort-by time start-time 01:00:00

トラフィックログのダウンロード

指定した場所でファイルを開くか、保存すると、ASCII テキストエディタ (メモ帳やワードパッドなど) でもログを表示することができます。

代わりに、トラフィックログエントリを外部保存スペースに送信することもできます (55 ページの「ログ情報の保存」を参照)。セキュリティ デバイスはセッションの終了時にトラフィック ログのエントリを作成します。外部の保存場所にトラフィック ログのエントリを送信するようにセキュリティ デバイスを設定すると、1 秒ごとに新しいエントリが送信されます。セキュリティ デバイスではセッションが閉じられたときにトラフィック ログのエントリが作成されるため、過去 1 秒以内に閉じられた全セッションのトラフィック ログのエントリが送信されます。E メールで管理者に送信したイベント ログ エントリ付きのトラフック ログのエントリを含めることもできます。

この例では、ID 番号 12 のポリシーに関するトラフィックログをダウンロードします。WebUI では、ローカルディレクトリ C:\netscreen\logs にダウンロードします。CLI では、IP アドレス 10.10.20.200 の TFTP サーバーのルートディレクトリにダウンロードします。ファイルに "traf_log11-21-02.txt" と名前をつけます。

WebUI

1. Reports > Policies > Logging (ポリシー ID 12): **Save** をクリックします。

   File Download ダイアログボックスが、(ASCII エディタを使って) ファイルを開くか、ディスクに保存するようにプロンプトを出します。

2. **Save** オプションを選択して **OK** をクリックします。

   ファイルダウンロード ダイアログボックスが、ディレクトリを選択するようプロンプトを出します。

3. C:\netscreen\logs を指定し、ファイルに traf_log11-21-02.txt と名前をつけ、**Save** をクリックします。

CLI

```
get log traffic policy 12 > tftp 10.10.20.200 traf_log11-21-02.txt
```

終了の理由フィールドを削除する

デフォルトでは、ScreenOS は、セッション作成メッセージとセッション終了メッセージを区別できるように、セッション終了の理由を記録し表示します。理由を表示しない場合、フィールドを表示しないようにデバイスを明示的に設定できます。

表 1 は、ScreenOS が識別するセッション終了の理由を示しています。識別できないセッションは OTHER というラベルが付きます。

表 1: セッション終了の理由コード

ログされた理由	意味
TCP FIN	FIN パケットのために切断された TCP 接続
TCP RST	RST パケットのために切断された TCP 接続
RESP	応答が受信されると、PING や DNS のような特別なセッションは終了
ICMP	ICMP エラーを受信
AGE OUT	接続が正常にエージアウト
ALG	ALG が、エラーあるいはその ALG に特有の他の理由のために、セッション終了を強制
NSRP	NSRP セッション終了メッセージを受信
AUTH	認証の失敗
IDP	IDP が終了
SYN PROXY FAIL	SYN プロキシの異常
SYN PROXY LIMIT	SYN プロキシセッションのシステム限界に到達
TENT2NORM CONV	一時的なセッションから通常のセッションへの転換の失敗
PARENT CLOSED	親セッションが終了
CLI	ユーザーコマンドが終了
OTHER	識別できなかった終了の理由

終了の理由を示したトラフィックログの例

```
ns-> get log traffic
PID 1, from Trust to Untrust, src Any, dst Any, service ANY, action Permit
Total traffic entries matched under this policy = 2300
================================================================================
Date Time Duration Source IP Port Destination IP Port Service
Reason Xlated Src IP Port Xlated Dst IP Port ID
================================================================================
2001-10-25 07:08:51 0:00:59 10.251.10.25 137 172.24.16.10 137 NETBIOS (NS)
Close - AGE OUT 172.24.76.127 8946 172.24.16.10 137
2001-10-25 07:08:51 0:00:59 10.251.10.25 137 172.240.244.10 137 NETBIOS (NS)
Close - AGE OUT 172.24.76.127 8947 172.24.244.10 137
2001-10-25 07:07:53 0:00:01 10.251.10.25 1028 172.24.16.10 53 DNS
Close - RESP 172.24.76.127 8945 172.24.16.10 53
2001-10-25 07:06:29 0:01:00 10.251.10.25 138 172.24.244.10 138 NETBIOS (DGM)
Close - AGE OUT 172.24.76.127 8933 172.24.244.10 138
2001-10-25 07:06:11 0:03:16 10.251.10.25 2699 172.24.60.32 1357 TCP PORT 1357
Close - TCP FIN 172.24.76.127 8921 172.24.60.32 1357
```

終了の理由を示さないトラフィックログの例

```
ns-> get log traffic
PID 1, from Trust to Untrust, src Any, dst Any, service HTTP, action Permit
Total traffic entries matched under this policy = 1538
================================================================================
Date Time Duration Source IP Port Destination IP Port Service
Xlated Src IP Port Xlated Dst IP Port ID
================================================================================
2002-07-19 15:53:11 0:01:33 10.251.10.25 2712 207.17.137.108 80 HTTP
10.251.10.25 2712 207.17.137.108 80
2002-07-19 15:51:33 0:00:12 10.251.10.25 2711 66.163.175.128 80 HTTP
10.251.10.25 2711 66.163.175.128 80
2002-07-19 15:41:33 0:00:12 10.251.10.25 2688 66.163.175.128 80 HTTP
10.251.10.25 2688 66.163.175.128 80
2002-07-19 15:31:39 00:00:18 10.251.10.25 2678 66.163.175.128 80 HTTP
10.251.10.25 2678 66.163.175.128 80
```

次の例では、トラフィックログで実行したいスクリプトに干渉するので、セッション終了の理由を表示しないようにデバイスを設定します。ログ出力スタイルを変更するには、コマンドラインインターフェースを使用しなければなりません。

WebUI

使用できません。

CLI

```
set log traffic detail 0
save
```

自己ログ

ScreenOS は、セキュリティ デバイスで終了したすべてのパケットを監視および記録する自己ログを提供します。たとえば、WebUI、SNMP、および ping などのインターフェースでいくつかの管理オプションを使用不能にした場合、HTTP、SNMP、または ICMP トラフィックがそのインターフェースに送信されると、落とされた各パケットの自己ログにエントリが表示されます。

自己ログをアクティブにするには、以下のいずれかを実行します。

WebUI

Configuration > Report Settings > Log Settings: **Log Packets Terminated to Self** チェックボックスを選択して、**Apply** をクリックします。

CLI

```
set firewall log-self
```

自己ログを使用可能にすると、セキュリティ デバイスは、自己ログおよびトラフィック ログと同様に、セキュリティ デバイスで終了するドロップされた各パケットの日付、時刻、ソース アドレス / ポート、宛先アドレス / ポート、継続期間、およびサービスを表示します。自己ログのエントリには、通常の Null のソースゾーンと「self」の宛先ゾーンがあります。

自己ログの参照

CLI または WebUI により、セキュリティ デバイスのフラッシュ ストレージに保存される自己ログを表示することができます。

WebUI

Reports > System Log > Self

CLI

get log self

自己ログのソーティングとフィルタリング

イベントログやトラフィックログと同じように、CLI を使用して自己ログを表示すると、以下の基準に従ってログエントリをソートまたはフィルタできます。

- **ソースまたは宛先 IP アドレス** : ソース IP アドレスや宛先 IP アドレスで自己ログをソートできます。ソース IP アドレスや先 IP アドレス、またはアドレスの範囲を指定して自己ログをフィルタすることもできます。
- **日付** : 日付のみ、または日付と時刻で自己ログをソートできます。ログエントリが日時に従って降順でリストされます。

  開始日と終了日、または日付の範囲を指定して自己ログのエントリをフィルタすることもできます。開始日を指定すると、開始日より後の日時のタイムスタンプが付いたログエントリが表示されます。終了日を指定すると、終了日より前の日時のタイムスタンプが付いたログエントリが表示されます。
- **時刻** : 時刻で自己ログをソートすると、ログ エントリは日付に関係なく時刻に従って降順で表示されます。開始時刻を指定すると、日付に関係なく指定した開始時刻より後のタイムスタンプが付いたログエントリが表示されます。終了時刻を指定すると、日付に関係なく指定した終了時刻より前のタイムスタンプが付いたログエントリが表示されます。開始時刻と終了時刻の両方を指定すると、指定した期間内のタイムスタンプが付いたログエントリが表示されます。

例 : 自己ログを時刻でフィルタリングする

この例では、終了時刻で自己ログのエントリをフィルタします。指定された終了時刻より前のタイムスタンプのログ エントリが表示されます。

WebUI

注 : 自己ログを時刻でフィルタする機能は、CLI からでのみ使用できます。

CLI

get log self end-time 16:32:57

日付	時刻	継続期間	ソース IP	ポート	宛先 IP	ポート	サービス
2003-08-21	16:32:57	0:00:00	10.100.25.1	0	224.0.0.5	0	OSPF
2003-08-21	16:32:47	0:00:00	10.100.25.1	0	224.0.0.5	0	OSPF
Total entries matched = 2							

自己ログのダウンロード

ログをテキストファイルとして指定する場所に保存することもでき、これを参照するために ASCII テキストエディタ (Notepad または WordPad) を利用します。

この例では、自己ログをローカルディレクトリ "C:\netscreen\logs" (WebUI)、または IP アドレス 10.1.1.5 (CLI) の TFTP サーバーのルートディレクトリにダウンロードします。ファイルには、"self_log07-03-02.txt" という名前をつけます。

WebUI

1. Reports > System Log > Self: Save をクリックします。

   File Download ダイアログボックスが、(ASCII エディタを使って) ファイルを開くか、ディスクに保存するようにプロンプトを出します。

2. **Save** オプションを選択して **OK** をクリックします。

   ファイルダウンロード ダイアログボックスが、ディレクトリを選択するようプロンプトを出します。

3. C:\netscreen\logs を指定し、ファイルに self_log07-03-02.txt と名前をつけ、**Save** をクリックします。

CLI

```
get log self > tftp 10.1.1.5 self_log07-03-02.txt
```

リカバリ ログのダウンロード

Juniper Networks セキュリティ デバイスは、リカバリの手順（41 ページの「デバイスのデフォルト設定へのリセット」を参照）を使用して、デバイスがデフォルト設定に戻されるたびに、その情報を表示するリカバリ ログを提供します。WebUI や CLI からリカバリログを参照できるだけでなく、指定する場所でファイルを開くか、保存することもできます。ファイルを表示するには ASCII テキストエディタ (例 : メモ帳) を使用します。

この例では、リカバリログをローカルディレクトリ "C:\netscreen\logs" (WebUI)、または IP アドレス 10.1.1.5 (CLI) にある TFTP サーバーのルートディレクトリにダウンロードします。ファイルには "sys_rst.txt" という名前をつけます。

WebUI

1. Reports > System Log > Asset Recovery: **Save** をクリックします。

   File Download ダイアログボックスが、(ASCII エディタを使って) ファイルを開くか、ディスクに保存するようにプロンプトを出します。

2. **Save** オプションを選択して **OK** をクリックします。

   ファイルダウンロード ダイアログボックスが、ディレクトリを選択するようプロンプトを出します。

3. C:\netscreen\logs を指定し、ファイルに sys_rst.txt と名前をつけ、**Save** をクリックします。

CLI

```
get log asset-recovery > tftp 10.1.1.5 sys_rst.txt
```

トラフィック警告

セキュリティ デバイスは、トラフィックがポリシーで定義したしきい値を超えた場合のトラフィックアラームをサポートします。トラフィック アラームが発行される場合はいつでも以下の 1 つ以上の方法でアラームを出すようにセキュリティ デバイスを構成することができます。

- コンソール
- 内部 (イベントログ)
- E メール
- SNMP
- Syslog
- WebTrends
- NetScreen-Global PRO

変則的なアクティビティを検出するために、警告しきい値を設定します。何が変則的なアクティビティであるかを知るためには、まず通常のアクティビティの基準を確立する必要があります。ネットワークトラフィックに関してこうした基準を作成するためには、一定期間トラフィックパターンを観察する必要があります。通常と考えられるトラフィック量を決定したら、これ以上の量を警告しきい値として設定できます。そのしきい値を超えるトラフィックがあれば、警告をトリガーし、基準からの逸脱に注意を引きます。その時点で状態を評価し、何が逸脱の原因になったか、対策をとる必要があるかどうかを判断できます。

また、ポリシーベースの侵入検出およびシステム妥協の通知を提供するために、トラフィック警告を利用できます。この目的によるトラフィック警告の使用例は以下に示されています。

例 : ポリシーベースの侵入試行を検出する

この例では、IP アドレス 211.20.1.5 の Web サーバー（名前は “web1”）が DMZ ゾーンにあります。Telnet を介してこの Web サーバーへのアクセスする Untrust ゾーンからの進入試行を検出します。これを行うには、DMZ ゾーンにある web1 という名前の Web サーバーを宛先とする Untrust ゾーンのアドレスからの Telnet トラフィックを拒否するポリシーを作成して、トラフィックの警告しきい値を 64 バイトに設定します。IP パケットの最小サイズが 64 バイトであるため、Untrust ゾーンから Web サーバーに達する Telnet パケットがたとえ 1 つであっても、警報を起動させます。

WebUI

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: web1
IP Address/Domain Name:
IP/Netmask: (選択), 211.20.1.5/32
Zone: DMZ

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), web1
Service: Telnet
Action: Deny

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Counting: (**選択**)
Alarm Threshold: 64 Bytes/Sec, 0 Kbytes/Min

CLI

```
set address dmz web1 211.20.1.5/32
set policy from untrust to dmz any web1 telnet deny count alarm 64 0
save
```

例: システム妥協通知をする

この例では、トラフィック警告を使ってシステム妥協通知を行います。DMZ ゾーンに IP アドレスが 211.20.1.10 の、の FTP サーバー (名称が ftp1) を持っています。FTP-get traffic がこのサーバーに到達するように許可します。FTP サーバーからは一切のトラフィックを送信したくありません。このようなトラフィックの存在は、FTP サーバーからトラフィックが発信された場合、NIMDA に類似したウィルスによってシステムが妥協していることを示唆します。2 つのグローバルポリシーを作成できるように、Global ゾーンの FTP サーバーにアドレスを定義します。

WebUI

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: ftp1
IP Address/Domain Name:
IP/Netmask: (**選択**), 211.20.1.10/32
Zone: Global

Policies > (From: Global, To: Global) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), ftp1
Service: FTP-Get
Action: Permit

Policies > (From: Global, To: Global) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), ftp1

Destination Address:
Address Book Entry: (選択), Any
Service: ANY
Action: Deny

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Counting: (選択)
Alarm Threshold: 64 Bytes/Sec, 0 Kbytes/Min

CLI

```
set address global ftp1 211.20.1.10/32
set policy global any ftp1 ftp-get permit
set policy global ftp1 any deny count alarm 64 0
save
```

例 : E メール警報を送信する

この例では、アラームが発生する場合の E メール警報による通知を設定します。メール サーバーは 172.16.10.254 にあり、最初に通知される E メール アドレスは jharker@juniper.net で、2 番目のアドレスは driggs@juniper.net です。セキュリティ デバイスには、E メールを介して送信されるイベント ログ付きのトラフィック ログが含まれます。

WebUI

Configuration > Report Settings > Email: 以下を入力して **Apply** をクリックします。

Enable E-Mail Notification for Alarms: (選択)
Include Traffic Log: (選択)
SMTP Server Name: 172.16.10.254
E-Mail Address 1: jharker@juniper.net
E-Mail Address 2: driggs@juniper.net

注 : DNS を使用可能にすると、mail.juniper.net のようなホスト名をメール サーバーに使用することができます。

CLI

```
set admin mail alert
set admin mail mail-addr1 jharker@juniper.net
set admin mail mail-addr2 driggs@juniper.net
set admin mail server-name 172.16.10.254
set admin mail traffic-log
save
```

Syslog

セキュリティ デバイスでは、事前に定義される重大度レベル（重大度レベルの一覧は、57 ページの「イベントログ」を参照）でのシステム イベントに関する syslog メッセージを生成できます。また、ポリシーがファイアウォール全体で許可するトラフィックの syslog メッセージもオプションで生成できます。UNIX/Linux システムで動作する syslog ホストを最大 4 つまで指定して syslog メッセージを送信できます。各 syslog ホストには以下の内容を指定できます。

- セキュリティ デバイスにトラフィック ログのエントリとイベント ログのエントリのいずれか、またはその両方を含めるかどうか
- VPN トンネルを介して syslog サーバーにトラフィックを送信するか、また VPN トンネルを介する場合、どのインターフェースをソースインターフェースとして使用するか（例は 79 ページの「例 : ルートベースのトンネルを経由する自己生成のトラフィック」および 86 ページの「例 : ポリシーベースのトンネルを経由する自己生成のトラフィック」を参照）
- セキュリティ デバイスが syslog メッセージを送信するポート
- Emergency（緊急）レベルと Alert（警報）レベルのメッセージを分類し syslog ホストへ送信するセキュリティ機能、およびセキュリティに関係しない他のすべてのイベントのメッセージを分類し送信する通常機能

デフォルトでは、セキュリティ デバイスは UDP（ポート 514）を介して syslog ホストへメッセージを送信します。メッセージ配信の信頼性を高める場合は、各 syslog ホストのトランスポートプロトコルを TCP に変更できます。

Syslog メッセージを使用すると、システム管理者のために E メール 警報を作成したり、UNIX syslog 規則を用いる専用ホストのコンソールにメッセージを表示したりすることができます。

注 : UNIX/Linux プラットホームでは、syslog がリモートソース (syslog -r) から情報を得られるように /etc/rc.d/init.d/syslog ファイルを変更します。

例 : 複数の Syslog サーバーを使用可能にする

この例では、IP アドレスとポート番号の組み合わせが 1.1.1.1/1514、2.2.2.1/2514、および 3.3.3.1/3514 となっている 3 つの syslog サーバーに、TCP を介してイベント ログとトラフィック ログを送信するようにセキュリティ デバイスを構成します。セキュリティレベルと機能レベルは両方とも Local0 に設定します。

WebUI

Configuration > Report Settings > Syslog: 以下を入力して **Apply** をクリックします。

Enable syslog messages: このオプションを選択して指定した syslog サーバーにログを
No.: 1、2、および 3 を選択して syslog サーバーを 3 つ追加することを示します。
IP/Hostname: 1.1.1.1, 2.2.2.1, 3.3.3.1
Port: 1514, 2514, 3514

Security Facility: Local0, Local0, Local0
syslogLocal0, Local0, Local0
Event Log: (選択)
Traffic Log: (選択)
TCP: (選択)

CLI

```
set syslog config 1.1.1.1 port 1514
set syslog config 1.1.1.1 log all
set syslog config 1.1.1.1 facilities local0 local0
set syslog config 1.1.1.1 transport tcp
set syslog config 2.2.2.1 port 2514
set syslog config 2.2.2.1 log all
set syslog config 2.2.2.1 facilities local0 local0
set syslog config 2.2.2.1 transport tcp
set syslog config 3.3.3.1 port 3514
set syslog config 3.3.3.1 log all
set syslog config 3.3.3.1 facilities local0 local0
set syslog config 2.2.2.1 transport tcp
set syslog enable
save
```

WebTrends を通知イベントで有効にする

NetIQ 社製の WebTrends Firewall Suite という製品を使用すると、セキュリティ デバイスが生成するログに基づいてカスタマイズ レポートを作成できます。WebTrends はログファイルを解析し、必要な情報を画像形式で表示します。すべてのイベントや重大度のレポートを作成したり、ファイアウォール攻撃など特定の領域に重点をおくことができます。(WebTrends についての詳細は、WebTrends の説明書を参照してください。)

また、VPN トンネルを介して WebTrend メッセージを送信することもできます。WebUI では、**Use Trust Zone Interface as Source IP for VPN** オプションを使用します。CLI では、**set webtrends vpn** コマンドを使用します。

次の例では、通知メッセージを WebTrends ホスト (172.10.16.25) に送信します。

WebUI

1. **WebTrends 設定**
   Configuration > Report Settings > WebTrends: 以下を入力して **Apply** をクリックします。

   Enable WebTrends Messages: (選択)
   WebTrends Host Name/Port: 172.10.16.25/514

2. **重大度レベル**
   Configuration > Report Settings > Log Settings: 以下を入力して **Apply** をクリックします。

   WebTrends Notification: (選択)

注 : Transparent モードで稼動しているセキュリティ デバイスで WebTrends を使用可能にするときは、静的ルートを設定する必要があります。**7**-1 ページの「静的ルーティング」を参照。

CLI

3. **WebTrends 設定**
   set webtrends host-name 172.10.16.25
   set webtrends port 514
   set webtrends enable

4. **重大度レベル**
   set log module system level notification destination webtrends
   save

簡易ネットワーク管理プロトコル

Juniper Networks セキュリティ デバイスの SNMP（簡易ネットワーク管理プロトコル）エージェントは、ネットワークとそれに属するデバイスに関するデータを参照し、関係するシステム イベントの通知を受信する方法をネットワーク管理者に提供します。

Juniper Networks セキュリティ デバイスは RFC-1157、*A Simple Network Management Protocol* に記載される SNMPv1 プロトコルをサポートします。また、以下の RFC に記載される SNMPv2c プロトコルもサポートします。

- *RFC-1901*、*Introduction to Community-based SNMPv2*
- *RFC-1905*、*Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- *RFC-1906*、*Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)*

セキュリティ デバイスはまた、RFC-1213 の *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II* に記載されているすべての関連する MIB II（管理情報ベース II）グループをサポートします。デバイスには専用のエンタープライズ MIB ファイルもあり、SNMP MIB ブラウザにロードすることができます。

注： SNMP MIB ブラウザを使用すると、ScreenOS と IDP（侵入検出保護）セキュリティモジュールの両方で、CPU 使用、メモリー使用量、セッション使用回数をチェックできます。

Juniper Networks SNMP エージェントは、指定されたイベントや状況が発生すると以下のトラップや通知を生成します。

- **Cold Start Trap (コールドスタートトラップ):** セキュリティ デバイスは、電源がオンになって動作可能になるとき、コールド スタート トラップを生成します。
- **Traps for SNMP Authentication Failure (SNMP 認証失敗のトラップ):** 誰かが不正な SNMP コミュニティ文字列を使用して接続を試みた場合や、接続を試みているホストの IP アドレスが SNMP コミュニティで定義されていない場合、セキュリティ デバイスの SNMP エージェントによって認証失敗トラップが起動されます。(このオプションはデフォルトで有効になっています。)

- **システム警告トラップ:** セキュリティ デバイス エラー状態とファイアウォール状態によって、システム アラームが起動されます。ハードウェア、セキュリティ、ソフトウェアに関連したアラームのための、3 つのエンタープライズ トラップが定義されています。(ファイアウォール設定とアラームの詳細については、**4**-240 ページの「ICMP フラグメント」および 69 ページの「トラフィック警告」を参照してください。)

- **Traps for Traffic Alarms:** トラフィック警告は、トラフィックがポリシーで設定された警告のしきい値を超えた場合に動作します。(設定ポリシーの詳細については、**2**-161 ページの「ポリシー」を参照してください。)

75 ページの「トラップ アラーム タイプ」に、アラームのタイプと、関連するトラップ番号を示します。

表 2: トラップ アラーム タイプ

トラップ企業 ID	説明
100	ハードウェア問題
200	ファイアウォール問題
300	ソフトウェア問題
400	トラフィック問題
500	VPN 問題
600	NSRP 問題
800	DRP 問題
900	フェールオーバー問題
1000	ファイアウォール攻撃

注 : ネットワーク管理者が SNMP MIB II のデータを参照したり、Trusted または Untrusted のインターフェースからトラップを受信したりするには、HP OpenView や SunNet Manager のような SNMP マネージャ アプリケーションが必要です。インターネットでシェアウェアやフリーウェアの SNMP マネージャ アプリケーションが提供されています。

セキュリティ デバイスは、デフォルトでは SNMP マネージャを使うように構成されていません。SNMP 用にセキュリティ デバイスを構成するには、まずコミュニティを作成して関連するホストを定義し、許可（読取 / 書込、もしくは読取専用）を割り当てます。

SNMP コミュニティを作成するときは SNMP 管理ステーションの要件に従い、コミュニティが SNMPv1 または SNMPv2c のいずれか、あるいは両方のバージョンの SNMP をサポートするのか指定できます。(SNMPv1 のみをサポートする以前のバージョンの ScreenOS との下位互換性を保つため、セキュリティ デバイスはデフォルトで SNMPv1 をサポートしています。) SNMP コミュニティが両方のバージョンの SNMP をサポートする場合は、コミュニティメンバーごとにトラップのバージョンを指定する必要があります。

セキュリティの都合上、読取 / 書込特権を持つ SNMP コミュニティのメンバーは、セキュリティ デバイスにある以下の変数のみを変更できます。

- **sysContact** - SNMP 管理者がセキュリティ デバイスの管理者と連絡を取るための、セキュリティ デバイスの管理者の連絡先。セキュリティ管理者の名前、E メール アドレス、電話番号、オフィスの位置、またはこれらの情報の組み合わせになります。
- **sysLocation** - セキュリティ デバイスの物理的な場所。国、都市、建物の名前から NOC（ネットワーク オペレーション センター）にあるラック上のデバイスの位置に至るまで、任意の場所を指定できます。
- **sysName** - SNMP 管理者がセキュリティ デバイスで使用する名前。規則ではこの名前は FQDN（完全修飾ドメイン名）ですが、他の名前を使用することもできます。
- **snmpEnableAuthenTraps** - 誰かが不正な SNMP コミュニティ名で SNMP エージェントに接続を試みた場合にセキュリティ デバイスの SNMP エージェントがトラップを生成するかどうかを切り替えます。
- **ipDefaultTTL** - トランスポート レイヤー プロトコルによって TTL（Time-to-Live）値が与えられない場合に、セキュリティ デバイスから発信されたデータグラムの IP ヘッダーの TTL フィールドに挿入されるデフォルトの値。
- **ipForwarding** - セキュリティデバイスがトラフィックを転送するかどうかを示します（セキュリティデバイス自体を宛先とするトラフィック以外）。デフォルトでは、セキュリティ デバイスはトラフィックを転送しません。

インプリメンテーションの概要

Juniper Networks では、次の方法でデバイスに SNMP が実装されています。

- SNMP 管理者は SNMP コミュニティごとにグループ分けされています。デバイスは、3 つまでのコミュニティをサポートでき、各コミュニティには 8 つまでのメンバーを含みます。
- コミュニティメンバーは、メンバーを定義したときに使用しているネットマスクによって単一のホストまたはホストのサブネットになります。デフォルトでは SNMP コミュニティ メンバーに 32 ビットネットマスク（255.255.255.255）が割り当てられ、このネットマスクによってコミュニティ メンバーは単一のホストとして定義されます。
- SNMP コミュニティ メンバーをサブネットとして定義した場合、そのサブネットのデバイスはセキュリティ デバイスに SNMP MIB 情報をポーリングできます。ただし、セキュリティ デバイスは SNMP トラップをサブネットに送信することはできず、個別のホストにだけ送信できます。
- 各コミュニティは、MIB II データの read-only もしくは read-write 許可を持っています。
- 各コミュニティは SNMPv1 または SNMPv2c のいずれか、またはその両方をサポートできます。コミュニティが両方のバージョンの SNMP をサポートする場合は、コミュニティメンバーごとにトラップのバージョンを指定する必要があります。
- 各コミュニティのトラップの受信を許可または拒否できます。
- MIB II データおよびトラップには、どの物理インターフェースからもアクセスできます。
- 各システム警告（Critical [クリティカル]、Alert [警報]、Emergency [緊急] の重大度で分類されたシステム イベント）は、トラップを受信するように設

定された各コミュニティの各ホストに 1 つのエンタープライズ SNMP トラップを生成します。

- コールド スタート / リンク アップ / リンク ダウンのトラップは、トラップを受信するように設定されたコミュニティ内のすべてのホストに送信されます。
- コミュニティにトラップオンを指定する場合には、トラフィック警告を許可するというオプションがあります。
- ルートベースまたはポリシーベースの VPN トンネルを介して SNMP メッセージを送信することができます。詳細については、78 ページの「自己開始トラフィックの VPN トンネル」を参照してください。

読取 / 書込 SNMP コミュニティを定義する

この例では、*MAge11 という SNMP コミュニティを作成します。*このコミュニティに読取 / 書込権限を割り当て、メンバーが MIB II データとトラップを受信できるようにします。コミュニティには 1.1.1.5/32 および 1.1.1.6/32 という 2 つのメンバーが含まれます。それぞれのメンバーには SNMP マネージャアプリケーションがあり、異なるバージョンの SNMP、すなわち SNMPv1 と SNMPv2c が実行されています。コミュニティ名はパスワードとして機能するため、保護する必要があります。

SNMP コミュニティメンバーがセキュリティデバイスのローカル管理者と連絡を取れるように、セキュリティデバイスの管理者の連絡先を al_baker@mage.com と指定します。セキュリティ デバイスの場所も 3-15-2 として指定します。この番号はデバイスが 3 階の 15 番目の列にあり、その列の 2 番目の位置にあることを示しています。

誰かがセキュリティ デバイスへの不正な SNMP 接続を試みた場合に SNMP エージェントがトラップを生成するのを使用可能に設定することもできます。認証失敗トラップは全 SNMP コミュニティに適用されるグローバル設定で、デフォルトでは使用不可に設定されています。

最後に、以前に Trust ゾーンにバインドしたインターフェースである ethernet1 の SNMP 管理容易性を使用可能にします。これが、SNMP マネージャ アプリケーションがセキュリティ デバイスの SNMP エージェントと通信するインターフェースになります。

WebUI

Configuration > Report Settings > SNMP: 以下を入力して **Apply** をクリックします。

System Contact: al_baker@mage.com
Location: 3-15-2
Enable Authentication Fail Trap: (選択)

Configuration > Report Settings > SNMP > New Community: 次のように入力してから **OK** をクリックします。

Community Name: MAge11
Permissions:
Write: (選択)
Trap: (選択)
Including Traffic Alarms: (オフ)

Version: ANY (選択)
Hosts IP Address/Netmask and Trap Version:
1.1.1.5/32 v1
1.1.1.6/32 v2c

Network > Interfaces > Edit (ethernet1): 次のように入力してから **OK** をクリックします。

Service Options:
Management Services: SNMP

CLI

```
set snmp contact al_baker@mage.com
set snmp location 3-15-2
set snmp auth-trap enable
set snmp community MAge11 read-write trap-on version any
set snmp host Mage 1.1.1.5/32 trap v1
set snmp host Mage 1.1.1.6/32 trap v2
set interface ethernet1 manage snmp
save
```

自己開始トラフィックの VPN トンネル

VPN（仮想プライベート ネットワーク）トンネルを利用して、固定 IP アドレスからのセキュリティ デバイスのリモート監視を保護することができます。VPN トンネルを利用することで、セキュリティ デバイス宛のトラフィックやセキュリティ デバイスから開始されるトラフィックを保護できます。セキュリティ デバイスから開始されるトラフィックのタイプには、NetScreen-Global PRO レポート、syslog サーバーおよび WebTrends サーバーに送信されるイベント ログのエントリ、および SNMP MIB トラップなどがあります。

Juniper Networks セキュリティ デバイスは、2 種類の VPN トンネル構成をサポートしています。

- **ルーティングベース VPN**: セキュリティ デバイスはルートテーブルのエントリを使用してトラフィックをトンネル インターフェースに導きます。トンネル インターフェースは VPN トンネルにバインドされています。

  ルートベースの VPN トンネルを経由してセキュリティ デバイスによって生成されたイベント ログのエントリ、NetScreen-Global PRO レポート、または SNMP トラップなどのトラフィックを送信するには適切な宛先へのルートを手動で入力しなければなりません。ルートは、セキュリティ デバイスがトラフィックを経由させる VPN トンネルにバインドされたトンネル インターフェースを指し示す必要があります。ポリシーは不要です。

- **ポリシーベース VPN**: セキュリティ デバイスは、ポリシーで具体的に参照された VPN トンネル名を使用してトラフィックが VPN トンネルを経由するようにします。

  ポリシーベースの VPN トンネルを経由して自己開始トラフィックを送信するには、ポリシーにソースアドレスと宛先アドレスを含める必要があります。ソース アドレスにはセキュリティ デバイスのインターフェースの IP アドレスを使用します。ストレージ サーバーや SNMP コミュニティ メンバーのワークステーションがリモート セキュリティ デバイスの背後に位置している場合、その IP アドレスを宛先アドレスに使用します。リモート SNMP

コミュニティ メンバーがローカル セキュリティ デバイスへの VPN 接続を確立するために NetScreen-Remote VPN クライアントを使用している場合は、NetScreen-Remote で定義された内部 IP アドレスを宛先アドレスとして使用します。

リモート ゲートウェイまたはエンド エンティティのいずれかが動的に割り当てられた IP アドレスを持つ場合、動的なアドレスはあらかじめ決定できずそれらのアドレスへのルートを定義できないため、セキュリティ デバイスは VPN トンネルの作成を開始できません。このような場合、リモートホストが VPN 接続を開始する必要があります。ポリシーベースまたはルートベースの VPN トンネルが確立された後、ポリシーで許可されている場合はトンネルの両端からトラフィックを開始できます。また、ルートベース VPN の場合は VPN トンネルへバインドされたトンネル インターフェースを経由するエンド エンティティへのルートが必ず存在するはずです。この理由はルートを手動で入力したからか、トンネルが確立された後、動的ルーティング メッセージの交換を介してローカル セキュリティ デバイスがルートを受信したためです。(動的ルーティング プロトコルの詳細については、*第 7 部: ルーティング*を参照してください。) トンネルが確立されたら VPN アクティビティと無関係に持続するように、再入力オプションが付いた VPN 監視や IKE ハートビート を使用することもできます。(これらのオプションの詳細については、**5**-243 ページの「VPN の監視」および **5**-296 ページの「監視機構」を参照してください。)

VPN トンネルの構成タイプごとに以下のタイプの VPN トンネルを使用できます。

- **手動鍵** : SA (Security Association) をトンネルの両端で確立する 3 つの要素— SPI (セキュリティパラメータインデックス)、暗号化鍵、および認証鍵は手動で設定します。また、これら SA の要素を変更する場合には、トンネルの両端で手動でその設定を変更する必要があります。

- **AutoKey IKE と事前共有鍵** : 1 つまたは 2 つの事前共有 (認証用と暗号化用) は、シード値として機能します。それらを用い、IKE プロトコルはトンネルの両端で対称鍵を生成します。つまり同じ鍵が暗号化と復号に使用されます。また、これらの鍵は、あらかじめ設定された間隔で、自動的に再生成されます。

- **証明書付き AutoKey IKE**: PKI (公開鍵暗号基盤) では、デジタル証明書 (認証用) と RSA 公開 / 秘密鍵ペア (暗号化用) を使用します。また、暗号化鍵は非対称あり、ペアの 1 つの鍵は暗号化に、もう 1 つは復号に使用されます。

注 : VPN トンネルの詳細については、*第 5 部: 仮想プライベート ネットワーク*を参照してください。NetScreen-Remote の詳細については、*NetScreen-Remote VPN Client Administrator Guide* を参照してください。

例 : ルートベースのトンネルを経由する自己生成のトラフィック

図 16 の例では、ローカル セキュリティ デバイス (デバイス A) を構成し、ルートベースの AutoKey IKE VPN トンネルを経由してリモート セキュリティ デバイス (デバイス B) の背後にある SNMP コミュニティ メンバーに SNMPv1 MIB トラップと syslog レポートを送信します。このトンネルは、データ発信元認証に事前共有鍵 (Ci5y0a1aAG) を使用し、フェーズ 1 とフェーズ 2 の両方の

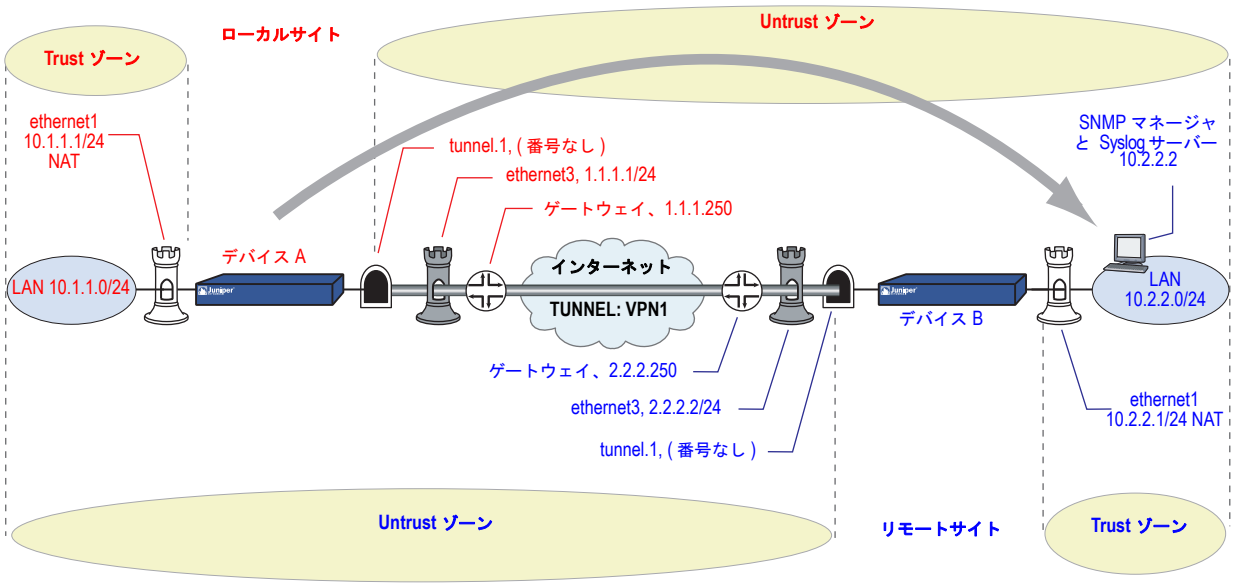
プロポーザルに関して “Compatible” と事前に定義されたセキュリティレベルを使用します。デバイス A のローカル管理者として tunnel.1 インターフェースを作成し、vpn1 にバインドします。デバイス B の管理者と共に、表 3 に示すプロキシ ID を定義します。

表 3: ルートベースのトンネルのプロキシ ID

デバイス A		デバイス B	
ローカル IP	10.1.1.1/32	ローカル IP	10.2.2.2/32
リモート IP	10.2.2.2/32	リモート IP	10.1.1.1/32
Service	Any	Service	Any

Trust ゾーンに ethernet1 をバインドし、Untrust ゾーンに ethernet3 をバインドします。デフォルトゲートウェイの IP アドレスは 1.1.1.250 です。すべてのゾーンは、trust-vr ルーティングドメインにあります。

図 16: ルートベースのトンネルを経由するトラフィック



デバイス B のリモート管理者は同様の設定を使用してデバイス B 側の AutoKey IKE VPN トンネルを定義し、事前共有鍵、プロポーザル、およびプロキシ ID が一致するようにします。

また、"remote_admin" という名前の読取 / 書込権限を持った SNMP コミュニティを構成し、コミュニティによるトラップの受信を有効にします。10.2.2.2/32 のホストをコミュニティメンバーとして定義します。

注： この例では、リモート管理者はすでに syslog サーバーと SNMPv1 をサポートする SNMP マネージャーアプリケーションを設定したと仮定します。リモート管理者が自分のセキュリティ デバイスに VPN トンネルを設定する場合は、1.1.1.1 をリモート ゲートウェイとして使用し、10.1.1.1 を宛先アドレスとして使用します。

WebUI (デバイス A)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT (選択)

注 : デフォルトでは、Trust ゾーンにバインドされたどのインターフェースも NAT モードになっています。そのため、Trust ゾーンにバインドされたインターフェースではこのオプションはすでに有効にしています。

リモート管理者が SNMP マネージャを構成する際には、**10.1.1.1** を Remote SNMP Agent フィールドに入力する必要があります。これは、SNMP マネージャがクエリを送信するアドレスになります。

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24
Service Options:
Management Services: SNMP

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (選択)
Interface: ethernet1(trust-vr)

2. Syslog と SNMP

Configuration > Report Settings > Syslog: 以下を入力して **Apply** をクリックします。

Enable Syslog Messages: (選択)
No.: 1 を選択して syslog サーバーを 1 つ追加することを示します。
IP / Hostname: 10.2.2.2
Port: 514
Security Facility: auth/sec
Facility: Local0

Configuration > Report Settings > SNMP > New Community: 次のように入力してから **OK** をクリックします。

Community Name: remote_admin
Permissions:
Write: (選択)
Trap: (選択)

Including Traffic Alarms: (オフ)
Version: V1
Hosts IP Address/Netmask:
10.2.2.2/32 V1
Trap Version:
V1

3. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: to_admin
Type: Static IP, Address/Hostname: 2.2.2.2
Preshared Key: Ci5y0a1aAG
Security Level: Compatible
Outgoing interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface: (選択する), tunnel.1
Proxy-ID: (選択)
Local IP/Netmask: 10.1.1.1/32
Remote IP/Netmask: 10.2.2.2/32
Service: ANY

4. ルート

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.2.2.2/32
Gateway: (選択)
Interface: tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: (選択), 1.1.1.250

CLI (デバイス A)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 manage snmp
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet1
```

注 : リモート管理者が SNMP マネージャを構成するときは、**10.1.1.1** を Remote SNMP Agent フィールドに入力する必要があります。これは、SNMP マネージャがクエリを送信するアドレスになります。

デフォルトでは、Trust ゾーンにバインドされたインターフェースは NAT モードになっています。そのため、Trust ゾーンにバインドされたインターフェースではこのオプションはすでに有効にしています。

2. VPN

```
set ike gateway to_admin address 2.2.2.2 outgoing-interface ethernet3 preshare
    Ci5y0a1aAG sec-level compatible
set vpn vpn1 gateway to_admin sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 10.1.1.1/32 remote-ip 10.2.2.2/32 any
```

3. Syslog と SNMP

```
set syslog config 10.2.2.2 auth/sec local0
set syslog enable
set snmp community remote_admin read-write trap-on version v1
set snmp host remote_admin 10.2.2.2/32
```

4. ルート

```
set vrouter trust-vr route 10.2.2.2/32 interface tunnel.1
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
save
```

WebUI (デバイス B)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.2.2.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (選択)
Interface: ethernet1(trust-vr)

2. アドレス

Policy > Policy Elements > Addresses > Lists > New: 次のように入力してから **OK** をクリックします。

Address Name: addr1
IP Address/Domain Name: IP/Netmask: 10.2.2.2/32
Zone: Trust

Policy > Policy Elements > Addresses > Lists > New: 次のように入力してから **OK** をクリックします。

Address Name: ns-a
IP Address/Domain Name: IP/Netmask: 10.1.1.1/32
Zone: Untrust

3. サービスグループ

Policy > Policy Elements > Services > Groups > New: 以下のグループ名を入力して、以下のサービスを移動し、**OK** をクリックします。

Group Name: s-grp1

Syslog を選択し、< < ボタンを使用して、Available Members 列から Group Members 列にサービスを移動します。

SNMP を選択し、< < ボタンを使用して、Available Members 列から Group Members 列にサービスを移動します。

4. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: to_admin
Type: Static IP, Address/Hostname: 1.1.1.1
Preshared Key: Ci5y0a1aAG
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface: (選択する), tunnel.1
Proxy-ID: (選択)
Local IP/Netmask: 10.2.2.2/32
Remote IP/Netmask: 10.1.1.1/32
Service: Any

5. ルート

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.1/32
Gateway: (選択)
Interface: tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: (選択) 2.2.2.250

6. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), addr1
Destination Address:
Address Book Entry: (選択) ns-a
Service: s-grp1
Action: Permit
Position at Top: (選択)

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), ns-a
Destination Address:
Address Book Entry: (選択), addr1
Service: s-grp1
Action: Permit
Position at Top: (選択)

CLI (デバイス B)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet1
```

2. アドレス

```
set address trust addr1 10.2.2.2/32
set address untrust ns-a 10.1.1.1/32
```

3. サービスグループ

```
set group service s-grp1
set group service s-grp1 add syslog
set group service s-grp1 add snmp
```

4. VPN

```
set ike gateway to_admin address 1.1.1.1 outgoing-interface ethernet3 preshare
    Ci5y0a1aAG sec-level compatible
set vpn vpn1 gateway to_admin sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 10.2.2.2/32 remote-ip 10.1.1.1/32 any
```

5. **ルート**
   set vrouter trust-vr route 10.1.1.1/32 interface tunnel.1
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250

6. **ポリシー**
   set policy top from trust to untrust addr1 ns-a s-grp1 permit
   set policy top from untrust to trust ns-a addr1 s-grp1 permit
   save

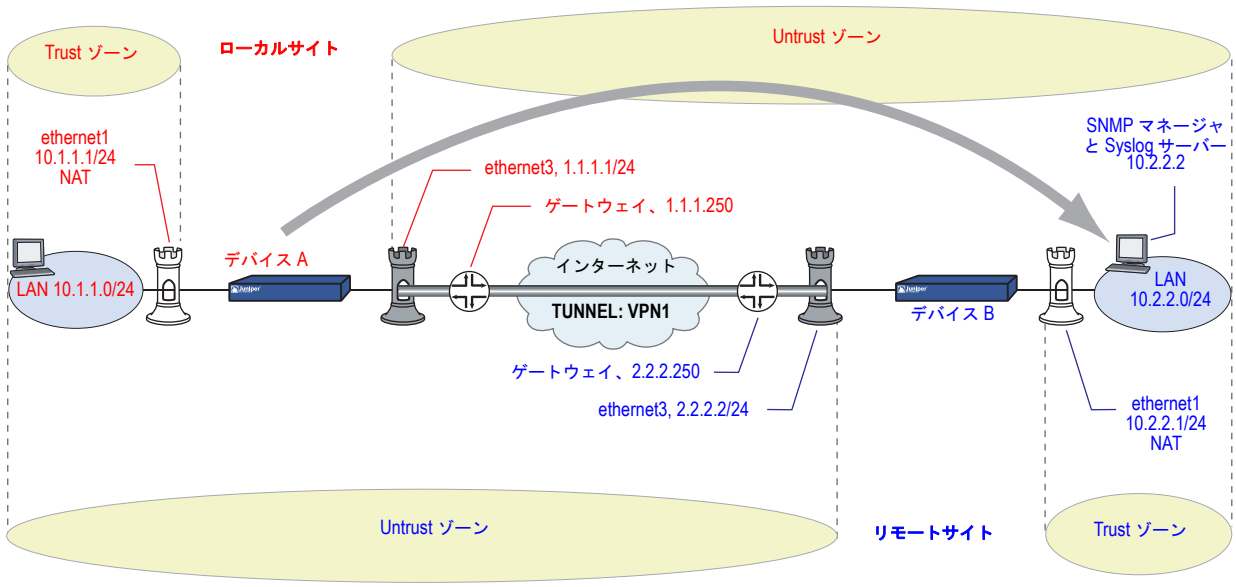
例: ポリシーベースのトンネルを経由する自己生成のトラフィック

図 17 の例では、ローカル セキュリティ デバイス（デバイス A）を構成し、ポリシーベースの AutoKey IKE VPN トンネル（vpn1）を経由してリモート セキュリティ デバイス（デバイス B）の背後にある SNMP コミュニティ メンバーに SNMPv2c MIB トラップと syslog レポートを送信します。このトンネルは、データ発信元の認証に事前共有鍵 (Ci5y0a1aAG) を使用し、フェーズ 1 およびフェーズ 2 の両方の提案には「Compatible (互換)」として定義済みのセキュリティレベルを使用します。

注： この例では、リモート管理者はすでに syslog サーバーと SNMPv2c をサポートする SNMP マネージャーアプリケーションを設定したと仮定します。リモート管理者が自分のセキュリティ デバイスに VPN トンネルを設定する場合は、1.1.1.1 をリモート ゲートウェイとして使用し、10.1.1.1 を宛先アドレスとして使用します。

ローカル管理者とリモート管理者の両方がデバイス A とデバイス B の Trust ゾーンに ethernet1 をバインドし、Untrust ゾーンに ethernet3 をバインドします。デバイス A のデフォルト ゲートウェイの IP アドレスは 1.1.1.250 です。デバイス B のデフォルト ゲートウェイの IP アドレスは 2.2.2.250 です。すべてのゾーンは、trust-vr ルーティング ドメインにあります。

図 17: ポリシーベースのトンネルを経由するトラフィック



また、“remote_admin” という名前の読取 / 書込権限を持った SNMP コミュニティを構成し、コミュニティによるトラップの受信を有効にします。10.2.2.2/32 のホストをコミュニティメンバーとして定義します。

デバイス A のインバウンドおよびアウトバウンドのポリシーはデバイス B のアウトバウンドおよびインバウンドのポリシーに一致します。ポリシーに使用されるアドレスとサービスは以下のとおりです。

- デバイス A の Trust ゾーン インターフェースのアドレス（10.1.1.1/32）
- SNMP コミュニティメンバーおよび syslog サーバーのホストのアドレス
- SNMP サービスと syslog サービスを含む“s-grp1”という名前が付いたサービスグループ

ローカル管理者とデバイス B のリモート管理者が作成したポリシーから、両方のセキュリティ デバイスは以下のように vpn1 用のプロキシ ID を導き出します。

表 4: ポリシーベースのトンネルのプロキシ ID

デバイス A		デバイス B	
ローカル IP	10.1.1.1/32	ローカル IP	10.2.2.2/32
リモート IP	10.2.2.2/32	リモート IP	10.1.1.1/32
Service	Any	Service	Any

注 : セキュリティデバイスはプロキシ ID 内でサービスグループを “any” として扱います。

WebUI (デバイス A)

1. **Interfaces ー Security Zones**
   Network > Interfaces > Edit (ethernet1): 次のように入力してから **OK** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24

   次のように選択してから **OK** をクリックします。

   Interface Mode: NAT (選択)

注 : リモート管理者が SNMP マネージャを構成するときは、**10.1.1.1** を Remote SNMP Agent フィールドに入力する必要があります。これは、SNMP マネージャがクエリを送信するアドレスになります。

デフォルトでは、Trust ゾーンにバインドされたインターフェースは NAT モードになっています。そのため、Trust ゾーンにバインドされたインターフェースではこのオプションはすでに有効にしています。

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24
Service Options:
Management Services: SNMP

2. アドレス

Policy > Policy Elements > Addresses > Lists > New: 次のように入力してから **OK** をクリックします。

Address Name: trust_int
IP Address/Domain Name:
IP/Netmask: 10.1.1.1/32
Zone: Trust

Policy > Policy Elements > Addresses > Lists > New: 次のように入力してから **OK** をクリックします。

Address Name: remote_admin
IP Address/Domain Name:
IP/Netmask: 10.2.2.2/32
Zone: Untrust

3. サービスグループ

Policy > Policy Elements > Services > Groups > New: 以下のグループ名を入力して、以下のサービスを移動し、**OK** をクリックします。

Group Name: s-grp1
Syslog を選択し、< < ボタンを使用して、Available Members 列から Group Members 列にサービスを移動します。

SNMP を選択し、< < ボタンを使用して、Available Members 列から Group Members 列にサービスを移動します。

4. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: to_admin
Type: Static IP, Address/Hostname: 2.2.2.2
Preshared Key: Ci5y0a1aAG
Security Level: Compatible
Outgoing Interface: ethernet3

5. Syslog と SNMP

Configuration > Report Settings > Syslog: 以下を入力して **Apply** をクリックします。

Enable Syslog Messages: (選択)
Source Interface: ethernet1
No.: 1 を選択して syslog サーバーを 1 つ追加することを示します。
IP/Hostname: 10.2.2.2

Port: 514
Security Facility: auth/sec
Facility: Local0

Configuration > Report Settings > SNMP > New Community: 次のように入力してから **OK** をクリックします。

Community Name: remote_admin
Permissions:
Write: (選択)
Trap: (選択)
Including Traffic Alarms: (オフ)
Version: V2C
Hosts IP Address/Netmask:
10.2.2.2/32 V2C
Trap Version:
V2C
Source Interface:
ethernet1 (選択)

Configuration > Report Settings > SNMP: 以下を入力して **Apply** をクリックします。

Enable Authentication Fail Trap: (選択)

6. ルート

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

7. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), trust_int
Destination Address:
Address Book Entry: (選択), remote_admin
Service: s-grp1
Action: Tunnel
Tunnel VPN: vpn1
Modify matching outgoing VPN policy: (選択)
Position at Top: (選択)

CLI (デバイス A)

1. Interfaces — Security Zones

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 manage snmp
```

注： デフォルトでは、Trust ゾーンにバインドされたどのインターフェースも NAT モードになっています。そのため、Trust ゾーンにバインドされたインターフェースではこのオプションはすでに有効にしています。

2. アドレス

```
set address trust trust_int 10.1.1.1/32
set address untrust remote_admin 10.2.2.2/32
```

3. サービスグループ

```
set group service s-grp1
set group service s-grp1 add syslog
set group service s-grp1 add snmp
```

4. VPN

```
set ike gateway to_admin address 2.2.2.2 outgoing-interface ethernet3 preshare
    Ci5y0a1aAG sec-level compatible
set vpn vpn1 gateway to_admin sec-level compatible
```

5. Syslog と SNMP

```
set syslog config 10.2.2.2 auth/sec local0
set syslog src-interface ethernet1
set syslog enable
set snmp community remote_admin read-write trap-on version v2c
set snmp host remote_admin 10.2.2.2/32 src-interface ethernet1
```

6. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

7. ポリシー

```
set policy top from trust to untrust trust_int remote_admin s-grp1 tunnel vpn vpn1
set policy top from untrust to trust remote_admin trust_int s-grp1 tunnel vpn vpn1
save
```

WebUI (デバイス B)

1. Interfaces ー Security Zones

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.2.2.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 2.2.2.2/24

2. アドレス

Policy > Policy Elements > Addresses > Lists > New: 次のように入力してから **OK** をクリックします。

Address Name: addr1
IP Address/Domain Name:
IP/Netmask: 10.2.2.2/32
Zone: Trust

Policy > Policy Elements > Addresses > Lists > New: 次のように入力してから **OK** をクリックします。

Address Name: ns-a
IP Address/Domain Name:
IP/Netmask: 10.1.1.1/32
Zone: Untrust

3. サービスグループ

Policy > Policy Elements > Services > Group: 以下のグループ名を入力して、以下のサービスを移動し、**OK** をクリックします。

Group Name: s-grp1

Syslog を選択し、< < ボタンを使用して、Available Members 列から Group Members 列にサービスを移動します。

SNMP を選択し、< < ボタンを使用して、Available Members 列から Group Members 列にサービスを移動します。

4. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: to_admin
Type: Static IP, IP Address: 1.1.1.1
Preshared Key: Ci5y0a1aAG
Security Level: Compatible
Outgoing interface: ethernet3

5. ルート

Network > Routing > Routing Table > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: (選択) 2.2.2.250

6. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), addr1
Destination Address:

Address Book Entry: (選択), ns-a
Service: s-grp1
Action: Tunnel
Tunnel VPN: vpn1
Modify matching outgoing VPN policy: (選択)
Position at Top: (選択)

CLI (デバイス B)

1. **Interfaces ー Security Zones**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.2.2.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 2.2.2.2/24

2. **アドレス**
   set address trust addr1 10.2.2.2/32
   set address untrust ns-a 10.1.1.1/32

3. **サービスグループ**
   set group service s-grp1
   set group service s-grp1 add syslog
   set group service s-grp1 add snmp

4. **VPN**
   set ike gateway to_admin address 1.1.1.1 outgoing-interface ethernet3 preshare Ci5y0a1sec-level compatible
   set vpn vpn1 gateway to_admin sec-level compatible

5. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250

6. **ポリシー**
   set policy top from trust to untrust addr1 ns-a s-grp1 tunnel vpn vpn1
   set policy top from untrust to trust ns-a addr1 s-grp1 tunnel vpn vpn1
   save

Screen カウンタを参照する

Juniper Networks セキュリティ デバイスはトラフィック監視のために、画面、ハードウェア、およびフロー カウンタを提供します。カウンターは特定のゾーンやインターフェースの処理情報を表示し、必要とするポリシーの構成を確認する手助けをします。

表 5 は、一般的なファイアウォールの振る舞いを監視するため、そして特定のポリシーに影響されたトラフィック量を表示するための Screen カウンタを表しています。

表 5: Screen カウンタ

カウンタ	説明
Bad IP Option Protection	不正もしくは不完全な IP オプションが原因で廃棄されたフレーム数
Dst IP-based session limiting	セッションしきい値に達した後でドロップされたセッション数
FIN bit with no ACK bit	違法なフラグの組み合わせが検出されドロップされたパケット数
Fragmented packet protection	ブロックされた IP パケット フラグメント数
HTTP Component Blocked	HTTP コンポーネントが含まれブロックされたパケット数
HTTP Component Blocking for ActiveX controls	ブロックされた ActiveX コンポーネント数
HTTP Component Blocking for .exe files	.exe ファイルが含まれブロックされた HTTP パケット数
HTTP Component Blocking for Java applets	ブロックされた Java コンポーネント数
HTTP Component Blocking for .zip files	.zip ファイルが含まれブロックされた HTTP パケット数
ICMP Flood Protection	ICMP フラッドの一部としてブロックされた ICMP パケット数
ICMP Fragment	More Fragments フラグが設定されているか、またはオフセット フィールドにオフセットが示されている ICMP フレーム数
IP Spoofing Attack Protection	IP スプーフィング攻撃の一部としてブロックされた IP アドレス数
IP Sweep Protection	検出されブロックされた IP スイープ攻撃パケット数
Land Attack Protection	Land アタックの疑いがあり、その一部としてブロックされたパケット数
Large ICMP Packet	1024 を超える IP 長が検出された ICMP フレーム数
Limit Session	セッションの制限に達したために送信できなかったパケット数
Loose Src Route IP Option	Loose Source Route オプションが使用可能になっていることが検出された IP パケット数
Malicious URL Protection	悪意があると疑われてブロックされた URL 数
Ping-of-Death Protection	サイズ超過または不正なサイズの疑いがあり拒否された ICMP パケット数
Port Scan Protection	検出されブロックされたポート スキャン数
Record Route IP Option	Record Route オプションが使用可能なことが検出されたフレーム数
Security IP Option	IP Security オプションが設定されているために廃棄されたフレーム数
Src IP-based session limiting	セッションしきい値に達した後でドロップされたセッション数
Source Route IP Option Filter	フィルタされた IP ソース ルート数
Stream IP Option	IP Stream 識別子が設定されているために廃棄されたパケット数
Strict Src Route IP Option	Strict Source Route オプションが使用可能なことが検出されたパケット数

カウンタ	説明
SYN-ACK-ACK-Proxy DoS	SYN-ACK-ACK-proxy DoS SCREEN オプションのためにブロックされたパケット数
SYN and FIN bits set	違法なフラグの組み合わせが検出されたパケット数
SYN Flood Protection	SYN フラッドの疑いがあり、その一部として検出された SYN パケット数
SYN Fragment Detection	SYN フラグメント攻撃の疑いがあり、その一部としてドロップされたパケット フラグメント数
Timestamp IP Option	Internet Timestamp オプションが設定されているために廃棄された IP パケット数
TCP Packet without Flag	フラグ フィールドが欠落しているか不正なためにドロップされた違法パケット数
Teardrop Attack Protection	ティアドロップ攻撃の一部としてブロックされたパケット数
UDP Flood Protection	UDP フラッドの疑いがあり、その一部としてドロップされた UDP パケット数
Unknown Protocol Protection	未知のプロトコルの一部としてブロックされたパケット数
WinNuke Attack Protection	WinNuke 攻撃の疑いがあり、その一部として検出されたパケット数

94 ページの表 6 は、ハードウェアの性能とエラーのあるパケットを監視するハードウェア カウンタを示しています。

表 6: ハードウェアカウンタ

カウンタ	説明
drop vlan	VLAN タグの欠落、未定義のサブインターフェース、もしくはセキュリティ デバイスが Transparent モードのときに VLAN トランキングが使用可能になっていなかったことが原因でドロップされたパケット数
early frame	イーサネット ドライバ バッファ記述子の管理に使用されるカウンタ数
in align err	ビット ストリームにアライメント エラーがあった受信パケット数
in bytes	受信したバイト数
in coll err	受信した衝突パケット数
in crc err	CRS（巡回冗長検査）エラーがあった受信パケット数
in dma err	DMA（ダイレクト メモリー アクセス）エラーがあった受信パケット数
in misc err	その他のエラーがある受信パケット数
in no buffer	バッファの空き容量がないため、受信されなかったパケット数
in overrun	転送されたオーバーラン パケット数
in packets	受信したパケット数
in short frame	64 バイトより短いイーサネット フレームの受信パケット数（フレーム チェックサムを含む）
in underrun	転送されたアンダーラン パケット数
late frame	イーサネット ドライバ バッファ記述子の管理に使用されるカウンタ数
out bs pak	未知の MAC アドレスを検索中に、バック ストアに保留されたパケット数 セキュリティ デバイスはパケットを転送する場合、まず ARP テーブルに宛先 MAC アドレスがあるかどうかをチェックします。ARP テーブルで宛先 Mac アドレスが見つからない場合には、ネットワークに ARP 要求を送信します。セキュリティ デバイスは、最初の ARP 要求に対する応答を受信する前に同じ宛先 MAC アドレスを持つ別のパケットを受信すると、out bs pak カウンタを 1 つ増やします。

カウンタ	説明
out bytes	送信したバイト数
out coll err	送信した衝突パケット数
out cs lost	CSMA/CD（キャリア センス多重アクセス / 衝突検出）プロトコルが信号を失ったためにドロップされた送信パケット数
out defer	据え置きされた送信パケット数
out discard	廃棄された送信パケット数
out heartbeat	送信したハートビート パケット数
out misc err	その他のエラーがある送信パケット数
out no buffer	バッファの空き容量がないため、送信されなかったパケット数
out packets	送信したパケット数
re xmt limit	インターフェースが半二重で動作中に、再送信制限を超過したためにドロップされたパケット数

95 ページの表 7 は、フロー レベルで検査されるパケット数を監視するフロー カウンタを示しています。

表 7: フローカウンタ

カウンタ	説明
address spoof	アドレス スプーフィング攻撃が疑われる受信パケット数
auth deny	ユーザー認証が拒否された回数
auth fail	ユーザー認証に失敗した回数
big bkstr	MAC-to-IP アドレス解決の待機中に ARP バック ストアのバッファに入れるには大きすぎるパケットの数
connections	前回のブート時以降に確立したセッション数
encrypt fail	失敗したポイントツーポイントトネリングプロトコル (PPTP) パケットの数
*icmp broadcast	受信した ICMP ブロードキャスト数
icmp flood	ICMP フラッドしきい値に対してカウントされた ICMP パケット数
illegal pak	プロトコル標準に準拠していないためにドロップされたパケット数
in arp req	受信した ARP 要求パケット数
in arp resp	送信した ARP 要求パケット数
in bytes	受信したバイト数
in icmp	受信した ICMP（インターネット制御メッセージ プロトコル）パケット数
in other	異なるイーサネット タイプの受信パケット数
in packets	受信したパケット数
in self	管理 IP アドレスを宛先としたパケット数
*in un auth	許可されていない受信 TCP、UDP、および ICMP パケット数
*in unk prot	未知のイーサネット プロトコルを使用する受信パケット数
in vlan	受信した VLAN パケット数
in vpn	受信した IPSec パケット数
invalid zone	無効なセキュリティ ゾーンを宛先としたパケット数
ip sweep	指定された IP スイープしきい値を超えたために、受信して廃棄されたパケット数
land attack	Land アタックが疑われる受信パケット数

カウンタ	説明
loopback drop	セキュリティ デバイスを経由してループバックできないためにドロップされたパケットの数。ループバックセッションの例として、Trust ゾーンにあるサーバーにマッピングされた MIP アドレスまたは VIP アドレスにそれ自体も Trust ゾーンにあるホストがトラフィックを送信する場合があります。セキュリティ デバイスはループバック セッションを作成し、このようなトラフィックをホストから MIP サーバーや VIP サーバーに導きます。
mac relearn	MAC アドレスの場所が変更されたために、その MAC アドレスと関連付けられたインターフェースを MAC アドレス学習テーブルが再学習した回数
mac tbl full	MAC アドレス学習テーブルがいっぱいになった回数
mal url	悪意があると判断された URL を宛先とするためブロックされたパケット数
***misc prot**	TCP、UDP、または ICMP 以外のプロトコルを使用しているパケット数
mp fail	マスター プロセッサ モジュールとプロセッサ モジュールの間で PCI メッセージを送信中に問題が発生した回数
no conn	NAT（ネットワーク アドレス変換）接続が使用不能なためにドロップされたパケット数
no dip	DIP（動的 IP）アドレスが使用不能なためにドロップされたパケット数
no frag netpak	NetPak バッファの使用可能な容量が 70％ を下回った回数
***no frag sess**	フラグメント化したセッションが NAT セッションの最大数の半数を超えた回数
no g-parent	親接続が見つからないためドロップされたパケット数
no gate	ゲートが使用可能でなかったためにドロップされたパケット数
no gate sess	ファイアウォールに該当するゲートがないために終了されたセッション数
no map	Trusted 側へのマッピングがないためドロップされたパケット数
no nat vector	NAT（ネットワークアドレス変換）接続がそのゲートで使用不能であったため、ドロップされたパケット数
***no nsp tunnel**	VPN トンネルがバインドされていないトンネル インターフェースに送信され、ドロップされたパケット数
no route	受信したルーティング不能なパケット数
no sa	SA（セキュリティ協会）が定義されていなかったためにドロップされたパケット数
no sa policy	SA に関連付けられたポリシーがなかったためにドロップされたパケット数
***no xmit vpnf**	フラグメント化のためにドロップされた VPN パケット数
null zone	Null ゾーンにバインドされたインターフェースに対して誤って送信されドロップされたパケット数
nvec err	NAT ベクター エラーのためにドロップされたパケット数
out bytes	送信したバイト数
out packets	送信したパケット数
out vlan	送信した VLAN パケット数
ping of death	Ping of Death 攻撃が疑われる受信パケットの数
policy deny	定義されたポリシーによって拒否されたパケット数
port scan	ポート スキャン攻撃としてカウントされたパケット数
proc sess	プロセッサ モジュールのセッションの合計数が最大しきい値を超えた回数
sa inactive	SA が非アクティブであったためにドロップされたパケット数
sa policy deny	SA ポリシーによって拒否されたパケット数
sessn thresh	セッションの最大数のしきい値
***slow mac**	時間がかかりすぎて MAC アドレスが解決できなかったフレーム数

カウンタ	説明
src route	フィルタ ソース ルート オプションのためにドロップされたパケット数
syn frag	フラグメント化のためにドロップされた SYN パケット数
tcp out of seq	シーケンス番号が許容範囲外の受信 TCP セグメント数
tcp proxy	SYN フラッド保護オプションやユーザー認証などの TCP プロキシを使用することでドロップされたパケットの数
teardrop	疑わしいティアドロップ攻撃の一部としてブロックされたパケット数
tiny frag	細かくフラグメント化された受信パケット数
trmn drop	トラフィック管理によってドロップされたパケット数
trmng queue	キューで待機中のパケット数
udp flood	UDP フラッドしきい値に対してカウントされた UDP パケット数
url block	ブロックされた HTTP 要求数
winnuke	受信した WinNuke 攻撃パケット数
wrong intf	プロセッサ モジュールからマスター プロセッサ モジュールに送信されたセッション作成メッセージ数
wrong slot	誤ったプロセッサ モジュールに送信された不正なパケット数

注 : キャリア検知多重アクセス / 衝突検出 (CSMA/CD) プロトコルの詳細については、http://standards.ieee.org にある IEEE 802.3 標準を参照してください。

この例では、Trust ゾーンのデバイス Screen カウンタを表示します。

WebUI

Reports > Counters > Zone Screen: Zone ドロップダウンリストから **Trust** を選択します。

CLI

```
get counter screen zone trust
```

索引

A

administrative traffic 29

C

CLI 9
CompactFlash 56

D

DIP 96

E

E メール警報通知 71, 73

F

filter source route 97

H

HTTP、セッション ID 4
HTTP（ハイパーテキスト転送プロトコル）、セッション ID 4

I

Ident-ResetIdent-Reset 28
in-short エラー 94
IP アドレス
    NetScreen-Security Manager サーバー 25
    管理 IP 31

M

MGT インターフェース、管理オプション 29
MIB II 28, 74

N

NAT ベクタエラー 96
NetScreen-Security Manager
    NSM エージェント 22, 25
    NSM エージェントを使用可能にする 24
    UI 22
    イベントのレポート 25
    管理オプション 28
    管理システム 22, 23, 25
    接続の初期設定 23
    定義 22
    ロギング 25
NSM エージェント 22, 23
    イベントのレポート 25
    使用可能 24

P

PCMCIA 56
ping
    管理オプション 28
PKI 鍵 6
protocol distribution、NetScreen-Security Manager へのレポート 25

R

RADIUS 39

S

SA ポリシー 96
SCP
    CLI コマンドの例 18
    使用可能 18
SMTP サーバー IP 71
SNMP 28, 74
    暗号化 77, 78
    管理オプション 28
    構成 77
    コールドスタートトラップ 74
SNMP トラップ
    100, ハードウェア問題 75
    200, ファイアウォール問題 75
    300, ソフトウェア問題 75
    400, トラフィック問題 75
    500, VPN 問題 75
    許可もしくは拒否 76
    システム アラーム 75
    種類 75
    トラフィック アラーム 75
SNMP コミュニティ
    公開 77
    非公開 77

SSH 11–16
PKA 15
PKA 認証 14
PKA 認証のみを強制 16
管理オプション 28
公開鍵をロードする、CLI 15
公開鍵をロードする、TFTP 15, 17
公開鍵をロードする、WebUI 15
自動ログイン 17
接続手続き 12
認証方法優先度 16
パスワード認証 14
SSL 5
SSL ハンドシェイクプロトコル
SSLHP を参照
SSLHP 5
SYSLOG 56
暗号化 78
機能 72, 81, 89
セキュリティ機能 73, 81, 89
ポート 72, 81, 89
ホスト 72
ホスト名 72, 73, 81, 88
メッセージ 72

T

TCP proxy 97
Telnet 9
Telnet 管理オプション 28
Telnet、によるログイン 10
Transparent モード、管理オプション 29

U

USB 56

V

VLAN1、管理オプション 29
VPN
AutoKey IKE 79, 43
管理トラフィック用 78
手動鍵 43, 79
VPN AutoKey IKE 43, 79

W

Web ユーザーインターフェース
WebUI を参照
WebTrends 56, 73
暗号化 73, 78
メッセージ 73
WebUI 1
管理オプション 28
ヘルプファイル 2
Web ブラウザ要件 2

あ

アラーム
トラフィック 69–71

い

イベントログ 57
インターフェース
Manageable 31
管理オプション 28

お

親接続 96

か

仮想システム
admins 34
read-only admins 34
仮想プライベート ネットワーク
VPN を参照
管理
CLI 9
WebUI 1
制限 42
管理 IP 31
管理オプション
Manageable 31
MGT インターフェース 29
NetScreen-Security Manager 28
ping 28
SNMP 28
SSH 28
SSL 28
Telnet 28
VLAN1 29
WebUI 28
インターフェース 28
透過モード 29
管理クライアント IP アドレス 42
管理情報ベース II
MIB II を参照
管理方法
CLI 9
SSL 5
Telnet 9
WebUI 1
コンソール 19

け

警告
E メール警報 69
NetScreen-Security Manager へのレポート 25
しきい値 69
ケーブル、シリアル 19

こ
構成の設定、ブラウザ要件 2
コマンドラインインターフェース
　CLI を参照
コンソール 56

し
自己ログ 66
手動鍵、VPN 43, 79
シリアルケーブル 19

せ
セキュアコピー
　SCP を参照
セキュアシェル
　SSH を参照
セキュアソケットレイヤー
　SSL を参照
セキュリティアソシエーション (SA) 96
セッション ID 4

そ
ソースルート 97

て
デバイス、工場出荷時のデフォルト設定にリセット 41
デフォルト設定、デバイスをリセット 41

と
統計、NSM へのレポート 25
動的 IP
　DIP を参照
トラフィック アラーム 69–71

な
内部フラッシュストレージ 56

ね
ネットワークアドレス変換 (NAT) 96

は
パケット 97
　IPSec 95
　アドレス spoofing 攻撃 95
　インターネット制御メッセージプロトコル (ICMP) 93, 95
　拒否 96
　受信 94, 95, 96
　受信不能 94, 95
　衝突 94, 95
　転送アンダーラン 94
　ドロップ 96, 97
　ネットワークアドレス変換 (NAT) 96
　フラグメント化 97
　ポイントツーポイントトネリングプロトコル (PPTP) 95
　ランド攻撃 95
　ルーティング不能 96
パスワード
　ルート管理者 41
　忘れたとき 39
バックストア 94

ひ
非アクティブ SA 96
ビットストリーム 94

ふ
ブラウザ要件 2

へ
ヘルプファイル 2

ほ
ポイントツーポイントトネリングプロトコル (PPTP) 95
ポート、モデム 20, 22

め
メッセージ
　WebTrends 73
　エラー 57
　緊急 57
　クリティカル 57
　警報 57
　情報 57
　注意 57
　通知 57
　デバッグ 57

も
モデム ポート 20, 22

ゆ

ユーザー、複数の管理ユーザー 33

り

リカバリログ 68

る

ルート管理者、ログイン 42

ろ

ロギング 55–68
CompactFlash (PCMCIA) 56
E メール 56
NetScreen-Security Manager 25
SNMP 56, 74
SYSLOG 56, 72
USB 56
WebTrends 56, 73
イベントログ 57
コンソール 56
自己ログ 66
内部 56
リカバリログ 68

概念と用例
ScreenOS リファレンス ガイド

第 4 部 :
攻撃の検出と防衛機能

リリース 6.0.0、改訂 02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

品番 : 530-017770-01-JP, 改訂 02

Copyright Notice

Copyright © 2007 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

目次

本編について xi

ドキュメントの規則 xii
Web ユーザーインターフェースの規則 xii
コマンドラインインターフェースの規則 xiii
ネーミング規則および文字タイプ xiii
説明図の規則 xiv
技術ドキュメントおよびテクニカルサポート xv

第 1 章 ネットワークの保護 1

攻撃の段階 2
検出と防衛機能 2
攻略の監視 5
例 : Untrust ゾーンからの攻撃を監視する 5

第 2 章 偵察阻止 7

IP アドレススイープ 7
ポートスキャン 9
IP オプションを使用したネットワーク偵察 10
オペレーティングシステム探査 12
SYN および FIN フラグセット 12
ACK フラグのない FIN フラグ 13
フラグが設定されていない TCP ヘッダー 14
回避技法 15
FIN スキャン 15
非 SYN フラグ 16
IP スプーフィング 19
例 : L3 IP スプーフィング保護 21
例 : L2 IP スプーフィング保護 23
IP スプーフィング保護 24

第 3 章 サービス拒否 (DoS) 攻撃の防御 29

ファイアウォール DoS 攻撃 30
セッションテーブルフラッド 30
ソースベースおよび宛先ベースセッション制限 30
例 : ソースベースのセッション制限 32
例 : 宛先ベースのセッション制限 32
アグレッシブエージング 33
例 : アグレッシブにエージアウトするセッション 34
SYN-ACK-ACK プロキシフラッド 34

ネットワーク DoS 攻撃 36
SYN フラッド 36
SYN クッキー 47
ICMP フラッド 49
UDP フラッド 50
ランド攻撃 51
OS 指定 DoS 攻撃 52
Ping of Death 52
ティアドロップ攻撃 53
WinNuke 54

第 4 章 コンテンツの監視とフィルタリング 57

フラグメントの再アセンブリ 58
不正な URL からの保護 58
アプリケーションレイヤーゲートウェイ 59
例 : パケットフラグメント内の不正な URL をブロックする 60
ウィルス対策スキャン 62
外部 AV スキャン 62
ロードバランスを行う ICAP サーバー 64
内部 AV スキャン 64
IM トラフィックの AV スキャン 66
IM クライアント 66
IM サーバー 66
IM プロトコル 67
インスタントメッセージのセキュリティの問題 67
IM のセキュリティ上の問題 68
チャットメッセージのスキャン 68
ファイル転送のスキャン 68
AV スキャンの結果 69
ポリシーベースの AV スキャン 70
アプリケーションプロトコルのスキャン 71
FTP トラフィックのスキャン 72
HTTP トラフィックのスキャン 73
内蔵スキャナの AV パターンファイルの更新 80
AV 署名サービスの利用契約 80
AV スキャナのグローバル設定 83
AV リソースの配分 83
故障モードの動作 83
最大コンテンツ容量と最大メッセージ数（内部 AV スキャンのみ） 84
HTTP キープアライブ 85
HTTP トリックリング（内部 AV スキャンのみ） 85
AV プロファイル 87
AV プロファイルを既存のファイアウォールポリシーに割り当て 88
内部 AV 用の AV プロファイルの起動 88
例 : (内部 AV) あらゆる種類のトラフィックのスキャンの設定 89
スパム対策フィルタリング 94
ブラックリストとホワイトリスト 95
基本構成 95
スパムトラフィックのフィルタリング 95
スパムメッセージのドロップ 96
ブラックリストの定義 96
ホワイトリストの定義 96
デフォルトアクションの定義 97

スパム対策フィルタリング（続き）
スパムブロッキングリストサーバーを使用可能に設定 97
スパム対策のテスト 98
Web フィルタリング 98
CLI で Web フィルタリングモードを開始 99
統合型 Web フィルタリング 99
SurfControl サーバー 100
Web フィルタリングキャッシュ 101
統合型 Web フィルタリングの構成 101
例 : 統合型 Web フィルタリング 107
Web フィルタリングの転送 108
仮想システムサポート 110
転送型 Web フィルタリングの構成 111
例 : Web フィルタリングの転送 114

第 5 章 徹底監視 (Deep Inspection) 117

概要 118
攻撃オブジェクトデータベースサーバー 122
定義済みのシグネチャパッケージ 122
シグネチャパッケージの更新 123
攻撃オブジェクトの更新を始める前に 124
即時更新 124
自動更新 125
自動通知と即時更新 126
手動更新 128
攻撃オブジェクトとグループ 130
サポートされているプロトコル 131
ステートフル署名 135
TCP ストリームシグネチャ 136
プロトコルアノーマリ (プロトコル異常) 136
攻撃オブジェクトグループ 137
重大度レベルの変更 137
例 : P2P の徹底監視 138
攻撃オブジェクトの無効化 140
攻撃アクション 141
例 : 攻撃アクション ー Close Server、Close、Close Client 142
ブルートフォース攻撃アクション 149
ブルートフォース攻撃オブジェクト 149
ブルートフォース攻撃ターゲット 150
ブルートフォース攻撃のタイムアウト 150
例 1 151
例 2 151
例 3 151
攻撃のログ出力 152
例 : 攻撃グループごとにログ出力を無効化 152
顧客サービスとアプリケーションのマッピング 154
例 : アプリケーションと顧客サービスのマッピング 155
例 : HTTP を悪用する攻撃に関するアプリケーションと
サービスの対応づけ 157
カスタマイズした攻撃オブジェクトとグループ 158
ユーザー定義のステートフルシグネチャ攻撃オブジェクト 158
正規表現 159
例 : ユーザー定義のステートフル署名攻撃オブジェクト 160

カスタマイズした攻撃オブジェクトとグループ（続き）
TCP ストリームシグネチャ攻撃オブジェクト 162
例 : ユーザー定義のストリームシグネチャ攻撃オブジェクト 163
プロトコルアノーマリパラメータの構成 164
例 : パラメータの変更 165
否定 165
例 : 攻撃オブジェクトの否定 166
HTTP コンポーネントの細分ブロッキング 170
ActiveX コントロール 170
Java アプレット 171
EXE ファイル 171
ZIP ファイル 171

第 6 章 侵入探知と阻止 173

IDP 対応のセキュリティデバイス 174
IDP 対応デバイスでのトラフィックフロー 175
侵入探知と阻止の構成 176
構成の前に 176
例 1: IDP の基本構成 177
例 2: アクティブ / パッシブフェールオーバー向けの IDP の構成 180
例 3: アクティブ / アクティブフェールオーバー向けの IDP の構成 182
セキュリティポリシーの構成 184
セキュリティポリシーについて 184
セキュリティポリシーの管理 184
セキュリティポリシーのインストール 185
IDP ルールベースの使用 185
IDP ルールベースの役割ベースの管理 186
オブジェクトの IDP ルール向け構成 186
セキュリティポリシーテンプレートの使用 187
ファイアウォールルールで IDP を使用可能にする 187
IDP を使用可能にする 188
インラインモードまたはインラインタップモードの指定 188
IDP ルールの構成 189
IDP ルールベースの追加 190
トラフィックとのマッチング 191
ソースゾーンおよび宛先ゾーン 191
ソースおよび宛先アドレスオブジェクト 192
例 : ソースと宛先の設定 192
例 : 複数のソースおよび宛先の設定 192
Services 193
例 : デフォルトサービスの設定 193
例 : 特定のサービスの設定 194
例 : 非標準サービスの設定 194
ターミナルルール 195
例 : ターミナルルールの設定 196
アクションの定義 197
攻撃オブジェクトの設定 198
攻撃オブジェクトを個別に追加する 198
攻撃オブジェクトのカテゴリ別の追加 198
例 : 攻撃オブジェクトのサービス別の追加 198
攻撃オブジェクトのオペレーティングシステム別の追加 199
重大度別攻撃オブジェクトの追加 199

IDP ルールの構成（続き）
IP アクションの設定 200
IP アクションの選択 200
ブロッキングオプションの選択 200
ロギングオプションの設定 201
タイムアウトオプションの設定 201
通知の設定 201
ロギングの設定 201
警報の設定 201
パケットのロギング 201
重大度の構成 202
ターゲットの設定 202
コメントの入力 202
免除ルールの構成 202
免除ルールベースの追加 203
一致の定義 204
ソースゾーンおよび宛先ゾーン 204
ソースおよび宛先アドレスオブジェクト 205
例 : ソース / 宛先ペアの免除 205
攻撃オブジェクトの設定 205
例 : 特定の攻撃オブジェクトの免除 205
ターゲットの設定 206
コメントの入力 206
ログビューアから免除ルールを作成 206
バックドアルールの構成 207
バックドアルールベースの追加 208
一致の定義 209
ソースゾーンおよび宛先ゾーン 209
ソースおよび宛先アドレスオブジェクト 209
Services 210
操作の設定 210
アクションの設定 210
通知の設定 210
ロギングの設定 210
警報の設定 211
パケットのロギング 211
重大度の構成 211
ターゲットの設定 211
コメントの入力 212
IDP 攻撃オブジェクトの構成 212
IDP 攻撃オブジェクトのタイプ 212
シグネチャ攻撃オブジェクト 212
プロトコルアノーマリ攻撃オブジェクト 213
複合攻撃オブジェクト 213
定義済み IDP 攻撃オブジェクトおよびグループの表示 213
定義済み攻撃の表示 213
定義済みグループの表示 214
カスタム IDP 攻撃オブジェクトの作成 215
シグネチャ攻撃オブジェクトの作成 217
プロトコルアノーマリ攻撃の作成 222
複合攻撃の作成 223
カスタム攻撃オブジェクトの編集 225
カスタム攻撃オブジェクトの削除 226

IDP 攻撃オブジェクトの構成（続き）
カスタム IDP 攻撃グループの作成 226
静的グループの構成 226
動的グループの構成 227
例 : 動的グループの作成 228
動的グループの更新 230
カスタム攻撃グループの編集 230
カスタム攻撃グループの削除 230
デバイスをスタンドアロンの IDP デバイスとして構成する 230
IDP を使用可能にする 231
例 : スタンドアロンの IDP 用のファイアウォールルールの構成 ... 231
役割ベースの管理の構成 232
例 : IDP 専用管理者の構成 232
IDP の管理 234
攻撃データベース更新 234
攻撃データベース更新のダウンロード 234
更新された攻撃オブジェクトの使用 234
IDP エンジンの更新 235
IDP ログの表示 237

第 7 章 不審なパケット属性 239

ICMP フラグメント 240
ラージ ICMP パケット 241
不良 IP オプション 242
不明のプロトコル 243
IP パケットフラグメント 244
SYN (周期) フラグメント 245

付録 A ユーザー定義シグネチャのコンテキスト A-I

索引 ..... IX-I

本編について

*第 4 部 : 攻撃の検出と防衛機能*では、ScreenOS で使用可能な Juniper Networks セキュリティオプションについて説明します。これらのオプションの多くは、セキュリティゾーンレベルで使用可能にできます。オプションが適用される対象は、オプションを使用可能にしたゾーンにバインドされたインターフェースを経由して Juniper Networks セキュリティデバイスに到達するトラフィックです。SCREEN オプションは IP アドレススキャンやポートスキャン、DoS（Denial of Service: サービス拒否）攻撃、および他の種類の悪意のあるアクティビティから保護します。Web フィルタリング、ウィルス対策、および IDP (侵入検出および防止) など、他のネットワークセキュリティオプションをポリシーレベルで適用できます。こうしたオプションは、これらのオプションが使用可能になっているポリシーの管轄下にあるトラフィックにのみ適用されます。

注 : 本編では、ポリシーレベルで使用可能にできるネットワークセキュリティオプションについても取り上げているため、ポリシー自体については簡単に説明するにとどめます。ポリシーの詳細については、**2**-161 ページの「ポリシー」を参照してください。

この巻のセクションは、以下のようになります。

- 第 1 章「ネットワークの保護」では攻撃の基本的な段階と、各段階でアタッカーと闘うために使用できるファイアウォールのオプションの概略を説明します。
- 第 2 章「偵察阻止」では、IP アドレススイープ、ポートスキャン、およびターゲットとなったシステムのオペレーティングシステム (OS) の種類を検出しようとする試みをブロックするために使用できるオプションについて説明します。
- 第 3 章「サービス拒否 (DoS) 攻撃の防御」では、ファイアウォールアタック、ネットワークアタック、および OS 別の DoS アタックと、ScreenOS がそれらのアタックを防ぐ方法について説明します。
- 第 4 章「コンテンツの監視とフィルタリング」では、不正な URL (ユニフォームリソースロケータ) からユーザーを保護する方法や、サードパーティ製品と連携してウィルス対策や Web フィルタリングを行うために Juniper Networks セキュリティデバイスを構成する方法について説明します。
- 第 5 章「徹底監視 (Deep Inspection)」では、IDP 攻撃オブジェクトの更新を取得するために Juniper Networks セキュリティ デバイスを構成する方法、ユーザー定義の攻撃オブジェクトおよび攻撃オブジェクトグループを作成する方法、およびポリシーレベルで IDP を適用する方法について説明します。

- 第 6 章「侵入探知と阻止」では、ネット - ワーク内へ進入しようとする企みを検出し攻撃を未然に阻止する Juniper Networks IDP（進入検出と阻止）テクノロジについて説明します。IDP をポリシーレベルで適用し、攻撃者がネットワークに入る前に不正なパケットや接続をドロップする方法について示します。
- 第 7 章「不審なパケット属性」では、異常な IP パケットおよび ICMP パケットの属性によって示される潜在的な攻撃からネットワークリソースを保護するためのいくつかの SCREEN オプションについて説明します。
- 付録 A「ユーザー定義シグネチャのコンテキスト」では、ステートフルなシグニチャ攻撃オブジェクトを定義する際に指定できるコンテキストを説明します。

ドキュメントの規則

このドキュメントは、次のセクションで説明されている規則を使用しています。

- x ページの「Web ユーザーインターフェースの規則」
- xi ページの「コマンドラインインターフェースの規則」
- xi ページの「ネーミング規則および文字タイプ」
- xii ページの「説明図の規則」

Web ユーザーインターフェースの規則

WebUI（Web ユーザーインターフェース）では、各作業の操作指示は、操作手順と構成設定値に分かれています。構成設定を入力できる WebUI ページを開くには、画面の左側にあるナビゲーション ツリーのメニュー項目をクリックして、そのページに移動します。先へ進むと、ナビゲーション パスが画面の上部に表示されます。各ページは角括弧で分離されています。

WebUI のパスおよびアドレスを定義するためのパラメータは、以下のとおりです。

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.2.2.5/32
Zone: Untrust

構成設定のオンラインヘルプを開くには、画面の左上にある疑問符（?）をクリックします。

ナビゲーションツリーにも、Help > Config Guide 構成ページがあり、セキュリティポリシーおよび IPSec （インターネットプロトコルセキュリティ）の構成に役立ちます。ドロップダウンメニューからオプションを選択して、そのページの指示に従います。構成設定のオンラインヘルプを開くには、左上にある **?** 文字をクリックします。

コマンドラインインターフェースの規則

次の規則は、例とテキストにおいて、コマンドラインインターフェース（CLI）コマンドの構文を示すために使用されます。

例においては、次のように使用されます。

- 角括弧 [ ] 内にあるものはすべてオプションです。
- 中括弧 { } 内にあるものはすべて必須です。
- 選択肢が複数ある場合、各選択肢はパイプ (|) で区切られています。例えば、次のように表示されます。

```
set interface { ethernet1 | ethernet2 | ethernet3 } manage
```

- 変数は*斜体*で表示されます。

```
set admin user name1 password xyz
```

テキストにおいては、コマンドは**太字**で、変数は*斜体*で表示されます。

注 : キーワード入力時には、単語を間違いなく識別できる数の文字を入力すれば十分です。**set admin user wheezer j12fmt54** というコマンドを入力する際には、**set adm u whee j12fmt54** と入力するだけで十分です。ただし、本編に記載されたコマンドはすべて本来の形式で記載されています。

ネーミング規則および文字タイプ

ScreenOS はオブジェクトの名前 (アドレス、管理ユーザー、認証サーバー、IKE ゲートウェイ、仮想システム、VPN トンネルおよびゾーンなど、ScreenOS 構成に定義されているもの) に関して、次の規則に従います。

- 名前文字列に 1 つまたは複数のスペースが含まれる場合、文字列全体を二重引用符で囲む必要があります。例 :

  set address trust “local LAN” 10.1.1.0/24

- 二重引用符で囲まれた文字列の先頭または末尾のスペースを取り除きます。たとえば、「 **local LAN** 」は「**local LAN**」となります。
- 連続した複数のスペースは、一つのスペースとして扱われます。
- CLI キーワードの多くはケースセンシティブではありませんが、名前文字列はケースセンシティブです。たとえば、「**local LAN**」は「**local lan**」とは異なります。

ScreenOS は、次の文字タイプをサポートします。

- 1 バイト文字セット (SBCS) およびマルチバイト文字セット (MBCS)。SBCS の例に、ASCII、欧州言語、およびヘブライ語があります。2 バイト文字セット (DBCS) とも呼ばれる MBCS の例に、中国語、韓国語、および日本語があります。

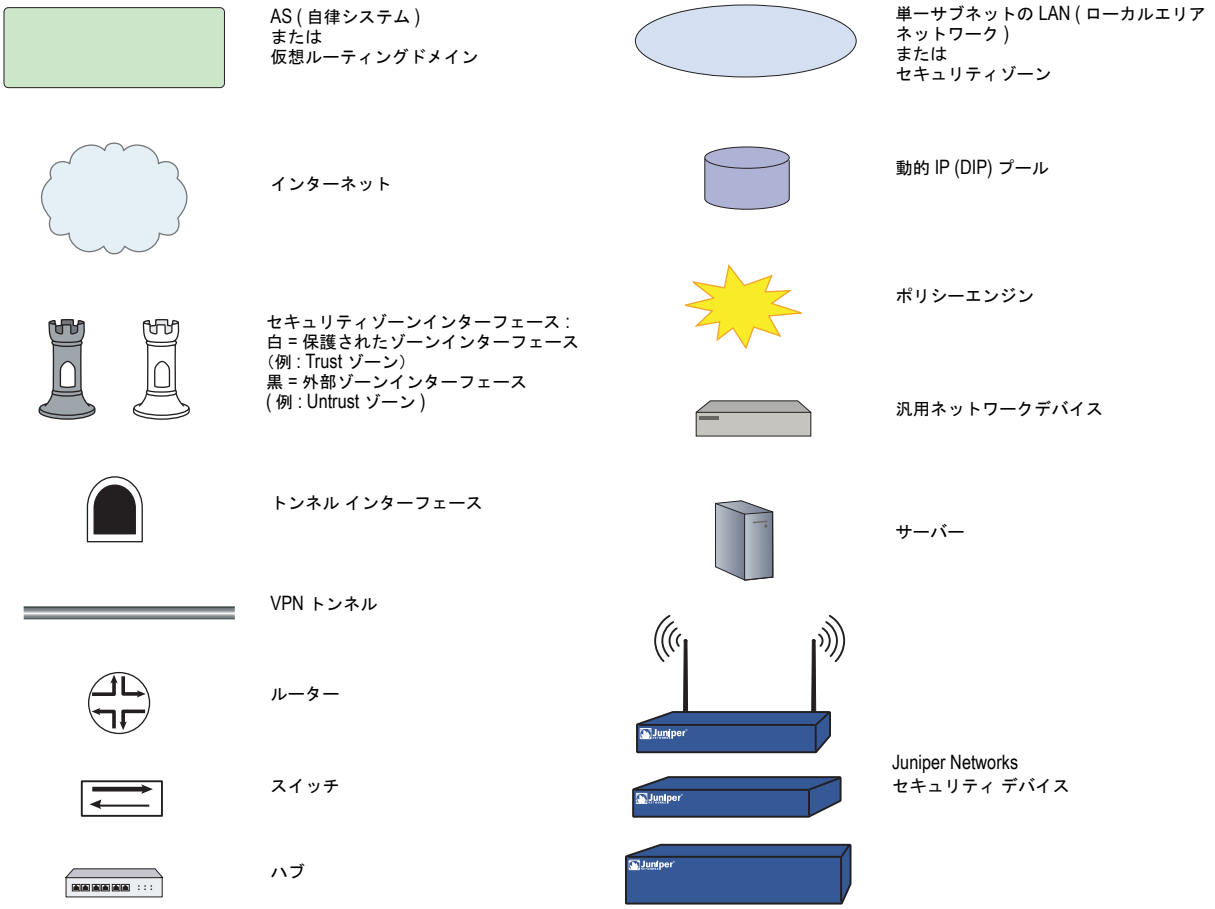
- ASCII 文字の 32（16 進数の 0x20）から 255（0xff)。ただし二重引用符 (“) は、スペースを含む名前文字列の先頭と末尾を示す特殊な意味をもつため、例外とします。

注： コンソール接続では、SBCS のみがサポートされます。ご利用のブラウザがサポートする文字セットに応じて、WebUI は SBCS および MBCS の両方をサポートします。

説明図の規則

次の図は、本編を通して説明図に使用されている画像の基本的なものです。

図 1: 説明図の画像



技術ドキュメントおよびテクニカルサポート

Juniper Networks 製品のいずれかの技術ドキュメントを入手するには、www.juniper.net/techpubs/ をご覧になってください。

テクニカルサポートについては、http://www.juniper.net/customers/support/ にある Case Manager を使って事例サポートを開くか、1-888-314-JTAC (米国内) か 1-408-745-9500 (その他の国) までお問い合わせください。

本書に間違いや欠落があった場合は、techpubs-comments@juniper.net までお知らせください。

第 1 章

ネットワークの保護

保護されたネットワークへの侵入にはさまざまな理由が考えられます。一般的な目的を以下のリストに示します。

- 保護されたネットワークに関する次の種類の情報を収集する
  - トポロジ
  - アクティブホストの IP アドレス
  - アクティブホストにあるアクティブポートの番号
  - アクティブホストのオペレーティングシステム
- 偽りのトラフィックで、保護されたネットワークのホストを圧倒し、DoS (サービス拒否) を引き起こす
- 偽りのトラフィックで保護されたネットワークを圧倒し、ネットワーク全体の DoS を引き起こす
- 偽りのトラフィックでファイアウォールを圧倒することによって、ファイアウォールの背後にあるネットワークに DoS を引き起こす
- 保護されたネットワークのホストに被害を引き起こし、データを盗む
- 保護されたネットワークのホストにアクセスし、情報を取得する
- ホストのコントロール権を掌握し、他の攻略を開始する
- ファイアウォールのコントロール権を掌握し、ファイアウォールによって保護されているネットワークへのアクセスをコントロールする

ScreenOS は、アタッカーが Juniper Networks セキュリティデバイスで保護されたネットワークを狙って上記の目的を達成しようとする場合、その試みを発見し阻止する検出ツールと防衛ツールを提供しています。

この章では攻撃の主な段階と、各段階で攻撃を阻止するために利用できるさまざまな防衛機構の概要を説明します。

- 2 ページの「攻撃の段階」
- 2 ページの「検出と防衛機能」
- 5 ページの「攻略の監視」

攻撃の段階

各攻撃は通常、2 つの主な段階で進行します。アタッカーはフェーズ 1 で情報を収集し、フェーズ 2 では攻撃を開始します。

1. 偵察の実行。

   a. ネットワークをマッピングし、どのホストがアクティブか判断します (IP アドレススイープ)。

   b. IP アドレススイープで発見したホストで、どのポートがアクティブか見分けます (ポートスキャン)。

   c. オペレーティングシステム (OS) を判断します。これによってその OS の弱点や OS が被害を受けやすい攻撃を知ることができます。

2. 攻撃を開始します。

   a. 攻撃の発信元を隠します。

   b. 攻撃を実行します。

   c. 証拠を取り除くか、隠します。

検出と防衛機能

攻略は情報収集を目的とした調査の場合と、ネットワークやネットワークリソースを妥協、使用不能、または損なうための攻撃の場合があります。場合によっては 攻略の 2 つの目的の区別がはっきりしない場合もあります。たとえば、TCP SYN セグメントによる集中攻撃は、アクティブなホストから応答を引き出すことを意図した IP アドレススイープの場合と、ネットワークを圧倒し正常に機能しないようにすることを意図とした SYN フラッド攻撃の場合があります。さらに、アタッカーは通常攻撃を行う前にターゲットに対する偵察を実行するため、情報収集の活動は差し迫った攻撃の前兆 (攻撃のフェーズ 1) と考えることができます。このように、*攻略*という語は偵察アクティビティと攻撃アクティビティの両方を含み、その 2 つの区別はいつも明確とは限りません。

Juniper Networks では攻略が実行される全段階で攻略と闘うために、さまざまな検出方法や防衛機構をゾーンレベルおよびポリシーレベルで提供しています。

- ゾーンレベルおよび SCREEN オプション
- 地域間、ゾーン内、およびスーパーゾーンの各ポリシーレベルのファイアウォールポリシー (ここではスーパーゾーンは、グローバルポリシーを意味し、セキュリティゾーンについて言及していません)。

注 : VLAN ゾーンと MGT ゾーンは機能ゾーンでありセキュリティゾーンではありませんが、SCREEN オプションを設定することができます。VLAN ゾーンはレイヤー 3 セキュリティゾーンと同じ SCREEN オプションのセットをサポートしています。(レイヤー 2 セキュリティゾーンは、レイヤー 3 ゾーンがサポートしない追加の SYN フラッドオプションである Drop Unknown MAC をサポートしています。) 次の SCREEN オプションは MGT ゾーンに適用されないため、MGT ゾーンでは使用できません : SYN フラッド保護、SYN-ACK-ACK プロキシフラッド保護、HTTP コンポーネントブロッキング、WinNuke 攻撃保護。

すべての接続の試みをセキュアにするために、Juniper Networks セキュリティデバイスはパケット状態監視として知られる動的パケットフィルタリング方法を使用します。この方法の使用により、IP パケットヘッダーと TCP セグメントヘッダーでさまざまなコンポーネント (ソース と宛先の IP アドレス、ソースと宛先のポート番号、およびパケットシーケンス番号) が確認され、ファイアウォールを通過する各 TCP セッションと擬似 UDP セッションの状態が維持されます。(また、動的ポートの変更あるいはセッションの終了など、要素の変更に応じてセッションの状態が変更されます)。受信 TCP パケットが到達すると、ヘッダーに含まれる情報が監視テーブルに保存されている関連セッションの状態と比較されます。適合した場合、受信パケットはファイアウォールの通過を許可されます。この 2 つが適合しない場合、パケットはドロップされます。

ScreenOS の SCREEN オプションは、ゾーンにバインドされたインターフェースを通過する必要がある接続の試みをすべて検査し、許可または拒否することによってゾーンを保護します。それから SCREEN フィルタを通過するトラフィックに対し、コンテンツフィルタリング、および IDP (侵入検出および防止) コンポーネントが含まれたファイアウォールポリシーが適用されます。

Juniper Networks ファイアウォールは、以下の防衛機構のセットを提供しています。

- 偵察阻止
  - IP アドレススイープ
  - ポートスキャン
  - オペレーティングシステム探査
  - 回避技法
- コンテンツの監視とフィルタリング
  - フラグメントの再アセンブリ
  - ウィルス対策スキャン
  - スパム防止フィルタリング
  - Web フィルタリング
- 徹底監視
  - ステートフルシグネチャ
  - プロトコルアノーマリ (プロトコル異常)
  - HTTP コンポーネントの細分ブロッキング

- DoS (サービス拒否) 攻撃の防御
  - ファイアウォール DoS 攻撃
    - セッションテーブルフラッド
    - SYN-ACK-ACK プロキシフラッド
  - ネットワーク DoS 攻撃
    - SYN フラッド
    - ICMP フラッド
    - UDP フラッド
  - OS 指定 DoS 攻撃
    - Ping of Death
    - ティアドロップ攻撃
    - WinNuke
- 不審なパケット属性
  - ICMP フラグメント
  - ラージ ICMP パケット
  - 不良 IP オプション
  - 未知のプロトコル
  - IP パケットフラグメント
  - SYN フラグメント

ScreenOS のネットワーク保護設定は、セキュリティゾーンとポリシーの 2 つのレベルで機能します。セキュリティゾーンレベルでは偵察の阻止と Dos 攻撃の防衛が実行されます。コンテンツの監視とフィルタングの分野では、ゾーンレベルでフラグメントの再アセンブリが適用され、ポリシーレベルでは AV (ウィルス対策) スキャンや URL (ユニフォームリソースロケータ) フィルタリングが適用されます。IDP はポリシーレベルで適用されますが、ゾーンレベルで発生する HTTP コンポーネントの検出とブロッキングは例外です。ゾーンレベルのファイアウォール設定は SCREEN オプションです。あるポリシーで設定されるネットワーク保護オプションは、そのポリシーのコンポーネントになります。

攻略の監視

通常、攻略はセキュリティデバイスによってブロックしますが、場合によってはユーザーが攻略に関する情報を収集したいと思うこともあります。攻略の意図やどれほど巧妙か、またアタッカーが不注意かそれほど巧妙でない場合はそのソースなどを発見するために、特定の攻略について具体的に知りたいと考えることもあります。

攻略の情報を収集する場合、攻略を実行させ、監視、分析、鑑識を行い、事前に準備した緊急対応プランに従って対応することができます。セキュリティデバイスに攻略を通知するように設定することはできますが、デバイスは行動を起こす代わりに攻略が実行されるのを許可します。それからユーザーは何が発生したかを研究し、アタッカーの手法、戦略、および目的を見極めます。ネットワークに対する脅威についての理解を深めるほど、防衛能力を高めることができます。巧妙なアタッカーは自分の場所や身元を隠すことができますが、攻撃が発信された場所を突き止めるのに十分な情報を集めることは可能です。アタッカーの能力を推測することもできます。このような情報により、どのような対応をするかを正しく判断できます。

例 : Untrust ゾーンからの攻撃を監視する

この例では、Untrust ゾーンからの IP スプーフィング攻撃が毎日、普通は午後 21:00 から午前 0:00 の間に発生しています。スプーフィングされた ソース IP アドレスが含まれたパケットをドロップする代わりに、セキュリティデバイスにパケットの到着を通知させる一方で通過を許可し、DMZ のインターフェースに接続したハニーポット (アタッカーをおびき寄せてから攻撃中のアクションを記録するように設計された、おとりのネットワークサーバー) などへ導くようにしたいとします。攻撃が検出された場合のファイアウォールの動作を、午後 20:55 にパケットの通知と拒否から通知と許可に変更します。攻撃が発生したら、ハニーポットを使用してファイアウォールを通過した後のアタッカーのアクティビティを監視できます。上流 ISP と協力して、パケットのソースまでのトラッキングを開始することもできます。

WebUI

Screening > Screen (Zone: Untrust): 以下を入力して **Apply** をクリックします。

Generate Alarms without Dropping Packet: (**選択**)
IP Address Spoof Protection: (**選択**)

CLI

```
set zone untrust screen alarm-without-drop
set zone untrust screen ip-spoofing
save
```

第 2 章

偵察阻止

攻撃者は、ターゲットとするネットワークのレイアウト (どの IP アドレスがアクティブホストを持つか)、可能なエントリポイント (どのポート番号がアクティブホスト上でアクティブか)、そして被害を受けるシステムの構成 (アクティブホストがどのオペレーティングシステムを実行しているか) を最初に把握できれば、より巧妙に攻撃を計画することができます。この情報を得るには、攻撃者は偵察を行う必要があります。Juniper Networks は、攻撃者の偵察行為を阻止し、保護されたネットワークとネットワークリソースに関する重要な情報を攻撃者に取得されるのを防ぐための、SCREEN オプションを提供します。

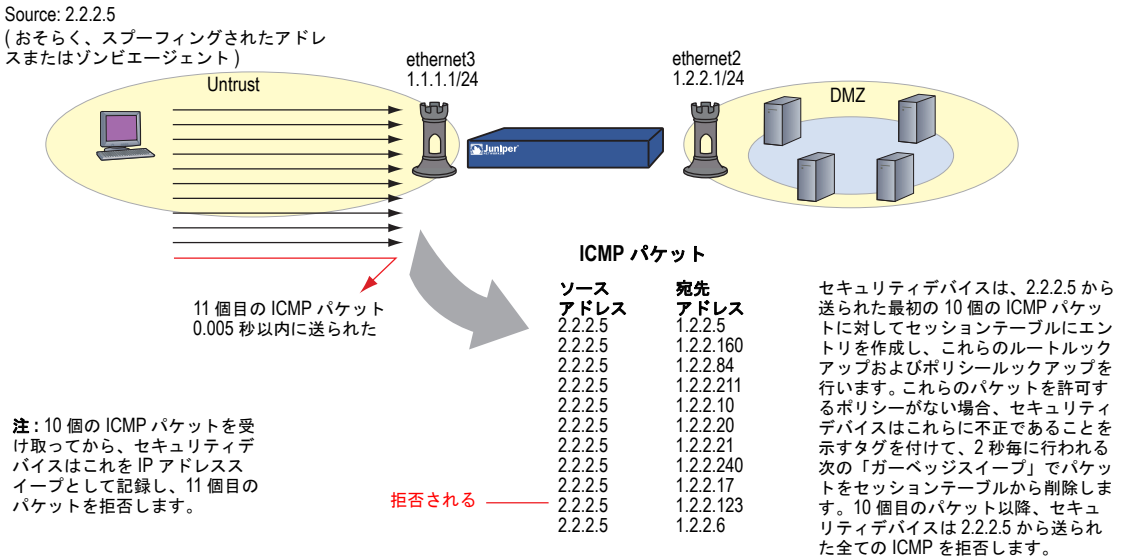
- 7 ページの「IP アドレススイープ」
- 9 ページの「ポートスキャン」
- 10 ページの「IP オプションを使用したネットワーク偵察」
- 12 ページの「オペレーティングシステム探査」
  - 12 ページの「SYN および FIN フラグセット」
  - 13 ページの「ACK フラグのない FIN フラグ」
  - 14 ページの「フラグが設定されていない TCP ヘッダー」
- 15 ページの「回避技法」
  - 15 ページの「FIN スキャン」
  - 16 ページの「非 SYN フラグ」
  - 19 ページの「IP スプーフィング」
  - 24 ページの「IP スプーフィング保護」

IP アドレススイープ

アドレススイープは、ソース IP アドレスが 10 個の ICMP パケットを異なるホストに、定義された間隔内で送信したときに発生します。この企みの目的は、少なくとも 1 つのホストが応答すればターゲットとするアドレスが発見できると期待して、さまざまなホストに ICMP パケット (通常、エコー要求) を送信することです。セキュリティデバイスは、1 つのリモートソースからさまざまなアドレスへ送信される ICMP パケットの数を内部で記録します。デフォルト設定を使用する

と、リモートホストが ICMP トラフィックを 10 個のアドレスに 0.005 秒 (5000 ミリ秒) 以内に送信した場合、セキュリティデバイスはこれがアドレススイープ攻撃であるとして警告を出し、指定したしきい値の残り期間、そのホストからそれ以降に送られる ICMP エコー要求をすべて拒否します。デバイスは、アドレススイープ攻撃基準に一致する 10 個目のパケットを検出してドロップします。

図 2: アドレススイープ



セキュリティゾーンに対してこの SCREEN オプションを使用可能にするのは、そのゾーンからの ICMP トラフィックを許可するポリシーが存在する場合にのみ、検討してください。そうでない場合は、使用可能にする必要はありません。そのようなポリシーがなければ、そのゾーンからのすべての ICMP トラフィックが拒否され、攻撃者が何らかの方法で IP アドレススイープを行うことも防ぐことができます。

特定のセキュリティゾーンから発生する IP アドレススイープをブロックするには、次のいずれかを行います。

WebUI

Screening > Screen (Zone: ゾーン名を選択): 以下を入力して **Apply** をクリックします。

IP Address Sweep Protection: (**選択**)
Threshold: (IP **アドレススイープ保護が起動するしきい値を入力**)

注 : 値の単位はマイクロ秒です。デフォルト値は 5000 マイクロ秒です。

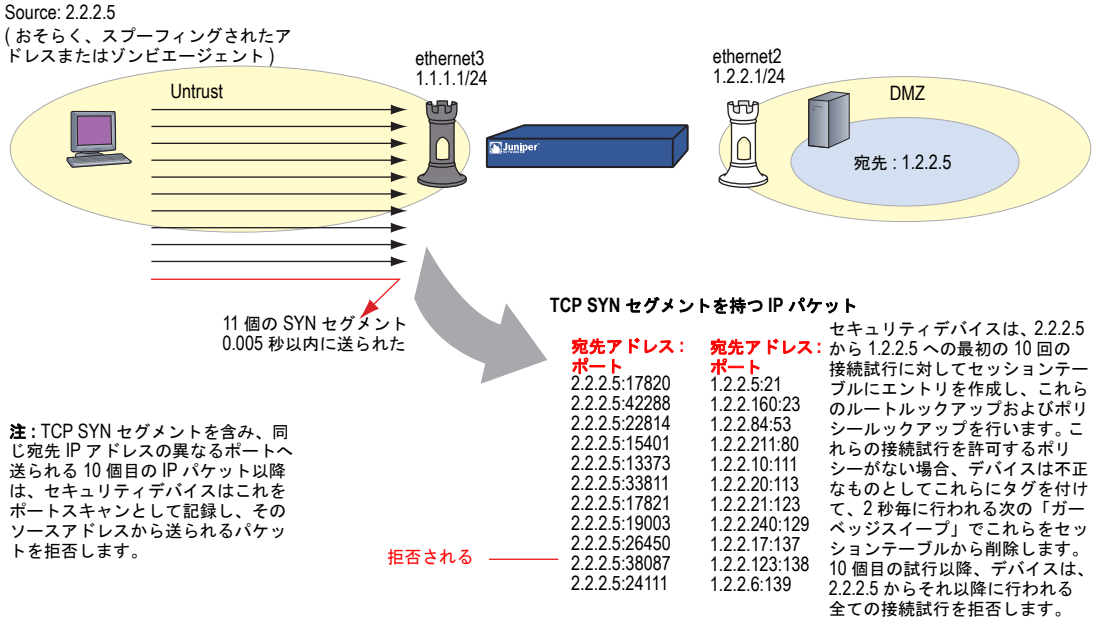
CLI

set zone *zone* screen ip-sweep threshold *number*
set zone *zone* screen ip-sweep

ポートスキャン

ポートスキャンは、1 つのソース IP アドレスが TCP SYN セグメントを含む IP パケットを同一の宛先 IP アドレスの 10 個の異なるポートに、定義された間隔 (デフォルトは 5000 マイクロ秒) 以内に送信した際に発生します。この企みの目的は、少なくとも 1 つのポートが応答すればターゲットとするサービスを特定できると期待して、利用可能なサービスをスキャンすることです。セキュリティデバイスは、1 つのリモートソースからスキャンされる異なるポートの数を内部で記録します。デフォルトの設定を使用すると、リモートホストが 10 個のポートを 0.005 秒間 (5000 マイクロ秒) にスキャンした場合、デバイスはこれがポートスキャンアタックであるとして警告を出し、指定したタイムアウトの残り期間、そのリモートソースからそれ以降に送られるすべてのパケットを拒否します。デバイスは、ポートスキャンアタック基準に一致する 10 個目のパケットを検出してドロップします。

図 3: ポートスキャン



特定のセキュリティゾーンから発生するポートスキャンをブロックするには、次のいずれかを行います。

WebUI

Screening > Screen (Zone: ゾーン名を選択): 以下を入力して **Apply** をクリックします。

Port Scan Protection: (選択)
Threshold: (ポートスキャンに対する保護が起動するしきい値を入力)

注 : 値の単位はマイクロ秒です。デフォルト値は 5000 マイクロ秒です。

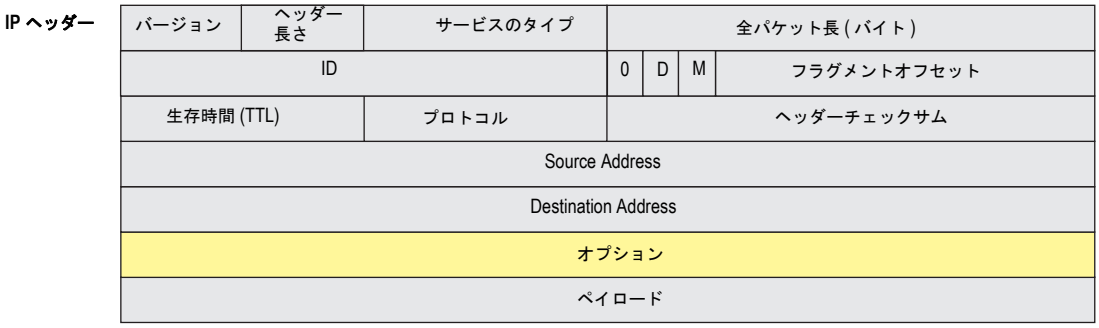
CLI

set zone *zone* screen port-scan threshold *number*
set zone *zone* screen port-scan

IP オプションを使用したネットワーク偵察

インターネット プロトコル規格の RFC 791、*Internet Protocol* では、特定のルーティング制御、診断ツール、およびセキュリティを提供するオプションのセットが指定されています。これらのオプションは、図 4 に表示されるように、IP パケットヘッダーの宛先アドレスの後にあります。

図 4: ルーティングオプション



RFC 791 では、これらのオプションは「unnecessary for the most common communications」(最も一般的な通信では不要) であり、実際には、これらが IP パケットヘッダーに現れることはほとんどないことを示します。仮にそれらが現れたときには、違法の目的で挿入されていることが多くあります。表 1 に IP オプションとその属性を一覧します。

表 1: IP オプションとその属性

タイプ	クラス	番号	長さ	使用目的	悪意的な用途
End of Options	0[1]	0	0	1 つまたは複数の IP オプションの終端を示します。	なし。
No Options	0	1	0	ヘッダーに IP オプションがないことを示します。	なし。
Security	0	2	11 ビット	ホストから、セキュリティ、TCC (閉域利用者グループ) パラメータ、および DoD (米国防総省) 要件に適合する Handling Restriction Codes を送信する方法が得られます (このオプションは、RFC 791、*Internet Protocol* と RFC 1038、*Revised IP Security Option* で指定されており、旧式のものです)。	不明。ただし、旧式のものであるため、IP ヘッダーに存在する場合は疑わしいと言えます。
Loose Source Route	0	3	変動	パケットがソースから宛先へ移動する際に利用する部分的なルートリストを指定します。パケットは指定されたアドレスの順に進む必要がありますが、指定されたルーター間にある他のルーターを通過することは許可されます。	回避。攻撃者が特定のルートを使用して、パケットの実際のソースを隠蔽したり、保護されたネットワークへのアクセスを取得したりするおそれがあります (24 ページの「IP スプーフィング保護」を参照してください。)

タイプ	クラス	番号	長さ	使用目的	悪意的な用途
Record Route	0	7	変動	IP パケットが移動するパスに沿って存在するネットワークデバイスの IP アドレスを記録します。宛先のシステムは、その時点でルート情報を抽出し処理することができます (オプションおよび記憶スペースは、どちらもサイズが 40 バイトに制限されているため、記録できる IP アドレスは 9 つまでです)。	偵察。宛先ホストが障害を起こし攻撃者に制御されているシステムであれば、パケットが通過したネットワークのトポロジおよびアドレススキームに関する情報を攻撃者に取得されるおそれがあります。
Stream ID	0	8	4 ビット	(旧式) ストリーム概念をサポートしないネットワークを介して、16 ビット SATNET ストリーム識別子を伝送する方法が得られます。不明。	不明ただし、旧式のものであるため、IP ヘッダーに存在する場合は疑わしいと言えます。
Strict Source Route	0	9	変動	パケットがソースから宛先へ移動する際に利用する完全なルートリストを指定します。宛先フィールドのアドレスは、リストの最後のアドレスに差し替えられます。	回避。攻撃者が特定のルートを使用して、パケットの実際のソースを隠蔽したり、保護されたネットワークへのアクセスを取得したりするおそれがあります。(See 24 ページの「IP スプーフィング保護」.)
Timestamp	2[2]	4		パケットがソースポイントから宛先ポイントへ移動する間に、各ネットワークデバイスがパケットを受信した時刻 (万国標準時[3]) を記録します。ネットワークデバイスは、IP ナンバーによって識別されます。 このオプションによって、パケットのパスに沿ったルーターの IP アドレスと各ルーター間の転送時間のリストを作成します。	偵察。宛先ホストが障害を起こし攻撃者に制御されているシステムであれば、パケットが通過したネットワークのトポロジおよびアドレススキームに関する情報が攻撃者に取得されるおそれがあります。

1.「0」で識別されるオプションのクラスは、特別なパケットまたはネットワーク制御を可能にするためのものです。
2.「2」で識別されるオプションのクラスは、診断、デバッグ、および測定のためのものです。
3.タイムスタンプは、万国標準時 (UT) の深夜零時からのミリ秒数を使用します。UT は、国際時刻標準の基礎であるグリニッジ標準時 (GMT) としても知られています。

次の SCREEN オプションは、攻撃者が偵察のために、または不明確であっても疑わしい目的で使用するおそれのある IP オプションを検出します。

- **Record Route:** セキュリティデバイスは、IP オプションが 7 (Record Route) であるパケットを検出し、イベントを ingress インターフェースの SCREEN カウンタリストに記録します。
- **Timestamp:** セキュリティデバイスは、IP オプションが 4 (Internet Timestamp) であるパケットを検出し、イベントを ingress インターフェースの SCREEN カウンタリストに記録します。
- **Security:** セキュリティデバイスは、IP オプションが 2 (Security) であるパケットを検出し、イベントを ingress インターフェースの SCREEN カウンタリストに記録します。
- **Stream ID:** セキュリティデバイスは、IP オプションが 8 (Stream ID) であるパケットを検出し、イベントを ingress インターフェースの SCREEN カウンタリストに記録します。

前述の IP オプションセットを持つパケットを検出するには、次のいずれかを行います。ここで指定するゾーンは、パケットが発生したセキュリティゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): 以下を入力して **Apply** をクリックします。

IP Record Route Option Detection: (**選択**)
IP Timestamp Option Detection: (**選択**)
IP Security Option Detection: (**選択**)
IP Stream Option Detection: (**選択**)

CLI

set zone *zone* screen ip-record-route
set zone *zone* screen ip-timestamp-opt
set zone *zone* screen ip-security-opt
set zone *zone* screen ip-stream-opt

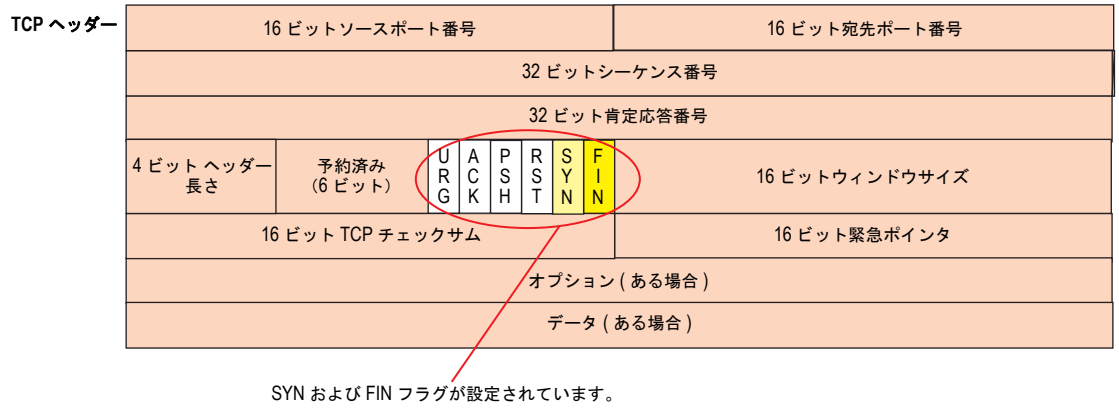
オペレーティングシステム探査

攻撃を開始する前に、攻撃者はターゲットホストを探査して、その OS (オペレーティングシステム) を確認しようとすることがあります。OS を確認することによって、攻撃者はどのような攻撃を行うか、そしてどの脆弱性を利用するかを決定できます。Juniper Networks セキュリティデバイスは、OS のタイプに関する情報収集によく使用される偵察探査をブロックします。

SYN および FIN フラグセット

通常、SYN および FIN 制御フラグはともに、同じ TCP セグメントヘッダーには設定されていません。SYN フラグは、TCP 接続を開始するためにシーケンス番号を同期化します。FIN フラグは、TCP 接続を終了するために、データ伝送の終了を示します。両フラグの目的は、相反するものです。TCP ヘッダーに SYN および FIN フラグが設定されるのは、異常な TCP 動作であり、OS によって異なるさまざまな応答が受信側から発生します。図 5 を参照してください。

図 5: SYN および FIN フラグが設定された TCP ヘッダー



攻撃者は、両方のフラグが設定されたセグメントを送信し、どのような種類のシステム応答が返されるかを確認することによって、受信側で動作している OS の種類を特定することがあります。そして攻撃者は、既知のシステムの脆弱性を利用して、さらに攻撃を行います。

この SCREEN オプションを有効にすると、セキュリティデバイスは、SYN および FIN フラグが TCP ヘッダーに設定されているかどうかをチェックします。そのようなヘッダーを検出すると、デバイスはパケットをドロップします。

SYN および FIN フラグの両方が設定されたパケットをブロックするには、次のいずれかを行います。ここで指定するゾーンは、パケットが発生したセキュリティゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): **SYN and FIN Bits Set Protection** を選択してから、**Apply** をクリックします。

CLI

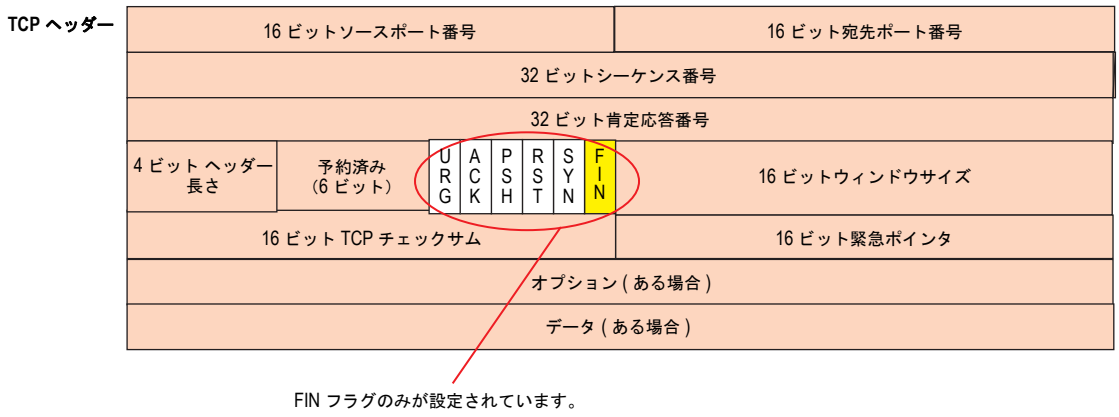
set zone *zone* screen syn-fin

ACK フラグのない FIN フラグ

図 6 に、FIN 制御フラグが設定 (セッションの終わりを合図し接続を終了するため) された TCP セグメントを表示します。通常、FIN フラグが設定された TCP セグメントには、ACK フラグも同時に設定 (前回のパケット受信を承認するため) されています。TCP ヘッダーに FIN フラグが設定され、ACK フラグが設定されないのは、異常な TCP 動作であるため、これに対する一様な応答はありません。OS は、RST フラグを設定した TCP セグメントを送信して応答することがあります。完全に無視するものもあります。被害側の応答によって、攻撃者はその OS に関する手がかり得ることがあります（FIN フラグを設定した TCP セグメントを送信する他の目的は、アドレスおよびポートスキャンの実行中に検出を逃れることと、FIN フラッドを代わりに実行することによって SYN フラッドを警戒する防御をくぐり抜けることです。FIN スキャンについては、15 ページの「FIN スキャン」を参照してください。）

注 : TCP/IP 実装の設計において、RFC 793、*Transmission Control Protocol* の解釈はベンダーによって違いが生じました。FIN フラグが設定されているのに ACK フラグが設定されていない TCP セグメントが到着したときに、RST セグメントを送信する実装もあります。また、RST を送信せずにパケットをドロップするものもあります。

図 6: FIN フラグが設定されている TCP ヘッダー



この SCREEN オプションを有効にすると、セキュリティデバイスは、TCP ヘッダーに FIN フラグが設定されているのに ACK フラグが設定されていないかどうかをチェックします。そのようなヘッダーを持つパケットを検出すると、デバイスはパケットをドロップします。

FIN フラグが設定されていて ACK フラグが設定されていないパケットをブロックするには、次のいずれかを行います。ここで指定するゾーンは、パケットが発生したセキュリティゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): **FIN Bit with No ACK Bit in Flags Protection** を選択してから、**Apply** をクリックします。

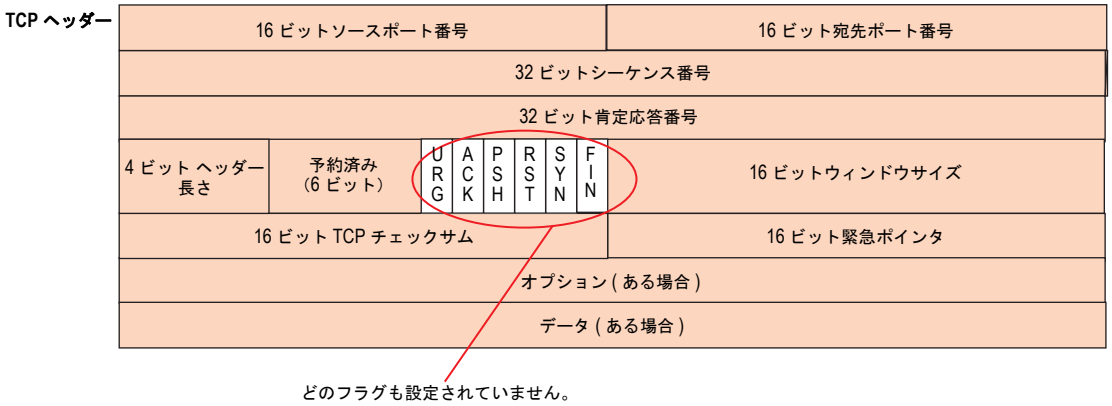
CLI

set zone *zone* screen fin-no-ack

フラグが設定されていない TCP ヘッダー

正常な TCP セグメントヘッダーには、少なくとも 1 つのフラグ制御が設定されています 。TCP セグメントに制御フラグが設定されないのは、異常な動作です。そのような異常に対する応答はオペレーティングシステムによって異なるため、標的のデバイスからの応答 (または応答がないこと) は、稼動している OS のタイプに関する手がかりとなるおそれがあります。図 7 を参照してください。

図 7: フラグが設定されていない TCP ヘッダー



設定されたフラグのない TCP セグメントヘッダーを検出できるようにセキュリティデバイスを設定すると、デバイスは、フラグフィールドのない、または不正な形式のフラグフィールドを持つ TCP パケットをすべてドロップします。

フラグが設定されていないパケットをブロックするには、次のいずれかを行います。ここで指定するゾーンは、パケットが発生したセキュリティゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): **TCP Packet without Flag Protection** を選択してから、**Apply** をクリックします。

CLI

set zone *zone* screen tcp-no-flag

回避技法

情報収集をする際にも攻撃を開始する際にも、攻撃者は検出を避けることが予期されます。IP アドレスおよびポートスキャンは露骨で容易に検出可能なものもありますが、したたかな攻撃者はさまざまな手段を用いて行動を隠します。SYN スキャンの代わりに FIN を使用するそのようなテクニックは、攻撃者がほとんどのファイアウォールや侵入検出プログラムを知っていることが多く、検出を逃れ、正常にタスクを遂行するための調査や発見技術が進化したことを示します。

FIN スキャン

FIN スキャンは応答 (RST フラグセットをもつ TCP セグメント) を引き起こそうとする FIN フラグをもつ TCP セグメントを送信するため、アクティブなホストまたはホストのアクティブなポートを発見します。攻撃者は、ICMP エコー要求を用いたアドレススイープや SYN セグメントを用いたアドレススキャンを行わず、FIN スキャン法を使用することがあります。攻撃者は、多くのファイアウォールは通常、前者の 2 つの手法に対する防御を行うことを知っています (ただし、FIN セグメントに対する防御がされないこともあります)。

FIN フラグが設定された TCP セグメントは検出できないことがあり、これを利用して攻撃者に偵察されるおそれがあります。

- FIN フラグセットをもつが TCP セグメントすべてを対象とする ACK フラグはもたない TCP セグメントを特別にブロックする SCREEN オプションを有効にします。

  WebUI: Screening > Screen: Zone ドロップダウンリストからこの SCREEN オプションを適用するゾーンを選択し、**FIN Bit With No ACK Bit in Flags Protection** を選択します。

  CLI: **set zone** *name* **screen fin-no-ack** を入力します。この場合、*name* は、この SCREEN オプションを適用するゾーンの名前です。

- CLI コマンド **set flow tcp-syn-check** を入力することにより、既存のセッションに属さない非 SYN パケットをすべて拒否するようにパケット処理方法を変更します。(SYN フラグのチェックに関する詳細は、16 ページの「非 SYN フラグ」を参照してください)。

注 : すべてのヌルスキャンなど (TCP フラグが設定されていないとき)、SYN フラグが既存のセッションに属さないパケットに対してその他のタイプの非 SYN スキャンも乗り越えることを確認できるようにパケットフローを変更します。

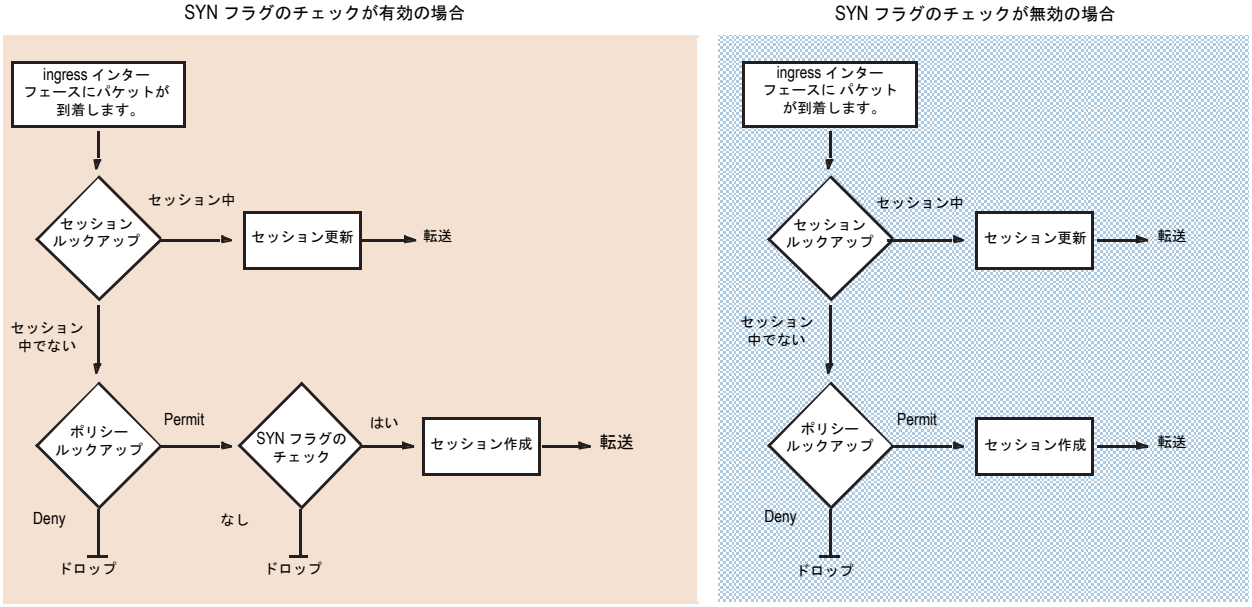
非 SYN フラグ

デフォルトでは、セキュリティデバイスはセッションの先頭パケットの SYN フラグを検査し、SYN フラグがオフになっているセッション開始 TCP セグメントを拒否します。このパケットのフローは変更しなくてもかまいません。または、デバイスがセッションを作成する前に SYN フラグのチェックを実施しないように変更することもできます。17 ページの図 8 に、SYN フラグのチェックが使用可能になっている場合と使用不可になっている場合のパケットフローの順序を示します。

注 : デフォルトでは、セッション先頭パケットの TCP SYN フラグ検査は、ScreenOS 5.1.0 以上が稼動する Juniper Networks セキュリティデバイスをインストールした時点で有効になっています。ScreenOS 5.1.0 より前のリリースからアップグレードした場合は、それまでに設定を変えていない限り、SYN フラグの検査は無効のままになっています。

ingress インターフェースがレイヤ 3 (Route モードまたは NAT モード) であってもレイヤ 2 (透過モード) であっても、このパケットフローは同じです。

図 8: SYN フラグのチェック



セキュリティデバイスの SYN フラグ検査機能を有効にすると、SYN フラグがオフになった TCP セグメントで、既存のセッションに属しないものが届いたとき、そのパケットをドロップし、ソースホストに TCP RST を返すようになります。ただしそのパケットのコードビットも RST である場合を除きます。この場合はパケットをドロップするだけで、送信元には通知しません。

以下の CLI コマンドを使用して SYN チェックを有効または無効に設定できます。

```
set flow tcp-syn-check
unset flow tcp-syn-check
```

最初のパケットの SYN フラグをチェックしないと、以下の利点があります。

- **非対称ルーティングをもつ NSRP:** 動的ルーティング環境のアクティブ / アクティブ NSRP 構成で、ホストは SYN フラグをもつ最初の TCP セグメントを送信して、1 台のセキュリティデバイス (Device-A) を設定する可能性がありますが、SYN/ACK はクラスタのその他のセキュリティデバイス (Device-B) にルーティングされる場合があります。Device-A が Device-B とセッションを同期させた後でこの非対称ルーティングが起こると、すべてがうまくいきます。一方、Device-A がセッションを同期させ、SYN チェックが有効になる前に SYN/ACK 応答が Device-B に到達すると、Device-B は SYN/ACK を拒否し、セッションを確立できなくなります。SYN チェックが無効に設定され、Device-B が SYN/ACK 応答を受け入れると、属する既存のセッションがない場合でも、新しいセッションテーブルエントリが作成されます。
- **中断なしのセッション :** SYN チェックが有効であり、透過モードで動作するセキュリティデバイスを作業ネットワークに追加した場合、すべての既存のセッションが中断され、後で再開される必要が出てきます。大きなデータ転送やデータベース バックアップなどの長いセッションでは、中断が起こるとやっかいです。同様に、デバイスをリセットしたり、ポリシーのコアセクションのコンポーネントを変更して SYN チェックが有効になっている場合、既存のセッションまたはポリシーの変更が適用されるセッションはすべて中断され、再開が必要になります。SYN チェックを無効にすると、ネットワークトラフィックのフローの中断を避けることができます。

注： このシナリオの解決策は、最初に SYN チェックを無効にしたセキュリティデバイスをインストールすることです。その数時間後に、確立されたセッションがデバイスを通じて実行されたら、SYN チェックを有効にします。

ポリシーのコアセクションには、以下のメインコンポーネントが含まれます。ソースと宛先ゾーン、ソースと宛先アドレス、1 つまたは複数のサービス、およびアクションです。

しかし、上記の利点には以下の欠点があります。

- **調査ホール：** ACK、URG、RST、FIN などの非 SYN フラグをもつ最初の TCP セグメントが閉じたポートに到達すると、多くのオペレーティングシステム (例えば、Windows) は RST フラグセットをもつ TCP セグメントに応答します。ポートが開いている場合、受信者は応答を生成しません。

  これらの応答を調査したり、その応答が欠落していると、情報の収集者は保護されたネットワーク上、および ScreenOS ポリシーセット上でも調査を実行できます。収集者が非 SYN フラグをもつ TCP セグメントを送信し、ポリシーがその通過を許可すると、そのセグメントを受信する宛先ホストがそれをドロップし、RST フラグセットをもつ TCP セグメントで応答する場合があります。そのような応答では、特定のアドレスでアクティブなホストがあり、目的のポート番号が閉じていることを悪意のある人に伝達します。情報収集者はまた、そのホストのポート番号へのアクセスをファイアウォールポリシーが許可することを学習します。

  SYN フラグのチェックを有効にすることで、セキュリティデバイスは SYN フラグをもたない TCP セグメントが既存のセッションに属さない場合にそれをドロップします。TCP RST セグメントを返しません。結果として、スキャナーはポリシーセットにかかわりなく、ポートが目的のホストで開いているか閉じているかにかかわりなく、応答を取得しません。

- **セッションテーブルのフラッド：** SYN チェックが無効の場合、攻撃者は非 SYN フラグセットをもつ TCP セグメントの集中攻撃で保護されたネットワークをフラッドすることにより、ScreenOS SYN フラッド保護機能をバイパスできます。目的のホストがパケットをドロップした場合でも、また応答で TCP RST セグメントを送信した可能性があった場合でも、そのようなフラッドはセキュリティデバイスのセッションテーブルを満たすことができます。セッションテーブルが満杯になると、デバイスは正当なトラフィックに対して新しいセッションを処理できなくなります。

  SYN チェックおよび SYN フラッド保護を有効にすることにより、この種の攻撃を回避できます。SYN フラッグがセッションの最初のパケットでセットされていることを確認すると、すべての新しいセッションで SYN フラグセットをもつ TCP セグメントが開始されます。SYN フラッド保護は、その後、1 秒間の TCP SYN セグメントの数を制限するため、セッションテーブルが溢れることはなくなります。

注： セッションテーブルフラッドに関する詳細は、30 ページの「セッションテーブルフラッド」を参照してください。SYN フラッドに関しては、36 ページの「SYN フラッド」を参照してください。

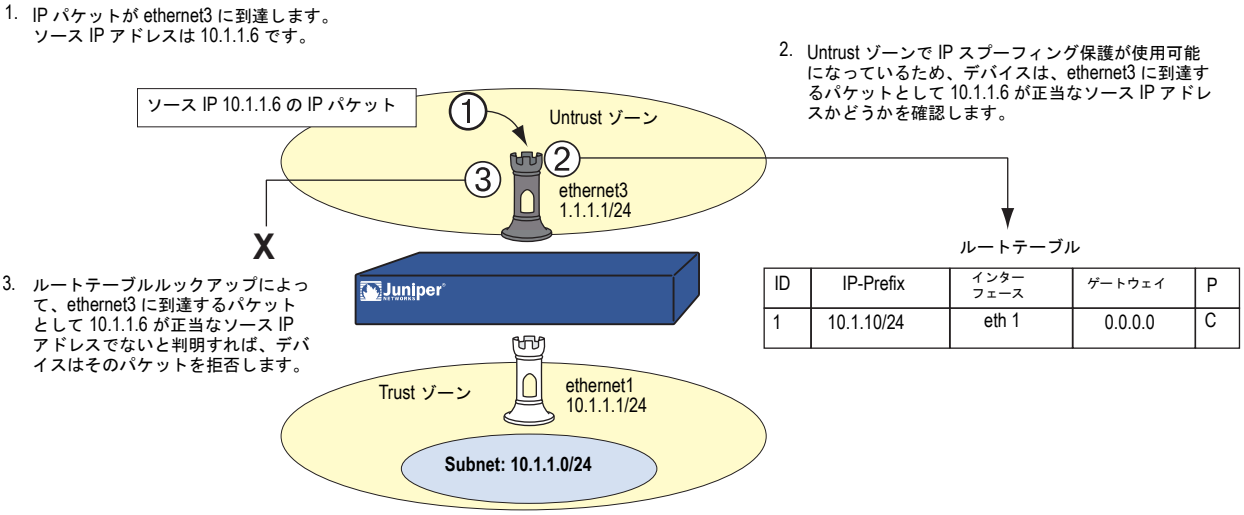
SYN フラグのチェック機能は、特殊な場合を除いて有効にしておくよう強く推奨します (ScreenOS ではこれがデフォルトの設定です)。コマンド **set flow tcp-syn-check** を実行すると、この機能が有効になります。SYN チェックを有効にすると、セキュリティデバイスは確立したセッションに属さない限り、非 SYN フラグセットをもつ TCP セグメントを拒否します。

IP スプーフィング

ネットワークの制限領域へのアクセスを得ようとする手法の 1 つは、偽のソースアドレスをパケットヘッダーに挿入し、そのパケットがトラステッドゾーンから到達したように見せかけることです。この技法は、IP スプーフィングと呼ばれています。ScreenOS には 2 つの IP スプーフィング検知方法があり、どちらの方法も同じタスクを行います。つまり、パケットがヘッダーに示された場所以外から到達したことを判定します。Juniper Networks セキュリティデバイスが使用する方法は、それが OSI モデルのレイヤ 3 で動作するか、レイヤ 2 で動作するかによって異なります。

- **レイヤ 3 :** セキュリティデバイス上のインターフェースが Route モードまたは NAT モードで動作している場合、IP スプーフィングの検出機構はルートテーブルエントリを活用します。たとえば、ソース IP アドレス 10.1.1.6 を持つパケットが ethernet3 に到達しても、セキュリティデバイスが ethernet1 を介して 10.1.1.0/24 へのルートを持つ場合は、IP スプーフィングチェックによって、このアドレスが無効なインターフェースに到達したと判断されます。つまり、ルートテーブルに定義されているように、10.1.1.6 からの正当なパケットは ethernet3 ではなく、ethernet1 にのみ到達できるからです。したがって、デバイスはそのパケットがスプーフィングされたソース IP アドレスと判断し破棄します。

図 9: レイヤ 3 IP スプーフィング

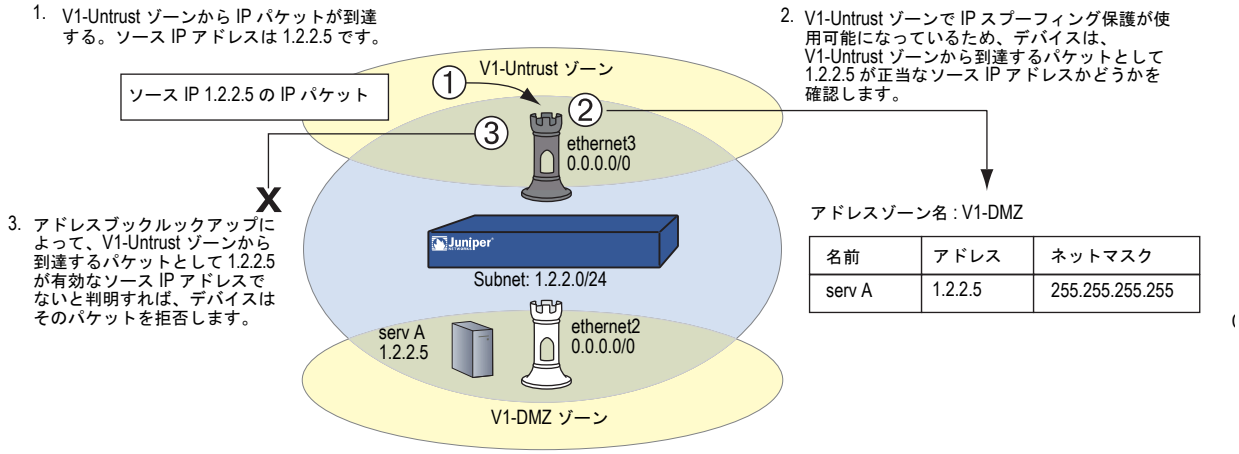


パケットのソース IP アドレスが、ルートテーブル内に見つからない場合は、デフォルトでセキュリティデバイスは、そのパケットの通過を許可します (それを許可するポリシーが存在する場合)。次の CLI コマンドを使用すると (ここで指定するセキュリティゾーンは、パケットが作成されたゾーンです)、ソース IP アドレスがルートテーブルに見つからないパケットをすべてドロップするように、セキュリティデバイスに指示できます。

```
set zone zone screen ip-spoofing drop-no-rpf-route
```

- **レイヤ 2** ― セキュリティデバイスのインターフェースが透過モードで動作している場合、IP スプーフィングチェック機構はアドレス帳エントリを利用します。たとえば、「serv A」のアドレスを V1-DMZ ゾーンの 1.2.2.5/32 と定義します。ソース IP アドレス 1.2.2.5 を持つパケットが V1-Untrust ゾーンインターフェース (ethernet3) に到達した場合、IP スプーフィングチェックによって、このアドレスが無効なインターフェースに到達したと判断されます。このアドレスは、V1-Untrust ゾーンではなく V1-DMZ ゾーンに属するものあって、V1-DMZ にバインドされた ethernet2 でのみ承認されます。デバイスは、そのパケットがスプーフィングされたソース IP アドレスと判断し破棄します。

図 10: レイヤ 2 IP スプーフィング



複数のセキュリティゾーンにまたがるサブネットのアドレスを定義する際には注意が必要です。図 10 では、1.2.2.0/24 は V1-Untrust および V1-DMZ ゾーンの両方に属します。次のようにセキュリティデバイスを構成すると、許可しようとする V1-DMZ ゾーンからのトラフィックがデバイスにブロックされます。

- 1.2.2.0/24 のアドレスを V1-Untrust ゾーン内に定義する。
- V1-DMZ ゾーン内の任意のアドレスから V1-Untrust ゾーン内の任意のアドレスへのトラフィックを許可するポリシーがある (**set policy from v1-dmz to v1-untrust any any any permit**)。
- IP スプーフィングチェックを使用可能にしている。

V1-DMZ ゾーンのアドレスは、1.2.2.0/24 サブネットにも存在するため、これらのアドレスからのトラフィックが ethernet2 に到達すると、IP スプーフィングチェックでアドレス帳が参照され、V1-Untrust ゾーンの 1.2.2.0/24 を見つけます。その結果、セキュリティデバイスはトラフィックをブロックします。

例 : L3 IP スプーフィング保護

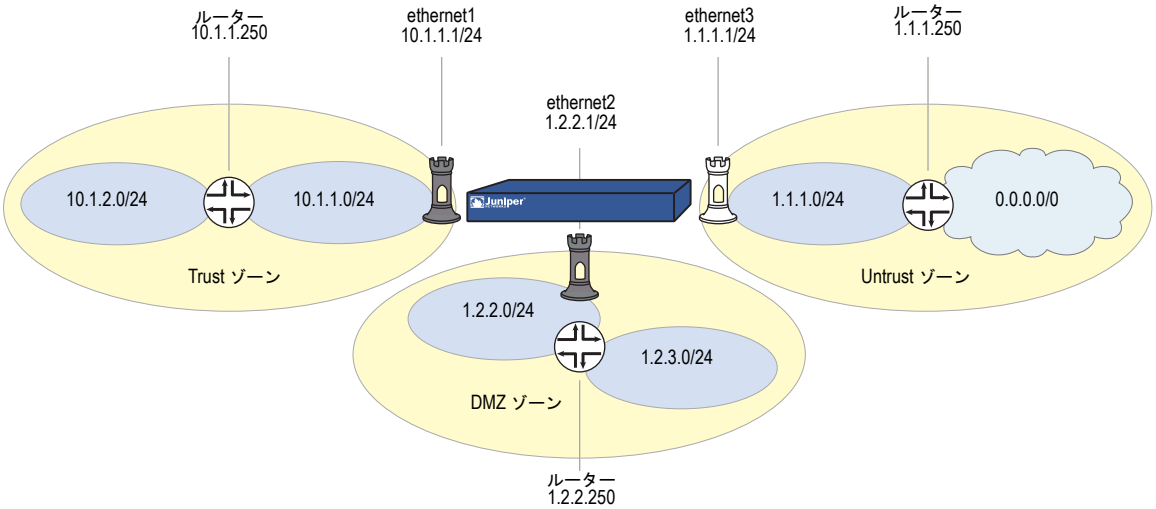
この例では、レイヤ 3 で動作する Juniper Networks セキュリティデバイスに対して、Trust、DMZ、および Untrust ゾーンの IP スプーフィング保護を使用可能にします。デフォルトでデバイスは、インターフェース IP アドレスに指定されたサブネットのルートテーブル内のエントリを自動的に作成します。これらの自動ルートテーブルエントリに加えて、次の表に表示されている 3 つのルートを手動で入力します。

宛先	出口インターフェース	隣接ゲートウェイ
10.1.2.0/24	ethernet1	10.1.1.250
1.2.3.0/24	ethernet2	1.2.2.250
0.0.0.0/0	ethernet3	1.1.1.250

IP スプーフィング保護 SCREEN オプションを有効にしても、上記の 3 つのルートを入力しなければ、デバイスは「宛先」列のアドレスからのすべてのトラフィックをドロップし、イベントログにアラームを入力します。たとえば、ソースアドレス 10.1.2.5 を持つパケットが ethernet1 に到達しても、ethernet1 を経由してサブネット 10.1.2.0/24 へ到達するルートがなければ、デバイスはそのパケットが無効なインターフェースに到達したと判断して、パケットをドロップします。

この例のすべてのセキュリティゾーンは、trust-vr ルーティングドメインに存在します。

図 11: レイヤ 3 IP スプーフィングの例



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24

   次のように入力してから **OK** をクリックします。

   Interface Mode:NAT

   Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

   Zone Name: DMZ
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.2.2.1/24

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. **ルート**
   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 10.1.2.0/24
   Gateway: (選択)
   Interface: ethernet1
   Gateway IP Address: 10.1.1.250

   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 1.2.3.0/24
   Gateway: (選択)
   Interface: ethernet2
   Gateway IP Address: 1.2.2.250

   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選択)
   Interface: ethernet3
   Gateway IP Address: 1.1.1.250

3. **IP スプーフィング保護**
   Screening > Screen (Zone: Trust): **IP Address Spoof Protection** を選択して、**Apply** をクリックします。

   Screening > Screen (Zone: DMZ): **IP Address Spoof Protection** を選択して、**Apply** をクリックします。

   Screening > Screen (Zone: Untrust): **IP Address Spoof Protection** を選択して、**Apply** をクリックします。

CLI

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet2 zone dmz
   set interface ethernet2 ip 1.2.2.1/24
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **ルート**
   set vrouter trust-vr route 10.1.2.0/24 interface ethernet1 gateway 10.1.1.250
   set vrouter trust-vr route 1.2.3.0/24 interface ethernet2 gateway 1.2.2.250
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

3. **IP スプーフィング保護**
   set zone trust screen ip-spoofing
   set zone dmz screen ip-spoofing
   set zone untrust screen ip-spoofing
   save

例 : L2 IP スプーフィング保護

この例では、V1-Untrust ゾーンで発生したトラフィック上の IP スプーフィングから V1-DMZ ゾーンを保護します。最初に、V1-DMZ ゾーンの 3 つの Web サーバーに対して、次のアドレスを定義します。

- servA: 1.2.2.10
- servB: 1.2.2.20
- servC: 1.2.2.30

そして、V1-Untrust ゾーンの IP スプーフィングを使用可能にします。

V1-Untrust ゾーン内の攻撃者が、V1-DMZ ゾーンの 3 つのアドレスのいずれかを使用してソース IP アドレスをスプーフィングしようとすると、セキュリティデバイスはこのアドレスとアドレス帳にあるアドレスとを照合します。V1-Untrust ゾーンから送られたパケットのソース IP アドレスが、V1-DMZ ゾーンに定義されたアドレスに属すると判明すると、デバイスはそのパケットを拒否します。

WebUI

1. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: servA
   IP Address/Domain Name:
   IP/Netmask: (**選択する**), 1.2.2.10/32
   Zone: V1-DMZ

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name:servB
   IP Address/Domain Name:
   IP/Netmask: (**選択する**), 1.2.2.20/32
   Zone: V1-DMZ

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: servC
   IP Address/Domain Name:
   IP/Netmask: (**選択する**), 1.2.2.30/32
   Zone: V1-DMZ

2. **IP スプーフィング保護**
   Screening > Screen (Zone: V1-Trust): **IP Address Spoof Protection** を選択して、**Apply** をクリックします。

CLI

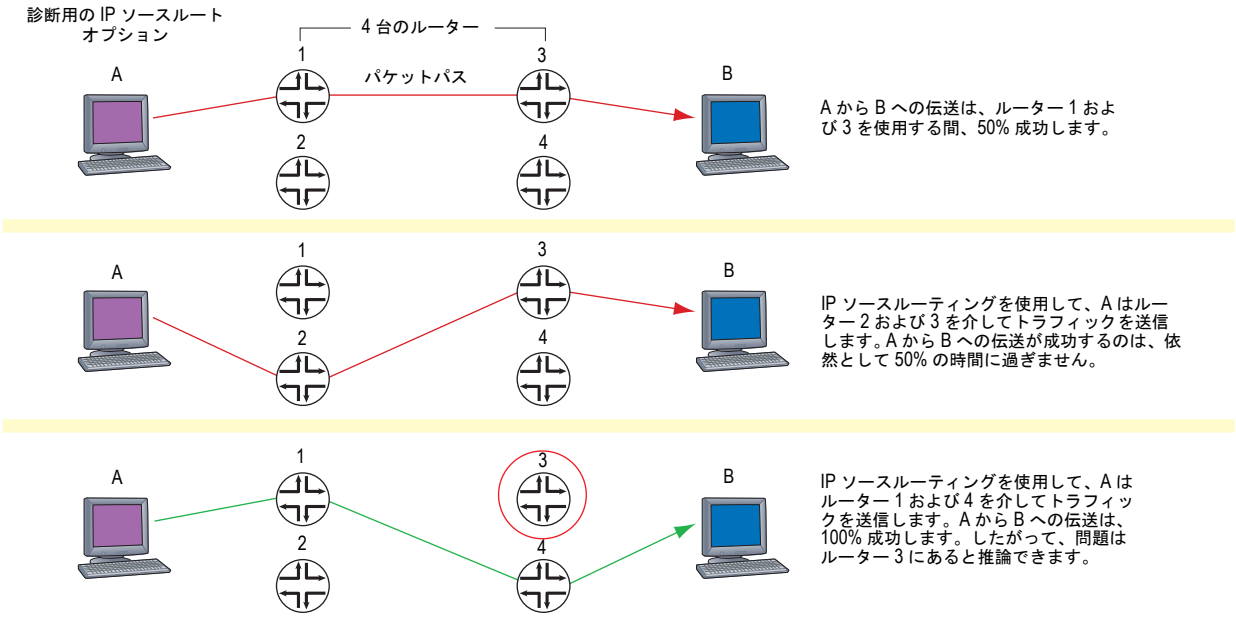
1. **アドレス**
   set address v1-dmz servA 1.2.2.10/32
   set address v1-dmz servB 1.2.2.20/32
   set address v1-dmz servC 1.2.2.30/32

2. **IP スプーフィング保護**
   set zone v1-untrust screen ip-spoofing
   save

IP スプーフィング保護

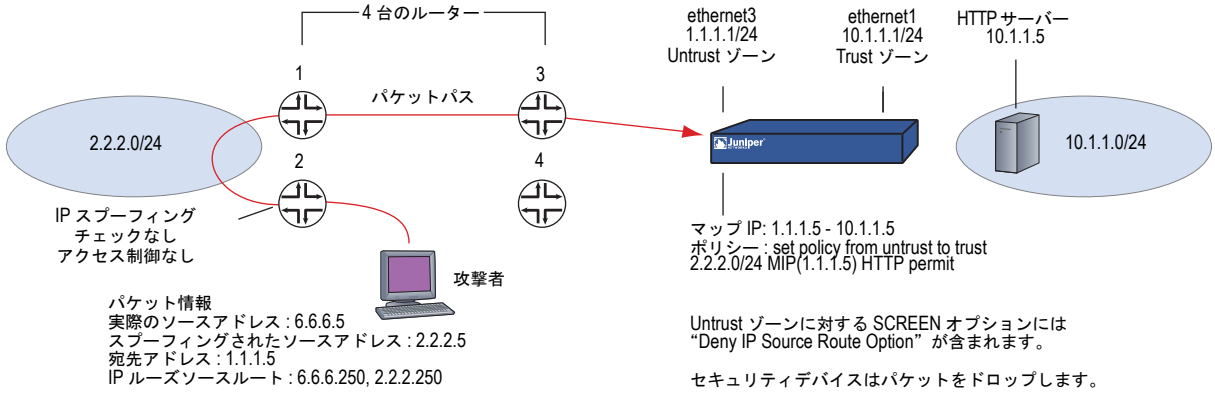
ソースルーティングは、IP パケット伝送のソース側のユーザーが、IP パケットがユーザーの希望に従って宛先までたどるパスに沿って存在する、ルーターの IP アドレスを指定できるようにするために設計されました。IP ソースルートオプションの本来の目的は、診断分析に役立つルート制御ツールを利用できるようにすることでした。たとえば、特定の宛先へのパケットの伝送が不規則に失敗する場合、まず最初に、レコードルートまたは IP タイムスタンプオプションを使用して、パスに沿ったルーターのアドレスまたはパケットが通ったパスを見つけることを考えます。そしてルーズあるいはストリクトソースルートオプションを利用し、レコードルートまたはタイムスタンプオプションの結果から判明したアドレスを使用すれば、特定のパスに沿うようにトラフィックを誘導できます。パスを変更するようにルーターアドレスを変更し、さまざまなパスに沿っていくつかのパケットを送信することによって、成功率が上昇したかまたは低下したかを知ることができます。分析と消去法によって、問題が存在する場所を推論できることもあります。

図 12: IP ソースルーティング



IP ソースルートオプションを使用することには、本来害はありませんが、攻撃者は有害な用途に使用するようになりました。攻撃者は IP ソースルートオプションを使用して自身の本当のアドレスを隠し、異なるパスを指定することによってネットワークの制限領域にアクセスします。攻撃者がどのようにこの 2 つの偽装方法を使用するのかを示す例として、図 13 に表示される次のシナリオを考えます。

図 13: 偽装用のルーズ IP ソースルートオプション



Juniper Networks セキュリティデバイスは、トラフィック 2.2.2.0/24 が Untrust ゾーンにバインドされたインターフェースである ethernet1 を経由して到達した場合、このトラフィック 2.2.2.0/24 のみを許可します。ルーター 3 および 4 はアクセス制御を強制しますが、ルーター 1 および 2 は強制しません。さらに、ルーター 2 は IP スプーフィングのチェックを行いません。攻撃者はソースアドレスをスプーフィングし、そしてルーズソースルートオプションを使用することによって、ルーター 2 から 2.2.2.0/24 ネットワークへ向かい、そこからルーター 1 を通り抜けるようにパケットを誘導します。ルーター 1 はそのパケットをルーター 3 へ転送し、ルーター 3 はパケットをセキュリティデバイスへ転送します。パケットは 2.2.2.0/24 サブネットから到達し、そのサブネットのソースアドレスを持つため、有効であるように見えます。しかし、それ以前にルーズソースルートオプションで偽装されている可能性があります。ルーズソースルートオプションがあります。この例では、Untrust ゾーンに対して「Deny IP Source Route Option」SCREEN オプションを使用可能にしています。パケットが ethernet3 に到達すると、デバイスはそのパケットを拒否します。

ルーズまたはストリクトソースルートオプションが設定された任意のパケットをブロックするか、またはそのようなパケットを検出してから、ingress インターフェースのカウンタリストにイベントを記録するかのいずれかが行えるように、セキュリティデバイスを設定できます。SCREEN オプションは、次のとおりです。

- **Deny IP Source Route Option:** このオプションを使用可能にすると、ルーズまたはストリクトソースルートオプションを利用するすべての IP トラフィックをブロックします。ソースルートオプションによって、攻撃者が虚偽の IP アドレスを使用してネットワークに侵入することがあります。

- **Detect IP Loose Source Route Option:** セキュリティデバイスは、IP オプションが 3 (ルーズソースルーティング) であるパケットを検出し、ingress インターフェースの SCREEN カウンタリストにイベントを記録します。このオプションは、パケットがソースから宛先へ移動する際に利用する部分的なルートリストを指定します。パケットは指定されたアドレスの順に進む必要がありますが、指定されたルーター間にある他のルーターを通過することは許可されます。

- **Detect IP Strict Source Route Option:** セキュリティデバイスは、IP オプションが 9 (ストリクトソースルーティング) であるパケットを検出し、ingress インターフェースの SCREEN カウンタリストにイベントを記録します。このオプションは、パケットがソースから宛先へ移動する際に利用する全ルートリストを指定します。宛先フィールドのアドレスは、リストの最後のアドレスに差し替えられます。

  (全 IP オプションの詳細については、10 ページの「IP オプションを使用したネットワーク偵察」を参照してください。)

ルーズまたはストリクトソースルートオプションのいずれかが設定されたパケットをブロックするには、次のいずれかを行います。ここで指定するゾーンは、パケットが発生したセキュリティゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): **IP Source Route Option Filter** を選択してから、**Apply** をクリックします。

CLI

set zone *zone* screen ip-filter-src

ルーズまたはストリクトソースルートオプションが設定されたパケットを検出し記録する (ただし、ブロックしない) するには、次のいずれかを行います。ここで指定するゾーンは、パケットが発生したセキュリティゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): 以下を入力して **Apply** をクリックします。

IP Loose Source Route Option Detection: (選択)
IP Strict Source Route Option Detection: (選択)

CLI

set zone *zone* screen ip-loose-src-route
set zone *zone* screen ip-strict-src-route

第 3 章

サービス拒否 (DoS) 攻撃の防御

DoS (サービス拒否) 攻撃の目的は、被害を与える標的に偽りのトラフィックを大量に送り、その偽りのトラフィックの処理に追われて合法トラフィックを処理できないようにすることです。標的となる可能性があるのは、Juniper Networks ファイアウォール、ファイアウォールがアクセスを制御するネットワークリソース、または各ホストの特定のハードウェアプラットフォームか OS (オペレーティングシステム) です。

DoS 攻撃が複数のソースアドレスから行われる場合、これは DDoS (分散サービス拒否) と呼ばれます。一般的に、DoS 攻撃のソースアドレスはスプーフィングされています。DDoS 攻撃のソースアドレスはスプーフィングされたアドレス、または攻撃者が既に障害を発生させて、「ゾンビエージェント」として攻撃を仕掛ける拠点に使用しているホストの実アドレスが考えられます。

セキュリティデバイスは、デバイス自身およびデバイスが保護するリソースを DoS および DDoS 攻撃から防御します。以降のセクションでは、利用可能なさまざまな防御オプションについて説明します。

- 30 ページの「ファイアウォール DoS 攻撃」
  - 30 ページの「セッションテーブルフラッド」
  - 34 ページの「SYN-ACK-ACK プロキシフラッド」
- 36 ページの「ネットワーク DoS 攻撃」
  - 36 ページの「SYN フラッド」
  - 47 ページの「SYN クッキー」
  - 49 ページの「ICMP フラッド」
  - 50 ページの「UDP フラッド」
  - 51 ページの「ランド攻撃」
- 52 ページの「OS 指定 DoS 攻撃」
  - 52 ページの「Ping of Death」
  - 53 ページの「ティアドロップ攻撃」
  - 54 ページの「WinNuke」

ファイアウォール DoS 攻撃

Juniper Networks ファイアウォールを発見すると、攻撃者はファイアウォールの背後にあるネットワークの代わりに、ファイアウォールそのものに DoS (サービス拒否) 攻撃を開始することがあります。ファイアウォールに対して効果的な DoS 攻撃は、合法トラフィックがファイアウォールを通過しようとするのを阻止するため、保護されたネットワークに対しても効果的な DoS 攻撃となります。このセクションでは、Juniper Networks セキュリティデバイスのセッションテーブルを満杯にして DoS を行うために、攻撃者が使用すると考えられる 2 つの方法、すなわち 「セッションテーブルフラッド」および「SYN-ACK-ACK プロキシフラッド」について説明します。

セッションテーブルフラッド

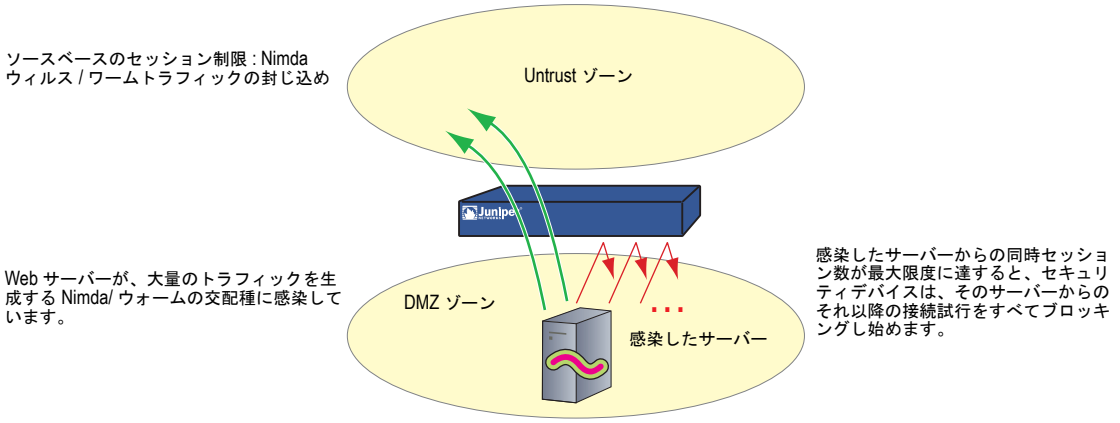
DoS 攻撃が成功すると、被害側は極めて大量の模造トラフィックを送りつけられ、合法的接続要求の処理が不可能になります。DoS 攻撃には、SYN フラッド、SYN-ACK-ACK フラッド、UDP フラッド、ICMP フラッドなどのさまざまな形式がありますが、その目的はすべて同じで、被害側のセッションテーブルを満杯にすることです。セッションテーブルが満杯になると、ホストは新しいセッションを作成できず、新しい接続要求を拒否し始めます。次の SCREEN オプションは、そのような攻撃を緩和するのに役立ちます。

- 「ソースベースおよび宛先ベースセッション制限」
- 「アグレッシブエージング」

ソースベースおよび宛先ベースセッション制限

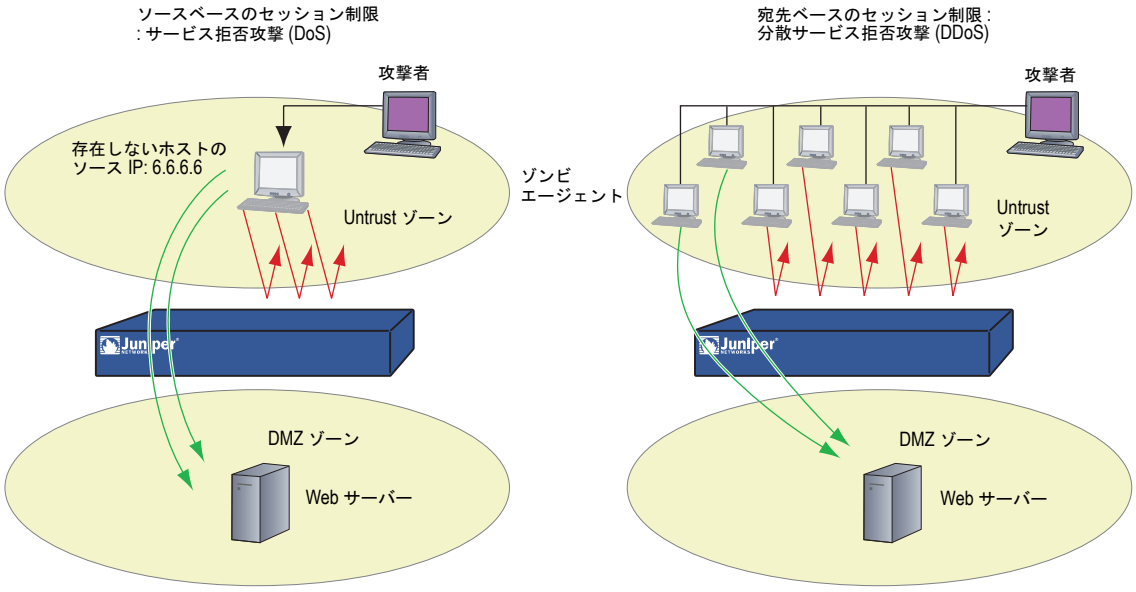
同一のソース IP アドレスからの同時セッション数を制限するのに加えて、同一の宛先 IP アドレスへの同時セッション数を制限することもできます。ソースベースのセッション制限を設定する利点の 1 つは、サーバーに伝染しそのサーバーから大量のトラフィックを生成し始める Nimda ウィルス (実際には、ウィルスでかつワームです) などの攻撃を抑制できることです。ウィルスが生成するトラフィックはすべて同一の IP アドレスから発生するため、ソースベースのセッション制限を行えば、ファイアウォールによってそのような過大量のトラフィックを確実に抑えることができます。

図 14: ソース IP アドレスベースのセッション制限



ソースベースのセッション制限を行うもう 1 つの利点は、すべての接続試行が同一のソース IP アドレスから行われる場合に、ScreenOS セッションテーブルを満杯にしようとするのを緩和できることです。しかし、策略に富む攻撃者は DDoS (サービス拒否) 攻撃を仕掛けることもあります。DDoS 攻撃では、*ゾンビエージェント*と呼ばれ密かに攻撃者によって制御される数百ものホストから、不正なトラフィックが発生することがあります。SYN、UDP、および ICMP フラッド検出と防止の SCREEN オプションに加えて、宛先ベースのセッション制限を設定することによって、セキュリティデバイスは、任意の 1 台のホストへの許容可能な数の同時接続要求 (ソースにかかわらず) のみを確実に許可します。

図 15: 分散 DoS 攻撃



接続要求の許容数をどの要素によって定めるかを決定するには、一定期間にわたり観測と分析を行い、標準的なトラフィックフローの基準を確立する必要があります。また、使用している特定の Juniper Networks プラットフォームのセッションテーブルを満杯にするのに必要となる同時セッションの最大数を考慮することも必要です。セッションテーブルがサポートするセッションの最大数を調べるには、CLI コマンドの **get session** を使用します。出力された最初の行には、現在の (割り当てられた) セッション数、セッションの最大数、および失敗したセッションの割り当て数がリスト表示されます。

```
alloc 420/max 128000, alloc failed 0
```

ソースベースおよび宛先ベースのセッション制限のデフォルト最大数はともに、128 の同時セッションですが、お使いのネットワーク環境およびプラットフォームに適するように調整が必要となることもあります。

例：ソースベースのセッション制限

この例では、DMZ および Trust ゾーンの任意の 1 台のサーバーから起動できるセッション数を制限します。DMZ ゾーンに存在するのは Web サーバーのみで、いずれもトラフィックを開始できないため、ソースセッション制限を設定可能な最低値である 1 セッションに設定します。また一方で、Trust ゾーンにはパーソナルコンピュータ、サーバー、プリンターなどが含まれ、それらの多数はトラフィックを開始します。Trust ゾーンには、ソースセッション制限最大数を 80 同時セッションに設定します。

WebUI

Screening > Screen (Zone: DMZ): 次のように入力してから **OK** をクリックします。

Source IP Based Session Limit: (選択)
Threshold: 1 Sessions

Screening > Screen (Zone: Trust): 次のように入力してから **OK** をクリックします。

Source IP Based Session Limit: (選択)
Threshold: 80 Sessions

CLI

```
set zone dmz screen limit-session source-ip-based 1
set zone dmz screen limit-session source-ip-based
set zone trust screen limit-session source-ip-based 80
set zone trust screen limit-session source-ip-based
save
```

例：宛先ベースのセッション制限

この例では、1.2.2.5 の Web サーバーへのトラフィック量を制限します。サーバーは DMZ ゾーンにあります。Untrust ゾーンからこのサーバーへのトラフィックフローを 1 ヶ月間にわたり観測した後、サーバーが受ける同時セッションの平均数は、2000 と判断しました。この情報に基づいて、新たにセッション制限を 4000 同時セッションに設定することにします。観測結果により、トラフィックがしばしば瞬間的にこの制限を越えることがあるのがわかりますが、散発的なサーバーアクセス不能が生じても、ファイアウォールセキュリティを優先させることにします。

WebUI

Screening > Screen (Zone: Untrust): 次のように入力してから **OK** をクリックします。

Destination IP Based Session Limit: (選択)
Threshold: 4000 Sessions

CLI

```
set zone untrust screen limit-session destination-ip-based 4000
set zone untrust screen limit-session destination-ip-based
save
```

アグレッシブエージング

デフォルトでは、初回の TCP セッション 3 方向ハンドシェイクは、タイムアウトするのに (つまり、アクティブでないために期限切れとなるのに) 20 秒を要します。TCP セッションが確立すると、それ以後は、タイムアウト値は 30 秒に変更されます。HTTP および UDP セッションに対しては、セッションタイムアウトはそれぞれ、5 分および 1 分です。セッションタイムアウトカウンタは、セッションが開始されたときに起動し、セッションがアクティブであれば 10 秒毎に更新されます。セッションが 10 秒以上にわたり待機状態になれば、タイムアウトカウンターはカウントダウンを始めます。

特定のハードウェアプラットフォームでは、ScreenOS が提供する機構では、セッションテーブル内のセッション数が指定された高水準しきい値を越えた場合に、タイムアウト処理を加速できます。この機能は、ハイエンドのシステムでは使用できません。

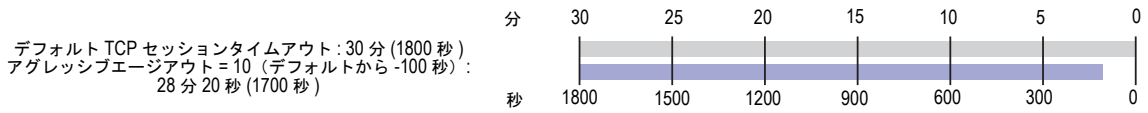
セッション数が指定した低水準しきい値を下回ると、タイムアウト処理は通常の状態に戻ります。アグレッシブエージアウト処理が実施されている間、セキュリティデバイスは、指定したエージアウト率を使用して、最も古いセッションを最初にエージアウトします。これらのエージアウトされたセッションは、無効のタグを付けられ、2 秒毎に発生する次の「ガーベッジスイープ」で削除されます。

アグレッシブエージアウトオプションは、入力した秒数だけデフォルトセッションタイムアウトを減らします。アグレッシブエージアウトオプションを設定し使用可能にすると、構成に表示される通常のタイムアウト値は、TCP に対しては 1800 秒間、HTTP に対しては 300 秒間、UDP セッションに対しては 60 秒間、変更されません。ただし、アグレッシブエージアウト期間が実施されている場合は、これらのセッションは、ゼロまで完全にカウントダウンせずに、早期エージアウトに指定した時間分早くタイムアウトします。

各ユニットにおける間隔が 10 秒であれば 、アグレッシブエージアウト値は、2 台から 10 台のユニット間に設定可能です (つまり、アグレッシブエージアウト設定は、20 秒と 100 秒の間に可能です)。デフォルト設定は 2 ユニットまたは 20 秒です。たとえば、アグレッシブエージアウト設定を 100 秒に定義すれば、TCP および HTTP セッションタイムアウトは次のように短縮されます。

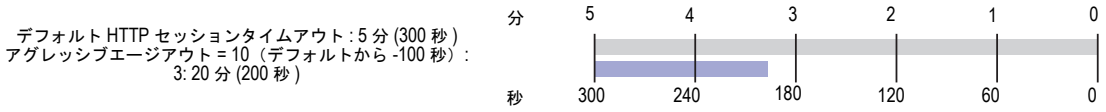
- TCP: アグレッシブエージング処理が実施されている間、セッションタイムアウト値は 1800 秒 (30 分) から 1700 秒 (28 分 20 秒) に短縮されます。その期間、セキュリティデバイスは、タイムアウト値が 1700 秒を超えた TCP セッションを、最も古いセッションから順にすべて削除します。

図 16: TCP セッションタイムアウト



- HTTP: アグレッシブエージング処理が実施されている間、セッションタイムアウト値は 300 秒 (5 分) から 200 秒 (3 分 20 秒) に短縮されます。その期間、セキュリティデバイスは、タイムアウト値が 200 秒を超えた HTTP セッションを、最も古いセッションから順にすべて削除します。

図 17: HTTP セッションタイムアウト

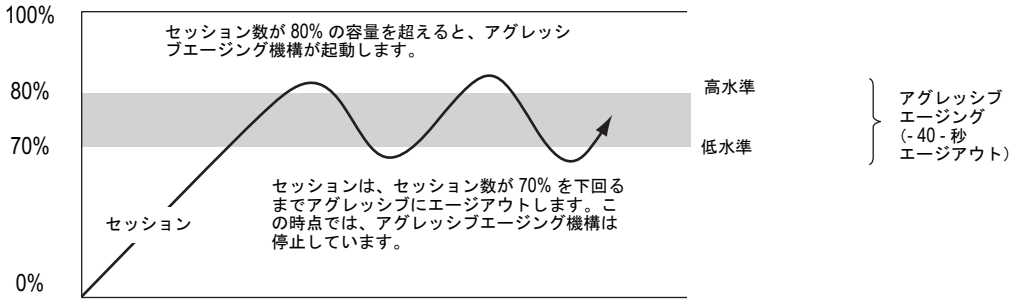


- UDP: デフォルト UDP セッションタイムアウトは 60 秒のため、早期エージアウト設定を 100 秒に定義すると、すべての UDP セッションがエージアウトし、次回のガーベッジスイープの削除対象となります。

例 : アグレッシブにエージアウトするセッション

この例では、トラフィックが 80 % の高水準値を上回るとエージアウト処理が開始し、トラフィックが 70 % の低水準値を下回るとエージアウト処理が停止するように設定します。アグレッシブエージアウト間隔に 40 秒を指定します。セッションテーブルが 80 % (高水準しきい値) を超えて埋められると、セキュリティデバイスはすべてのセッションのタイムアウトを 40 秒減らし、テーブルのセッション数が 70 % (低水準しきい値) を下回るまで、最も古いセッションのアグレッシブエージアウトを開始します。

図 18: アグレッシブにエージアウトするセッション



WebUI

注 : アグレッシブエージアウト設定を構成するには、CLI を使用する必要があります。

CLI

```
set flow aging low-watermark 70
set flow aging high-watermark 80
set flow aging early-ageout 4
save
```

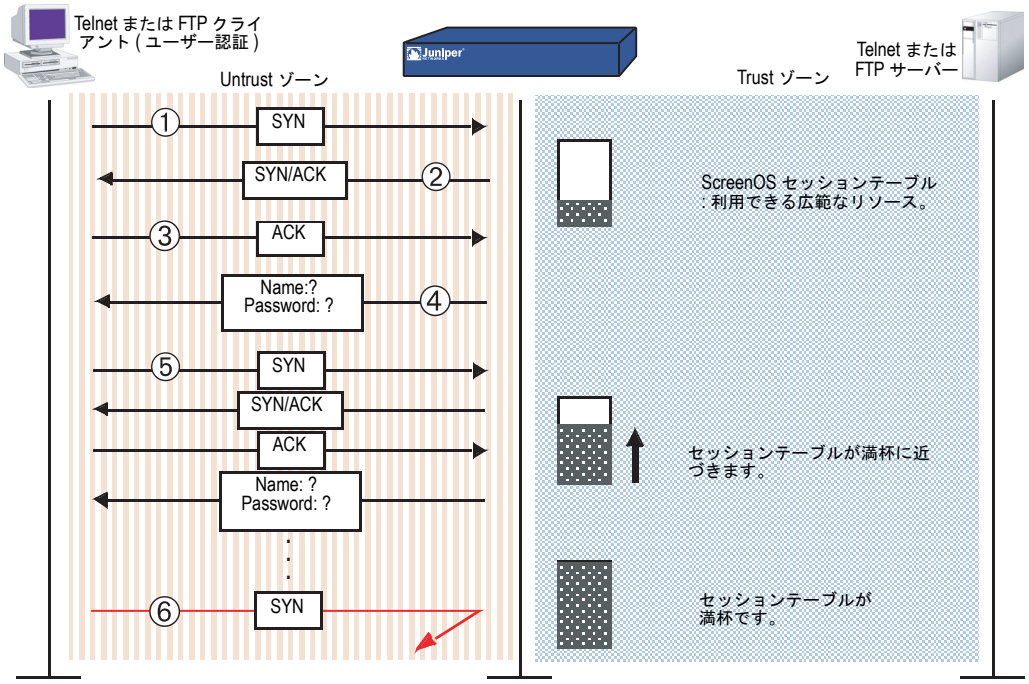
SYN-ACK-ACK プロキシフラッド

認証ユーザーが Telnet または FTP 接続を開始するとき、ユーザーは SYN セグメントを Telnet または FTP サーバーに送信します。セキュリティデバイスは SYN セグメントを代行受信し、セッションテーブルにエントリを作成して SYN-ACK セグメントをユーザーにプロキシします。その後に、ユーザーは ACK セグメントで応答します。この時点で、初回の 3 方向ハンドシェイクが完了します。デバイスは、認証ユーザーにログインプロンプトを送信します。仮にユーザーに悪意があり、ログインせずに SYN-ACK-ACK セッションを起動し続けると、ScreenOS セッションテーブルは満杯になり、合法的接続要求を拒否し始めます。

操作の手順については、図 19 を参照してください。

1. クライアントが SYN セグメントをサーバーに送信します。
2. セキュリティデバイスは SYN/ACK セグメントをプロキシします。
3. クライアントは ACK セグメントで応答します。
4. セキュリティデバイスは、クライアント (認証ユーザー) にログインを要求します。
5. クライアントはログインプロンプトを無視し、セッションテーブルが満杯になるまで手順 1 から 4 までを繰り返します。
6. セッションテーブルが満杯のため、セキュリティデバイスはこれ以降のすべての接続要求を拒否する必要があります。

図 19: SYN-ACK-ACK プロキシフラッド



このような攻撃を阻止するために、SYN-ACK-ACK プロキシ保護 SCREEN オプションを使用可能にできます。同一の IP アドレスからの接続数が SYN-ACK-ACK プロキシしきい値に達すると、セキュリティデバイスはそれ以降、その IP アドレスからの接続要求を拒否します。デフォルトでしきい値は、任意の単一の IP アドレスから 512 接続です。このしきい値は、ご利用のネットワーク環境の要件に適するように、(1 から 250,000 の任意の数に) 変更できます。

SYN-ACK-ACK プロキシフラッドに対する保護を使用可能にするには、次のいずれかを行います。ここで指定するゾーンは、攻撃が発生したゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): 以下を入力して **Apply** をクリックします。

SYN-ACK-ACK Proxy Protection: (選択)
Threshold: (SYN-ACK-ACK プロキシフラッド保護が起動するしきい値を入力)

注 : 値の単位は、ソースアドレスあたりの接続数です。デフォルト値は、任意の単一の IP アドレスから 512 接続です。

CLI

set zone *zone* screen syn-ack-ack-proxy threshold *number*
set zone *zone* screen syn-ack-ack-proxy

ネットワーク DoS 攻撃

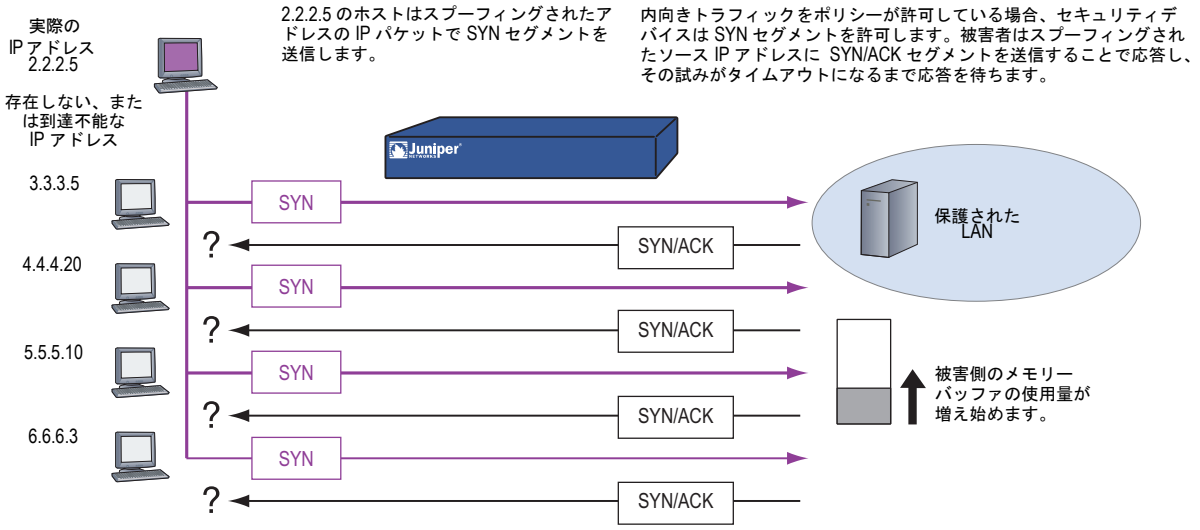
1 つまたは複数のネットワークリソースに向けられたサービス拒否 (DoS) 攻撃では、その標的には大量の SYN、ICMP、または UDP パケット、あるいは大量の SYN フラグメントがフラッドされます。攻撃者の目的、およびそれ以前の情報収集の程度と成功度合いに応じて、攻撃者は、ルーターやサーバーなどの特定のホストを選び出すか、標的のネットワークにわたる任意のホストに狙いを定めます。いずれのアプローチも、被害を受けたホストのネットワーク全体に対する役割に応じて、単一のホストまたはネットワーク全体のサービスを混乱させる可能性があります。

SYN フラッド

SYN フラッドは、これ以上合法的接続要求を処理できなくなるような、不正な大量の接続要求を開始する SYN セグメントによってホストが圧倒されたときに発生します。

2 台のホストは、*3 方向ハンドシェイク*として知られるように、パケットを 3 回交換して TCP 接続を確立します。つまり、A が SYN セグメントを B に送信し、B は SYN/ACK セグメントで応答し、そして A が ACK セグメントで応答します。SYN フラッド攻撃は、存在しないまたは到達不能なアドレスとともに、偽造の (スプーフィングされた) IP ソースアドレスを含む SYN セグメントでサイトを氾濫させます。B は SYN/ACK セグメントでこれらのアドレスに応答し、応答の ACK セグメントを待ちます。SYN/ACK パケットは存在しない、または到達不能な IP アドレスに送信されるため、応答を得ることはなく、結果としてタイムアウトします。

図 20: SYN フラッド攻撃



不正な TCP 接続でホストを氾濫させることによって、攻撃者は最終的に被害側のメモリバッファを満杯にします。このバッファが満杯になると、ホストはそれ以降、新しい TCP 接続要求を処理できません。フラッドによって、被害側のオペレーティングシステムも損傷を受けることがあります。いずれの場合も、攻撃により被害を受けたホスト、およびそのホストの正常な動作が不可能になります。

SYN フラッド保護

Juniper Networks セキュリティデバイスは、ファイアウォールの通過を許可される SYN パケットの 1 秒当たりの数を制限できます。攻撃しきい値は、宛先アドレスとポート、宛先アドレスのみ、またはソースアドレスのみに設けることができます。1 秒あたりの SYN セグメント数が、これらのしきい値のいずれか 1 つを超えると、セキュリティデバイスは受信 SYN セグメントのプロキシ、SYN/ACK セグメントでの応答、そして不正な接続要求の接続キューへの保存を開始します。不完全な接続要求は、接続が完了するまであるいは要求がタイムアウトするまでキューに残ります。図 21 では、SYN セグメント数が SYN 攻撃しきい値に到達し、デバイスが SYN セグメントのプロキシを開始したところです。

図 21: SYN セグメントのプロキシ

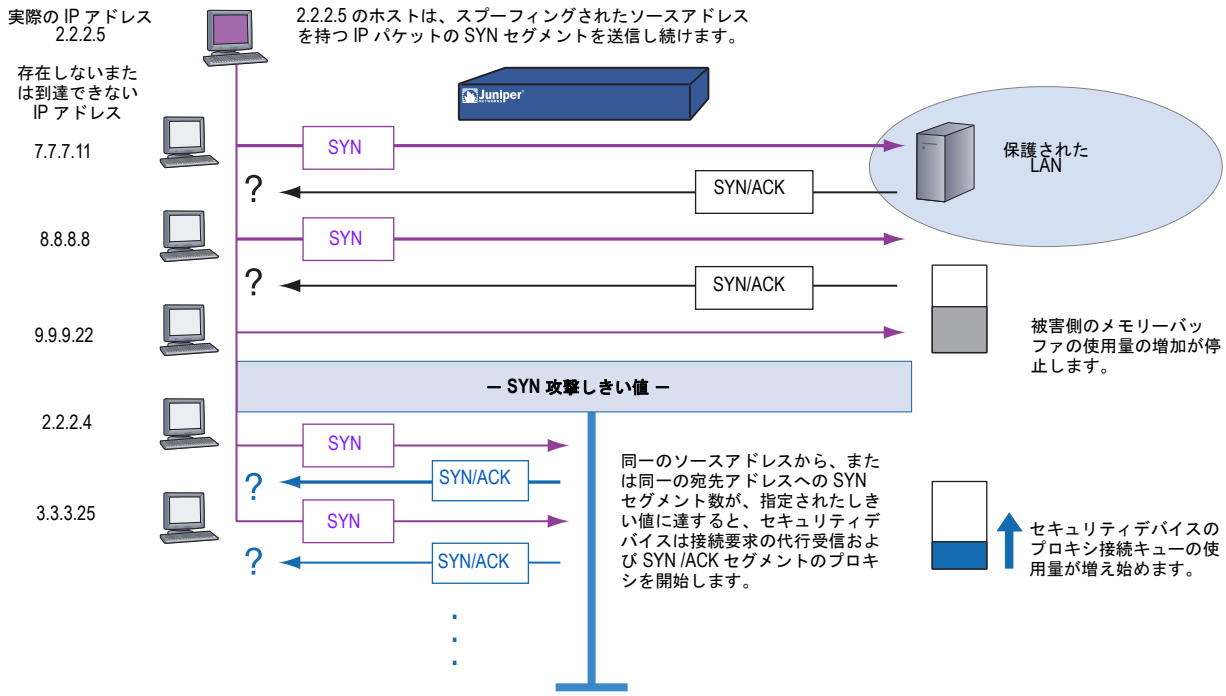
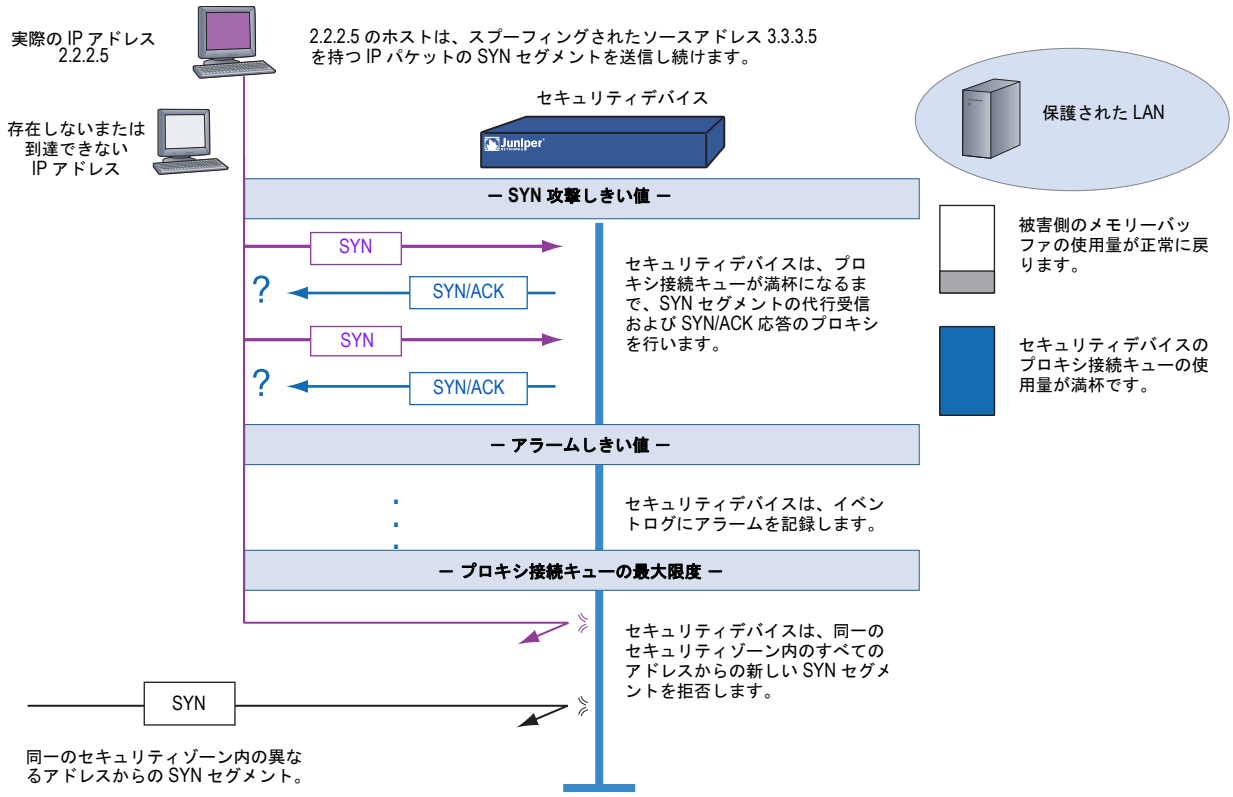


図 22 では、プロキシ接続キューが完全に満杯となり、セキュリティデバイスは新しい受信 SYN セグメントを拒否しています。このアクションは、保護されたネットワーク上のホストを不完全な 3 方向ハンドシェイクの攻撃からシールドします。

図 22: 新しい SYN セグメントの拒否



プロキシキューが最大限度未満に低下すると、セキュリティデバイスは新しい SYN パケットを受信し始めます。

注 : 設定したしきい値を越える不正な SYN 接続をプロキシする手順は、既存のポリシーにより許可されたトラフィックのみに関するものです。ポリシーが存在しないトラフィックはすべて、自動的にドロップされます。

SYN フラッド保護 SCREEN オプションを使用可能にし、そのパラメータを定義するには、次のいずれかを行います。ここで指定するゾーンは、フラッドが発生したと考えられるゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): 以下を入力して **Apply** をクリックします。

SYN Flood Protection: (使用可能に選択する)
Threshold: (SYN プロキシ機構をアクティブにするのに要する 1 秒あたりの SYN パケット数、つまり SYN フラグが設定された TCP セグメント数を入力する)

Alarm Threshold: (イベントログにアラームを書き込むのに要するプロキシされた TCP 接続要求数を入力する)

Source Threshold: (セキュリティデバイスがそのソースからの新しい接続要求を拒否し始めるのに要する、単一の IP アドレスからの 1 秒あたりの SYN パケット数を入力する)

Destination Threshold: (セキュリティデバイスがその宛先への新しい接続要求を拒否し始めるのに要する、単一の IP アドレスへの 1 秒あたりの SYN パケット数を入力する)

Timeout Value: (セキュリティデバイスが不正な TCP 接続試行をプロキシ接続キューに保持する時間を秒単位で入力する)

Queue Size: (セキュリティデバイスが新しい接続要求を拒否し始めるまで、プロキシ接続キューに保持されるプロキシ TCP 接続要求の数を入力する)

注 : これらのパラメータそれぞれの詳細については、次の CLI のセクションの説明を参照してください。

CLI

SYN フラッド保護を使用可能にするには :

set zone *zone* **screen syn-flood**

次のパラメータを設定して、不正な TCP 接続要求をプロキシできます。

- **Attack Threshold:** SYN プロキシ機構をアクティブにするのに必要な、同じ宛先アドレスとポート番号への 1 秒あたりの SYN セグメント数 (つまり、SYN フラグが設定された TCP セグメント)。しきい値は任意の値に設定できますが、適切なしきい値を設定するためには、サイトの正常なトラフィックパターンを知る必要があります。たとえば、通常 1 秒当たり 20,000 SYN セグメントを受信する電子ビジネスサイトの場合は、しきい値を 30,000/ 秒に設定してください。小規模なサイトが通常 1 秒あたり 20 SYN セグメントを受信する場合は、しきい値を 40 に設定することもできます。

  set zone *zone* **screen syn-flood attack-threshold** *number*

- **Alarm Threshold:** セキュリティデバイスがイベントログにアラームを入力する前の、プロキシされた 1 秒あたりの不完全 TCP 接続要求数。同じ宛先アドレスおよびポート番号への、プロキシされた不完全接続要求の 1 秒あたりの数がアラームしきい値に設定した値を超えると、アラームが起動します。たとえば、SYN 攻撃しきい値を 1 秒あたり 2000 SYN セグメントに、アラームを 1000 に設定した場合、ログにアラームエントリを発生させるには、同じ宛先アドレスとポート番号へ合計で 1 秒あたり 3001 SYN セグメントが必要になります。より正確に説明すると、次のとおりです。

  1. ファイアウォールは、ポリシー要件を満たす最初の 1 秒当たり 2000 SYN セグメントを通過させます。

2. ファイアウォールは、同じ秒内に次の 1000 SYN パケット をプロキシします。

3. 1001 番目のプロキシ接続要求 (あるいはその秒内の 3001 番目の接続要求) によってアラームが発生します。

set zone *zone* **screen syn-flood alarm-threshold** *number*

同じアドレスおよびポート番号への SYN セグメントで、アラームしきい値を超えたものそれぞれに対して、攻撃検出モジュールはメッセージを生成します。この 1 秒間の最後には、アラームしきい値を超えた後に、同じ宛先アドレスとポート番号への SYN セグメントが到達した数を示す単一のログエントリに、ロギングモジュールがすべての類似メッセージを圧縮します。攻撃が最初の 1 秒を越えて継続する場合、イベントログは、攻撃が停止するまで 1 秒毎にアラームを入力します。

- **Source Threshold:** このオプションでは、セキュリティデバイスが単一のソース IP アドレスからの接続要求をドロップし始めるまでに、そのソース (宛先 IP アドレスおよびポート番号にかかわらず) から受信する 1 秒あたりの SYN セグメント数を指定できます。

set zone *zone* **screen syn-flood source-threshold** *number*

ソースアドレスによる SYN フラッドのトラッキングでは、宛先アドレスおよび宛先ポート番号による SYN フラッドのトラッキングとは異なる検出パラメータを使用します。SYN 攻撃しきい値およびソースしきい値を設定すると、基本 SYN フラッド保護機構およびソースベース SYN フラッドトラッキング機構の両方が有効になります。

- **Destination Threshold:** このオプションでは、セキュリティデバイスは単一の宛先 IP アドレスへの接続要求をドロップし始めるまで受信する、その宛先への SYN セグメントの 1 秒あたりの数を指定します。保護されたホストが複数のサービスを実行する場合は、宛先ポート番号にかかわらず、宛先 IP アドレスに基づいてしきい値を設定することもできます。

set zone *zone* **screen syn-flood destination-threshold** *number*

SYN 攻撃しきい値および宛先しきい値を設定すると、基本 SYN フラッド保護機構および宛先ベース SYN フラッドトラッキング機構の両方が有効になります。

宛先アドレスによる SYN フラッドのトラッキングでは、宛先アドレスおよび宛先ポート番号による SYN フラッドのトラッキングとは異なる検出パラメータを使用します。次の例で、セキュリティデバイスが、同じサーバーへの FTP 要求 (ポート 21) および HTTP 要求 (ポート 80) を許可するポリシーを持つ場合を考えます。SYN フラッド攻撃しきい値が毎秒 1000 パケット (pps) で、攻撃者が毎秒 999 FTP パケットおよび 999 HTTP パケットを送信しても、どちらのパケット (同じ宛先アドレスとポート番号を持つように設定されている) によっても SYN プロキシ機構はアクティブになりません。基本 SYN フラッド攻撃機構は、アドレスおよびポート番号をトラッキングし、どちらのセットも攻撃しきい値の 1000 pps を超えません。ところが、宛先しきい値が 1000 pps であれば、デバイスは同じ宛先アドレスをもつ FTP および HTTP パケットをともに 1 つのセットとして扱い、その宛先への 1001 番目のパケット (FTP または HTTP) を拒否します。

- **Timeout:** 不完全接続がキューからドロップされるまでの最長時間。デフォルトは 20 秒で、タイムアウトは 0 ～ 50 秒に設定できます。タイムアウト値は、正常なトラフィック状態の間に接続がドロップしない程度にまで、短くすることもできます。3 方向ハンドシェイク ACK 応答に対しては、20 秒が無難なタイムアウトです。

  set zone *zone* **screen syn-flood timeout** *number*

- **Queue size:** セキュリティデバイスが新しい接続要求を拒否し始めるまで、プロキシ接続キューに保持されるプロキシ接続要求数。待ち行列の長さが長いほど、デバイスはプロキシ接続要求への有効な ACK 応答と適合するキューを、長時間にわたってスキャンする必要があります。このために、初期接続設定がわずかに遅くなることがあります。しかし、データ転送を開始する時間は通常、初期接続設定でのわずかな遅れよりはるかに長いため、ユーザーが大きな違いを感じることはありません。

  set zone *zone* **screen syn-flood queue-size** *number*

- **Drop Unknown MAC:** セキュリティデバイスは、SYN 攻撃を検出すると、すべての TCP 接続要求をプロキシします。しかし、透過モードのデバイスは、宛先 MAC アドレスが MAC 学習テーブルにない場合には、TCP 接続要求をプロキシできません。デフォルトでは、SYN 攻撃を検出した透過モードのデバイスは、未知の MAC アドレスを含む SYN パケットを通過させます。このオプションを使用すれば、未知の宛先 MAC アドレスを含む SYN パケットを通過させる代わりに、それらをドロップするようデバイスに指示できます。

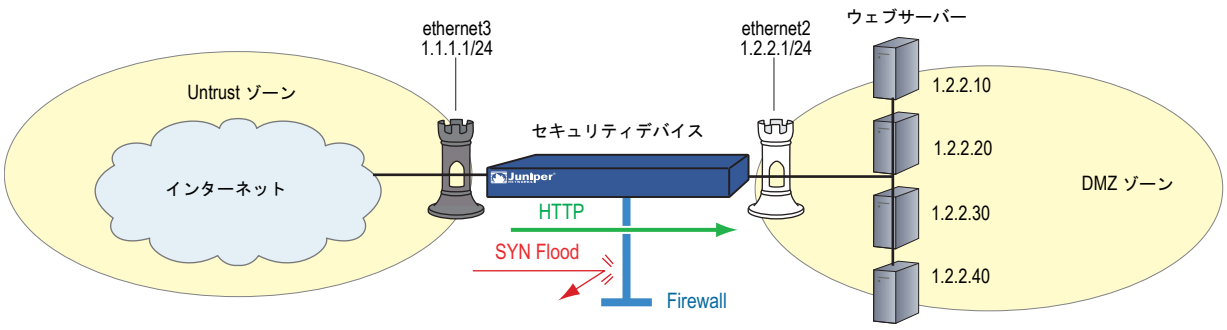
  set zone *zone* **screen syn-flood drop-unknown-mac**

例 : SYN フラッド保護

この例では、Untrust ゾーンに対する SYN フラッド保護 SCREEN オプションを使用可能にすることによって、Untrust ゾーンから発生する SYN フラッド攻撃から DMZ ゾーンの 4 台の Web サーバーを保護します。

注 : セキュリティデバイスを利用して、各 Web サーバー上のデバイスレベルの SYN フラッド保護に利用可能な SYN フラッド保護を強化することをお勧めします。この例では、Web サーバーは UNIX を稼動させており、接続要求キューの長さの調整や不正な接続要求のタイムアウト期間の変更などの、いくつかの SYN フラッド防御を利用することもできます。

図 23: デバイスレベルの SYN フラッド保護



使用するネットワークに適した値で SYN フラッド保護パラメータを構成するには、まず典型的なトラフィックフローの基準を確立する必要があります。1 週間にわたり、Untrust ゾーンにバインドされたインターフェースである ethernet3 上で探知機能を稼動させ、DMZ の 4 台の Web サーバーへ向けて到着する 1 秒あたりの新しい TCP 接続要求数を監視します。1 週間監視を行って収集したデータを分析した結果、次の統計結果が得られました。

- サーバー 1 台あたりの新しい接続要求の平均数 : 250/ 秒
- サーバー 1 台あたりの新しい接続要求の平均ピーク数 : 500/ 秒

注 : 探知機能とはネットワークを分析するデバイスで、このデバイスを装着したネットワークセグメント上のパケットをキャプチャします。ほとんどの探知機能では、目的のトラフィックのタイプのみを収集するようにフィルタを定義できます。その後に、収集した情報を検討し評価できます。この例では、SYN フラグが設定されたパケットを持ち、ethernet3 に到着し DMZ の 4 台の Web サーバーの中の 1 台に向かうすべての TCP パケットを探知機能で収集することにします。

定期的な間隔で探知機能を稼動させ続け、日時、曜日、月日、または季節に応じたトラフィックパターンが存在するかを確認することもできます。たとえば、企業によっては、トラフィックはクリティカルイベント時に劇的に増加することも考えられます。顕著な変化があれば、さまざまなしきい値に調整を行うべきです。

この情報に基づいて、表 2 に表示されるように、Untrust ゾーンに対して次の SYN フラッド保護パラメータを設定します。

表 2: SYN フラッド保護パラメータ

パラメータ	値	各値の説明
Attack Threshold	毎秒 625 パケット (pps)	これは、サーバー 1 台あたり 1 秒あたりの新しい接続要求の平均ピーク数よりも 25% 高く、このネットワーク環境に対しては一般的ではありません。4 台の Web サーバーのいずれかに対する 1 秒あたりの SYN パケット数がこの数値を超えると、デバイスはそのサーバーへの新しい接続要求のプロキシを開始します (言い換えれば、1 秒以内の同じ宛先アドレスとポート番号への 626 番目の SYN パケットから、デバイスはそのアドレスとポート番号への接続要求のプロキシを開始します)。
Alarm Threshold	250 pps	250 pps は、キューサイズ (1000 プロキシ不完全接続要求[1]) の 1/4 です。デバイスが 1 秒間に 251 の新しい接続要求をプロキシする場合は、イベントログにアラームエントリを作成します。アラームしきい値を攻撃しきい値より幾分高く設定すると、トラフィックスパイクが攻撃しきい値をわずかに超えたために起こるアラームエントリを防ぐことができます。
Source Threshold	25 pps	ソースしきい値を設定すると、デバイスは、宛先アドレスおよびポート番号にかかわらず、SYN パケットのソース IP アドレスをトラッキングします (このソースベースのトラッキングは、基本 SYN フラッド保護機構を構成する宛先アドレスおよび宛先ポートナンバーに基づく、SYN パケットのトラッキングとは異なるものであることに注意が必要です)。 アクティビティを 1 週間監視した結果、すべてのサーバーの新しい接続要求の 1/25 が、1 秒以内の間隔で 1 つのソースから発生することが観測されました。従って、このしきい値を超える接続要求は一般的ではないため、デバイスでプロキシ機構を実行するのに十分な条件となります (25 pps は 625 pps の攻撃しきい値の 1/25 です)。 デバイスは、同じソース IP アドレスから 25 SYN パケットをトラッキングすると、26 番目のパケットに始まりそれ以降、その 1 秒の残り期間と次の 1 秒間にわたり、そのソースからの SYN パケットを拒否します。
Destination Threshold	0 pps	宛先しきい値を設定すると、デバイスは、宛先ポート番号にかかわらず、宛先 IP アドレスのみの分離したトラッキングを実行します。4 台の Web サーバーは HTTP トラフィック (宛先ポート 80) のみを受信し、他の宛先ポート番号へのトラフィックはそれらのサーバーには到達しないため、別途に宛先しきい値を設定しても利点はありません。
Timeout	20 秒	待ち行列の長さは比較的短い (1000 プロキシ接続要求) ため、デフォルト値の 20 秒は、この構成で不正な接続要求をキューに保持するのに、適切な時間です。
Queue size	1000 プロキシ不完全接続	1000 プロキシ不完全接続要求は、新しい接続要求の平均ピーク数 (500 pps) の 2 倍です。デバイスは、新しい要求をドロップするまで、毎秒 1000 要求までプロキシします。新しい接続要求の平均ピーク数の 2 倍をプロキシすることにより、合法的接続要求を確実に処理するバッファが得られます。

1.不完全接続要求は、不正な 3 方向ハンドシェイクです。3 方向ハンドシェイクは、TCP 接続の初期段階です。これは、SYN フラグを設定した TCP セグメント、SYN および ACK フラグを設定した応答、およびそれに対する ACK フラグを設定した応答からなります。

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

   Zone Name: DMZ
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.2.2.1/24

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: ws1
   IP Address/Domain Name:
   IP/Netmask: (選択する), 1.2.2.10/32
   Zone: DMZ

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: ws2
   IP Address/Domain Name:
   IP/Netmask: (選択する), 1.2.2.20/32
   Zone: DMZ

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: ws3
   IP Address/Domain Name:
   IP/Netmask: (選択する), 1.2.2.30/32
   Zone: DMZ

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: ws4
   IP Address/Domain Name:
   IP/Netmask: (選択する), 1.2.2.40/32
   Zone: DMZ

   Policy > Policy Elements > Addresses > Groups > (Zone: DMZ) New: 以下のグループ名を入力して、以下のアドレスを移動し、**OK** をクリックします。

   Group Name: web_servers

   ws1 を選択し、< < ボタンを使用して Available Members 列から Group Members 列にアドレスを移動します。

ws2 を選択し、< < ボタンを使用して Available Members 列から Group Members 列にアドレスを移動します。

ws3 を選択し、< < ボタンを使用して Available Members 列から Group Members 列にアドレスを移動します。

ws4 を選択し、< < ボタンを使用して Available Members 列から Group Members 列にアドレスを移動します。

3. **ポリシー**
   Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   　Address Book Entry: (**選択**), Any
   Destination Address:
   　Address Book Entry: (**選択する**), web_servers
   Service: HTTP
   Action: Permit

4. **スクリーン**
   Screening > Screen (Zone: Untrust): 以下を入力して **Apply** をクリックします。

   SYN Flood Protection: (**選択**)
   　Threshold: 625
   　Alarm Threshold: 250
   　Source Threshold: 25
   　Destination Threshold: 0
   　Timeout Value: 20
   　Queue Size: 1000

注 : 20 秒がデフォルト設定のため、これまでに他の値に設定していない限り、タイムアウトを 20 秒に設定する必要はありません。

CLI

1. **インターフェース**
   set interface ethernet2 zone dmz
   set interface ethernet2 ip 1.2.2.1/24
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **アドレス**
   set address dmz ws1 1.2.2.10/32
   set address dmz ws2 1.2.2.20/32
   set address dmz ws3 1.2.2.30/32
   set address dmz ws4 1.2.2.40/32
   set group address dmz web_servers add ws1
   set group address dmz web_servers add ws2
   set group address dmz web_servers add ws3
   set group address dmz web_servers add ws4

3. **ポリシー**
   set policy from untrust to dmz any web_servers HTTP permit

4. **スクリーン**

```
set zone untrust screen syn-flood attack-threshold 625
set zone untrust screen syn-flood alarm-threshold 250
set zone untrust screen syn-flood source-threshold 25
set zone untrust screen syn-flood timeout 20
set zone untrust screen syn-flood queue-size 1000
set zone untrust screen syn-flood
save
```

注 : 20 秒がデフォルト設定のため、これまでに他の値に設定していない限り、タイムアウトを 20 秒に設定する必要はありません。

SYN クッキー

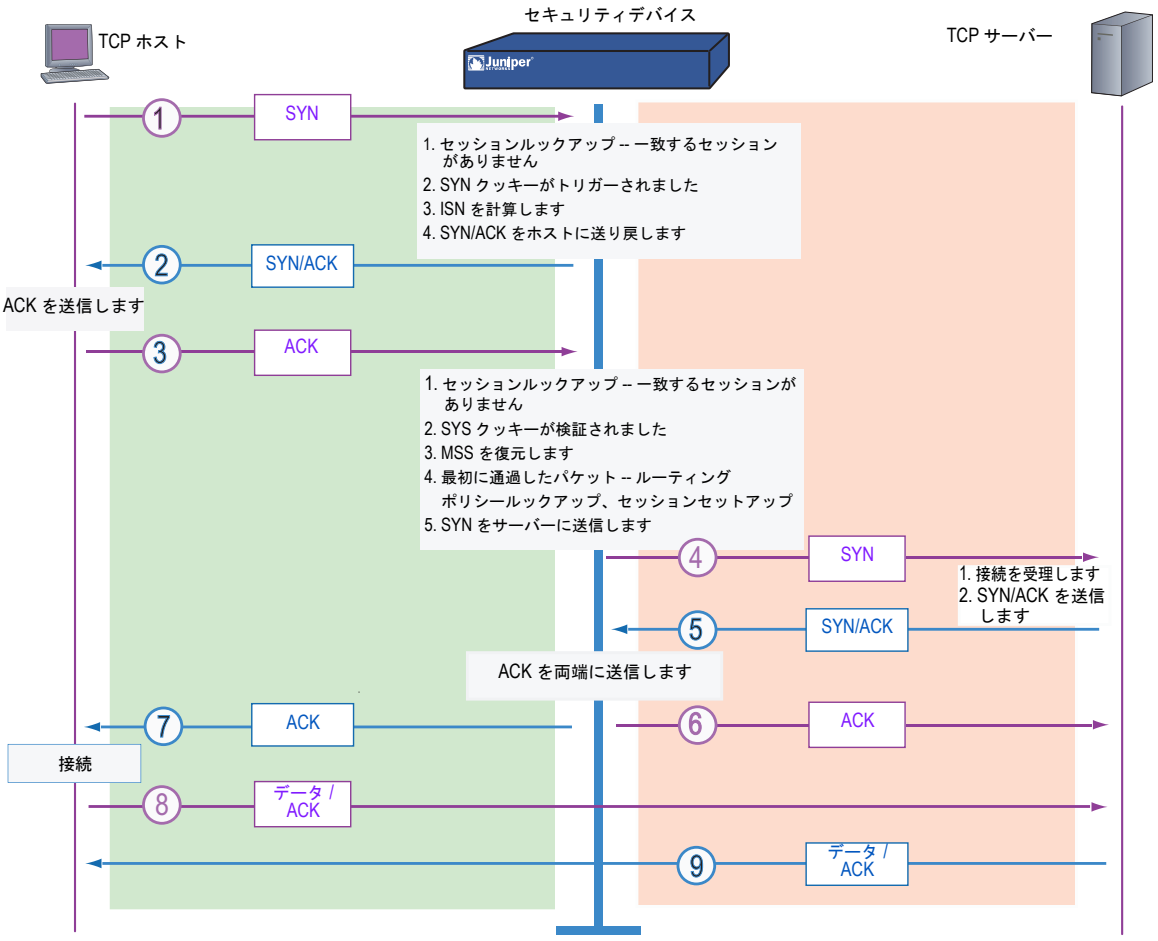
SYN クッキーは、36 ページの「SYN フラッド」に記載されている SYN フラッド攻撃に対する防衛と併用できるステートレス SYN プロキシ機構です。従来の SYN プロキシと同様に、SYN フラッド攻撃のしきい値が超過する場合に SYN クッキーがアクティブになりますが、SYN クッキーはステートレスなので、セッションを設定したり、SYN セグメントを受信した場合にポリシールックアップとルートルックアップを行ったりせず、接続要求キューも管理しません。これは、CPU およびメモリの使用量を大幅に減らし、従来の SYN プロキシ機構上で SYS クッキーを使用する主な利点となります。

SYN クッキーがセキュリティデバイスで有効になっており、宛先サーバーの TCP ネゴシエーションプロキシになる場合、ISN (Initial Sequence Number) として暗号化されたクッキーを含む SYN/ACK を使用して、各受信 SYN セグメントに応答します。クッキーは、元のソースアドレスとポート番号、宛先アドレスとポート番号、元の SYN パケットからの ISN の MD5 ハッシュです。クッキーの送信後、デバイスは元の SYN パケットをドロップし、メモリから計算されたクッキーを削除します。クッキーを含むパケットへの応答がない場合は、攻撃がアクティブ SYN 攻撃とみなされ、的確に停止させられます。

開始側ホストが TCP ACK フィールドにクッキー +1 を含む TCP パケットに応答する場合、デバイスはクッキーを抽出し、値から 1 を引きクッキーを再計算して、クッキーが合法的な ACK であることを確認します。クッキーが合法的であると確認されると、デバイスはセッションを設定し、元の SYN からのソース情報を含む サーバーに SYN を送信することによって、TCP プロキシ処理を開始します。デバイスがサーバーから SYN/ACK を受信すると、サーバーおよび開始側ホストに ACK を送信します。接続が確立された時点で、ホストとサーバーは互いに直接交信することができます。

図 24 に、セキュリティデバイスで SYN クッキーがアクティブになっている場合に、開始側ホストとサーバー間で接続を確立する方法を示します。

図 24: SYN クッキーがアクティブの場合の、接続の確立



SYN クッキーを有効にするには、SYN フラッド攻撃のしきい値 (36 ページの「SYN フラッド」に記載) を設定し、以下のいずれかを実行します。

WebUI

Configuration > Advanced > Flow: 以下を入力して **Apply** をクリックします。

TCP SYN-proxy SYN-cookie: (選択)

CLI

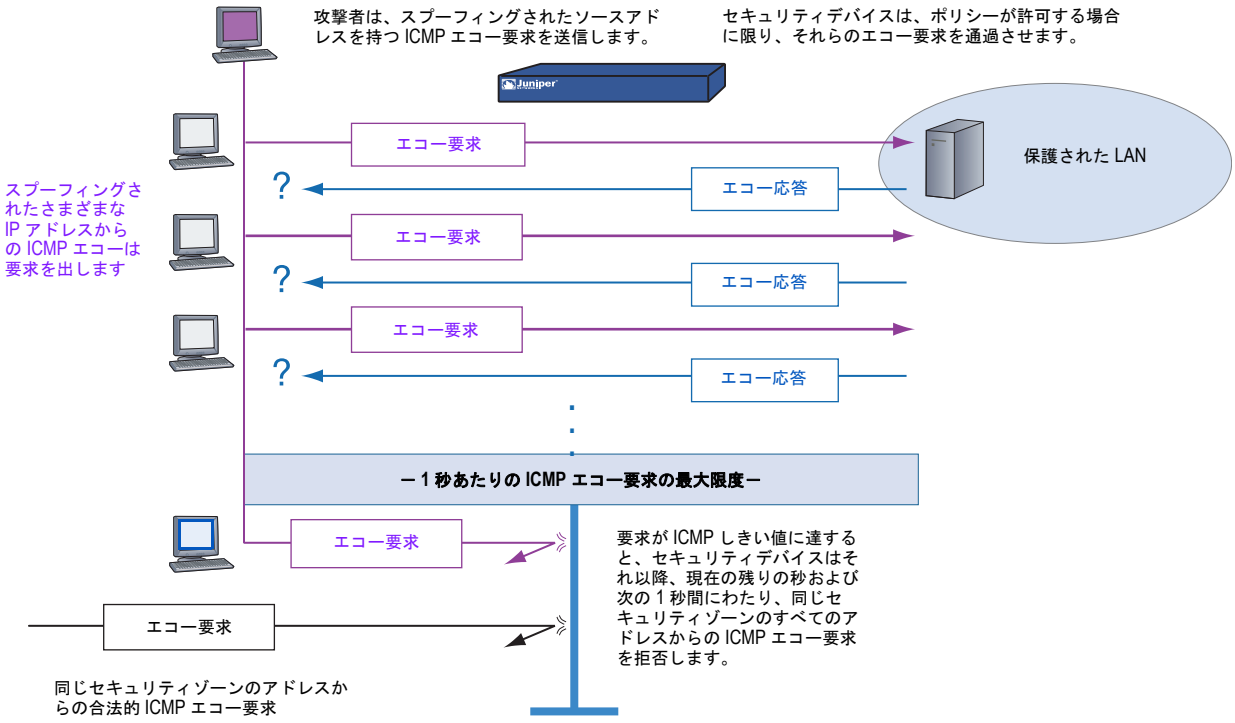
set flow syn-proxy syn-cookie

ICMP フラッド

ICMP フラッドは通常、ICMP エコー要求が被害側のシステムに大量の要求を送って過負荷状態にし、そのシステムが要求への応答にすべてのリソースを費やして、正当なネットワークトラフィックを処理できなくなった場合に発生します。ICMP フラッド保護機能を有効にする際に、一度超過すると ICMP フラッド攻撃保護機能を呼び出すしきい値を設定することができます (デフォルトしきい値は、毎秒 1000 パケットです)。しきい値を超えると、セキュリティデバイスはその秒の残りおよび次の 1 秒間は、それ以降の ICMP エコー要求を無視します。

注 : ICMP フラッド攻撃には、ICMP メッセージであればどんなタイプのものでも使われる可能性があります。したがって Juniper Networks セキュリティデバイスは、エコー要求以外の ICMP メッセージもすべて監視の対象とします。

図 25: ICMP フラッディング



ICMP フラッド保護を使用可能にするには、次のいずれかを行います。ここで指定するゾーンは、フラッドが発生したと考えられるゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): 以下を入力して **Apply** をクリックします。

ICMP Flood Protection: (選択)
Threshold: (ICMP フラッド保護が起動するしきい値を入力)

注 : 値の単位は、ICMP パケット毎秒です。デフォルト値は、毎秒 1000 パケットです。

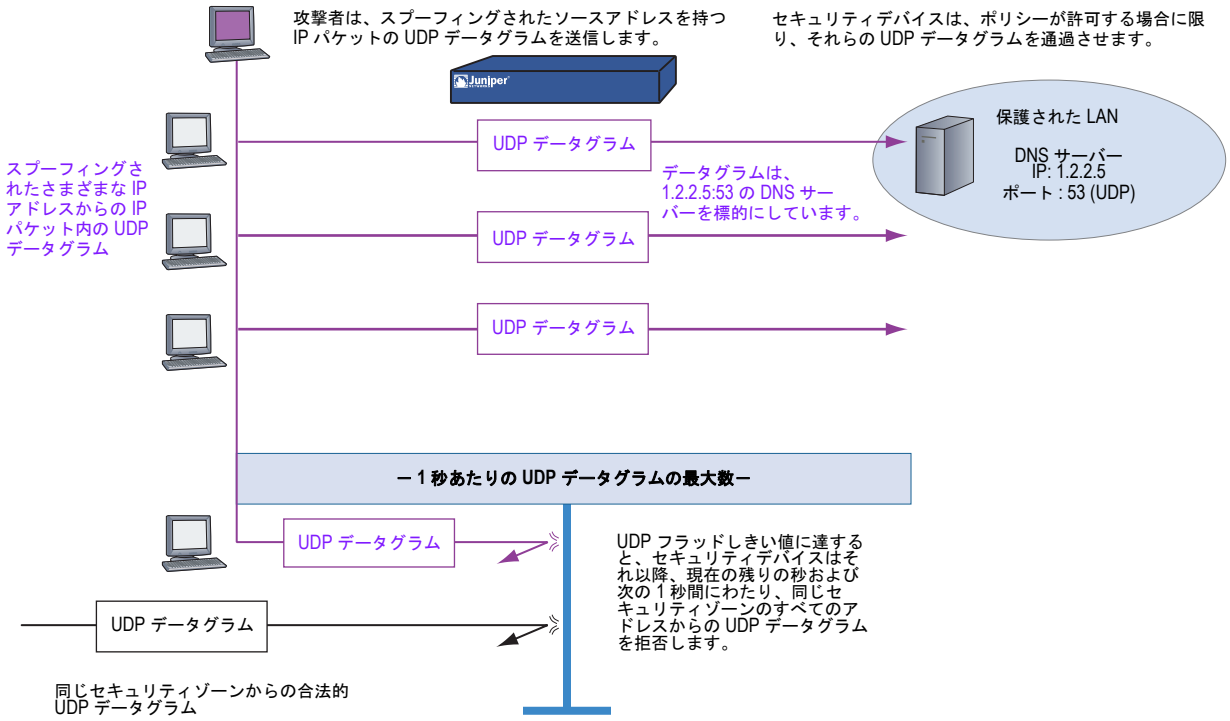
CLI

set zone *zone* screen icmp-flood threshold *number*
set zone *zone* screen icmp-flood

UDP フラッド

ICMP フラッドと同じように、UDP フラッドは、有効な接続をこれ以上処理できなくなるまで被害側のシステムを低下させる目的で、攻撃者が UDP データグラムを含む IP パケットを送信したときに発生します。UDP フラッド保護機能を使用可能にすると、一度超過すると UDP フラッド攻撃保護機能を呼び出すしきい値を設定することができます (デフォルトしきい値は、毎秒 1000 パケットです)。1 つまたは複数のソースから 単一の宛先へ向かう UDP データグラム数がこのしきい値を超えると、セキュリティデバイスはそれ以降、その宛先への UDP データグラムをその秒の残りの間および次の 1 秒間無視します。

図 26: UDP フラッディング



UDP フラッド保護を使用可能にするには、次のいずれかを行います。ここで指定するゾーンは、フラッドが発生したと考えられるゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): 以下を入力して **Apply** をクリックします。

UDP Flood Protection: (選択)
Threshold: (UDP フラッド保護が起動するしきいを入力)

注 : 値の単位は、UDP パケット毎秒です。デフォルト値は、毎秒 1000 パケットです。

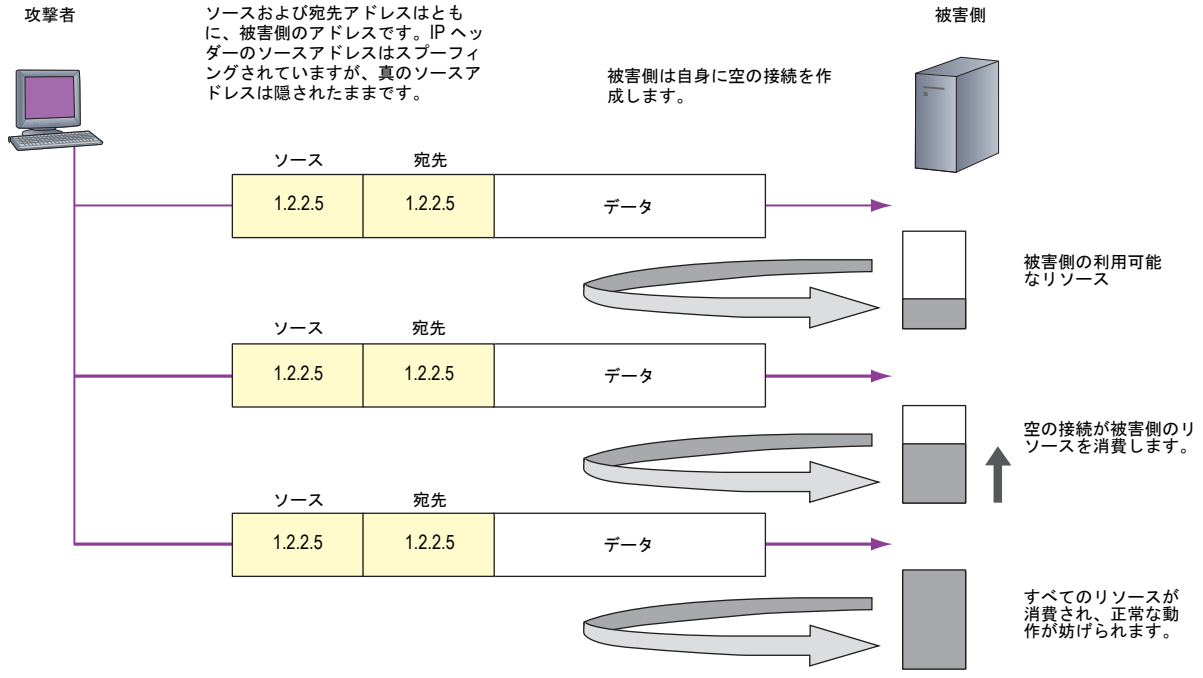
CLI

set zone *zone* screen udp-flood threshold *number*
set zone *zone* screen udp-flood

ランド攻撃

宛先およびソース IP アドレスの両方として被害側の IP アドレスを含み、スプーフィングされた SYN パケットを攻撃者が送信すると、SYN 攻撃と IP スプーフィングを組み合わせたランド攻撃が発生します。受信システムは、SYN-ACK パケットを自身に送信することにより応答し、アイドルタイムアウト値に達するまで続く空接続を作成します。そのような空接続でシステムをフラッドすると、システムは過負荷状態となり、サービス拒否を引き起こす可能性があります。

図 27: ランド攻撃



ランド攻撃をブロックするために SCREEN オプションを使用可能にすると、セキュリティデバイスは SYN フラッド防御および IP スプーフィング保護の要素を組み合わせ、この類の攻撃試行を検出しブロックします。

Land 攻撃に対する保護を使用可能にするには、次のいずれかを行います。ここで指定するゾーンは、攻撃が発生したゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): **Land Attack Protection** を選択してから、**Apply** をクリックします。

CLI

set zone *zone* screen land

OS 指定 DoS 攻撃

アクティブホストの IP アドレスおよび応答するポート番号だけでなく、その OS (オペレーティングシステム) までも識別している場合、攻撃者は強引な攻撃を行う代わりに、1 パケットまたは 2 パケットを「消滅」させるようなより巧妙な攻撃を仕掛けることがあります。このセクションで述べる攻撃は、最小の労力でシステムを動作不能にするおそれがあります。これらの攻撃に脆弱なホストを Juniper Networks セキュリティデバイスで保護している場合は、攻撃者が標的に到達する前に、セキュリティデバイスでこれらの攻撃を検出しブロックできます。

Ping of Death

最大許容 IP パケットサイズは、通常 20 バイト長のパケットヘッダーを含めて、65,535 バイトです。ICMP エコー要求は、8 バイト長の擬似ヘッダーを持つ IP パケットです。従って、ICMP エコー要求のデータ領域の最大許容サイズは、65,507 バイト (65,535 - 20 - 8 = 65,507) です。

ただし、多くの ping 実装では、65,507 バイトを超えるパケットサイズが指定できます。過大サイズの ICMP パケットは、DoS (サービス拒否)、クラッシュ、フリーズおよび再起動などさまざまな有害なシステム反応を引き起こす可能性があります。

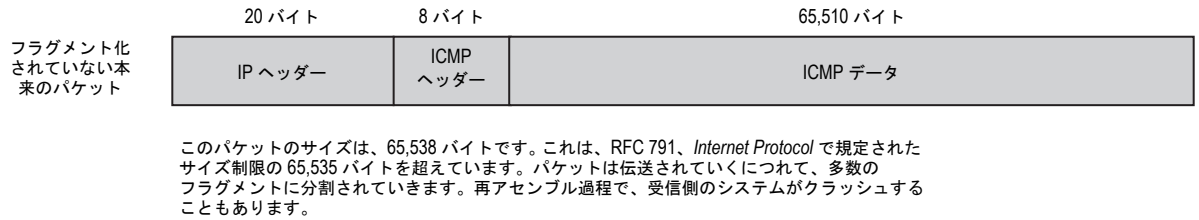
Ping of Death SCREEN オプションを使用可能にすると、たとえ攻撃者が意図的にパケットをフラグメント化してトータルパケットサイズを隠しても、セキュリティデバイスは、そのような過大で変則的なパケットサイズを検出し拒否します。

注 : IP 規格については、RFC 791、*Internet Protocol* を参照してください。

ICMP 規格の詳細については、RFC 792、*Internet Control Message Protocol* を参照してください。

Ping of Death については、http://www.insecure.org/sploits/ping-o-death.html を参照してください。

図 28: Ping of Death



Ping of Death 攻撃に対する保護を使用可能にするには、次のいずれかを行います。ここで指定するゾーンは、攻撃が発生したゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): **Ping of Death Attack Protection** を選択してから、**Apply** をクリックします。

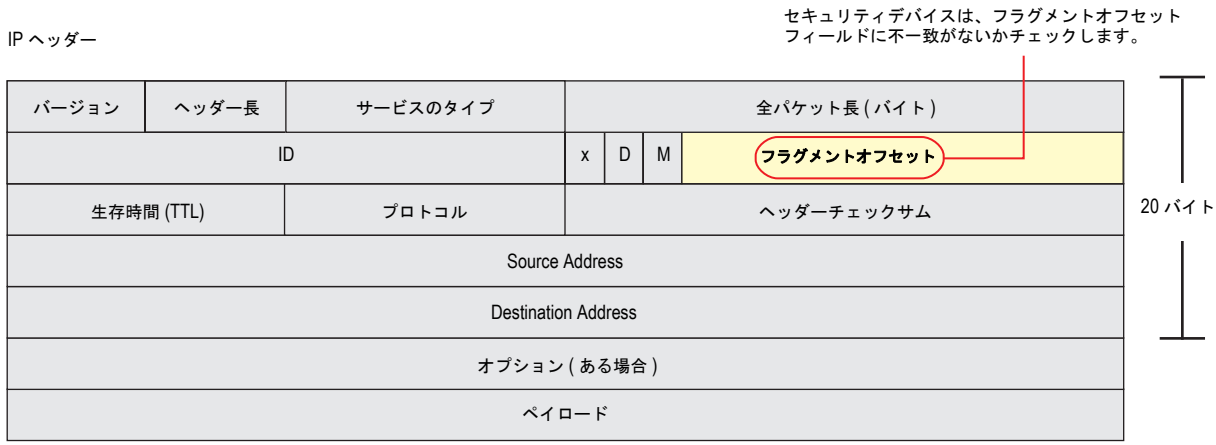
CLI

set zone *zone* screen ping-death

ティアドロップ攻撃

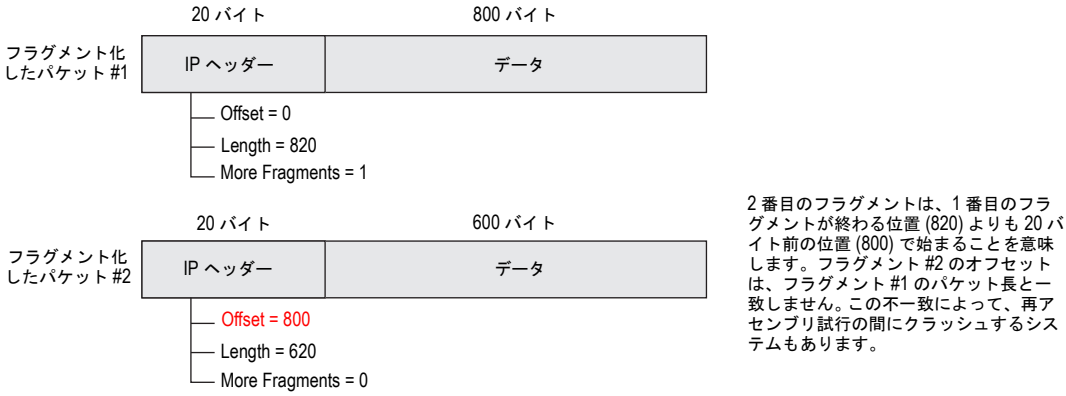
ティアドロップ攻撃は、フラグメント化した IP パケットの再アセンブリを利用します。IP ヘッダー内のフィールドの 1 つにフラグメントオフセットフィールドがあります。このフィールドは、フラグメント化されていない本来のパケットのデータに関して、フラグメント化されたパケットに含まれるデータの開始位置、すなわちオフセットを示します。

図 29: ティアドロップ攻撃



フラグメント化した 1 つのパケットのオフセットとサイズの合計が、フラグメント化した次のパケットのものと異なる場合、パケットは重複し、パケットを再アセンブリするサーバーがクラッシュする可能性があります。サーバーがこの脆弱性を持つオペレーティングシステムを稼動させている場合は特に、クラッシュしやすくなります。

図 30: フラグメントの不一致



Teardrop Attack SCREEN オプションを使用可能にすると、デバイスはフラグメント化したパケットにこの不一致を検出するたびに、そのパケットをドロップします。

ティアドロップ攻撃に対する保護を使用可能にするには、次のいずれかを行います。ここで指定するゾーンは、攻撃が発生したゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): **Teardrop Attack Protection** を選択してから、**Apply** をクリックします。

CLI

set zone *zone* screen tear-drop

WinNuke

WinNuke とは、Windows を稼動させているインターネット上の任意のコンピュータを標的とする DoS 攻撃です。攻撃者は、接続を確立したホストに (通常は、緊急 (URG) フラグを設定した NetBIOS ポート 139 に) TCP セグメントを送信します。これによって NetBIOS フラグメントオーバーラップが誘発され、その結果、Windows を稼動させている多くのシステムがクラッシュします。攻撃されたシステムを再起動すると、攻撃が発生したことを示す次のメッセージが表示されます。

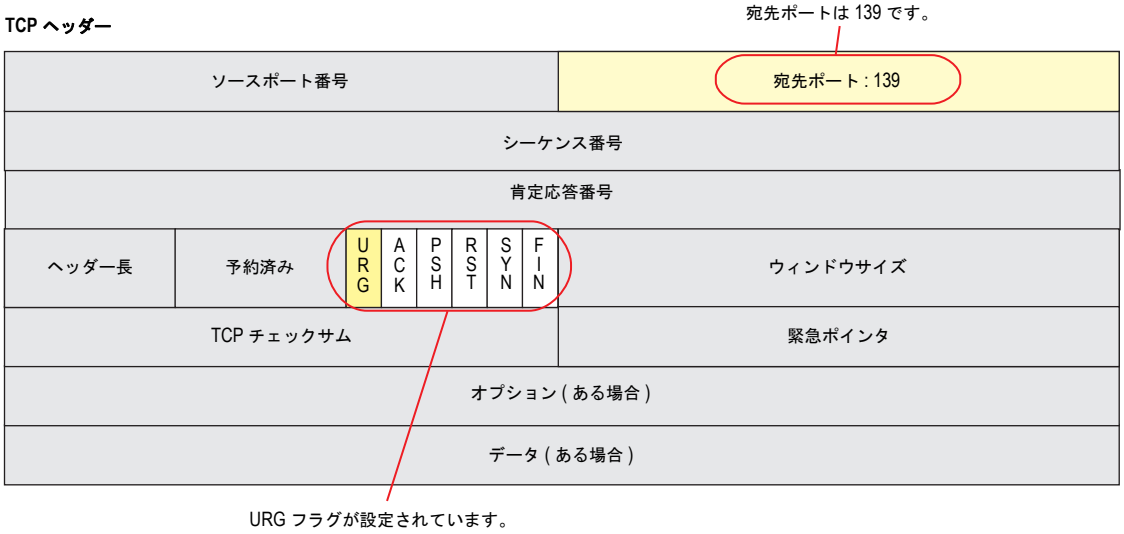
An exception 0E has occurred at 0028: [address] in VxD MSTCP(01) + 000041AE. This was called from 0028: [address] in VxD NDIS(01) + 00008660. It may be possible to continue normally.

Press any key to attempt to continue.

Press CTRL+ALT+DEL to restart your computer.You will lose any unsaved information in all applications.

Press any key to continue.

図 31: WinNuke 攻撃の指標



WinNuke 攻撃防御の SCREEN オプションを有効にすると、セキュリティデバイスは受信するすべての Microsoft NetBIOS セッションサービス (ポート 139) パケットをスキャンします。デバイスは、これらのパケットの 1 つに URG フラグが設定されているのを観測すると、URG フラグの設定解除、URG ポインタのクリア、修正パケットの転送を行い、イベントログにエントリを作成して WinNuke 攻撃試行をブロックしたことを示します。

WinNuke 攻撃に対する保護を使用可能にするには、次のいずれかを行います。ここで指定するゾーンは、攻撃が発生したゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): **WinNuke Attack Protection** を選択してから、**Apply** をクリックします。

CLI

set zone *zone* screen winnuke

第 4 章

コンテンツの監視とフィルタリング

Juniper Networks の ScreenOS 機能を使用し、ScreenOS を Websense、SurfControl および Kaspersky Lab 製品と組み合わせることにより、ネットワークアクティビティの幅広い保護と制御が可能です。

この章では、デバイスを構成してセグメントとパケットの再アセンブリ実行、HTTP トラフィックに不正な URL がないかの監視、そして他のデバイスと通信して AV スキャンや Web フィルタリングを行う方法について説明します。この章は以下のセクションから構成されています。

- 58 ページの「フラグメントの再アセンブリ」
  - 58 ページの「不正な URL からの保護」
  - 59 ページの「アプリケーションレイヤーゲートウェイ」
- 62 ページの「ウィルス対策スキャン」
  - 62 ページの「外部 AV スキャン」
  - 64 ページの「内部 AV スキャン」
  - 70 ページの「ポリシーベースの AV スキャン」
  - 71 ページの「アプリケーションプロトコルのスキャン」
  - 80 ページの「内蔵スキャナの AV パターンファイルの更新」
  - 83 ページの「AV スキャナのグローバル設定」
  - 87 ページの「AV プロファイル」
- 94 ページの「スパム対策フィルタリング」
- 98 ページの「Web フィルタリング」
  - 99 ページの「統合型 Web フィルタリング」
  - 108 ページの「Web フィルタリングの転送」

フラグメントの再アセンブリ

通常、ルーターやスイッチなどのネットワーク転送デバイスは、フラグメント化された受信パケットを再アセンブリしません。受信したフラグメント化されたパケットは、パケットがすべて到達したときに宛先ホストが再構成します。転送デバイスの主目的はトラフックを効率的に配信することです。すべてのパケットをキューに入れ、再アセンブリし、さらに再びフラグメント化して転送するのは不効率です。ただし、フラグメント化されたパケットにファイアウォールを通過させることは安全ではありません。通常はファイアウォールにより検出されブロックされるトラフィック文字列を隠すために、アタッカーが故意にパケットを細分化する場合があります。

ScreenOS では、フラグメントの再アセンブリをゾーンごとに行えます。これによってセキュリティデバイスは不正な URL 文字列を検出しブロックする能力を拡張できます。デバイスを NAT モードに構成している場合に限って、ALG（アプリケーションレイヤーゲートウェイ）が使用可能になっているトラフィックについてフラグメントの再アセンブリが発生します。

不正な URL からの保護

Web フィルタリング機能（108 ページの「Web フィルタリングの転送」を参照）に加えて、不正 URL からゾーンレベルで保護するために、不正 URL 文字列のパターンをゾーンごとに最大 48 個まで定義できます。各パターンは最長 64 文字です。不正な URL のブロッキング機能を有効にすると、セキュリティデバイスはすべての HTTP パケットのデータペイロードを調べます。デバイスが URL を検索し、文字列の始まりが（指定した文字数まで）定義したパターンに適合することを検出した場合は、デバイスはパケットがファイアウォールを通過しないようにブロックします。

情報に通じた攻撃者は特定の文字列が知られていて防御されている可能性があることを意識しているため、IP パケットや TCP セグメントを故意にフラグメント化し、パケットごとの検査ではパターンが認識できないようにすることがあります。たとえば、不正な URL 文字列が **120.3.4.5/level/50/exec** の場合、IP フラグメント化によって文字列が次のセクションに細分化されるとします。

- 1 番目のパケット : **120**
- 2 番目のパケット : **3.4.5/level/50**
- 3 番目のパケット : **/exec**

20 文字の長さで文字列 **120.3.4.5/level/50/exec** を定義していても、フラグメント化された各文字列は検出されずにセキュリティデバイスを通過します。1 番目のパケットの文字列「120.」は定義したパターンの最初の部分と一致しますが、一致する文字に必要な長さである 20 文字に足りません。2 番目と 3 番目のパケットの文字列は定義したパターンの始まりに適合せず、この場合も妨害されずに通過します。

ただし、パケットが再アセンブリされるとフラグメントは認識可能な文字列を構成し、デバイスでブロックできます。フラグメント再アセンブリ機能を使用すると、デバイスはフラグメントをキューにバッファしてから完全なパケットとして再アセンブリし、不正な URL かどうかパケットを検査します。この再アセンブリ処理と検査の結果に基づき、デバイスは次の手順の 1 つを実行します。

- デバイスが不正な URL を発見した場合は、パケットをドロップしログにイベントを入力します。
- デバイスが再アセンブリ処理を完了できない場合は、時間制限を設けてエージングしフラグメントを廃棄します。
- デバイスが URL は不正ではないが再アセンブリしたパケットが大きすぎて転送できないと判断した場合、デバイスはそのパケットを複数のパケットにフラグメント化して転送します。
- デバイスが URL は不正ではなくフラグメント化する必要がないと判断した場合、パケットを転送します。

アプリケーションレイヤーゲートウェイ

ScreenOS は DNS、FTP、H.323、および HTTP など多数のプロトコルのために ALG（アプリケーションレイヤーゲートウェイ）を提供しています。こうしたプロトコルでは、フラグメントの再アセンブリは FTP サービスや HTTP サービスに関係したポリシーを実施するために重要なコンポーネントとなります。Juniper Networks ファイアウォールが、FTP-Get や FTP-Put などのプロトコルのパケットをスクリーニングできるようにするには、パケットヘッダーだけでなくペイロードのデータも調べる必要があります。

たとえば、Untrust ゾーンから DMZ ゾーンへの FTP-put を拒否するポリシーがあるとします。

set policy from untrust to dmz any any ftp-put deny

セキュリティデバイスが **STOR** *ファイル名*を見つけた場合、クライアントはサーバーに指定したファイルを保存（Store）する要求を送信しているため、デバイスはパケットをブロックします。

注 : 拒否ポリシーにとっては、FTP-Put、Ftp-Get および FTP サービスは、全パケットをブロックすることにより、同じように動作します。

許可ポリシーでは、Ftp-Get、Ftp-Put、および Ftp は異なったサービスです。たとえば、Untrust ゾーンから DMZ ゾーンへの FTP-Get を許可するポリシーがあるとします。

set policy from untrust to dmz any any ftp-get permit

RETR *ファイル名*を読み取った場合、FTP クライアントは FTP サーバーから指定したファイルを取得（Retrieve）する要求を送信しているため、セキュリティデバイスはパケットが通過するのを許可します。

2 つのポリシーがあり、1 つは Untrust ゾーンから DMZ ゾーンへの FTP-put を拒否し、もう 1 つは Untrust ゾーンから DMZ ゾーンへの FTP-get を許可する場合、デバイスは、パケットをブロックします。

set policy from untrust to dmz any any ftp-put deny
set policy from untrust to dmz any any ftp-get permit

この防御の裏をかくため、攻撃者は単一の FTP-put パケットを故意に 2 つのパケットにフラグメント化することがあります。それぞれのパケットのペイロードには次のテキストが含まれています。

- パケット 1: **ST**
- パケット 2: **OR** *ファイル名*

セキュリティデバイスが各パケットを検査しても、文字列 **STOR** *ファイル名*を発見せず、その結果両方のパケットの通過を許可します。

ただし、パケットが再アセンブリされるとフラグメントは認識可能な文字列を構成し、セキュリティデバイスが処理できます。フラグメント再アセンブリ機能を使用すると、デバイスはフラグメントをキューにバッファしてから完全なパケットに再アセンブリし、完全な FTP 要求かどうかパケットを検査します。この再アセンブリ処理と検査の結果に基づき、デバイスは次の手順の 1 つを実行します。

- デバイスが FTP-put 要求を発見した場合、パケットをドロップしログにイベントを入力します。
- デバイスが再アセンブリ処理を完了できない場合は、時間制限を設けてエージングしフラグメントを廃棄します。
- デバイスが FTP-get 要求を検出したものの再アセンブリしたパケットが大きすぎて転送できないと判断した場合、デバイスはそのパケットを複数のパケットにフラグメント化して転送します。
- デバイスが FTP-get 要求を発見しフラグメント化する必要がないと判断した場合、パケットを転送します。

例 : パケットフラグメント内の不正な URL をブロックする

この例では次の 3 つの不正 URL 文字列を定義し、不正 URL ブロッキングオプションを使用可能にします。

- 不正 URL #1
  - ID: Perl
  - Pattern: scripts/perl.exe
  - Length: 14
- 不正 URL #2
  - ID: CMF
  - Pattern: cgi-bin/phf
  - Length: 11
- 不正 URL #3
  - ID: DLL
  - Pattern: 210.1.1.5/msadcs.dll
  - Length: 18

「長さ」の値は、一致する場合に必ず URL に含まれるパターン内の文字数（最初の文字から数えます）を示しています。#1 と #3 が示すように、すべての文字が必要なわけではありません。

それからフラグメントの再アセンブリを有効にして、Untrust ゾーンのインターフェースに到達した、フラグメント化された HTTP トラフィック内の URL を検出できるようにします。

WebUI

Security > Screening > Mal-URL (Zone: Untrust): 次のように入力してから **OK** をクリックします。

ID: perl
Pattern: scripts/perl.exe
Length: 14

Security > Screening > Mal-URL (Zone: Untrust): 次のように入力してから **OK** をクリックします。

ID: cmf
Pattern: cgi-bin/phf
Length: 11

Security > Screening > Mal-URL (Zone: Untrust): 次のように入力してから **OK** をクリックします。

ID: dll
Pattern: 210.1.1.5/msadcs.dll
Length: 18

Network > Zones > Edit (Untrust): TCP/IP Reassembly for ALG チェックボックスをオンにして、**OK** をクリックします。

CLI

```
set zone untrust screen mal-url perl “scripts/perl.exe” 14
set zone untrust screen mal-url cmf “cgi-bin/phf” 11
set zone untrust screen mal-url dll “210.1.1.5/msadcs.dll” 18
set zone untrust screen reassembly-for-alg
save
```

ウィルス対策スキャン

ウィルスは、他の実行可能コードを感染させるか自らを添付して、自己複製できるようにする実行可能コードです。一部の悪質なウィルスはファイルを消去したりシステムをロックしたりします。それ以外のウィルスはファイルを感染させたり、ターゲットホストやネットワークを偽のデータで過負荷状態にしようとしたりします。

Juniper Networks の高性能セキュリティデバイスは、内蔵および外部ウィルス対策（AB）スキャンエンジンをサポートします。セキュリティデバイスの一覧、およびサポートされる AV スキャンエンジンについては、*ScreenOS リリースノート*を参照してください。

ISG 製品シリーズ用ウィルス対策ソリューションには、次の 2 種類があります。

- ICAP（インターネットコンテンツアダプテーションプロトコル）AV

  T-3 およびフラクショナル T-3 架線などの低速用のソリューションです。詳細については、62 ページの「外部 AV スキャン」を参照してください。

- PBR（ポリシーベースルーティング）

  OC-3 架線などの高速用のソリューションです。この例では、ISG 上の PRB が内臓 AV スキャナを作動しているハイエンドのセキュリティデバイスに特定のトラフィックを転送して負荷を軽減します。この構成の詳細については、**7**-144 ページの「高度な PBR の例」を参照してください。内臓 AV スキャナの詳細については、64 ページの「内部 AV スキャン」を参照してください。

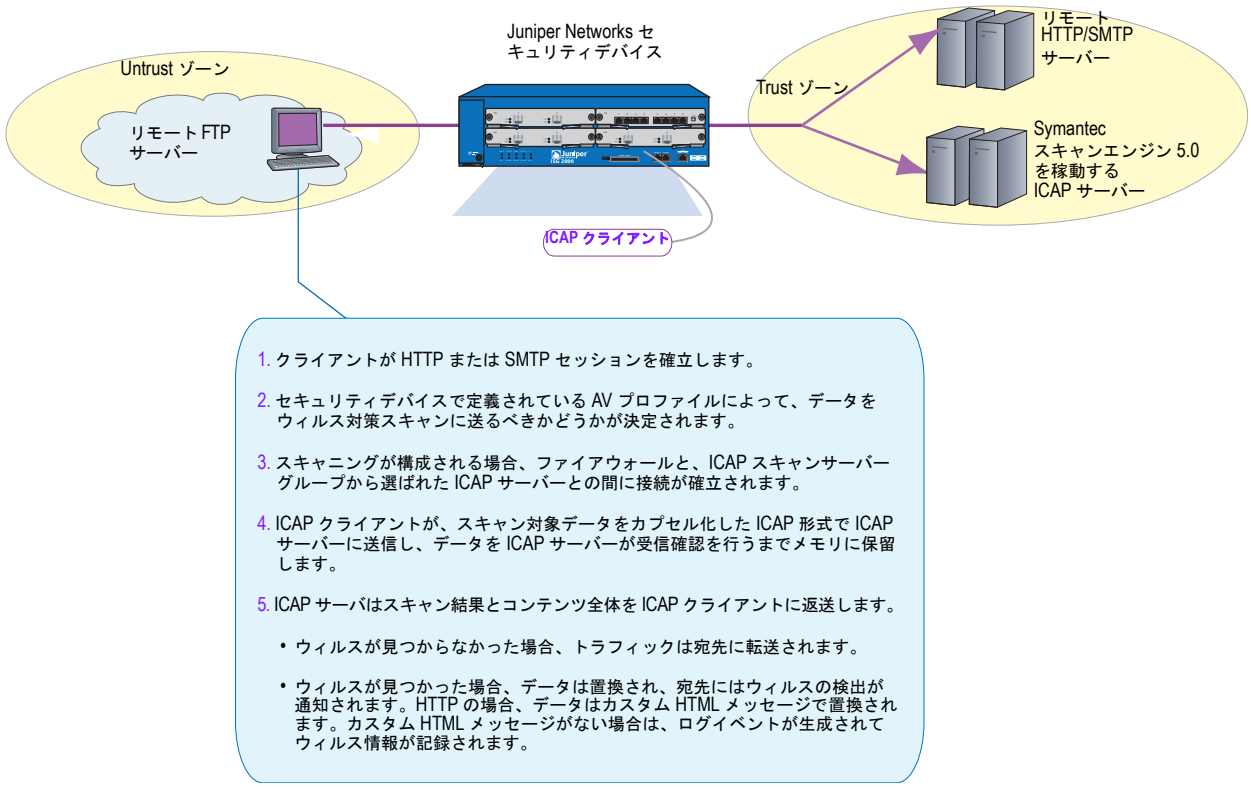
外部 AV スキャン

外部 AV スキャンは、セキュリティデバイスがトラフィックを外部 ICA AV スキャンサーバーに転送したときに発生します。ICAP クライアントはセキュリティデバイス上で、次に示す機能を提供するために外部 ICA AV スキャンサーバーと交信します。

- ICAP v1.0 のサポート、および RFC 3507 に完全に準拠
- Symantec Scan Engine 5.0 ICAP サーバーのサポート
- 拡張可能なウィルス対策スキャン機能（ICAP スキャンサーバーの追加）
- 複数のデバイス（ファイアウォール）で一つの ICAP スキャンサーバーを共有
- 一連の ICAP サーバー間におけるトラフィックのロードバランス
- HTTP および SMTP トラフィックのカプセル化
- HTTP トラフィックのカスタム HTML メッセージのサポート
- カスタム x - 応答ヘッダーのサポート
- 同じ ICAP サーバーへの持続接続のサポート
  持続接続は、オーバヘッド処理量を軽減し、AV スキャニングのスループットを増強させます。

図 32 に、セキュリティデバイスで AV スキャンがどのように機能するかを示します。

図 32: 外部スキャンの動作



スキャンモード

トラフィックがウィルス対策スキャンで処理された後、Symantec Scan Engine 5.0 を稼動している ICAP サーバーが次の結果の 1 つを提供します。

- **スキャンのみ :** 感染したファイルへのアクセスを拒否し、ファイルに対しては何もしない。
- **スキャンして削除する :** アーカイブファイルに格納されたファイルも含めてすべての感染ファイルを、修復する代わりに削除する。
- **スキャンしファイルを修復する :** 感染したファイルの修復を試みて、修復できないファイルには何もしない。
- **スキャンし、修復または削除する :** 感染したファイルの修復を試みて、アーカイブファイルから回復できないファイルは削除する。

スキャン動作とスキャン結果の詳細については、ICAP サーバーの文書を参照してください。

ロードバランスを行う ICAP サーバー

ScreenOS 5.4 の外部 AV スキャン機能を使用すると、ICAP サーバーグループで構成されている ICAP スキャンサーバーに対してロードバランス処理を実行できます。グループ内の ICAP スキャンサーバーに適用されるロードバランス機能のアルゴリズムは、最も低い要求です。ICAP サーバー間のロードバランスは、各サーバーのヘルスと交通量（保留中の要求の数）を基に実行されます。ヘルシーでないサーバーはバイパスされ、過負荷状態のサーバーの交通量まで自動的に削減されます。

構成されている ICAP サーバーの状態は、使用可能であっても、または使用不可であってもかまいません。使用可能な ICAP サーバーの状態は、*サービス中*または*サービス休止中*のどちらかです。使用不可に構成されている ICAP サーバーの場合は、サーバーが新しい要求をサービスすることに使用されません。

ICAP サーバーは探査機構によって監視されます。たとえば、探査間隔の設定値が 30 の場合は、使用可能な ICAP サーバーは、30 秒間隔で自動的に探査され、サーバーの状態（サービス中またはサービス休止中）が判断されます。

自動探査は、次の状態の場合にサービス休止中の結果を返します。

- ファイアウォールが ICAP サーバーへの TCP 接続を正常に確立できない
- ICAP サーバーの AV ライセンスが無効
- ICAP オプション要求に対するクライアント側のエラー応答
- ICAP オプション要求に対するサーバー側のエラー応答

探査が連続して 3 回失敗した場合、サーバーはサービス休止状態に変わります。

内部 AV スキャン

内部 AV スキャンは、セキュリティデバイスのスキャンエンジンが、トラフィックをスキャンしウィルスの有無をチェックするときに実行されます。内部エンジンすなわち内蔵エンジンは、Juniper-Kaspersky スキャンエンジンです。

注： 内部 AV スキャナを使用するには、セキュリティデバイスで AV ライセンスをインストールする必要があります。外部 AV スキャナを使用する場合は、AV ライセンスは必要ありません。

内蔵スキャンエンジンは、次の機能を提供します。

- コンテンツの種類とファイル拡張子に基づき、スキャニングを使用可能および使用不可に設定

  たとえば、文書ファイル (.doc あるいは .pdf) ではなく実行可能ファイル (.exe) をスキャンするプロファイルを設定できます。

- 特定のアプリケーションプロトコルの解凍レイヤーの構成

  各プロファイルには、プロトコルのタイプ別 (HTTP、SMTP、POP3、IMAP、FTP) に異なる解凍レベルを構成できます。たとえば使用しているネットワーク環境に基づき、解凍したい内蔵 zip ファイルの数をプロトコル別に指定したい場合があります。

- インスタントメッセージ（IM）トラフィックの AV スキャンの構成

  IM トラフィックのスキャンの詳細については、66 ページの「IM トラフィックの AV スキャン」を参照してください。

- 送信者または受信者に検出したウィルスやスキャンエラーを知らせる E メール通知の構成

- スパイウェアやフィッシングを防御するスキャンレベルの構成

  Juniper-Kaspersky のスキャンエンジンは、デフォルトで最高レベルのセキュリティを提供します。ポリモーフィック型ウィルスやその他の巧妙なウィルスを含むあらゆるウィルスを阻止する機能に加えて、このスキャンエンジンは、スパイウェアやフィッシングに対するインバウンド防御機能も備えています。

  スパイウェアの防御 : スパイウェア防御機能は、Juniper Networks のスパイウェア対策およびアドウェア対策のソリューションを一層強化するもので、送信されるスパイウェアやアドウェア、キーロガー、その他の悪質なトラフィックが企業内に侵入する前にブロックする機能を配備します。

  このソリューションはスパイウェアのフォンホーム保護機能 (ノートパソコン / デスクトップ / サーバーに侵入したスパイウェアが機密データを外部に送信するのを阻止する機能）を追加することで Juniper Networks IDP（Intrusion Detection and Prevention）製品を補完します。

  フィッシングの防御 : フィッシング防御機能を配備すると、機密情報を盗むためにユーザーを偽 (フィッシング) サイトに誘導する E メールをブロックできます。

  以下の 2 つのオプションのいずれかを選択することにより、スキャンのデフォルトのセキュリティレベルを変更できます。

  - **In-the-wild (感染報告のあるウィルス) に対する基本スキャン :** このレベルのスキャンでは、一般に出回っているウィルスをスキャンする低レベルのセキュリティ対策を実施しますが、スキャンのパフォーマンスは強化されます。in-the-wild 基本スキャンを使用可能にするには、次のコマンドを入力します。

    set av scan-mgr pattern-type itw

  - **拡張スキャン :** このレベルのスキャンは、元来ノイズの多いスパイウェアやアドウェアも標準スキャンします。スキャンの対象となるスパイウェアの範囲は広くなりますが、偽陽性が返される可能性も高まります。拡張スキャンを有効にするには、次のコマンドを入力します。

    set av scan-mgr pattern-type extended

注 : スキャンのデフォルトのセキュリティレベルを変更するには、CLI を使用する必要があります。

デフォルトは、標準オプション（**set av scan-mgr pattern-type standard**）です。

IM トラフィックの AV スキャン

インスタントメッセージ（IM）ネットワークは、クライアントとサーバー、およびそれらを接続するために必要なプロトコルからなります。

IM クライアント

各 IM クライアントには、3 つの主要コンポーネントがあります。

- 友人リストまたはあなたが通信したい友達の他のリスト。
- 進行中のテキストチャットを示す別のウィンドウ。ユーザーがメッセージを入力し、相手の応答がこのウィンドウに表示されます。
- 映像と音声によるチャット、およびユーザー間のファイル転送用の追加機能。

  主要な IM クライアントはすべて、簡単なテキストチャットから、リアルタイムの音声およびビデオ通話を含む、より多くの統合された高度な通信に移っています。

ScreenOS は、次のような一般的な公開 IM アプリケーションのスキャンをサポートします。

- AOL インスタントメッセンジャー（AIM）
- I Seek You (ICQ)
- Yahoo! Messenger（YMSG）
- MSN Messenger

ScreenOS のこのリリースでの AV スキャン機能は、次の IM サービスに適用されます。

- テキストチャットメッセージ
- グループチャットメッセージ
- ファイル転送 / ファイル共有

IM サーバー

IM サーバーは、ユーザーアカウントのディレクトリを維持し、誰がオンラインであるかを追跡し、ほとんどの場合ユーザー間のメッセージをルーティングします。IM サーバーは、リアルタイムで作動し、テキストの各行をタイプし終えると、2 人のユーザー間でメッセージを送信し合います。サーバーは、さらに、いつオンラインになるか、ステータスメッセージを変更するかのような、ディレクトリにある様々なユーザーの利用可能性に関するリアルタイムな情報を渡します。

各 IM サーバーは、インターネットを横断して、割り当てられたポート番号上のクライアントと通信します。ただし、IM クライアントは、デフォルトのポートが拒否するポリシーによってブロックされると、他のポートを使用してログインできます。通常のポート番号には次の表に示すものがあります。

IM アプリケーション	サービスポート番号	プロキシ
AIM	5190	SOCKS 4, SOCKS 5, HTTP, HTTPS
ICQ	5190	
YMSG	5050[1] (443 および 80)	SOCKS 4, SOCKS 5, HTTP
MSN Messenger	1863	SOCKS 4, SOCKS 5, HTTP

1. ポート 5050 に加えて、トラフィックがポート 443（HTTPS）および 80（HTTP）で許可されていることを確認します。

注 : AV スキャンは、暗号化されたフォーマットで通信する AIM または ICQ トラフィックではサポートされません。

IM プロトコル

IM ネットワークは、クライアントサーバーモデルを使用し、次のテーブルで示されたプロトコルを使用して、サービスへの認証および他のクライアントとの通信を行います。

IM アプリケーション	サポートされているプロトコル
AIM/ICQ	Open System for Communication in Realtime (OSCAR) プロトコル
YMSG	Yahoo Messenger Service Gateway (YMSG) プロトコル
MSN Messenger	Mobile Status Notification (MSNP) プロトコル

各 IM アプリケーション用の専用のプロトコルは絶えず更新されているので、ScreenOS は、ファイアウォールの活動をコントロールするため構成可能なパラメータを提供します。サポートされるクライアントおよびプロトコルのバージョンについては、製品のリリースノートを参照してください。ただし、ScreenOS は、次の 2 つの方法の 1 つで、サポートなしのプロトコルのバージョンについてトラフィックを処理します。

- Best Effort: トラフィックを処理するのに既存のプロトコル知識を使用します。
- Pass: スキャンせずにトラフィックを通過させます。

インスタントメッセージのセキュリティの問題

一般に、ワームは、インスタントメッセージサービス上で広まり、URL として現れます。「友人」リストの誰かからのもののように見えるので、これらの URL にアクセスします。URL をクリックすると、ワームがあなたの PC が感染し、「友人」リストの全員へ広がります。

「友人リスト」は、さらにソーシャル エンジニアリングに至ります。人がコンピュータシステムの合法的ユーザーから情報、特に特定のシステムへの権限外のアクセスを可能にする情報を得ると、ソーシャルエンジニアリングが発生します。

インスタントメッセージアプリケーションがトロイの木馬やウィルスを送信できるファイル転送サービスも、セキュリティ上危険です。

IM のセキュリティ上の問題

インスタントメッセージ（IM）サービスは、以下の方式による、ウィルス、ワームおよびトロイの木馬のような攻撃に脆弱です。

- 友人リスト

  通常はインスタントメッセージに URL として現れるので、ワームは IM サービスによって拡がることができます。これらの URL は、しばしば友人リストの誰かから来ているように見えます。そのような悪意のある URL をクリックすると、あなたの PC がワームに感染し、友人リストの全員に簡単に拡がることができます。

- ソーシャルエンジニアリング

  攻撃者が、システムまたはサービスの合法的ユーザーから機密情報（友人リストなど）、権限外のアクセスを獲得するために攻撃者が使用する情報を不正に獲得すると、ソーシアルエンジニアリングが生じます。

- ファイル転送

  ファイルが IM セッションによってあるユーザーから別のユーザーのもとへ送られると、トロイの木馬やウィルスは簡単に拡がることができます。

チャットメッセージのスキャン

デバイスが AV に使用可能な場合、ファイアウォールは IM クライアントとサーバーの間で送信されるデータパケットを処理します。ファイアウォールは、データパケットで個々のチャットメッセージの始めを検出し、チャットメッセージが完了するまで続くデータパケットを保持します。完了したメッセージは、次の表で示す手順を使用して、ウィルススキャンのために AV スキャンエンジンへ送られます。

状況	チャットメッセージ	結果
ウィルスを発見	破棄されます。	ウィルス破棄通知メッセージは、元のメッセージの宛先へ転送されます。
スキャンエラーが発生（スキャンエラー許可は無効）	破棄されます。	スキャンエラー破棄通知メッセージは、元のメッセージの宛先へ転送されます。
AV スキャンがウィルスの検出またはスキャンエラーなしで終了	宛先へ転送されます。	メッセージが宛先に到着します。

ファイル転送のスキャン

ファイアウォールは、IM クライアントとサーバーの間で通信されるデータパケットを処理します。通常、ファイル共有とはファイル取得を意味しますが、AIM ファイル転送には、ファイル送信、ファイル取得、およびディレクトリ送信を含みます。ファイアウォールがファイル転送コマンドを検出すると、以下のようになります。

ファイルサイズ	ファイル転送 / ファイル共有	結果
< = AV max_content_size	AV スキャンを実行	■ ウィルスを検出。ファイル内容はウィルス通知メッセージと交換されます。 ■ スキャンエラー（AV スキャンエラー許可は無効）ファイル内容はスキャンエラー通知メッセージと交換されます。
> AV max_content_size (max_content_size drop が有効)	AV スキャンをスキップ	ファイルを破棄し、元のメッセージの宛先へ破棄通知メッセージを転送します。
> AV max_content_size (max_content_size drop が無効)	AV スキャンをスキップ	ファイルが宛先へ転送されます。

注 : ScreenOS のこのリリースは、ファイアウォールによるインスタントメッセージ P2P トラフィックをサポートしません。

AV スキャンの結果

AV スキャンが実行されない場合、理由がいくつかあります。デバイスが外部スキャンを行うように構成されている場合、デバイスはトラフィックを単に外部 ICAP サーバーに転送します。AV スキャンの動作と結果の詳細については、ICAP サーバーの文書を参照してください。

デバイスが内部 AV スキャンを実行するように構成されている場合、**get av stat** コマンドによってスキャンの失敗が表示されます。このコマンドは、次のスキャンコードに加えて、スキャン結果に関する詳細情報を含むイベントログを生成します。

```
Scan Code: Clear
Scan Code: Infect
Scan Code: Psw Archive File
Scan Code: Decompress Layer
Scan Code: Corrupt File
Scan Code: Out Of Resource
Scan Code: Internal Error
Scan Code: Error
Scan Eng: Error:
Fail Mode:
```

次のシナリオでは、トラフィックは破棄され、置換データがその宛先へ転送されます。

- AV スキャンエンジンは、次のスキャンエラーの 1 つを返します。また、対応する構成破棄設定が有効になります。
  - max-decompress-layer setting is exceeded（max-decompress-layer 設定を超過）
  - password protected file（パスワードで保護されたファイル）
  - corrupted file（破損したファイル）
  - out of resource（リソース不足）

AV スキャンでリソース不足エラーが発生すると、ファイルは max-content-size 設定に基づいて破棄されるか通過しますが、リソース不足カウンタは増分されます。

- AV スキャンエンジンは、上記のスキャンエラーのいずれかを返し、fail-mode 許可が無効になります
- ファイル転送のサイズが AV max-content-size 設定を超過し、max-content-size drop が有効になります

注： max-decompress-layer 設定が、解凍レイヤー設定を超過するとデータパケットを破棄するように設定されている場合、置換ファイルが受信側へ送られます。ただし、MSN サーバーは、ダウンロードエラーに関する置換ファイルまたはエラーメッセージを送信しません。

データ を正しくスキャンできない場合のインスタンスも含めて、AV スキャンの失敗については、71 ページの「アプリケーションプロトコルのスキャン」を参照してください。

AV スキャン処理で生成されるエラーメッセージの一覧は、*ScreenOS Message Log Reference Guide* を参照してください。

ポリシーベースの AV スキャン

AV スキャンプロファイルを使用すると、AV スキャンの柔軟性と細分性が高まります。プロファイルベースのスキャンでは、プロファイルを構成して、トラフィックをスキャンしプロファイルをポリシーに割り当てることができます。ポリシーベースのスキャンは次の目的に使用します。

- AV スキャンの対象にする特定のデータトラフックを選択
- AV スキャンエンジンの性能および制御能力を強化する

ポリシーベースのスキャンを構成するには、次の手順を実行し、AV プロファイルを構成してポリシーで使える状態にします。

1. AV プロファイルコンテキストを起動します。詳細については、88 ページの「内部 AV 用の AV プロファイルの起動」を参照してください。
2. 次の表に示されたプロトコルのネットワークトラフィックを調べるために、プロファイル（内部 AV スキャン用のプロファイル *ns-profile* が事前定義されています）を構成します。

プロトコル	詳細は、
File Transfer Protocol (FTP)	72 ページの「FTP トラフィックのスキャン」
HyperText Transfer Protocol (HTTP)	73 ページの「HTTP トラフィックのスキャン」
Internet Mail Access Protocol (IMAP)	75 ページの「IMAP/POP3 トラフィックのスキャン」
Post Office Protocol, version 3 (POP3)	75 ページの「IMAP/POP3 トラフィックのスキャン」
Simple Mail Transfer Protocol (SMTP)	77 ページの「SMTP トラフィックのスキャン」
ICAP（インターネットコンテンツアダプテーションプロトコル）	79 ページの「トラフィックを ICAP AV スキャンサーバーに転送」

3. AV プロファイルコンテキストを終了します。

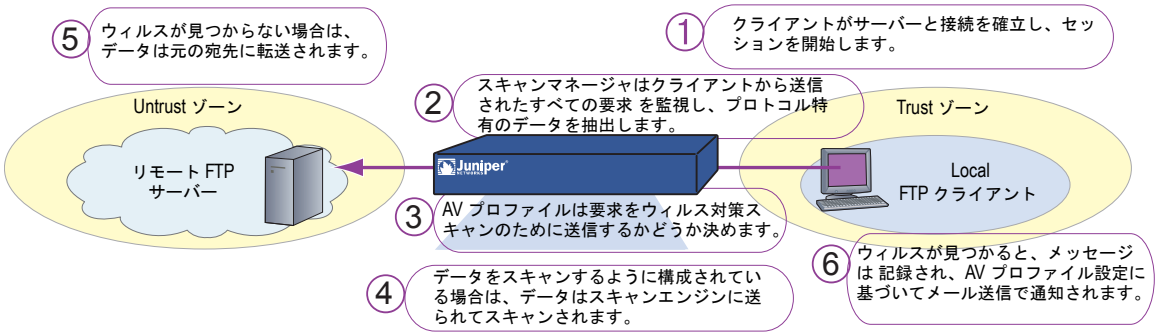
4. AV プロファイルを既存のファイアウォールポリシーに割り当てます。（ファイアウォールポリシーにリンクできる AV プロファイルは 1 つだけです。）

   AV 機能を適用するには、AV プロファイルを使う旨をセキュリティポリシーに記述する必要があります。AV スキャンが必要とポリシーで設定されたトラフィックを受け取ると、セキュリティデバイスはそのコンテンツを AV スキャナ（内部または外部）に転送します。

5. プロファイルを保存します。

図 33 は、AV プロファイルが AV スキャナ（内部または外部）と連動して動作する方法を示しています。

図 33: AV スキャナと連動した AV プロファイルの機能



アプリケーションプロトコルのスキャン

内部 AV スキャンの内蔵エンジンは特定のアプリケーションレイヤートランザクションのスキャンをサポートするため、スキャンするコンテンツ（FTP、HTTP、IMAP、POP3、または SMTP トラフィック）を選択することができます。たとえば、あるコンテンツについてはスキャンをしないことによって、スキャンのパフォーマンスを高めることができます。同様に、外部 AV スキャンは HTTP および SMTP プロトコルのみに適用できます。

注 : リスクを評価し、安全性とパフォーマンスの間で最良のトレードオフを決定する必要があります。

このセクションでは、次のアプリケーションプロトコルを AV スキャンの対象として構成する方法について説明します。

- 72 ページの「FTP トラフィックのスキャン」
- 73 ページの「HTTP トラフィックのスキャン」
- 75 ページの「IMAP/POP3 トラフィックのスキャン」
- 77 ページの「SMTP トラフィックのスキャン」

これらのアプリケーションの各々について、次の 1 つ以上の設定を構成できます。

コマンド	解説
decompress-layer	内部 AV スキャナがウィルス検査を開始する前に、スキャナが解凍できる圧縮ファイルの入れ子の階層数を指定します。
extension list	スキャンの対象に含める、または対象から除外する拡張子リスト名（*string*）を指定します。
scan-mode	スキャンエンジンが特定のプロトコルのトラフィックをスキャンする方法を指定します。
タイムアウト	特定のプロトコルの AV セッションのタイムアウト値を指定します。
http skipmime	指定した MIME リストを AV スキャン対象から外します。 **注記 : skipmime** リストを無効にすると、セキュリティデバイスは MIME コンテンツのタイプに関わらず、あらゆる種類の HTTP トラフィックをスキャンすることができます。
email-notify	IMAP、POP3、および SMTP トラフィックに限って、ウィルスの検出やスキャンエラーを送信側または受信側に通知します。

FTP トラフィックのスキャン

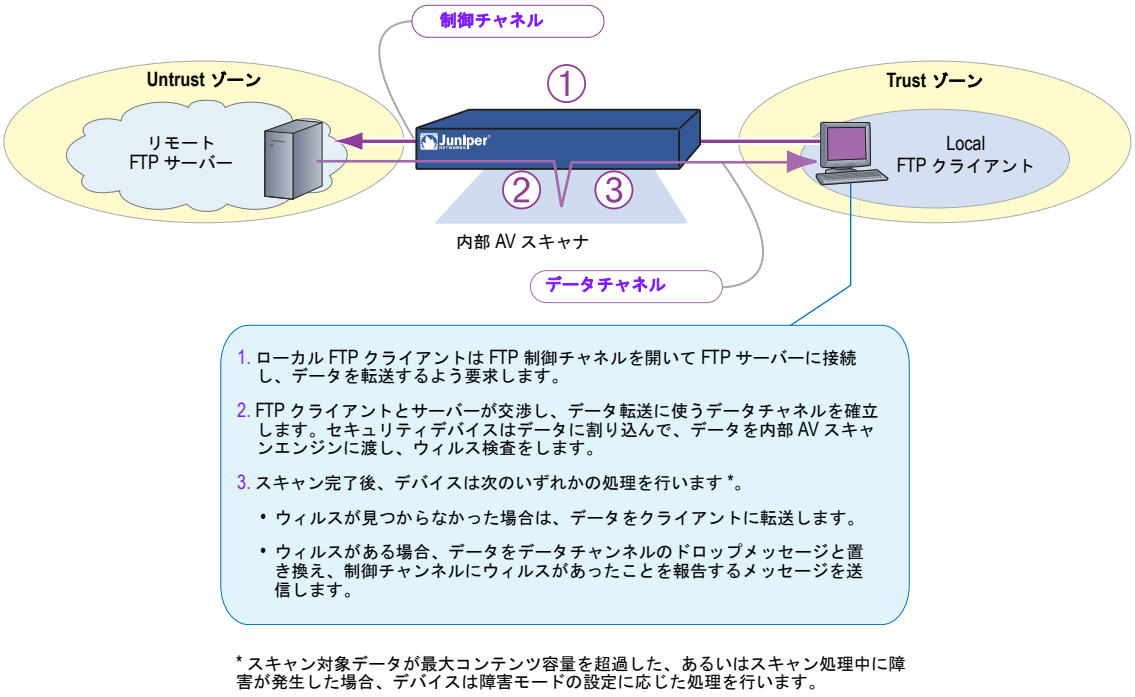
FTP (ファイル転送プロトコル) トラフィックに関しては、セキュリティデバイスは制御チャネルを監視し、データ転送用の FTP コマンド (RETR、STOR、STOU、APPE、NLST) のいずれかが現れた場合に、データチャネルを通して転送されるデータをスキャンします。

スキャン結果と故障モードの動作の設定に応じて、セキュリティデバイスは次の手順の 1 つを実行します。

スキャン結果	動作の設定	セキュリティデバイス
ウィルス非感染		データチャネルを介してデータを FTP クライアントに転送
ウィルス感染		データチャネルに届いたデータをドロップし、制御チャネルを介して FTP クライアントにウィルス検出通知メッセージを送信
最大コンテンツ容量を超過	**drop** が設定されている	データチャネルに届いたデータをドロップし、制御チャネルを介して FTP クライアントに「ファイルが大き過ぎる」という内容のメッセージを送信

スキャン結果	動作の設定	セキュリティデバイス
最大コンテンツ容量を超過	**drop** が設定されていない	データチャネルを介して調べられていないデータを FTP クライアントに転送
スキャン処理に失敗	**fail mode** が設定されていない（ドロップ）	データチャネルに届いたデータをドロップし、制御チャネルを介して FTP クライアントに「スキャン処理でエラーが発生した」という内容のメッセージを送信
スキャン処理に失敗	**fail mode** が許可されている（**traffic permit** が設定されている）	データチャネルを介してデータを FTP クライアントに転送
最大同時メッセージを超過	**drop** が設定されている	データチャネルに届いたデータをドロップし、制御チャネルを介して FTP クライアントに「最大メッセージ設定を超過した」という内容のメッセージを送信
最大同時メッセージを超過	**drop** が設定されていない	データチャネルを介してデータを FTP クライアントに転送

図 34: FTP トラフィックのウィルス対策スキャン



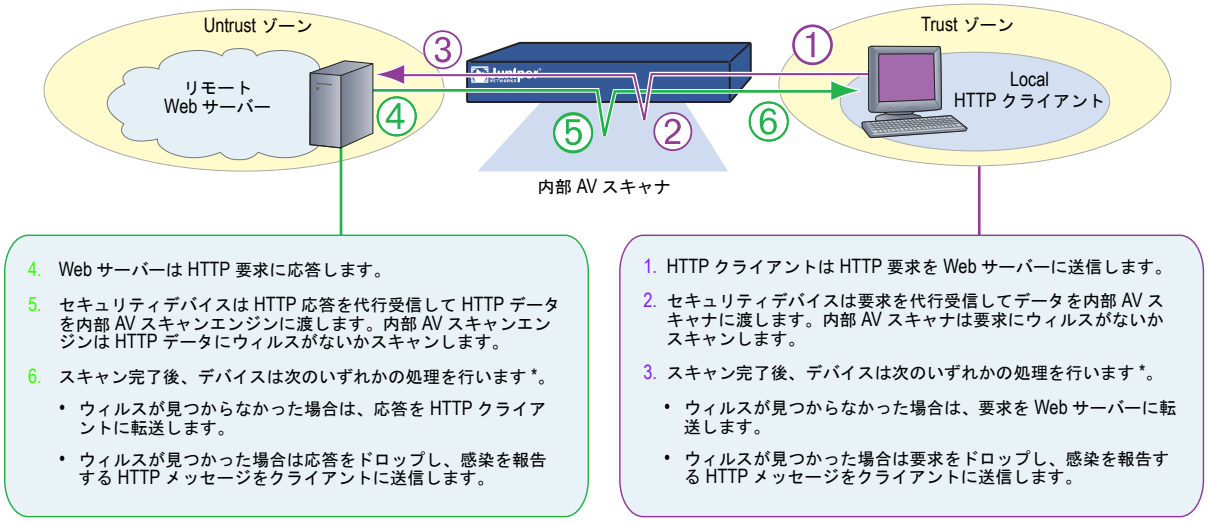
HTTP トラフィックのスキャン

HTTP トラフィックに関しては、セキュリティデバイスは応答と要求（**get**、**post**、および **put** コマンド）の両方をスキャンの対象とします。内部 AV スキャナは HTTP のダウンロード、すなわちクライアントからの HTTP 要求に対する Web サーバーからの応答に含まれる HTTP データを調べます。内部 AV スキャナはアップロードデータもスキャンします。これには HTTP クライアントが Web サーバー上のアンケートに記入する場合や、クライアントが Web サーバー上で送信する E メールにメッセージを書く場合などがあります。

スキャン結果と故障モードの動作の設定に応じて、セキュリティデバイスは次の手順の 1 つを実行します。

スキャン結果	動作の設定	セキュリティデバイス
ウィルス非感染		データを HTTP クライアントに転送
ウィルス感染		データを破棄し、ウィルスを検出した旨を HTTP クライアントに通知
最大コンテンツ容量を超過	**drop** が設定されている	データを破棄し、「ファイルが大き過ぎる」という内容のメッセージを HTTP クライアントに通知
最大コンテンツ容量を超過	**drop** が設定されていない	データを HTTP クライアントに転送
スキャン処理に失敗	**fail mode** が設定されていない（ドロップ）	データを破棄し、「スキャン処理でエラーが発生した」という内容のメッセージを HTTP クライアントに通知
スキャン処理に失敗	**traffic permit** が設定されている（**fail mode** は許可）	データを HTTP クライアントに転送
最大同時メッセージを超過	**drop** が設定されている	データチャネルに届いたデータをドロップし、制御チャネルを介して HTTP クライアントに「最大メッセージ設定を超過した」という内容のメッセージを送信
最大同時メッセージを超過	**drop** が設定されていない	データチャネルを介してデータを HTTP クライアントに転送

図 35: HTTP トラフィックのウィルス対策スキャン



* スキャン対象データが最大コンテンツ容量を超過した、あるいはスキャン処理中に障害が発生した場合、セキュリティデバイスは障害モードの設定に応じた処理を行います。

HTTP MIME 拡張

デフォルトでは、HTTP エンティティのうち、次のような MIME（Multipurpose Internet Mail Extensions）タイプおよびサブタイプ（スラッシュの後に記述されている部分）が設定されているものは、スキャンの対象になりません。

- Application/x-director
- Application/pdf
- Image/
- Video/
- Audio/
- Text/css
- Text/html

処理性能を重視して、上記の MIME タイプのコンテンツはスキャンしないようになっています。ほとんどの HTTP エンティティがこのいずれかの MIME コンテンツタイプに属するので、実際にスキャンの対象となるのは、application/zip や application/exe などごく一部です。ウィルスの多くは、このような MIME タイプのコンテンツ内に入っています。

HTTP スキャン処理の動作を変更して、セキュリティデバイスで MIME コンテンツタイプに関係なくすべての HTTP トラフィックをスキャンするには、次コマンドを入力します。

```
set av profile jnpr-profile
(av: jnpr-profile)-> unset av http skipmime
(av: jnpr-profile)-> exit
save
```

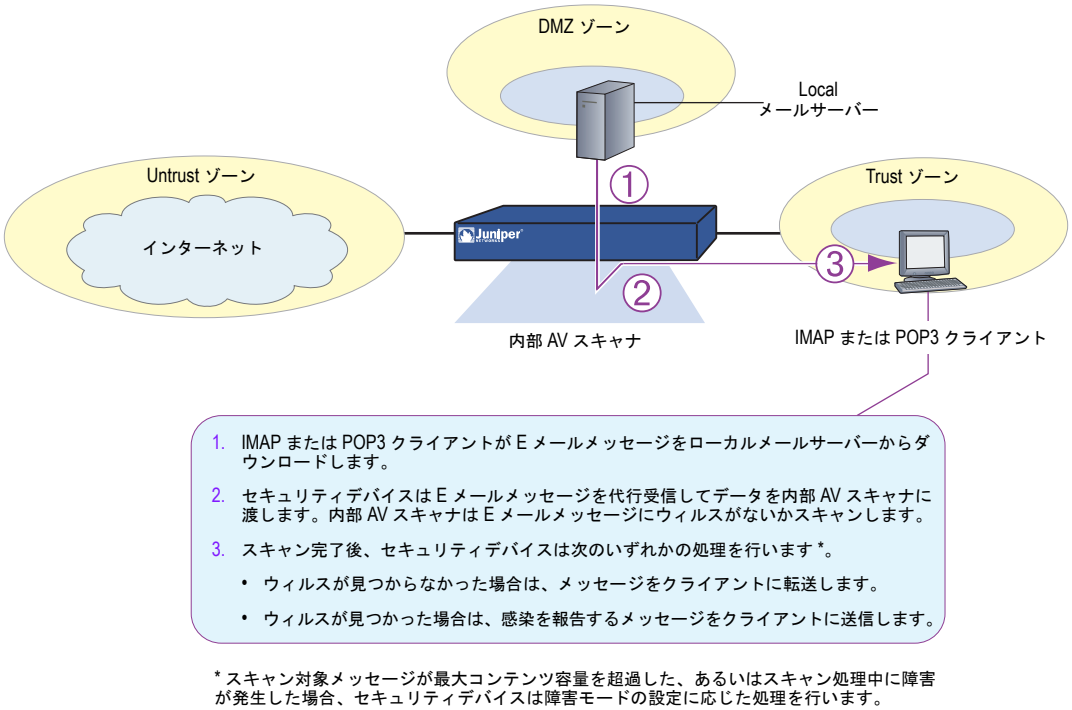
IMAP/POP3 トラフィックのスキャン

IMAP トラフィックおよび POP3 トラフィックの場合、セキュリティデバイスはローカルメールサーバーからのトラフィックをローカル IMAP または POP3 クライアントに送信する前に、内部 AV スキャナに転送します。スキャン結果と故障モードの動作の設定に応じて、セキュリティデバイスは次の手順の 1 つを実行します。

スキャン結果	動作の設定	セキュリティデバイス
ウィルス非感染		IMAP/POP3 クライアントにメッセージを転送
ウィルス感染	**email notification** が設定されている	コンテンツタイプを text/plain に変更し、メッセージの本文を次の通知文に差し替えて IMAP または POP3 クライアントに転送し、次の内容で送信側に通知 `VIRUS WARNING.` `Contaminated File: filename` `Virus Name: virus_name`

スキャン結果	動作の設定	セキュリティデバイス
最大コンテンツ容量を超過 または スキャン処理に失敗 または 最大同時メッセージを超過	**drop** が設定されている **fail mode** が設定されていない（ドロップ） **email notification** が設定されている	コンテンツタイプを text/plain に変更し、本文を次の通知文に差し替えて IMAP/POP3 クライアントに転送 *reason_text_str* (code *number*) のため、コンテンツにはウィルススキャンが行われず、破棄されました。 ここで、*reason_text_str* の部分には次のいずれかが挿入されます。 ■ The file was too large. ■ An error or a constraint was found. ■ The maximum content size was exceeded. ■ The maximum number of messages was exceeded. ウィルスの検出、またはスキャン処理エラーを送信側または受信側に通知
最大コンテンツ容量を超過 または スキャン処理に失敗 または 最大同時メッセージを超過	**drop** が設定されていない **traffic permit** が設定されている（**fail mode** は許可） **drop** が設定されていない **email notification** が設定されている	Subject: 行を次のように差し替えて、メッセージをそのまま IMAP/POP3 クライアントに転送 *original_subject_text_str* (*reason_text_str*, code *number* のためウィルスチェックなし) ウィルスの検出、またはスキャン処理エラーを送信側または受信側に通知

図 36: IMAP/POP3 トラフィックのウィルス対策スキャン



SMTP トラフィックのスキャン

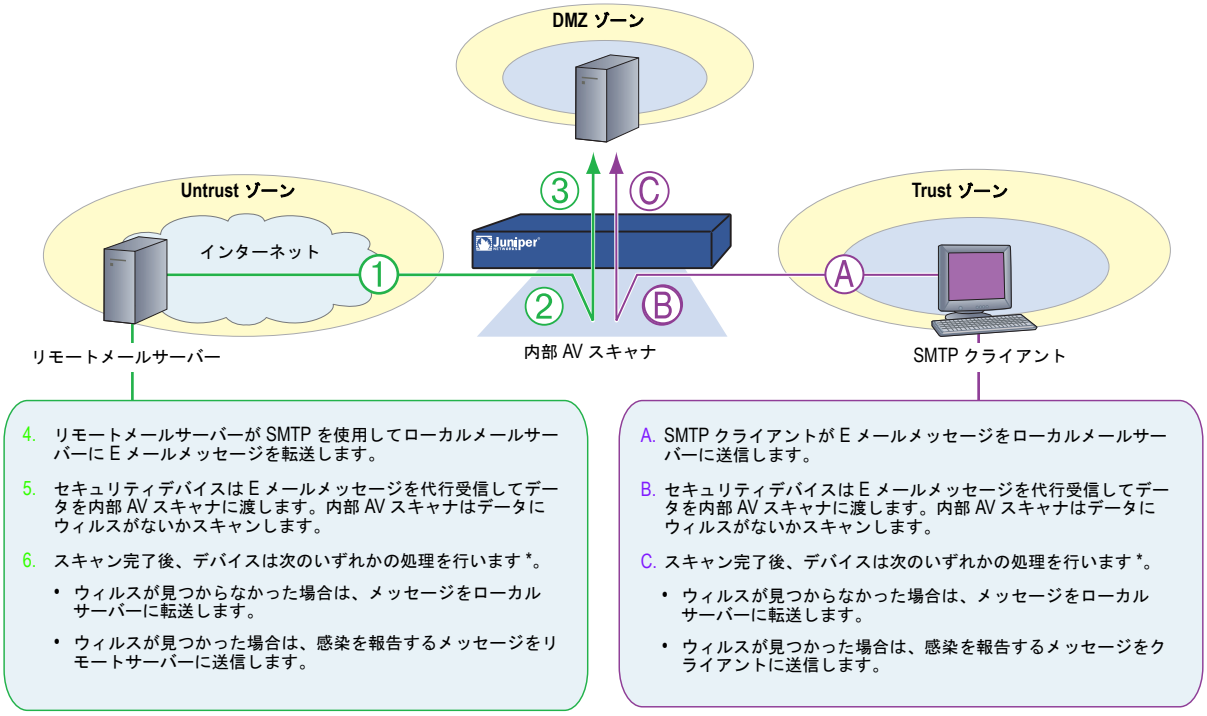
SMTP トラフィックの場合、セキュリティデバイスはローカル SMTP クライアントからのトラフィックをローカルメールサーバーに送信する前に、内部 AV スキャナに転送します。スキャン結果と故障モードの動作の設定に応じて、セキュリティデバイスは次の手順の 1 つを実行します。

スキャン結果	動作の設定	セキュリティデバイス
ウィルス非感染		SMTP の受け取り手にメッセージを転送
ウィルス感染	**email notification** が設定されている	コンテンツタイプを「text/plain」に変更し、メッセージの本文を次の通知文に差し替えて SMTP の受信側に転送し、次の内容で送信側に通知 `VIRUS WARNING.` `Contaminated File: filename` `Virus Name: virus_name`

スキャン結果	動作の設定	セキュリティデバイス
最大コンテンツ容量を超過 または スキャン処理に失敗 または 最大同時メッセージを超過	**drop** が設定されている **fail mode** が設定されていない（ドロップ） **drop** が設定されている **Email notification** が設定されている	コンテンツタイプを「text/plain」に変更し、メッセージ本文を次の通知文に差し替えて SMTP の受信側に転送 *reason_text_str* (code *number*) のため、コンテンツにはウィルススキャンが行われず、破棄されました。 ここで、*reason_text_str* の部分には次のいずれかが挿入されます。 ■ The file was too large. ■ An error or constraint was found. ■ The maximum content size was exceeded. ■ The maximum number of messages was exceeded. ウィルスの検出、またはスキャン処理エラーを送信側または受信側に通知
最大コンテンツレベルを超過 または スキャン処理に失敗 または 最大同時メッセージを超過	**drop** が使用不可である **traffic permit** が設定されている（故障モードは許可） **drop** が設定されていない **Email notification** が設定されている	Subject: 行を次のように差し替えて、メッセージをそのまま SMTP の受け取り手に転送 *original_subject_text_str* (*reason_text_str*, code *number* のためウィルスチェックなし) ウィルスの検出、またはスキャン処理エラーを送信側または受信側に通知

注： SMTP の*クライアント*とは E メールの送信元を指すので、クライアントが別の SMTP サーバーである可能性もあります。

図 37: SMTP トラフィックのウィルス対策スキャン



* スキャン対象メッセージが最大コンテンツ容量を超過した、あるいはスキャン処理中に障害が発生した場合、セキュリティデバイスは障害モードの設定に応じた処理を行います。

1. リモートメールサーバーが SMTP を使用してローカルメールサーバーに E メールメッセージを転送します。
2. セキュリティデバイスは E メールメッセージを代行受信してデータを内部 AV スキャナに渡します。内部 AV スキャナは E メールメッセージにウィルスがないかスキャンします。
3. スキャン完了後、デバイスは次のいずれかの処理を行います *。
   • ウィルスが見つからなかった場合は、メッセージをローカルサーバーに転送します。
   • ウィルスが見つかった場合は、感染を報告するメッセージをリモートサーバーに送信します。

トラフィックを ICAP AV スキャンサーバーに転送

Juniper Networks セキュリティデバイスは、ICAP（インターネットコンテンツアダプテーションプロトコル）で外部 AV スキャンエンジンと交信します。ScreenOS 5.4 は、HTTP トラフィックと SMTP トラフィックの転送のみをサポートします。

外部 ICAP AV スキャンを使用できるようにセキュリティデバイスを構成するには、次の手順を実行します。

1. **set icap** コマンドを使って、外部 ICAP スキャンサーバーを構成します。

2. ICAP プロファイルを構成し、次の 1 つまたは複数を指定します。

コマンド	解説
タイムアウト	特定のプロトコル（HTTP または SMTP）の AV セッションのタイムアウト値を指定します。
http skipmime	MIME リスト内の指定ファイルを AV スキャン対象から外します。 **注記 :** skipmime リストを使用不可にすると、セキュリティデバイスは MIME コンテンツのタイプに関係なくすべての HTTP トラフィックをスキャンすることができます。
email-notify	SMTP トラフィックについてのみ、ウィルスの検出やスキャンエラーを送信側または受信側に通知します。

WebUI

Objects > Antivirus > ICAP Server > New: 以下を入力して **Apply** をクリックします。

ICAP AV Server Name: ICAP_Server1
Enable:（選択）、Scan Server Name/IP: 1.1.1.1
Scan Server Port: 1344, Scan URL:/SYMCScan-Resp-AV
Probe Interval: 10, Max Connections:

CLI

```
set icap server icap_server1 host 1.1.1.1
save
```

ICAP サーバーは、設定されたときに自動的に使用可能になります。

内蔵スキャナの AV パターンファイルの更新

内部 AV スキャンでは、AV パターンのデータベースを Juniper Networks セキュリティデバイスにロードし、パターンファイルを定期的に更新する必要があります。

AV パターンファイルを更新する前に、ご使用のデバイスが次の項目をサポートしていることを確認してください。

前提条件	解説
有効な AV ライセンスキー	av_v2_key
インターネットアクセス	デバイスにインターネットへのルートがあること
DNS とポート設定	DNS 設定とポート 80 を検証
AV 署名サービス	80 ページの「AV 署名サービスの利用契約」を参照してください。

AV 署名サービスの利用契約

AV 署名サービス利用契約を購入するには、まずご使用のデバイスを登録する必要があります。契約が有効な間は、現在のバージョンのデータベースをロードできます。また、それ以降のバージョンが使用可能になればデータベースを更新できます。AV 署名サービスの開始手続きは、次の条件によって異なります。

- AV 機能が付属したセキュリティデバイスを購入した場合、最初に購入してから短期間は AV パターンファイルをロードできます。ただし、パターンの

更新を継続して受けるためにはデバイスを登録し AV 署名の契約を購入する必要があります。

- 現在のセキュリティデバイスを内部 AV スキャンを使用できるようにアップグレードしている場合、デバイスを登録し AV 署名の契約を購入しなければ AV パターンファイルのロードを開始することはできません。登録処理が完了した後、AV パターンファイルのダウンロードを開始するまで最長 4 時間待つ必要があります。

注 : AV 署名サービスについての詳細は、2-255 ページの「ライセンスサービスの登録およびアクティブ化」を参照してください。

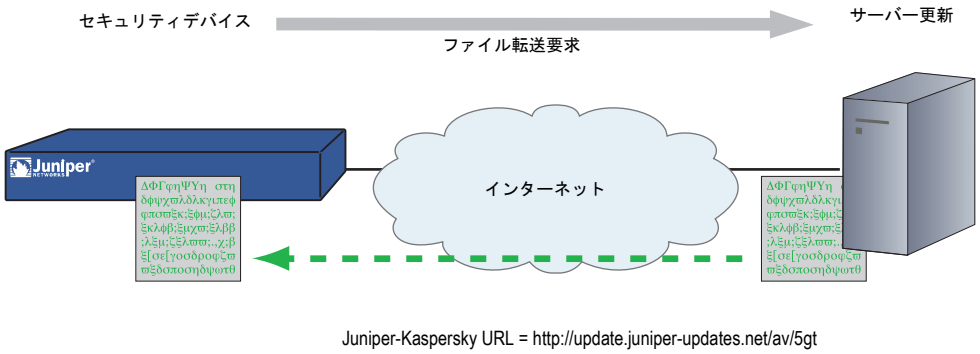
AV パターンファイルの更新

図 38 および図 39 は、パターンファイルがどのように更新されるのかを示しています。以下に、AV パターンファイルを更新する手順を示します。

1. セキュリティデバイスにパターン更新サーバーの URL を指定します。

   http://update.juniper-updates.net/av/5gt

図 38: パターンファイルの更新 - 手順 1

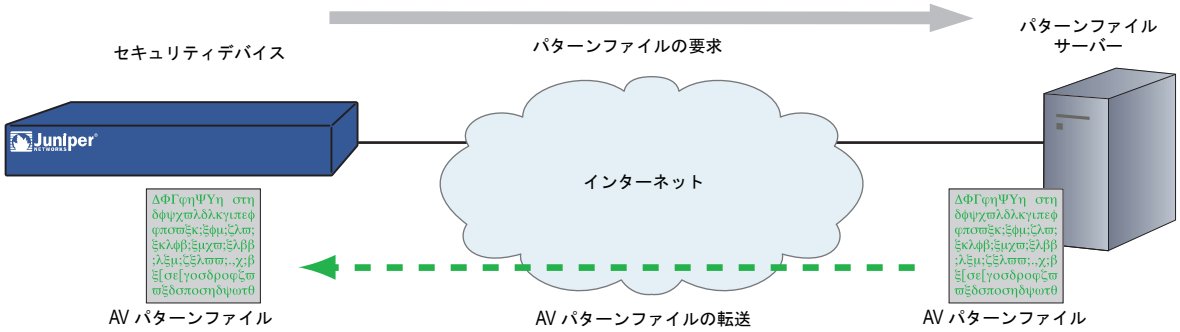


2. セキュリティデバイスは、サーバー初期化ファイルをダウンロードし、パターンファイルが有効かどうか確認します。次に、デバイスはファイルを解析し、ファイルのバージョンとサイズ、およびパターンファイルサーバーの位置などのファイル情報を取得します。

注 : ScreenOS には、パターン更新ファイルサーバーとの通信を認証する CA 証明書が含まれています。

3. セキュリティデバイスに保存されているパターンファイルが最新でない（または今回が初めてのローディングであるためにファイルがない）場合で、AV パターン更新サービス利用契約が今も有効な場合には、デバイスが自動的にサーバーから最新のパターンファイルを取得します。

図 39: パターンファイルの更新 - 手順 1



4. デバイスは、新しいパターンファイルをフラッシュメモリーや RAM に保存します。古いパターンファイルがある場合には上書きします。

新しいウィルスが広まると、パターンファイルの更新が追加されます。パターンファイルを定期的に自動更新するようにセキュリティデバイスを構成できるほか、随時手動で更新することも可能です。

注 : 契約の期限が切れると、更新サーバーは AV パターンファイルの更新を許可しません。

例: Automatic Update

この例では、120 分ごとにパターンファイルを自動更新するようにセキュリティデバイスを構成します。(AV パターンのデフォルトの更新間隔は 60 分です。) たとえば、パターン更新サーバーの URL が http://update.juniper-updates.net/av/5gt だと想定し、次の手順で自動更新を構成します。

WebUI

Security > Antivirus > Scan Manager: 以下を入力して **Apply** をクリックします。

Pattern Update Server: http://update.juniper-updates.net/av/5gt
Auto Pattern Update: (**選択**), Interval: 120 minutes (10~10080)

CLI

```
set av scan-mgr pattern-update-url http://update.juniper-updates.net/av/5gt
    interval 120
save
```

例: 手動更新

パターンファイルを手動で更新する操作例です。パターン更新サーバーは次の URL に位置しています。http://update.juniper-updates.net/av/5gt

WebUI

Security > Antivirus > Scan Manager: 以下を入力して **Apply** をクリックします。

Pattern Update Server: http://update.juniper-updates.net/av/5gt
Update Now: (**選択**)

CLI

```
exec av scan-mgr pattern-update
```

URL アドレスはデフォルトのため **set** コマンドは必要ありません。

AV スキャナのグローバル設定

AV スキャナの設定は、ネットワーク環境の必要性に応じて変更できます。CLI のグローバルな **scan-mgr** は、スキャンエンジンと連携する AV コンポーネントである、スキャンマネージャを構成します。たとえば、**set** または **get av scan-mgr** CLI コマンドは、max-content-size、max-msgs、pattern-type、pattern-update、および queue-size のようなパラメータを制御するグローバルコマンドを設定します。

以下のセクションでは、AV スキャナのグローバル設定について説明しています。

- 83 ページの「AV リソースの配分」
- 83 ページの「故障モードの動作」
- 84 ページの「最大コンテンツ容量と最大メッセージ数（内部 AV スキャンのみ）」
- 85 ページの「HTTP キープアライブ」
- 85 ページの「HTTP トリックリング（内部 AV スキャンのみ）」

デバイスのグローバルなアンチウィルス設定を確認するには、**get av all** または **get av scan-mgr** を使用します。

AV リソースの配分

悪意を持つユーザーが、同時に大量のトラフィックを送りつけてリソースを浪費させ、AV スキャナが他のトラフィックをスキャンできないよう妨害することも考えられます。こうした行為を成功させないために、Juniper Networks セキュリティデバイスでは単一のソースからのトラフィックが一度に消費できる AV リソースの最大パーセンテージを制限することができます。デフォルトの最大パーセンテージは 70 パーセントです。この設定は 1 から 100 パーセント の間の任意の値に変更できます。100 パーセントに設定した場合は単一のソースからのトラフィックが消費できる AV リソースの量に制限が課されません。

WebUI

注 : このオプションを設定するには CLI を使用する必要があります。

CLI

```
set av all resources number
unset av all resources
```

上記の **unset av** コマンドは、ソースごとの AV リソースの最大パーセンテージをデフォルト (70 パーセント) に戻します。

故障モードの動作

故障モードとは、スキャン処理を最後まで実行できないときにセキュリティデバイスが適用する動作で、調べられていないトラフィックを許可するかブロックするかのどちらかに設定します。デフォルトでは、スキャン処理ができない場合、ウィルス対策チェックが有効に設定されているポリシーで許可されたトラフィックをブロックします。このデフォルトの動作をブロックから許可に変更できます。

AV スキャンエンジンがファイルをスキャンしている途中でメモリが足りなくなった場合（通常は、ファイルを解凍している時)、故障モード設定ではなく、リソース不足（set av scan-mgr max-content-size）設定に基づいて、コンテンツがドロップされるか、または通過を許可されます。

WebUI

Security > Antivirus > Global: 調べられていないトラフィックをそのまま通過させる場合は **Fail Mode Traffic Permit** をオン、ブロックする場合はオフにして、**Apply** をクリックします。

CLI

```
set av all fail-mode traffic permit
unset av all fail-mode traffic
```

上記の **unset av** コマンドは、故障モードの動作をデフォルト (調べられていないトラフィックをブロックする) に戻します。

最大コンテンツ容量と最大メッセージ数（内部 AV スキャンのみ）

最大コンテンツ容量と最大メッセージ数のスキャンマネージャ設定は、内部 AV スキャンでのみサポートされます。ICAP AV スキャンは、最大コンテンツ容量設定と最大メッセージ数設定をサポートしません。

デバイスによっては、AV スキャナは一度に最高 256 件のメッセージ、および最大 10 MB の解凍されたファイルのコンテンツを調べます。最大コンテンツ容量と最大メッセージ数の値は、デバイスに依存します（製品のリリースノートを参照)。

同時に受信したメッセージの合計数やコンテンツの合計容量がデバイスで許される上限値を超えた場合、デフォルトではスキャナはウィルスの検査を行わずにコンテンツをドロップします。ISDN のような遅いリンクについては、AV スキャンがタイムアウトしないように、max-content-size をより小さい値に減らします (set av scan-mgr max-content-size 20)。

注 : セキュリティデバイスによっては、デフォルトの最大コンテンツ容量は 10 MB です。ただし、DI が使用可能になっている場合は、値を 6 MB に設定するようお勧めします。

たとえば、スキャナは 4 MB のメッセージを 4 つ同時に受信し、調べることができます。スキャナが 2 MB のメッセージ 9 件を同時に受信した場合、最後に受信した 2 件のファイルをスキャンを行わずにそのコンテンツをドロップします。このデフォルトの動作を変更して、スキャナがトラフィックをドロップせずに*通過*させることができます。それには、次の手順を実行します。

WebUI

Security > Antivirus > Scan Manager

Content Oversize: ファイルサイズが 10,000 KB を超える場合にトラフィックを通過させるには **permit** を選択します。

もしくは

Msgs Overflow: ファイル数がデバイスの最大メッセージ数を超えている場合 **permit** を選択肢、**Apply** をクリックします。

CLI

```
unset av scan-mgr max-content-size drop
unset av scan-mgr max-msgs drop
```

AV スキャンエンジンがファイルをスキャンしている途中でメモリが足りなくなった場合（通常は、ファイルを解凍している時)、故障モード（set av all failmode）設定ではなく、リソース不足（set av scan-mgr max-content-size）設定に基づいて、コンテンツがドロップされるか、または通過を許可されます。

HTTP キープアライブ

デフォルトでは、セキュリティデバイスは HTTP “keep-alive”接続オプションを使用します。このオプションは、データ転送の終了を示す TCP FIN を送信しません。HTTP サーバーは HTTP ヘッダーのコンテンツの長さを送信したり、ある種のコード化を使用したりして、データをすべて送信したことを別の方法で示す必要があります。(サーバーが使用する方法はサーバーのタイプによって異なります。この方法ではウィルス検査の間 TCP 接続が開かれた状態になり、これによって待ち時間を減らし、プロセッサのパフォーマンスが向上します。

セキュリティデバイスのデフォルトの動作を、データ転送の終了を示す HTTP「close」接続オプションを使用するように変更できます。(デバイスは必要に応じて接続ヘッダーフィールドのトークンを「キープアライブ」から「クローズ」に変更します。) この方法では、HTTP サーバーはデータ転送を完了すると TCP FIN を送信して TCP 接続を閉じ、データの送信が終了したことを示します。デバイスは TCP FIN を受信すると、サーバーからのすべての HTTP データを受信したことになり、AV スキャナにスキャンを開始するよう指示します。

注 : ただし、「keep-alive」は「close」接続方法ほど安全ではありません。HTTP 接続がウィルス検査の間にタイムアウトすることがある場合は、デフォルトの動作を変更できます。

WebUI

Security > Antivirus > Global:「キープアライブ」接続オプションを使用する場合は **Keep Alive** をオンにし、「クローズ」接続オプションを使用する場合はオフにします。それから **Apply** をクリックします。

CLI

```
set av http keep-alive
unset av http keep-alive
```

HTTP トリックリング（内部 AV スキャンのみ）

HTTP トリックリングとは、ダウンロードされた HTTP ファイルをスキャンマネージャが調べている間にブラウザウィンドウがタイムアウトしないよう、要求を出した HTTP クライアントのスキャンされていない HTTP トラフィックを指定した量だけ転送することです。(セキュリティデバイスはスキャンされたファイル全体を転送する前に少量のデータを転送します。)) デフォルトでは、HTTP トリックリングは使用不可になっています。HTTP トリックリングを使用可能にして デフォルトの HTTP トリックリングパラメータを使用するには、次のいずれかを実行します。

WebUI

Security > Antivirus > Global: Trickling Default チェックボックスをオンにして、**Apply** をクリックします。

CLI

set av http trickling default

注： HTTP トリックリングは内部 AV スキャンでのみサポートされます。ただし、YMSG については、トリックリングはチャットおよびファイル転送には無効です。ICAP AV スキャンは HTTP トリックリングをサポートしません。

デフォルトのパラメータでは、HTTP ファイルのサイズが 3MB 以上の場合にトリックリングが適用されます。デバイスは、スキャンのために 1MB が送信されるごとに 500 バイトのコンテンツを転送します。

AV スキャニング中にブラウザがタイムアウトした場合、ScreenOS では、さらに精細なトリックリングオプションを構成できます。セキュリティデバイスがトラフィックをスキャンするのにより多くの時間を必要とする場合、またはトラフィックが遅い場合、ブラウザはタイムアウトします。お使いの環境に基づいて、以下のようにトリックリング HTTP をトリガーする時およびデータの値をカスタマイズします。

WebUI

Security > Antivirus > Global: 以下を入力して **Apply** をクリックします。

Trickling:
Custom: (**選択**)
Minimum Length to Start Trickling: ***number1***.
Trickle Size: ***number2***.
Trickle for Every KB Sent for Scanning: ***number3***.
Trickle Timeout: ***number4***.

CLI

set av http trickling threshold *number1* segment-size *number3* trickle-size *number2* timeout *number4*

4 つの数字には次の意味があります。

- *number1:* トリックリングを起動させるために必要な HTTP ファイルの最小サイズ（単位 : KB）ダウンロードが遅いためブラウザがタイムアウトする場合、もっと早くトリックリングをトリガーするようにこの値を小さくしてください。
- *number2:* セキュリティデバイスが転送するスキャンされていないトラフィックのバイト単位のサイズ (ゼロでない値)
- *number3:* セキュリティデバイスがトリックリングを適用するトラフィックのブロックのサイズ (単位 : KB)
- *number4:* トリックリングイベントをトリガーする時間（秒）。時間ベースのトリックリングは、初期サイズ（*number1*）に到達したら始まります。値が 0 の場合、時間ベースのトリックリングは無効になります。

注 : クライアントのブラウザにトリックリングされたデータは小規模な使用不能のファイルの形を取ります。トリックリングはスキャンをせずに少量のデータをクライアントに転送する仕組みになっているため、セキュリティデバイスがクライアントにトリックリングしたデータにはウィルスコードが含まれている場合があります。トリックリングされたファイルは削除するようお勧めします。

HTTP トリックリングを使用不可にするには、WebUI (Security > Antivirus: Trickling セクションの **Disable** をクリック) や CLI コマンド **unset av http trickling enable** を使用できます。ただし、ダウンロード中のファイルが 8MB より大きく、HTTP トリックリングが使用不可の場合、ブラウザウィンドウがタイムアウトする可能性が非常に高くなります。

AV プロファイル

ポリシーは AV プロファイルを使って、AV 検査を受けるトラフィックおよび検査結果に対するアクションを決定します。ScreenOS は、以下のタイプのプロファイルをサポートします。

- 定義済みの AV プロファイル

  ScreenOS がサポートする 2 つの定義済みプロファイルは、デフォルトの **ns-profile** (読み取りのみ) および **scan-mgr profile** (読み書き) です。両方のプロファイルとも、内蔵 AV のみでサポートされます。

  scan-mgr profile は、ScreenOS 5.2 以前から ScreenOS 5.3 以降へアップグレードすると、後方互換性のため自動的に生成されます。**scan-mgr profile** は、グローバルなスキャンマネージャコマンドに移行するため作成されます。

  スキャンマネージャは、スキャンエンジンを管理する AV コンポーネントです。スキャンマネージャに関する詳細は、83 ページの「AV スキャナのグローバル設定」を参照してください。

  scan-mgr profile は、コマンドが今、プロファイルコンテキストの内部から入力されているように、以下のコマンドを実行します。

```
set ftp decompress-layer 2
set http decompress-layer 2
set imap decompress-layer 2
set pop3 decompress-layer 2
set smtp decompress-layer 2
set http skipmime enable
set http skipmime mime-list ns-skip-mime-list
```

  たとえば、**get av profile ns-profile** または **get av profile scan-mgr** コマンドは、サポートされているプロトコルのプロファイル設定を表示します。

```
device->get av profile ns-profile
ftp Setting:
    status: enable
    mode: scan-intelligent
    decompress layer: 3
    timeout: 180 秒
    include ext list: なし
    exclude ext list: なし
http Setting:
    status: enable
```

```
    mode: scan-intelligent
    decompress layer: 2
    timeout: 180 秒
    include ext list: なし
    exclude ext list: なし
    skip scanning: text/html;text/css;audio/;video/;image/;
    application/x-director
---
```

- カスタム AV プロファイル

  各プロトコルの設定をカスタマイズするために自分の AV プロファイルを作成します。各 vsys（およびルート）につき最高 8 つの AV プロファイルを定義できます。

AV プロファイルを既存のファイアウォールポリシーに割り当て

ファイアウォールポリシーにリンクできる AV プロファイルは 1 つだけです。AV プロファイルをファイアウォールポリシーにリンクさせるには、次の操作を実行します。

WebUI

Policy > Policies: AV プロファイルをリンクさせたいポリシーの **Edit** をクリックし、**Antivirus Profile** からポリシーを選択します。**OK** をクリックする。

CLI

device-> **set policy id** *policy_num* **av ns-profile**

以下のセクションでは、AV プロファイルの起動方法とプロファイル設定の構成方法について説明します。

- 88 ページの「内部 AV 用の AV プロファイルの起動」
- 89 ページの「例 : (内部 AV) あらゆる種類のトラフィックのスキャンの設定」
- 89 ページの「例 : SMTP および HTTP トラフィックのみの AV スキャン」
- 90 ページの「AV プロファイル設定」

内部 AV 用の AV プロファイルの起動

次のコマンドは *jnpr-profile* という独自の AV プロファイルを起動します。デフォルトでは、FTP、HTTP、IMAP、POP3、SMTP の各トラフィックをスキャンするように設定されています。

WebUI

Security > Antivirus > Profile: **New** を選択してプロファイル名 *jnpr-profile* を入力し、**OK** をクリックします。

CLI

set av profile *jnpr-profile*
device(av: jnpr-profile)->

device-> **set av profile jnpr-profile**
device(av: jnpr-profile)->

AV プロファイルコンテキストを入力すると、それ以降のコマンドが実行される度に、指定した AV プロファイル (*jnpr-profile*) が変更されます。

例 : (内部 AV) あらゆる種類のトラフィックのスキャンの設定

この例では、FTP、HTTP、IMAP、POP3、IM、および SMTP の各トラフィックをスキャンするように構成します。大量のトラフィックを処理することになるため、タイムアウト値を 180 秒 (デフォルト) から 300 秒に変更します。

WebUI

Security > Antivirus > Profile: *profile_name* を入力して **OK** をクリックします。

デフォルトでは、6 つのすべてのプロトコルのトラフィックがスキャンの対象になります。

注 : タイムアウト値の変更には CLI を使う必要があります。

CLI

```
set av profile jnpr-profile
(av:jnpr-profile)-> set http enable
(av:jnpr-profile-> set http timeout 300
(av:jnpr-profile)-> set ftp enable
(av:jnpr-profile)-> set ftp timeout 300
(av:jnpr-profile)-> set imap enable
(av:jnpr-profile)-> set imap timeout 300
(av:jnpr-profile)-> set pop3 enable
(av:jnpr-profile)-> set pop3 timeout 300
(av:jnpr-profile)-> set smtp enable
(av:jnpr-profile)-> set smtp timeout 300
(av:jnpr-profile)-> exit
save
```

例 : SMTP および HTTP トラフィックのみの AV スキャン

デフォルトでは、FTP、HTTP、IMAP、POP3、SMTP の各トラフィックが AV スキャン対象です。スキャナがネットワークトラフィックのみを調べるようにデフォルトの動作を変更することができます。

タイムアウト値はプロトコルごとに構成できます。デフォルトでは、すべてのデータが揃った後にスキャンが開始されないと、AV スキャンは 180 秒でタイムアウトになります。1 秒から 1800 秒の範囲で指定できます。

この例では、AV スキャナが SMTP と HTTP のトラフィックをすべて調べるように構成します。両方のプロトコルに対するタイムアウト値をデフォルトである 180 秒に戻します。

注 : 内部 AV スキャナは特定の HTTP Web メールパターンだけを調べます。Yahoo!、Hotmail、および AOL のメールサービスのパターンは定義済みです。

WebUI

Security > Antivirus > **New** を選択して、プロファイル名 *jnpr-profile.* を入力します。

次のように入力してから **OK** をクリックします。

Protocols to be scanned:
HTTP: (選択)
SMTP: (選択)
POP3: (オフ)
FTP: (オフ)
IMAP: (オフ)

注 : タイムアウト値の変更には CLI を使う必要があります。

CLI

```
set av profile jnpr-profile
(av:jnpr-profile)-> set smtp timeout 180
(av:jnpr-profile)-> set http timeout 180
(av:jnpr-profile)-> unset pop3 enable
(av:jnpr-profile)-> unset ftp enable
(av:jnpr-profile)-> unset imap enable
(av:jnpr-profile)-> exit
save
```

AV プロファイル設定

以下のスキャンのオプションは、アプリケーションプロトコルごとに構成します。

- 90 ページの「添付ファイルの解凍」
- 91 ページの「ファイル拡張子に基づく AV スキャン」
- 92 ページの「HTTP コンテンツタイプに基づく AV スキャン」
- 92 ページの「送信側と受信側に E メールで通知」
- 93 ページの「例 : 大容量ファイルをドロップする」

添付ファイルの解凍

セキュリティデバイスがコンテンツを受信すると、内部 AV スキャナは圧縮されたファイルを解凍します。ウィルススキャンを実行する前に、圧縮ファイルを最大 4 つまで解凍するように内部 AV スキャナを構成できます。

たとえば、メッセージが、別の圧縮した .zip ファイルを含む圧縮した .zip ファイルを含んでいる場合、2 つの圧縮レイヤーがあり、両方のファイルの解凍は、2 の解凍レイヤー設定を必要とします。

WebUI

Security > Antivirus > Profile: **New** または **Edit** を選択して、既存のプロファイルを編集します。Decompress Layer を 2 に更新して、**Apply** をクリックします。

CLI

```
set av profile jnpr-profile
(av:jnpr-profile)-> set smtp decompress-layer 2
```

データのコンテンツを暗号化して転送するプロトコルがあります。AV スキャンエンジンはこの階層を復号化する必要があります。エンジンはスキャンを開始する前のこの階層を解凍レベルであるとみなします。

ファイル拡張子に基づく AV スキャン

ScreenOS は、3 つのスキャンモードをサポートします。

- **scan-all**: AV エンジンはウィルススキャン用のスキャンエンジンへファイルをすべて転送します。

- **scan-intelligent**: AV エンジンは、ファイルをスキャンする必要があるかどうか判断するために組み込みアルゴリズムを使用します。

  このデフォルトの scan-intelligent オプションは、AV エンジンが、ファイルタイプが正しいか、他のファイルに直接感染させないかの確認を含め、最も一般的で普及しているウィルスがないかトラフィックをスキャンするアルゴリズムを使用するよう指定します。このオプションは scan-all ほど範囲が広くありませんが、パフォーマンスは向上します。

- **scan-extension**: AV エンジンは、拡張子、排他・包含リスト（次のセクションを参照）に基づいてスキャンするため、ファイルを転送します。

ファイル拡張子リストを使用すると、特定のプロトコルのどのファイルを AV スキャンするかを決定できます。ファイル拡張子リストはプロトコルごとに、含める場合は *Include*、含めない場合は *Exclude* を選択できます

メッセージのファイル拡張子がインクルード用ファイル拡張子リストに載っているものがスキャンの対象です。メッセージのファイル拡張子がエクスクルード用ファイル拡張子リストに載っているものはスキャンされません。ファイル拡張子がインクルードリストにもエクスクルードリストにも載っていない場合は、スキャンするか否かはデフォルトのファイル拡張子スキャン設定に従います。デフォルトのファイル拡張子リストはスキャンエンジンのデータベースにあり、読み取り専用です。**get av scan-mgr** コマンドを使用して、スキャンエンジンのデフォルトのファイル拡張子リストを表示します。プロトコルごとの定義済みファイル拡張子リストはありません。

IMAP トラフィックを拡張子別にスキャンするように AV スキャナを構成し、ace、arj、chm の拡張子の付いたファイルは除外します。

WebUI

Security > Antivirus > Ext-list > New > 拡張子リストの名前（elist1）を入力して、拡張子のリスト（ace;arj;chm）を入力します。**OK** をクリックする。

Security > Antivirus > Profile > Select the Profile to **Edit** > **IMAP** を選択 > 次のオプションを選択して、**OK** をクリックします。

```
Enable
Scan Mode: Scan by Extension
Exclude Extension List: elist1
```

CLI

```
set av extension-list elist1 ace;arj;chm
set av profile test1
(av:test1)-> set imap scan-mode scan-ext
(av:test1)-> set imap extension-list exclude elist1
```

HTTP コンテンツタイプに基づく AV スキャン

このオプションは、AV スキャンが必要な HTTP トラフィックを決めるときに使用します。HTTP トラフィックは、デフォルトで定義済みの MIME (Multipurpose Internet Mail Extensions) のタイプごとに分類されます。MIME のタイプには、application/x-director、application/pdf、画像などがあります。

特定の MIME のタイプを含む MIME リストをスキップするように AV プロファイルを構成することができます。デフォルトで定義済みの MIME リストは ns-skip-mime-list です。HTTP プロトコルを使用するので、Yahoo Messenger ファイル転送は、MIME リストで指定された MIME 拡張子を無視します。HTTP GET/PUT 操作の一部として、content-type ヘッダーは、すべてのファイルについて text または html に指定されます。

この例では、MIME コンテンツのタイプに関わらず、HTTP トラフィック全体をスキャンするように構成します。

WebUI

Security > Antivirus > Profile > Select the Profile to **Edit** > HTTP を選択して、Skipmime Enable オプションをクリアします。**OK** をクリックする。

CLI

```
set av profile jnpr-profile
(av:jnpr-profile)-> unset av http skipmime
(av:jnpr-profile)-> exit
save
```

MIME タイプ詳細については、*ScreenOS CLI Reference Guide IPv4 Command Descriptions* を参照してください。

送信側と受信側に E メールで通知

E メール通知オプションを適用できるのは、IMAP、POP3、SMTP のプロトコルのみです。スキャンエラーやウィルス情報を送信側または受信側に通知するように AV プロファイルを構成できます。

E メールメッセージにウィルスが検出されると、警告メッセージの内容 (ウィルス名、ソース / 宛先 IP) が通知レベルのメッセージに記載されます。警告レベルのメッセージは、SMTP プロトコルで E メールで送信されます。

メッセージでスキャンエラーが生じたときは、スキャンエラーメッセージの内容が警告レベルのメッセージに記載されます。このメッセージは、SMTP プロトコル経由で メール送信されます。

この例では、次の操作を実行するようにセキュリティデバイスを構成します。

- ウィルスが検出されたときに、送信側に通知する
- スキャンエラーが生じたら、送信側および受信側に通知する

WebUI

Security > Antivirus > Profile > Select the Profile to **Edit** > **IMAP** を選択して、**OK** をクリックします。

次のように入力してから **OK** をクリックします。
Protocols to be scanned:
Email Notify > Select **Virus Sender**
Email Notify > Select **Scan-error Sender**
Email Notify > Select **Scan-error Recipient**

CLI

```
set av profile jnpr-profile
(av:jnpr-profile)-> set imap email-notify virus sender
(av:jnpr-profile)-> set imap email-notify scan-error sender
(av:jnpr-profile)-> set imap email-notify scan-error recipient
(av:jnpr-profile)-> exit
save
```

例: 大容量ファイルをドロップする

この例では、相互のファイル内にレイヤーされた最大 3 つのファイルの HTTP トラフィックを解凍するように AV スキャナを構成します。また、同時に受信したメッセージの合計数が 4 件を超えた場合、あるいは解凍されたコンテンツの合計サイズが構成されている値を超えた場合には、コンテンツをドロップするようにスキャナを構成します。ScreenOS が扱うことができる合計解凍ファイルコンテンツ容量は、各デバイスの仕様に依存しますが、最小容量は 10 MB です。

注 : 解凍ファイルのコンテンツ容量のデフォルトの値は、メッセージごとの値であって、同時に検査されるメッセージの合計の容量ではありません。

最大同時メッセージ数と最大キューサイズのデフォルトの値は、AV ス キャナが一度に同時に検査できる合計メッセージ数 256 です。257 番目のメッセージは、構成されている指示に従ってドロップされるかまたは通過を許可されます。

WebUI

Security > Antivirus > Scan Manager: 次のように入力してから **OK** をクリックします。

Content Oversize: Drop Max Content Size: 3000 KB (20~10000)
Msg Overflow: Drop Max Concurrent messages is 256

Security > Antivirus > Profile: Select Edit > HTTP: 次のように入力してから **OK** をクリックします。

File decompression: 3 layers (1~4)

CLI

```
set av scan-mgr max-msgs drop
set av scan-mgr max-content-size 3000
set av scan-mgr max-content-size drop
set av profile jnpr-profile
(av:jnpr-profile)-> set http decompress-layer 3
(av:jnpr-profile)-> exit
save
```

スパム対策フィルタリング

スパムとは迷惑な内容のメッセージを含む E メールで、通常は販売目的の業者、悪質な業者、あるいは詐害的な組織から送信されます。スパム対策機能は、送信されたメッセージを調べてスパムを識別します。デバイスは、スパムと思われるメッセージを検出すると、メッセージフィールドに事前プログラムされた文字列でタグを付けるか、またはメッセージをドロップします。

このスパム対策機能は、ご使用のスパム対策サーバーに取って代わるのではなく補完するものです。このコマンドを構成することによって、企業内部の E メールサーバーがスパムを受信および配信することを防止します。企業のユーザーは、ファイアウォールを通ることなく内部 E メールサーバーから E メールを取り出します。これは企業内部における一般的な構成といえます。

Juniper Networks のスパム対策は、世界中から収集された情報を基に、常時更新される IP ベースのスパムブロッキングサービスを利用します。このサービスは堅牢で偽陽性が生じることが極めて少ないため、ブラックリストのチューニングや構成は必要がありません。ただし、管理者はオプションで、ローカルのホワイトリストやブラックリストに特定のドメインや IP を追加することができます。これらのリストはデバイスがローカルで実施できます。

注： このリリースでは、SMTP プロトコルのスパム対策のみをサポートしています。

スパムメッセージを阻止したり、受信量を減らしたりするには、スパム対策プロファイルを構成できます。ポリシーのプロファイルを使用して、疑わしいスパムメッセージを検出し、フィルタリングで除去できます。スパム対策プロファイルを使用すると、悪質（スパム）または無害（スパム以外）と指定した IP アドレスや E メール、ホスト名、ドメイン名のリストを設定することができます。スパム対策プロファイルには、次のタイプのリストを含めることができます。

- 公開ベースのブラックリストまたはホワイトリスト

  接続がメール転送エージェントからの場合は、デバイスのリストを使用して、IP アドレスが無害（ホワイトリスト）か悪質（ブラックリスト）かを判断し、接続のソース IP アドレス をフィルタリングすることができます。

- カスタム定義のブラックリストまたはホワイトリスト

  - ドメイン名ベースのブラックリストまたはホワイトリスト

    デバイスは上記のリストを使用して、ドメイン名が正当か悪質かのどちらと判断されるかによって、そのドメイン名を使用する接続をフィルタリングすることができます。

  - アドレス帳ベースのホワイトリストまたはブラックリスト

    デバイスは上記のリストを使用して、送信側の E メールアドレスまたはドメインを基にフィルタリングすることができます。デフォルトでは、どの E メールサーバーもそのユーザーの E メールを受理するようになっています。

ブラックリストとホワイトリスト

スパム対策機能を利用するには、ファイアウォールが SBL（Spam Block List）サーバーにインターネット接続されている必要があります。また、SBL サーバーにアクセスできる DNS（ドメイン名サーバー）が使用可能でなければなりませんファイアウォールは、SMTP 送信側 (または中継エージェント) のソース上で DNS 逆引きを実行し、SBL サーバーの名前 (例、sbl-server) を権限のあるドメインとして追加します。次に DNS サーバーは各要求を SBL サーバーに転送します。SBL サーバーはファイアウォールに値を戻します。

代わりに、ローカルのホワイトリストやブラックリストを構成できます。この場合、デフォルトでは、まずブラック / ホワイトリストのローカルのデータベースを確認します。ホスト名が見つからなければ、ファイアウォールはインターネットにある SBL サーバーに問い合わせます。

基本構成

以下のコマンドを使用すると、基本的なスパム対策の一例が構成できます。これによって、smpt サーバー（または中継サーバー）がスパム E メールを受信するのを阻止します。

```
set anti-spam profile ns-profile
set policy from untrust to trust any mail-server SMTP permit log anti-spam
    ns-profile
```

次の例では、ファイアウォールがテストを実行して、spammer.org がホワイトリストにあるかブラックリストにあるかを調べます。

```
exec anti-spam testscan spammer.org
```

spammer.org がブラックリストに掲載されている場合、デバイスは次のような出力を生成します。

```
AS: anti spam result: action Tag email subject, reason: Match local blacklist
```

また、spammer.org がホワイトリストに掲載されている場合は、デバイスが次のような出力を生成します。

```
AS: anti spam result: action Pass, reason: Match local whitelist
```

ブラックリスト、およびホワイトリストの作成方法については、96 ページの「ブラックリストの定義」および 96 ページの「ホワイトリストの定義」を参照してください。

スパムトラフィックのフィルタリング

次の例では、スパムを含む SMTP トラフィックがシステム内を行き来しているものと想定します。そして ScreenOS が DNS 名または IP アドレスのどちらかでスパムをチェックしています。

次のコマンドを使用すると、基本的なスパム対策の一例が構成できます。

```
device-> exec anti-spam test 2.2.2.2
AS: anti spam result: action Tag email subject, reason: Match local black list
exec anti-spam testscan spammer.org
AS: anti spam result: action Tag email subject, reason: Match local black list
```

スパムメッセージのドロップ

set anti-spam profile コマンドを、**ns-profile** オプションだけを指定して実行すると、CLI を新規または既存のスパム対策プロファイルのコンテキスト内に配置します。たとえば、次のコマンドは **ns-profile** という名前のプロファイルを定義し、次に **ns-profile** コンテキストを入力して、疑わしいスパムメッセージをドロップするようにデバイスに指示します。

```
device-> set anti-spam profile ns-profile
device(ns-profile)-> set default action drop
```

スパム対策コンテキストを入力すると、それ以降のコマンドが実行される度に、指定したスパム対策プロファイル（この例では **ns-profile**）が変更されます。変更内容を保存するには、まずスパム対策を終了してから、**save** コマンドを入力します。

```
device(ns-profile)-> exit
device-> save
```

ブラックリストの定義

IP アドレス、E メールアドレス、ホスト名、またはドメイン名をロカールのスパム対策ブラックリストに追加またはリストから削除するには、ブラックリストコマンドを使用します。ブラックリストの各入力が、スパマーの可能性があるものを識別します。

ブラックリストを定義するには、次の手順を実行します。

1. プロファイルコンテキスト（**ns-profile**）を起動する。
2. www.wibwaller.com というホスト名の接続を阻止するブラックリスト入力をプロファイルに追加する。
3. スパムコンテキストを終了し、プロファイルを既存のポリシー (id 2) に適用する。

```
device-> set anti-spam profile ns-profile
device(anti-spam:ns-profile)-> set blacklist www.wibwaller.com
device(anti-spam:ns-profile)-> exit
device-> set policy id 2 anti-spam ns-profile
```

ホワイトリストの定義

IP アドレス、E メールアドレス、ホスト名、またはドメイン名をロカールのスパム対策ホワイトリストに追加またはリストから削除するには、ホワイトリストコマンドを使用します。ホワイトリストの各入力が、スパマーの疑いのないエンティティを識別します。下表は入力例を示しています。

ホワイトリストを定義するには、次の手順を実行します。

1. プロファイルコンテキスト（**ns-profile**）を起動する。
2. www.fiddwicket.com というホスト名の接続を許可するホワイトリスト入力をプロファイルに追加する。

3. スパムコンテキストを終了し、プロファイルを既存のポリシー (id 2) に適用する。

```
device-> set anti-spam profile ns-profile
device(anti-spam:ns-profile)-> set whitelist www.fiddwicket.com
device(anti-spam:ns-profile)-> exit
device-> set policy id 2 anti-spam ns-profile
```

デフォルトアクションの定義

デフォルトのコマンドを使用して、スパムと思われるメッセージの処理方法を指定します。デバイスは、スパムメッセージをドロップするか、メッセージにタグを付けてスパムと識別できるようにします。

タグは、メッセージのヘッダーまたは subject 行のいずれかに挿入できます。

デフォルトのスパム処理動作を定義するには、次の手順を実行します。

1. プロファイルコンテキスト（**ns-profile**）を起動する。

2. スパムと思われる E メールメッセージにはメッセージのヘッダーに「This is spam」という文字列を付けるように指定する。

3. スパムコンテキストを終了し、プロファイルを既存のポリシー (id 2) に適用する。

```
device-> set anti-spam profile ns-profile
device(anti-spam:ns-profile)-> set default action tag header "This is spam"
device(anti-spam:ns-profile)-> exit
device-> set policy id 2 anti-spam ns-profile
```

スパムブロッキングリストサーバーを使用可能に設定

sbl コマンドを使って、外部のスパムブロッキングサービスを有効にします。このサービスは、ブラックリストを使用して既知のスパムソースを識別するものです。サービスは、IP アドレスが既知のスパマーに属するものかどうかというデバイスからの問合せに応答します。

例 : これらのコマンドは、以下のタスクを実行します。

1. プロファイルコンテキスト（**ns-profile**）を起動する。

2. デフォルトのスパム対策サービスを有効にする。

3. スパムコンテキストを終了し、プロファイルを既存のポリシー (id 2) に適用する。

```
device-> set anti-spam profile ns-profile
device(anti-spam:ns-profile)-> set sbl default-server-enable
device(anti-spam:ns-profile)-> exit
device-> set policy id 2 anti-spam ns-profile
```

スパム対策のテスト

セキュリティデバイスに既知のスパマーの IP アドレスをスキャンさせるには、**exec anti-spam testscan** <*IP addr*> コマンドを使用します。

例 : これらのコマンドは、IP アドレス 12.13.2.3 for spam をテストします。

```
device-> set console dbuf
device-> exec anti-spam testscan 12.13.2.3
device-> get dbuf stream
anti spam result: action Pass, reason: No match
```

Web フィルタリング

Web フィルタリングは、インターネットアクセスを管理して不適切な Web コンテンツへのアクセスを防ぎます。ScreenOS には、次の 2 つの Web フィルタリング機能があります。

- 統合型

  高性能のセキュリティデバイスは、SurfControl の CPA （Content Portal Authority ）サーバーを使用する統合型 Web フィルタリング機能をサポートします。

注 : 統合型 Web フィルタリング機能を使用するには、セキュリティデバイスにライセンスキーをインストールする必要があります。

  統合型 Web フィルタリングは、Web フィルタリングプロファイルをファイアウォールポリシーに組み込むことにより、要求したサイトへのアクセスを許可またはブロックできるようにします。Web フィルタリングプロファイルは、URL のカテゴリを特定し、アクセス要求があったときのセキュリティデバイスのアクション (許可またはブロック) を指定するものです。URL カテゴリは、SurfControl が事前定義し管理しているものを使用するか、ユーザーが定義します。統合型 Web フィルタリング機能の構成方法については、99 ページの「統合型 Web フィルタリング」を参照してください。

- 転送

  高性能のセキュリティデバイスは、SurfControl サーバーの SurfControl サービス、または Websense サーバーの Websense サービス を使用して Web フィルタリングソリューションをサポートします。

  転送型 Web フィルタリングの場合、セキュリティデバイスは TCP 接続の HTTP 要求があるとこれをいったん Websense または SurfControl のサーバーに送ります。サーバーでは、URL やドメイン名、IP アドレスなどにもとづいて、要求をブロックするか、本来のサイトへのアクセスを許可するかを判断します。転送型 Web フィルタリング機能の構成方法については、108 ページの「Web フィルタリングの転送」を参照してください。

注 : HTTPS トラフィックを管理するには、統合型 Web フィルタリングを使用します。転送型 Web フィルタリングは、HTTPS トラフィックをサポートしません。

CLI でWeb フィルタリングモードを開始

セキュリティデバイスで Web フィルタリングを構成するには、WebUI または CLI を使用します。CLI を使用する場合、次の手順で Web フィルタリングソリューションの一つを構成します。

1. プロトコルを選択する。

   たとえば、**set url protocol type { sc-cpa | scfp | websense }** コマンドでプロトコルを選択します。

2. Web フィルタリングモードを開始する。

   set url protocol { sc-cpa | scfp | websense } コマンドを実行すると、CLI が Web フィルタリングコンテキストに置かれます。Web フィルタリングコンテキストが開始されると、それ以降のすべてのコマンドの実行がこの Web フィルタリングモードに適用されます。

表 3 に、Web フィルタリングモードを開始または終了する 3 種類のコマンドを示します。

表 3: Web フィルタリングモードの開始と終了

	統合型 Web フィルタリング	Websense サーバーに 転送	Websense サーバーに 転送
1. プロトコルを選択	**set url protocol type sc-cpa**	**set url protocol type scfp**	**set url protocol type websense**
2. Web フィルタリングコンテキストを開始	**set url protocol sc-cpa** **(url:sc-cpa)-> :**	**set url protocol scfp** **(url:scfp)-> :**	**set url protocol websense** **(url:websense)-> :**
3. Web フィルタリングモードを終了	**(url:sc-cpa)-> :exit**	**(url:scfp)-> :exit**	**(url:websense)-> :exit**

統合型 Web フィルタリング

Web フィルタリングを使用可能にするには、まず Web フィルタリングプロファイルをファイアウォールポリシーに組み込みます。統合型 Web フィルタリングを使用する場合、Juniper Networks セキュリティデバイスは HTTP 要求を傍受して、その URL をカテゴリ分けすることによってアクセスを許可するかブロックするかを判定します。そしてさらに、URL カテゴリを Web フィルタリングプロファイルと照合します。Web フィルタリングプロファイルは、URL へのアクセス要求があったときにセキュリティデバイスのアクション (許可 / ブロック) を定義します。

URL カテゴリとは、内容に応じて URL を分類したリストのことです。セキュリティデバイスは、SurfControl の事前定義 URL カテゴリを使って、要求された URL のカテゴリを決定します。SurfControl Content Portal Authority (CPA) サーバーには、あらゆる種類の Web コンテンツを約 40 のカテゴリに分類した、大規模なデータベースがあります。102 ページの「URL カテゴリの定義（オプション）」に、URL カテゴリのリストの一部を示します。

SurfControl の完全な URL カテゴリ リストについては、SurfControl の Web サイト http://www.surfcontrol.com を参照してください。さらに、必要に応じて独自に URL を分類して、URL カテゴリを作成することもできます。ユーザー定義のカテゴリについては、102 ページの「URL カテゴリの定義（オプション）」を参照してください。

ここでは、Trust ゾーンにあるホストが Untrust ゾーンにあるサーバーに HTTP 接続を試みる場合に発生する、基本的なイベントを順を追って説明します。

1. セキュリティデバイスは、あるトラフィックに適用されるファイアウォールポリシーがあるかを調べます。
   - 該当するポリシーがない場合は、トラフィックを破棄します。
   - ポリシーが存在し、Web フィルタリングを適用する旨が記述されている場合は、HTTP 要求をすべて傍受します。
2. ユーザー定義のプロファイルがファイアウォールポリシーにバインドされていないかどうか調べます。ない場合はデフォルトのプロファイルである **ns-profile** を適用します。
3. 要求された URL が属するカテゴリが、既にキャッシュに記録されているかどうかを判断します。入っていなければ、デバイスはその URL を SurfControl CPA サーバーに送ってカテゴリ分けし、結果をキャッシュします。
4. URL が属するカテゴリがわかると、そのカテゴリがファイアウォールポリシーにバインドされた Web フィルタリングプロファイルに記述されているかどうかを調べます。
   - プロファイルに記述されていれば、その定義に従ってアクセスを許可またはブロックします。
   - 記述がない場合、デバイスは構成されているデフォルトの動作を実行します。

このセクションでは、以下に示す統合型 Web フィルタリング について説明します。

- 100 ページの「SurfControl サーバー」
- 108 ページの「Web フィルタリングの転送」
- 101 ページの「Web フィルタリングキャッシュ」
- 101 ページの「統合型 Web フィルタリングの構成」
- 107 ページの「例 : 統合型 Web フィルタリング」

SurfControl サーバー

SurfControl では、アメリカ、アジア / 太洋州、欧州 / 中東 / アフリカの 3 地域のそれぞれにサーバーを配備しています。デフォルトではまずアメリカ、それが不調の場合にはアジア / 大洋州のサーバーを使うようになっています。プライマリサーバーを変更すると、バックアップサーバーはこれに応じて自動的に決まります。（アジア / 大洋州のサーバーがアメリカのバックアップとなり、またアメリカのサーバーはそれ以外の 2 地域のサーバーのバックアップとして機能します。）

SurfControl CPA サーバーは定期的にカテゴリリストを更新しています。しかし CPA サーバー側から更新の旨を通知することはないので、サーバーデバイス側から定期的に、CPA サーバーに対して状況を問い合わせる必要があります。デフォルトでは、2 週間ごとに問い合わせるようになっています。この間隔はネットワーク環境に合わせて変更できます。また、随時手動で更新することもできます。それには、CLI で Web フィルタリングコンテキストを入力し、**exec cate-list-update** コマンドを実行します。カテゴリリストを手動で更新するには、次の手順を実行します。

```
device-> set url protocol sc-cpa
device(url:sc-cpa)-> exec cate-list-update
```

Web フィルタリングキャッシュ

デフォルトでは、セキュリティデバイスは URL カテゴリをキャッシュします。このアクションは、同じ URL に対するアクセス要求が繰り返しあった場合でも、SurfControl CPA サーバーに毎回問い合わせる必要がないようにするためです。キャッシュの容量と保存しておく時間は、ネットワーク環境の性能とメモリ必要条件によって構成できます。キャッシュ容量のデフォルト値はプラットフォームごとに異なります。保存時間のデフォルトは 24 時間です。

この例では、キャッシュ容量を 500 キロバイト（KB）、タイムアウト値を 18 時間に変更します。

WebUI

Security > Web Filtering > Protocol Selection > **Integrated (SurfControl)** を選択して、**Apply** をクリックします。

```
Enable Cache: ( 選択 )
Cache Size: 500 (K)
Cache Timeout: 18 (Hours)
```

CLI

```
device-> set url protocol sc-cpa
device(url:sc-cpa)-> set cache size 500
device(url:sc-cpa)-> set cache timeout 18
device(url:sc-cpa)-> exit
device-> save
```

統合型 Web フィルタリングの構成

セキュリティデバイスで Web フィルタリングを構成するには、次の手順を実行します。

1. 102 ページの「DNS（ドメイン名システム）サーバーの設定」
2. 102 ページの「Web フィルタリングを使用可能に設定する」
3. 102 ページの「URL カテゴリの定義（オプション）」
4. 104 ページの「Web フィルタリングプロファイルの定義 (オプション)」
5. 106 ページの「Web フィルタリング、およびポリシーを使用可能に設定」

具体的な手順は、以下のセクションで説明されています。

1. DNS（ドメイン名システム）サーバーの設定

Juniper Networks セキュリティデバイスは、位置の識別のためにドメイン名および IP アドレスの使用を許可する DNS (ドメイン名システム) サポートを実装しています。セキュリティデバイスが CPA サーバーのアドレス解決に使うため、DNS サーバーを少なくとも 1 台を構成する必要があります。DNS の詳細は、2-219 ページの「ドメイン名システムサポート」を参照してください。

2. Web フィルタリングを使用可能に設定する

セキュリティデバイスで統合型 Web フィルタリングを使用可能にするには、WebUI または CLI コマンドで操作します。CLI の場合、先に Web フィルタリングコンテキストを入力してから、統合型 Web フィルタリング用のコマンドを入力しなければなりません。

WebUI

Security > Web Filtering > Protocol Selection: **Integrated (SurfControl)** を選択して **Apply** をクリックします。次に **Enable Web Filtering via CPA Server** を選択し、もう一度 **Apply** をクリックします。

CLI

```
device-> set url protocol type sc-cpa
device-> set url protocol sc-cpa
device(url:sc-cpa)-> set enable
device(url:sc-cpa)-> exit
device-> save
```

*device***(url:sc-cpa)-** > プロンプト は、統合型 Web フィルタリングコンテキストが入力されたので統合型 Web フィルタリングのパラメータを構成できることを示します。

3. URL カテゴリの定義（オプション）

カテゴリとは、内容に応じて URL を分類したリストのことです。カテゴリには、事前定義とユーザー定義の 2 種類があります。SurfControl では約 40 の事前定義カテゴリを管理しています。103 ページの表 4 に、URL カテゴリのリストの一部を示します。SurfControl が作成した URL カテゴリのリストの全容および説明は、SurfControl のウェブサイト、http://www.surfcontrol.com をご覧ください。

SurfControl の事前定義 URL カテゴリのリストを表示するには、次の手順を実行します。

WebUI

Security > Web Filtering > Profiles > Predefined category

CLI

```
device-> set url protocol type sc-cpa
device-> set url protocol sc-cpa
device(url:sc-cpa)-> get category pre
```

表示された URL カテゴリリストは、表 4 のリストに類似しています。

表 4: SurfControl URL カテゴリの部分リスト

タイプ	コード	カテゴリ名
事前定義	76	広告
事前定義	50	芸術、娯楽
事前定義	3001	雑談
事前定義	75	コンピュータ、インターネット

事前定義カテゴリのリストにはカテゴリ名のほか、SurfControl が内部的に使用するコード番号が表示されます。カテゴリの個々の URL は列挙されません。しかし特定の Web サイトがどのカテゴリに属しているかは、SurfControl の Web サイト、www.surfcontrol.com にある Test A Site 機能を使用して判断できます。

これ以外にも独自にカテゴリを設定し、URL を分類することも可能です。各カテゴリには、最大 20 の URL が登録できます。また、URL ではなく IP アドレスで登録することも可能です。URL をユーザー定義のカテゴリに追加しようとすると、デバイスは DNS ルックアップを使って IP アドレスを調べ、キャッシュします。したがって、URL ではなく IP アドレスを使ってサイトにアクセスしようとしても、デバイスはキャッシュを参照してホスト名を調べます。

動的 IP アドレスを割り当てているサイトも多いので、IP アドレスが変わってしまうこともあります。そのため、デバイスのキャッシュに保存されていない IP アドレスを指定して、そのサイトにアクセスすることもできてしまいます。したがって、あるカテゴリにサイトを登録する際、IP アドレスも分かっている場合は両方を登録するとよいでしょう。

注 : URL がユーザー定義のカテゴリと事前定義のカテゴリの両方に登録されている場合は、デバイスはユーザー定義の方を優先します。

次の例では、**Competitors** という名前のカテゴリを作成し、次の URL を追加します。**www.games1.com**、および **www.games2.com**

WebUI

Security > Web Filtering > Profiles > Custom > New: 以下を入力して **Apply** をクリックします。

Category Name: Competitors
URL: www.games1.com

次のように入力してから **OK** をクリックします。

URL: www.games2.com

CLI

```
device-> set url protocol sc-cpa
device(url:sc-cpa)-> set category competitors url www.games1.com
device(url:sc-cpa)-> set category competitors url www.games2.com
device(url:sc-cpa)-> exit
device-> save
```

4. Web フィルタリングプロファイルの定義 (オプション)

Web フィルタリングプロファイルには、URL カテゴリのグループごとに、次のセキュリティデバイスのアクションの 1 つを設定します。

- Permit - セキュリティデバイスはいつも、このカテゴリにある Web サイトへのアクセスを許可します。
- Block - セキュリティデバイスは、このカテゴリにある Web サイトへのアクセスをブロックします。デバイスがこのカテゴリの Web サイトへのアクセスをブロックする場合、この URL カテゴリを示すメッセージをご使用のブラウザに表示します。
- Black List - セキュリティデバイスはいつも、ブラックリストに載っている Web サイトへのアクセスをブロックします。ユーザー定義カテゴリを作成しても、事前定義カテゴリを割り当てても構いません。
- White List - セキュリティデバイスはいつも、ホワイトリストに載っている Web サイトへのアクセスを許可します。ユーザー定義カテゴリを作成しても、事前定義カテゴリを割り当てても構いません。

Juniper Networks セキュリティデバイスには最初から、**ns-profile** というデフォルトのプロファイルがあります。このプロファイルには SurfControl が作成した事前定義カテゴリと、それに対応するアクションが設定されています。このデフォルトのプロファイルは編集できません。事前定義のプロファイルは、次のコマンドで参照できます。

WebUI

Security > Web Filtering > Profiles > Predefined

CLI

```
device-> set url protocol sc-cpa
device(url:sc-cpa)-> get profile ns-profile
```

事前定義プロファイルは、セキュリティデバイスで次のように表示されます。

```
Profile Name: ns-profile
black-list category: None
white-list category: None
Default Action: Permit

Category                Action
 Advertisements         block
 Arts & Entertainment   permit
 Chat                   permit
 Computing & Internet   permit
 .
 .
 .
 Violence               block
 Weapons                block
 Web-based Email        permit
 other                  permit
```

HTTP 要求に現れる URL がデフォルトプロファイルに列挙されたどのカテゴリにも属しない場合は、アクセスを許可するというのがデフォルトのアクションです。

カスタムプロファイルを作成できます。それには既存のプロファイルを複製し新しい名前で保存してから、内容を変更します。WebUI で次の手順を実行すると、**ns-profile** の複製ができます。

WebUI

Security > Web Filtering > Profiles > Custom: ns-profile: **Clone** を選択します。

注 : **ns-profile** を複製するには、WebUI で操作する必要があります。

また、独自の Web フィルタリングプロファイルを作成することもできます。独自のプロファイルを作成すると、次のようなことができるようになります。

- ユーザー定義カテゴリ、SurfControl の事前定義カテゴリの両方を登録。
- ブラックリスト、ホワイトリストに入れるカテゴリの指定。
- デフォルトの動作を変更。

この例では、**my-profile** という名前で独自のプロファイルを作成し、それにデフォルトの動作 **permit** を設定します。次に、先の例で成したカテゴリを追加し、対応するアクションを **block** とします。

WebUI

Security > Web Filtering > Profiles > Custom > New: 以下を入力して **Apply** をクリックします。

Profile Name: my-profile
Default Action: Permit
次のように選択してから **OK** をクリックします。
Subscribers Identified by:
Category Name: Competitors (**オン**)
Action: Block (**オン**)
Configure: Add (**オン**)

注 : CLI でデフォルトの動作を構成する場合、Other カテゴリの動作を指定します。

CLI

```
device-> set url protocol type sc-cpa
device-> set url protocol sc-cpa
device(url:sc-cpa)-> set profile my-profile other permit
device(url:sc-cpa)-> set profile my-profile competitors block
device(url:sc-cpa)-> exit
device-> save
```

5. Web フィルタリング、およびポリシーを使用可能に設定

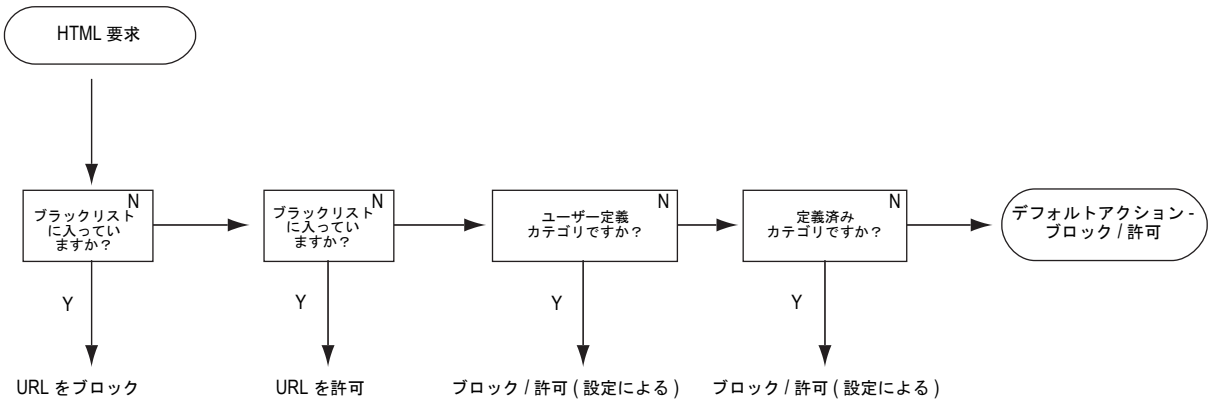
ファイアウォールのポリシーは、2 点間で、指定された一方向トラフィック タイプの許可または拒否を行います。（ファイアウォールのポリシーについては、2-161 ページの「ポリシー」を参照してください。）ポリシーの記述により、ウィルススキャン (AV) と統合型 Web フィルタリングの両方を有効にすることもできます。（AV スキャンについては、62 ページの「ウィルス対策スキャン」を参照してください。）

ポリシーの Web フィルタリング機能を使用可能にし、プロファイルをポリシーにバインドします。ポリシーの統合型 Web フィルタリングを有効にすると、セキュリティデバイスは HTTP 要求をすべて傍受するようになります。ポリシーに Web フィルタリングプロファイルがバインドされている場合、デバイスは入ってきた HTTP 要求の URL を次の順でプロファイル中のカテゴリと照合します。

1. ブラックリスト
2. ホワイトリスト
3. ユーザー定義カテゴリ
4. SurfControl 事前定義 URL カテゴリ

合致するカテゴリがなかった場合、アクセスを許可するかブロックするかは、プロファイルのデフォルトの構成に従います。

図 40: Web フィルタリングプロファイルとポリシーの流れ図



URL が許可されているカテゴリに属し、かつそのポリシーの AV スキャン機能が使用可能になっている場合、デバイスはコンテンツをスキャンしてウィルスを検査します。URL がブロックされているカテゴリに属する場合、デバイスは TCP 接続を閉じて、ユーザーへの警告メッセージを送信しますが、AV スキャンは実行しません。

例 : 統合型 Web フィルタリング

この例では、次の手順を実行して、セキュリティデバイスで統合型 Web フィルタリング機能を使用可能に設定し、Competitors のサイトへのアクセスをブロックするよう設定します。

1. **Competitors** というカテゴリを作成します。
2. 次の URL をカテゴリに追加します。**www.comp1.com** と **www.comp2.com**
3. **my-profile** というプロファイルを作成し、**Competitors** カテゴリを追加します。
4. ファイアウォールポリシーに **my-profile** を適用します。

WebUI

1. Web フィルタリング

Security > Web Filtering > Protocol > **Integrated (SurfControl)** を選択して、**Apply** をクリックします。次に **Enable Web Filtering via CPA Server** を選択し、もう一度 **Apply** をクリックします。

2. URL カテゴリ

Security > Web Filtering > Profile > Custom List > New: 以下を入力して **Apply** をクリックします。

Category Name: Competitors
URL: www.comp1.com

次のように入力してから **OK** をクリックします。

URL: www.comp2.com

3. Web フィルタリングプロファイル

Security > Web Filtering > Profile > Custom Profile > New: 以下を入力して **Apply** をクリックします。

Profile Name: my-profile
Default Action: Permit

Category Name: Competitors (**オン**)
Action: Block (**オン**)
Configure: Add (**オン**)

4. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), Any
Service: HTTP
Web Filtering: (**オン**), my-profile
Action: Permit

CLI

1. **Web フィルタリング**
   device-> set url protocol sc-cpa
   device(url:sc-cpa)-> set enable

2. **URL カテゴリ**
   device(url:sc-cpa)-> set category competitors url www.comp1.com
   device(url:sc-cpa)-> set category competitors url www.comp2.com

3. **Web フィルタリングプロファイル**
   device(url:sc-cpa)-> set profile my-profile other permit
   device(url:sc-cpa)-> set profile my-profile competitors block
   device(url:sc-cpa)-> exit

4. **ファイアウォールポリシー**
   device-> set policy id 23 from trust to untrust any any http permit url-filter
   device-> set policy id 23
   device(policy:23)-> set url protocol sc-cpa profile my-profile
   device(policy:23)-> exit
   device-> save

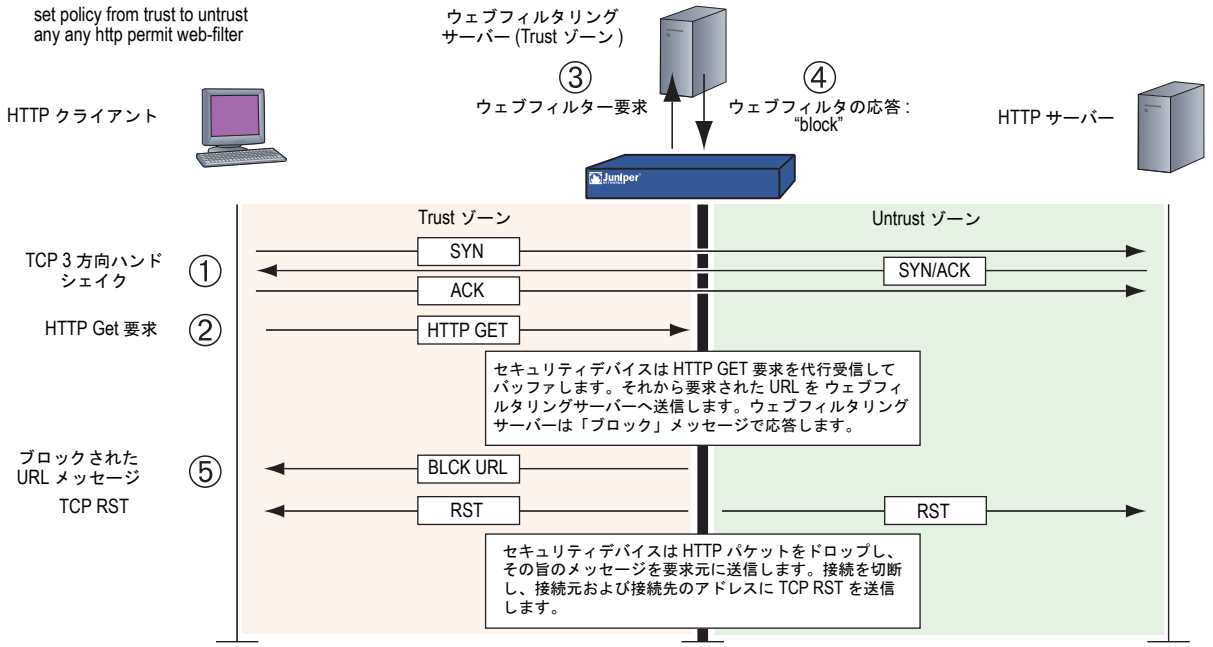
Web フィルタリングの転送

Juniper Networks セキュリティデバイスは、Websense エンタープライズエンジンまたは SurfControl Web フィルタを使用して転送型 Web フィルタリングをサポートします。Websense エンタープライズエンジンや SurfControl Web フィルタによって、異なるサイトへのアクセスを URL、ドメイン名、IP アドレスに基づいてブロックまたは許可することができます。セキュリティデバイスは、WebSense や SurfControl の Web フィルタリングサーバーに直接接続できます。

注： Websense の詳細については、www.websense.com を参照してください。また、SurfControl の詳細については、www.surfcontrol.com を参照してください。

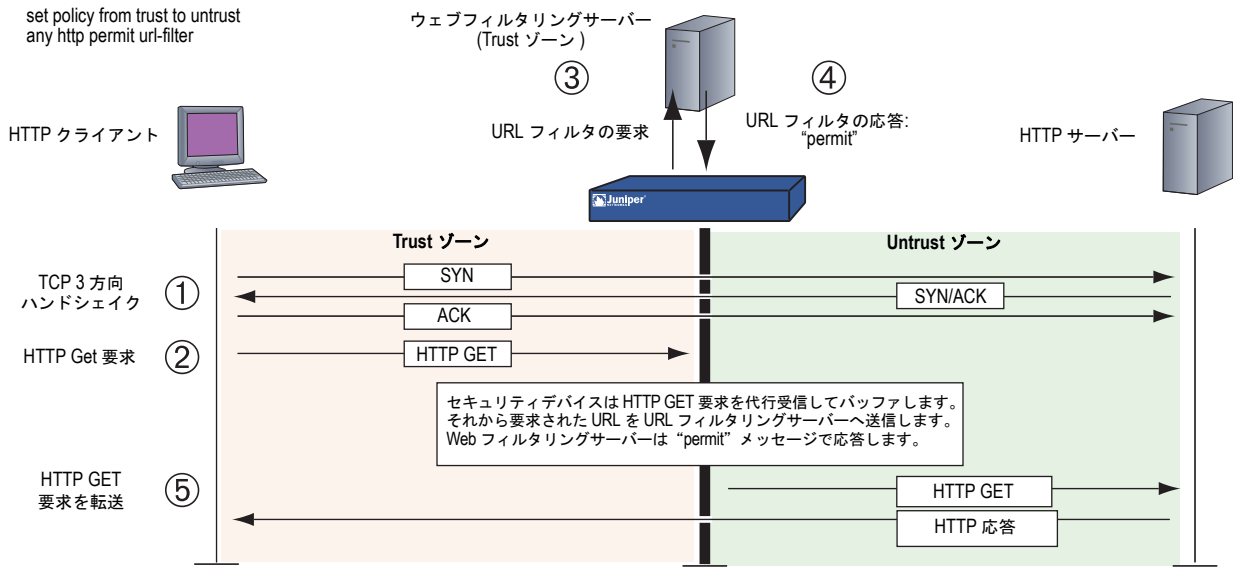
図 41 は、Trust ゾーンにあるホストが Untrust ゾーンにあるサーバーに HTTP 接続を試みる場合に発生する、イベントの基本的な順序を示しています。ただし、Web フィルタリングが要求された URL は禁止されていると判断します。

図 41: Trust ゾーンから Untrust ゾーンへの接続をブロックされる URL



サーバーが URL へのアクセスを許可する場合、図 42 に示すとおり、HTTP 接続を確立するまでイベントが順次発生します。

図 42: Trust ゾーンから Untrust ゾーンへの接続を許可される URL



転送型 Web フィルタリングの詳細については、以下のセクションを参照してください。

- 110 ページの「仮想システムサポート」
- 111 ページの「転送型 Web フィルタリングの構成」
- 114 ページの「例 : Web フィルタリングの転送」

仮想システムサポート

仮想システム（vsys）を使用しているセキュリティデバイスは、Web フィルタリングサーバーを 8 つまでサポートします。1 つのサーバーはルートシステム用に予約されており、無制限の数の仮想システムと共有できます。7 つの Web フィルタリングサーバーは仮想システムがプライベートで利用するために予約されています。ルートレベル管理者は、ルートレベルおよび仮想システムレベルで Web フィルタリングモジュールを構成できます。Vsys レベル管理者は自分の Vsys 専用の Web フィルタリングサーバーがある場合、Vsys 用の URL モジュールを構成できます。Vsys レベル管理者がルートの Web フィルタリングサーバー設定を使用している場合、その管理者はルートレベルの Web フィルタリング設定を表示することはできますが、編集はできません。

あるいは、Websense の Web フィルタリングサーバーを使用する仮想システムのあるでデバイスでは、ルートサーバーのみならず、8 つすべての Websense サーバーを共有できます。Websense サーバーはそれぞれ無制限の数の仮想システムをサポートすることができるため、8 つのサーバー間のトラフィック負荷のバランスが保たれます。

Websense の Web フィルタリングサーバーに複数の仮想システムを接続させるように構成する場合、ルートレベルまたは vsys 管理者が次の操作を実行する必要があります。

1. 各 Vsys のアカウント名を作成します。以下の CLI コマンドを使用します。

   ```
   device-> set url protocol type websense
   device-> set url protocol websense
   device(url:websense)-> set account name
   ```

   Vsys のホストが送信する URL 要求にはアカウント名が記載されます。この名前によって、Websense サーバーは、どの仮想システムが URL 要求を送信したかを識別できるようになります。

2. Websense の Web フィルタリングサーバーを共有する各 vsys に、同一の Web フィルタリングサーバー設定とシステムレベルのパラメータを構成します。次のセクションでは、Web フィルタリング設定およびパラメータの構成について説明します。

転送型 Web フィルタリングの構成

セキュリティデバイスで転送型の Web フィルタリングを構成するには、次の手順を実行します。

1. DNS（ドメイン名システム）サーバーを設定します。

Juniper Networks セキュリティデバイスは、位置の識別のためにドメイン名および IP アドレスの使用を許可する DNS (ドメイン名システム) サポートを実装しています。セキュリティデバイスが CPA サーバーのアドレス解決に使うため、DNS サーバーを少なくとも 1 台を構成する必要があります。DNS の詳細については、2-219 ページの「ドメイン名システムサポート」を参照してください。

2. Web フィルタリングサーバーとの通信を設定します。

以下のサーバーの 1 つと通信するセキュリティデバイスを構成します。

- Websense サーバー
- SCFP（SurfControl Content Filtering Protocol）を使用する SurfControl サーバー

Web フィルタリングサーバーとの通信を 8 つまで設定できます。

WebUI

Security > Web Filtering > Protocol > **Redirect (Websense)** または **Redirect (SurfControl)** を選択して、**Apply** をクリックします。

CLI

SurfControl（scfp）または Websense（websense）転送型フィルタリングの Web フィルタリングコンテキストを入力します。詳細については、99 ページの「CLI で Web フィルタリングモードを開始」を参照してください。

```
device-> set url protocol type { websense | scfp }
device-> set url protocol { websense | scfp }
device(url:scfp)-> set server { ip_addr | dom_name } port_num timeout_num
```

Web フィルタリングサーバーの通信用に、システムレベルで次の Web フィルタリング設定を構成します。

- **Source Interface:** デバイスが Web フィルタリングサーバーに対して、どこから Web フィルタリング要求を送信するかの設定です。
- **Server Name:** Websense サーバーまたは SurfControl サーバーを実行しているコンピュータの IP アドレスまたは FQDN (完全修飾ドメイン名)。
- **Server Port:** サーバーのデフォルトポートを変更した場合は、セキュリティデバイス側のポート番号も変える必要があります。(デフォルトポート番号は、WebSense ならば 15868、SurfControl ならば 62252 です。) 詳細については、Websense または SurfControl の資料を参照してください。
- **Communication Timeout:** デバイスが Web フィルタリングサーバーからの応答を待つ時間 (秒)。サーバーが時間間隔内に応答しなかった場合、デバイスは、ユーザーの選択によって、要求をブロックするか、または許可します。時間間隔には、10 ～ 240 までの値を入力します。

複数の仮想システムを持つデバイスが Websense サーバーに接続する場合、仮想システムの間でサーバーを共有できます。複数の仮想システムが Websense サーバーを共有するように構成するには、次の CLI コマンド を使って各 Vsys にアカウント名を作成します。

```
device-> set url protocol type websense
device-> set url protocol websense
device(url:websense)-> set account name
```

Vsys 名を構成したら、Web フィルタリングを適用したときのセキュリティ デバイスの動作について Web フィルタリングサーバーとパラメータの設定を定義します。これらの設定をルートシステムで構成した場合、Web フィルタリング構成をルートシステムと共有する Vsys にもこの設定が適用されます。Vsys の場合は、ルート管理者および Vsys 管理者が設定を個別に構成する必要があります。同一の Websense の Web フィルタリングサーバーを共有する仮想システムは、Web フィルタリング設定も同一にする必要があります。

3. Web フィルタリングをルートレベルと Vsys レベルで使用可能に設定。

Web フィルタリングはシステムレベルで使用可能にする必要があります。仮想システムをホストしているデバイスでは、Web フィルタリングを適用するシステムごとに Web フィルタリングを有効にする必要があります。たとえば、ルートシステムと Vsys に Web フィルタリングを適用する場合は、ルートシステムと Vsys の両方で Web フィルタリングを有効にする必要があります。

Web フィルタリングを使用可能にするには、次のいずれかを実行します。

WebUI

Security > Web Filtering > Protocol > **Redirect (Websense)** または **Redirect (SurfControl)** を選択して、**Apply** をクリックします。
Web Filtering チェックボックスを使用可能に設定します。

CLI

```
device-> set url protocol type { websense | scfp }
device-> set url protocol { websense | scfp }
device(url:scfp)-> set config enable
```

Web フィルタリングがシステムレベルで有効になっているときは、HTTP 要求は Websense または SurfControl サーバーに転送されます。このアクションにより、デバイスがすべての HTTP トラフィックを、Web フィルタリングを必要とする (そのシステムで定義された) ポリシーと照合します。システムレベルで Web フィルタリングを無効にすると、デバイスはポリシー内の Web フィルタリング構成要素を無視し、ポリシーを “Permit” ポリシーとして扱います。

4. システムレベルの動作パラメータの定義

Web フィルタリングを適用したときにシステム（ルートまたは vsys）が使用するパラメータを定義します。ルートシステムと、Web フィルタリング構成をルートシステムと共有する Vsys に 1 セットのパラメータを適用できます。専用の Web フィルタリングサーバーのある仮想システムには他のセットを適用できます。

以下にオプションを示します。

- **サーバーへの接続性が消失した場合は :** セキュリティデバイスが Web フィルタリングサーバーとの接続を失った場合に、すべての HTTP 要求を **Block** (ブロック) するか、または **Permit** (許可) するか指定できます。

- **Blocked URL Message Type: NetPartners Websense/SurfControl** を選択した場合、セキュリティデバイスは Websense または SurfControl サーバーからの “block” 応答で受信したメッセージを転送します。**Juniper Networks** を選択した場合、デバイスは **Juniper Networks Blocked URL Message** フィールドにあらかじめ入力されているメッセージを送信します。

注 : **Juniper Networks** を選択した場合は、Websense が提供している転送などの一部の機能が使用できなくなります。

- **Juniper Networks の ブロックされた URL メッセージ**これは、サイトをブロックした後、セキュリティデバイスがユーザーに返送するメッセージです。Websense または SurfControl サーバーから送信されたメッセージを使用するか、またはデバイスから送信するメッセージ（500 文字まで）を作成することができます。

これらの設定を構成するには、以下のいずれかを実行します。

WebUI

Security > Web Filtering > Protocol > **Redirect (Websense)** または **Redirect (SurfControl)** を選択して、**Apply** をクリックします。

CLI

```
device-> set url protocol type { websense | scfp }
device-> set url protocol { websense | scfp }
device(url:scfp)-> set fail-mode permi
device(url:scfp)-> set deny-message use-server
```

5. 個別のポリシーで Web フィルタリングを使用可能に設定。

デバイスがポリシーに基づき Web フィルタリングサーバーに接続するように構成します。

Web フィルタリングをポリシーで使用可能にするには、以下のいずれかを実行します。

WebUI

Policy > device-> set url protocol type { websense | scfp } > **Edit** (Web フィルタリングを提供したポリシーを編集) をクリックし、**Web Filter** チェックボックスをオンにします。
ドロップダウンボックスから Web フィルタリングプロファイルを選択します。

CLI

set policy from *zone* to *zone src_addr dst_addr service* permit url-filter

注： デバイスが Websense または SurfControl サーバーの状態を報告します。状態レポートを更新するには、WebUI の **Server Status** アイコンをクリックします。

Security > Web Filtering > Protocol >**Redirect (Websense)** または **Redirect (SurfControl)** を選択して、**Apply** をクリックします。

例：Web フィルタリングの転送

この例では、次の操作を実行するようにセキュリティデバイスを構成します。

1. IP アドレス 10.1.2.5、ポートナンバー 62252 (デフォルト) の SurfControl サーバーと連携するようにインターフェースを設定し、Trust セキュリティゾーンに Web フィルタリングサーバーを設置します。

2. Trust セキュリティゾーンのホストから Untrust セキュリティゾーンのホストへの HTTP アウトバウンドトラフィックすべての Web フィルタリングを使用可能にします。デバイスが Web フィルタリングサーバーとの接続を失った場合も、デバイスが HTTP アウトバウンドトラフィックを許可するようにします。禁止された URL へのアクセスを HTTP クライアントが要求したときは、デバイスが「We're sorry, but the requested URL is prohibited. Contact ntwksec@mycompany.com.」のメッセージを送信します。

3. 両方のセキュリティゾーンを trust-vr ルーティングドメインに配置し、Untrust ゾーンのインターフェースを ethernet3、IP アドレス 1.1.1.1/24 とし、Trust ゾーンのインターフェースを ethernet1、IP アドレス 10.1.1.1/24 と設定します。Web フィルタリングサーバーは、いずれのデバイスインターフェースの直系のサブネットでもないため、このサーバーに ethernet1 および 10.1.1.250 にある内部ルート経由でルートが追加されます。

4. Web フィルタリングを使用可能にするポリシーを構成し、Trust から Untrust ですべてのソースアドレスとすべての宛先アドレスの HTTP サービスを許可するようにします。

WebUI

1. インターフェース

Network > Interfaces > List > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24

次のように入力してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > List > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

2. Web フィルタリングサーバー

Security > Web Filtering > Protocol: **Redirect (SurfControl)** を選択して **Apply** をクリックします。次のように入力して、もう一度 **Apply** をクリックします。

Enable Web Filtering: (選択)
Server Name: 10.1.2.5
Server Port: 62252
Communication Timeout: 10 (秒)
If connectivity to the server is lost … all HTTP requests: Permit
Blocked URL Message Type: Juniper Networks
Juniper Blocked URL Message: We're sorry, but the requested URL is prohibited.Contact ntwksec@mycompany.com.

3. ルート

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.2.0/24
Gateway: (選択)
Interface: ethernet1
Gateway IP Address: 10.1.1.250

4. ポリシー

Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), Any
Service: HTTP
Action: Permit
Web Filtering: (選択)

CLI

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. Web フィルタリングサーバー

```
device-> set url protocol type scfp
device-> set url protocol scfp
device(url:scfp)-> set server 10.1.2.5 62252 10
device(url:scfp)-> set fail-mode permi
device(url:scfp)-> set deny-message "We're sorry, but the requested URL is
    prohibited.Contact ntwksec@mycompany.com."
device(url:scfp)-> set config enable
```

3. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
   set vrouter trust-vr route 10.1.2.0/24 interface ethernet1 gateway 10.1.1.250

4. **ポリシー**
   set policy from trust to untrust any any http permit url-filter
   save

第 5 章
徹底監視 (Deep Inspection)

徹底監視 (DI) 機能をポリシー内で有効にして許可されたトラフィックを調べ、ScreenOS の DI モジュールが攻撃シグネチャやプロトコルアノーマリ (異常) を見つけた場合に対応策をとることができます。この章の次のセクションでは、ポリシーにおける DI の要素について扱い、その構成方法について説明します。

- 118 ページの「概要」
- 122 ページの「攻撃オブジェクトデータベースサーバー」
- 130 ページの「攻撃オブジェクトとグループ」
  - 131 ページの「サポートされているプロトコル」
  - 135 ページの「ステートフル署名」
  - 136 ページの「TCP ストリームシグネチャ」
  - 136 ページの「プロトコルアノーマリ (プロトコル異常)」
  - 137 ページの「攻撃オブジェクトグループ」
  - 140 ページの「攻撃オブジェクトの無効化」
- 141 ページの「攻撃アクション」
  - 149 ページの「ブルートフォース攻撃アクション」
- 152 ページの「攻撃のログ出力」
- 154 ページの「顧客サービスとアプリケーションのマッピング」
- 158 ページの「カスタマイズした攻撃オブジェクトとグループ」
  - 158 ページの「ユーザー定義のステートフルシグネチャ攻撃オブジェクト」
  - 162 ページの「TCP ストリームシグネチャ攻撃オブジェクト」
  - 164 ページの「プロトコルアノーマリパラメータの構成」
- 165 ページの「否定」

DI は、HTTP コンポーネントのセキュリティゾーンレベルでも有効にできます。これらの SCREEN オプションについては、本章の最終セクションで説明します。

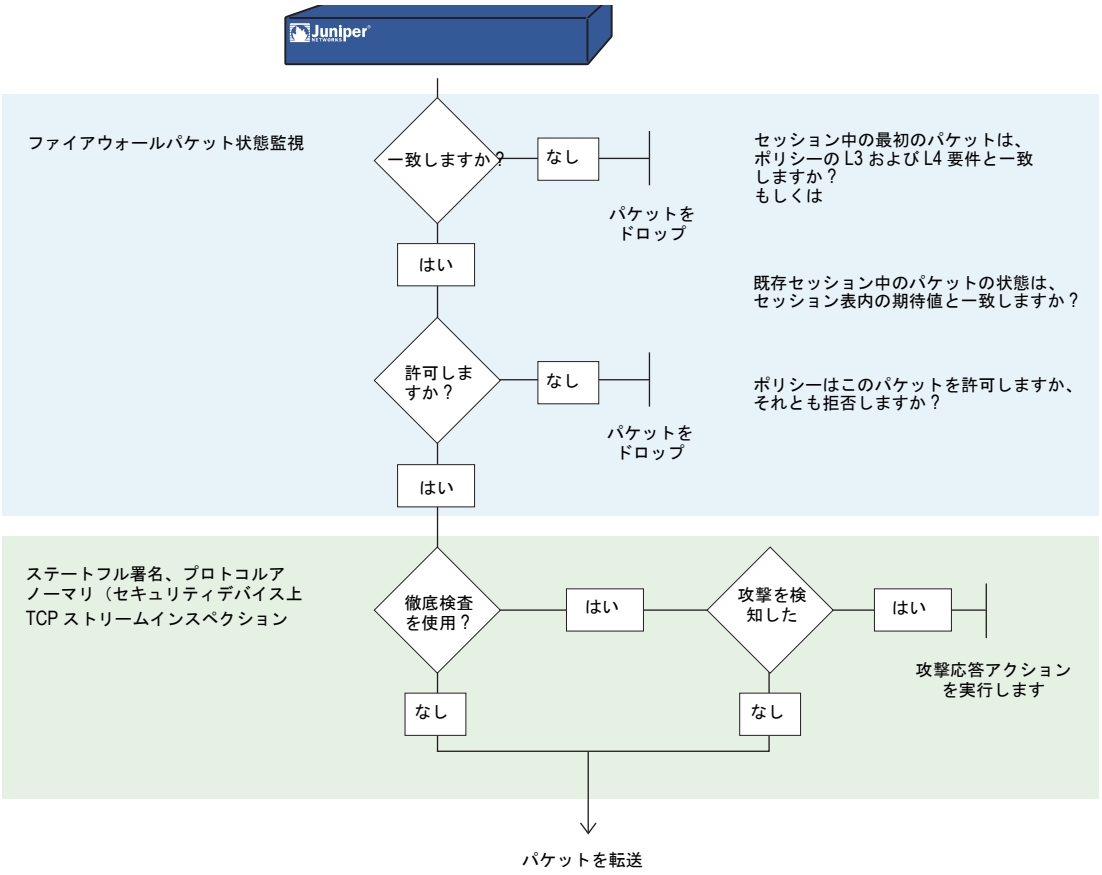
- 170 ページの「HTTP コンポーネントの細分ブロッキング」
  - 170 ページの「ActiveX コントロール」
  - 171 ページの「Java アプレット」
  - 171 ページの「EXE ファイル」
  - 171 ページの「ZIP ファイル」

概要

DI (徹底監視) は、Juniper Networks ファイアウォールが許可したトラフィックをフィルタリングするための機構です。DI は、あらゆる攻撃や異常動作を検知して防御するために、レイヤ 3 およびレイヤ 4 のパケットヘッダーとレイヤ 7 のアプリケーションコンテンツおよびプロトコル特性を調べます。図 43 では、パケットがどのようにレイヤ 3 監視を受けるかを示します。

注 : Juniper Networks セキュリティデバイスは、レイヤ 3 および 4 (IP および TCP) の異常トラフィックパターンを、ポリシーレベルではなくゾーンレベルで設定した SCREEN オプションを介して検知します。IP および TCP トラフィック異常検出の例を 7 ページの「IP アドレススイープ」、9 ページの「ポートスキャン」で述べ、さまざまなフラッド攻撃について 36 ページの「ネットワーク DoS 攻撃」で説明しています。

図 43: ファイアウォールパケット状態監視



セキュリティデバイスはセッションの最初のパケットを受信すると、IP パケットヘッダー中のソースおよび宛先 IP アドレス (レイヤ 3 検査) と、TCP セグメントまたは UDP データグラムヘッダー中のソースおよび宛先ポート番号とプロトコル (レイヤ 4 検査) を調べます。レイヤ 3 および 4 のコンポーネントがポリシーで指定された基準と一致すると、デバイスは指定されたアクション (許可、拒否またはトンネル) をこのパケットで実行します。デバイスは確立されたセッションのパケットを受信すると、そのパケットをセッション表の中の状態情報と比較し、このパケットがこのセッションのものかどうかを判断します。

注 : 指定されたアクションがトンネルの場合、許可の概念が含意されています。アクションがトンネルのポリシーで DI を有効にすると、セキュリティデバイスは指定された DI 動作を、アウトバウンドパケットを暗号化する前とインバウンドパケットを復号した後で実行します。

このパケットに適用するポリシーで DI を有効にしてあり、このポリシーのアクションが「許可」または「トンネル」の場合、セキュリティデバイスはさらに攻撃オブジェクトについてこのパケットとその関連するデータストリームを調べます。パケットをスキャンして、攻撃オブジェクトのいずれかのグループで定義されたパターンと合致するものがないかどうか調べます。攻撃オブジェクトは、攻撃シグネチャの場合もあればプロトコルアノーマリの場合もあり、これはユー

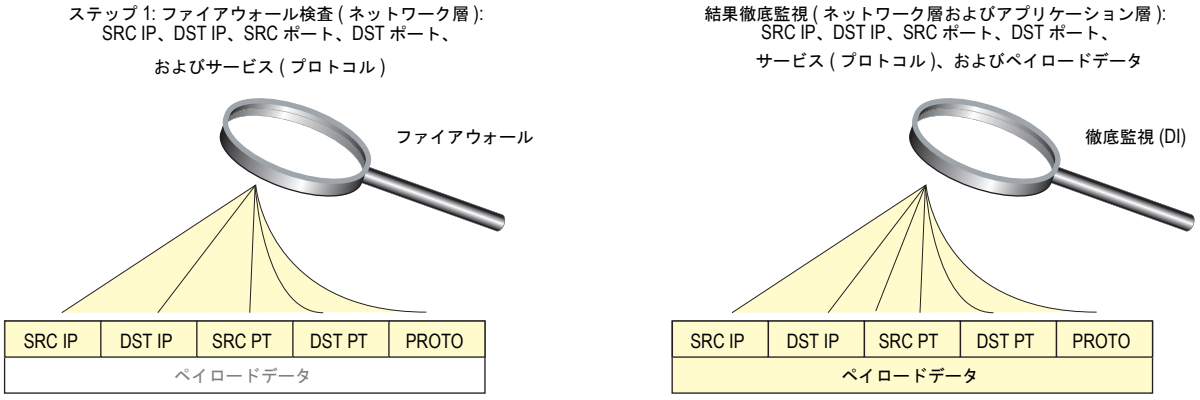
ザーが自分で定義するかデータベースサーバーからセキュリティデバイスへダウンロードするか、どちらを選ぶことができます (詳細については、130 ページの「攻撃オブジェクトとグループ」および 158 ページの「カスタマイズした攻撃オブジェクトとグループ」を参照してください。)

注 : DI (徹底監視) 機能は、アドバンスモードのライセンスキーを取得してロードした後に使用できるようになります (ScreenOS の 5.0.0 以前のバージョンからアップグレードする場合、モードは自動的に「アドバンス」モードになるので、アドバンスモードのライセンスキーは不要です)。データベースサーバーからシグネチャパッケージをダウンロードするには、先にこのサービスに加入する必要があります。詳細については、**2**-255 ページの「ライセンスサービスの登録およびアクティブ化」を参照してください。

ポリシー内で指定された攻撃オブジェクトに基づいて、セキュリティデバイスは次の検査を行います (図 44 を参照)。

- パケット状態の攻撃シグネチャのヘッダー値とペイロードデータを調べます。
- 送信されたプロトコルの形式をこのプロトコルの RFC および RFC 拡張で指定されている標準と比較して、何者かが不正な目的のためにこのプロトコルを変造していないか判断します。

図 44: ファイアウォール検査と徹底監視の比較



セキュリティデバイスは攻撃オブジェクトを検知すると、パターンが合致した攻撃オブジェクトが属する攻撃オブジェクトグループに指定されているアクション (閉鎖、クライアント閉鎖、サーバー閉鎖、ドロップ、パケットドロップ、無視、何もしない) を実行します。攻撃を検知できなければ、そのままパケットを転送します。(攻撃アクションの詳細については、141 ページの「攻撃アクション」を参照してください。)

set policy コマンドは概念的に 2 つの部分、コアセクションと DI コンポーネントに分けることができます。

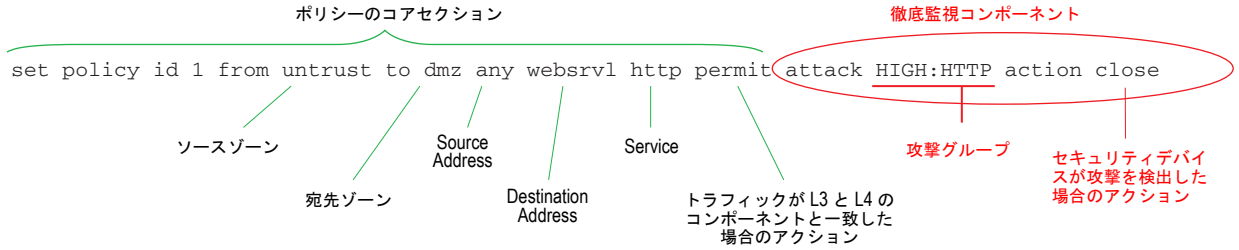
- コアセクションは、ソースゾーンと宛先ゾーン、ソースアドレスと宛先アドレス、1 つ以上のサービス、そしてアクションで構成されます。

- DI コンポーネントは、パターンマッチングを指示するポリシーのコアセクションが許可したトラフィックに、攻撃オブジェクトグループに含まれた攻撃オブジェクトがないか調べるようセキュリティデバイスに指示します。セキュリティデバイスは、攻撃オブジェクトを検知すると、対応するグループで定義されたアクションを実行します。

注 : **set policy** コマンドのコアコンポーネントに任意で追加できる他の拡張機能には、VPN および L2TP トンネル参照、スケジュール参照、アドレス変換仕様、ユーザー認証仕様、アンチウィルスチェック、ロギング、カウンティング、およびトラフィック管理設定があります。これらの拡張機能は任意ですが、ポリシーのコアを構成する要素であるソースと宛先ゾーン、ソースと宛先アドレス、サービス、およびアクションは必須です。(これに対する例外として、ソースおよび宛先ゾーンは指定されないグローバルポリシー「set policy global *src_addr dst_addr service action*」があります。グローバルポリシーの詳細については、**2**-164 ページの「グローバルポリシー」を参照してください。)

次の **set policy** コマンドには DI コンポーネントが含まれています。

図 45: set policy コマンドの DI コンポーネント



上のコマンドはセキュリティデバイスに、Untrust ゾーンのあらゆるアドレスから DMZ ゾーンの宛先アドレス「websrv1」への HTTP トラフィックを許可するよう指示します。またデバイスに、このポリシーが許可するすべての HTTP トラフィックを検査するようにも指示します。トラフィック中のパターンが、攻撃オブジェクトグループ「HIGH:HTTP:ANOM」で定義された攻撃オブジェクトに合致すると、デバイスはパケットをドロップし、TCP RST 通知をソースおよび宛先アドレスのホストへ送信して接続を閉じます。

既存のポリシーの ID 番号を使用して、そのポリシーのコンテキストを入力することができます。例えば、次のように表示されます。

```
device-> set policy id 1
device(policy:1)->
```

注 : コマンドプロンプトが変わって、その後のコマンドが特定のポリシーコンテキスト内であることを知らせます。

ポリシーコンテキストの入力は、1 つのポリシーに関連した複数のコマンドを入力する場合に便利です。たとえば次のコマンドのセットは、Untrust 内のあらゆるアドレスから DMZ ゾーン内の websrv1 および websrv2 への HTTP および HTTPS トラフィックを許可し、高度およびクリティカルな HTTP ステートフルシグネチャ攻撃とプロトコルアノーマリ攻撃を探すポリシーを作成します。

```
device-> set policy id 1 from untrust to dmz any websrv1 http permit attack
    CRITICAL:HTTP:ANOM action close
device-> set policy id 1
device(policy:1)-> set dst-address websrv2
device(policy:1)-> set service https
device(policy:1)-> set attack CRITICAL:HTTP:SIGS action close-server
device(policy:1)-> set attack HIGH:HTTP:ANOM action drop
device(policy:1)-> set attack HIGH:HTTP:SIGS action close-server
device(policy:1)-> exit
device-> save
```

上記構成により HTTP トラフィックと HTTPS トラフィックは許可されますが、HTTP トラフィック内の攻撃のみ検査が行われます。ポリシーコンテキストに攻撃オブジェクトグループを追加できるようにするには、最初に最上位コマンド内で DI 攻撃とアクションを指定する必要があります。上の例では、最初に DI のポリシーが CRITICAL:HTTP:ANOM グループにより構成されているため、CRITICAL:HTTP:SIGS、HIGH:HTTP:ANOM、および HIGH:HTTP:SIGS の攻撃オブジェクトグループを追加できます。

注： 攻撃オブジェクトグループごとに異なる攻撃アクションをポリシーに指定することも可能です。複数の攻撃を同時に検知した場合、セキュリティデバイスはその中で最も安全な (重大度の高い) アクションを実行します。したがって、例えば上の例では「close」が実行されます。攻撃アクションとその重大度レベルについて詳しくは、141 ページの「攻撃アクション」を参照してください。

攻撃オブジェクトデータベースサーバー

攻撃オブジェクトデータベースサーバーには定義済みの全攻撃オブジェクトが入っており、プロトコルおよび重大度レベル別の攻撃オブジェクトグループに分けられています。Juniper Networks は、攻撃オブジェクトデータベースを https://services.netscreen.com/restricted/sigupdates のサーバーに格納しています。

定義済みのシグネチャパッケージ

攻撃オブジェクトデータベースは、Base (ベース)、Server-protection (サーバー保護)、Client-protection (クライアント保護)、Worm-mitigation (ワーム軽減) の 4 つのシグネチャパッケージで構成されています。このアプローチは、シグネチャパッケージのデバイスメモリが制限され、プロトコルのサポートが強化されるので、理想的です。表 5 は、定義済みの各シグネチャパッケージと脅威の範囲について説明しています。

表 5: 定義済みのシグネチャパッケージ

シグネチャパッケージ	解説	脅威の範囲
Base[1]	中小企業のほか、リモートオフィスと支店オフィスに対して最適化されたクライアント / サーバーとワーム保護に対して選択したシグネチャセット	HTTP、DNS、FTP、SMTP、POP3、IMAP、NetBIOS/SMB、MS-RPC、P2P、IM (AIM、YMSG、MSN、IRC) など、インターネットに面しているプロトコルおよびサービスに対するワームのサンプル、クライアントからサーバーへのシグネチャ、サーバーからクライアントへのシグネチャを含みます。
Server-protection	IIS、Exchange などのサーバーインフラストラクチャに対して周辺防衛と整合性が必要となる、中小企業、大企業のリモートオフィス / 支店オフィスが対象	サーバーファームを保護することに重点を置きます。HTTP、DNS、FTP、SMTP、IMAP、MS-SQL、LDAP など、サーバー指向のプロトコルの包括的なセットを含みます。サーバーを対象とするワームシグネチャも含みます。
Client-protection	デスクトップやラップトップなどのホストに対して周辺防衛と整合性が必要となる中小企業、大企業のリモートオフィス / 支店オフィス対象	ネットサーフィン中のユーザーを破壊工作ソフト、トロイの木馬などから守ることに重点に置きます。HTTP、DNS、FTP、IMAP、POP3、P2P、IM (AIM、YMSG、MSN、IRC) など、クライアント指向のプロトコルの包括的なセットを含みます。クライアントを対象とするワームシグネチャも含みます。
Worm-mitigation	中小企業のほか、大企業のリモートオフィス / 支店オフィスが対象で、ワーム攻撃に対して最も包括的な防衛を提供	ストリームシグネチャを含み、包括的なワーム保護を提供することに重点を置きます。全プロトコルのサーバーからクライアントおよびクライアントからサーバーへのワーム攻撃を検出します。

1.新しい追加機能でメモリの割り当てが必要になるため、NS-5XT/GT デバイスはクリティカルな重大度の DI シグネチャだけを提供します。

表 6 に、定義済みのシグネチャパッケージと対応する URL を示します。

表 6: 定義済みのシグネチャパッケージの URL

シグネチャパッケージ	URL
Base（デフォルト）	https://services.netscreen.com/restricted/sigupdates セキュリティデバイスは、デフォルトでこの URL を使用します。
サーバー	https://services.netscreen.com/restricted/sigupdates/server
クライアント	https://services.netscreen.com/restricted/sigupdates/client
Worm-mitigation	https://services.netscreen.com/restricted/sigupdates/worm

シグネチャパッケージの更新

Juniper Networks は、https://services.netscreen.com/restricted/sigupdates にある攻撃オブジェクトデータベースサーバーに、定義済みのシグネチャパッケージを 4 つ格納しています。このデータベースサーバーへのアクセス権を得るには、次のセクションで説明するように、最初にデバイスで使用するための DI シグネチャサービスに加入する必要があります。

データベースを更新するには次の 4 つの方法があります。

- 124 ページの「即時更新」
- 125 ページの「自動更新」

- 126 ページの「自動通知と即時更新」
- 128 ページの「手動更新」

注： また、Netscreen-Security Manager を使ってシグネチャパッケージをダウンロードすることもできます。詳しくは *NetScreen-Security Manager Administration Guide* を参照してください。

攻撃オブジェクトの更新を始める前に

攻撃オブジェクトのダウンロードおよび更新を始める前に、次を行う必要があります。

1. ご使用のセキュリティデバイスを登録し、許可コードを取得します。
2. ライセンスキーを購入し、徹底監視のサブスクリションを有効にします。
3. デバイス上のシステムクロックと DNS (ドメイン名システム) の設定が正しいことを確認します。

詳細については、**2**-255 ページの「ライセンスサービスの登録およびアクティブ化」を参照してください。

WebUI

Configuration > Date/Time

Network > DNS > Host

4. **Update Now** ボタンをクリックします。

   このオプションは、徹底監視のライセンスキーを取得した後で利用できます。

   すると、セキュリティデバイスは、デフォルトの URL である https://services.netscreen.com/restricted/sigupdates でサーバーとの接続を試みます。ユーザーが Database Server フィールドに別の URL を入力している場合は、その URL から接続を試みます。123 ページの表 6 に、定義済みのシグネチャパッケージと対応する URL を示します。

   しばらくして、更新が正常に行われたかどうかを示すメッセージが表示されます。更新が正常に行われなかった場合は、イベントログをチェックして、失敗の原因を調べてください。

注： シグネチャパッケージを初めてダウンロードする場合は、ダウンロード後にセキュリティデバイスをリセットする必要があります。その後のダウンロードでは、デバイスのリセットは必要ありません。

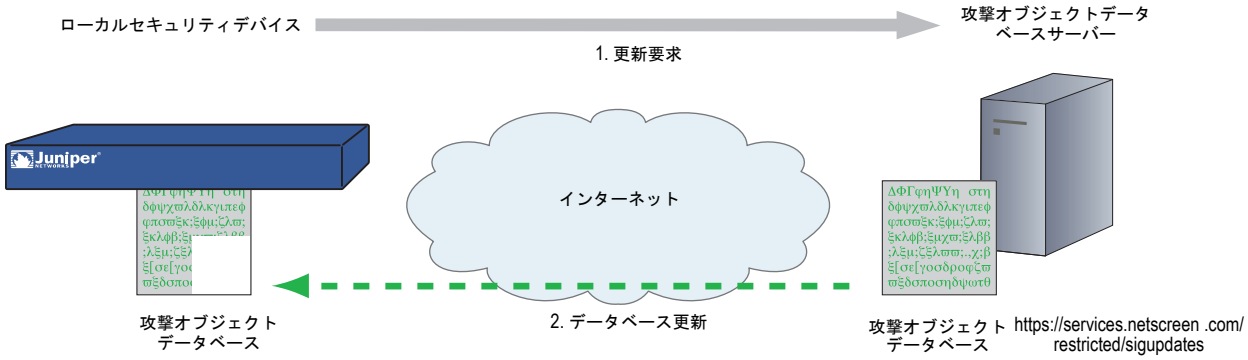
即時更新

Immediate Update オプションを使って、セキュリティデバイスのシグネチャパッケージをデータベースサーバー上のシグネチャパッケージで直ちに更新できます。この更新を機能させるには、最初に攻撃オブジェクトデータベースサーバー設定を構成する必要があります。

この例 (図 46 を参照) では、定義済みのシグネチャパッケージを攻撃オブジェクトデータベースサーバーからセキュリティデバイスに直ちに保存します。

セキュリティデバイスのデータベースを更新するためのスケジュールは設定しません。代わりに、サーバー上のデータベースをセキュリティデバイスに直ちに保存します。

図 46: DI シグネチャの即時更新



WebUI

Configuration > Update > Attack Signature:
Signature Pack: Client
Update Now ボタンをクリックします。

CLI

```
set attack db sigpack client
exec attack-db update
Loading attack database.............
Done.
Done.
Switching attack database...Done
Saving attack database to flash...Done.
```

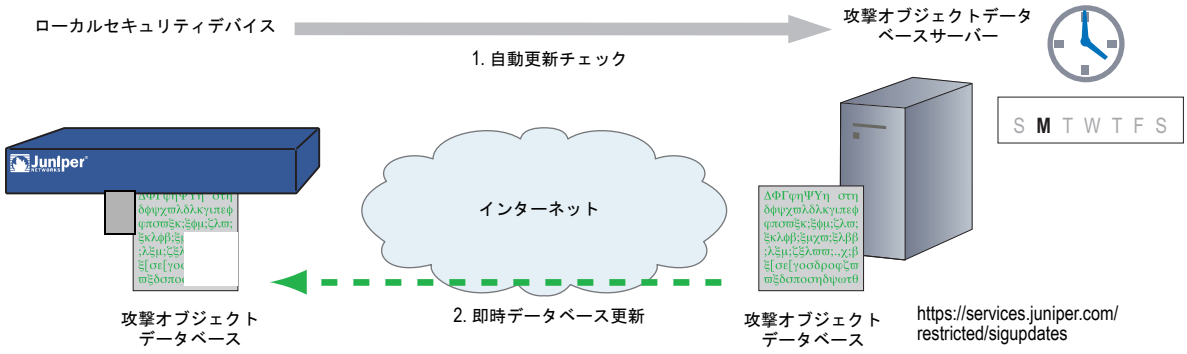
自動更新

Automatic Update オプションは、サーバー上のデータベースが、デバイスに以前ロードされたものよりバージョンが新しい場合、ユーザーが予定した時刻にシグネチャパッケージをダウンロードします。Juniper Networks は、新しく発見した攻撃パターンで、シグネチャパッケージを定期的に更新しています。そのため、シグネチャパッケージが変わるので、セキュリティデバイス上のシグネチャパッケージも定期的に更新する必要があります。この更新を機能させるには、最初に攻撃オブジェクトデータベースサーバー設定を構成する必要があります。

この例（図 47 を参照）では、セキュリティデバイスのデータベースを毎週月曜日の午前 4:00 に更新するスケジュールを設定します。このスケジュール時間になると、デバイスは、サーバーのデータベースのバージョンをデバイスのデータベースのバージョンと比較します。サーバーのバージョンの方が新しい場合、セキュリティデバイスはデータベースを自動的に新しいバージョンに置換えます。

たとえば、サーバーのシグネチャパッケージは更新するには、Server を選択します。定義済みのシグネチャパッケージおよび対応する URL のリストについては、123 ページの表 6 を参照してください。

図 47: DI シグネチャの自動更新



WebUI

Configuration > Update > Attack Signature: 次のように入力してから **OK** をクリックします。

Signature Pack: Server
Update Mode: Automatic Update
Schedule:
Weekly on: Monday
Time (hh: mm): 04:00

注 : 毎月の更新をスケジュールして選択した日付が月中に発生しない場合 (たとえば 31 日のない月)、セキュリティデバイスはその月の最後の日付を代わりに使用します。

CLI

```
set attack db sigpack server
set attack db mode update
set attack db schedule weekly monday 04:00
save
```

自動通知と即時更新

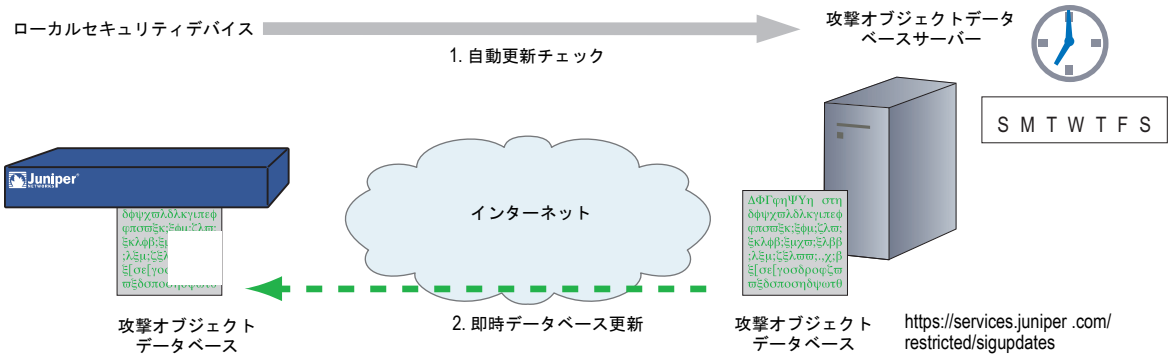
Automatic Notification および **Immediate Update** オプションを使って、ユーザーが予定した時間に、データベースサーバーのデータがセキュリティデバイスのデータより新しいかどうかを確認できます。サーバーのデータの方が新しければ、通知が WebUI のホームページと、セキュリティデバイスにログインした後のコマンドラインインターフェースに表示されます。ここで exec attack-db update コマンドを入力するか WebUI の Configuration > Update > Attack Signature ページで Update Now ボタンをクリックすると、サーバー上のシグネチャパッケージをデバイスに保存できます。サーバーをチェックする半自動手順を機能させるには、最初に攻撃オブジェクトデータベースサーバー設定を構成する必要があります。

この例（図 48 を参照）では、セキュリティデバイスのデータベースを毎日午前 7:00 にチェックするスケジュールを設定します。

サーバーのデータベースが更新されたという通知を受信したとき、WebUI で Configuration > Update > Attack Signature ページの **Update Now** ボタンをクリックするか、**exec attack-db update** コマンドを入力してデータベースをサーバーからデバイスに保存します。

たとえば、次を行って、Client シグネチャパッケージを更新します。定義済みのシグネチャパッケージおよび対応する URL のリストについては、123 ページの表 6 を参照してください。

図 48: シグネチャ更新の通知



WebUI

1. **スケジュールしたデータベースのチェック**
   Configuration > Update > Attack Signature: 次のように入力してから **OK** をクリックします。

   Signature Pack: Client
   Update Mode: Automatic Notification
   Schedule:
   Daily
   Time (hh: mm): 07:00

2. **即時データベース更新**
   サーバーの攻撃データベースがセキュリティデバイスのデータベースより新しいという通知を受信したとき、次の操作を行います。

   Configuration > Update > Attack Signature

   Signature pack: Client
   Update Now ボタンをクリックします。

CLI

1. **スケジュールしたデータベースのチェック**
   set attack db sigpack client
   set attack db mode notification
   set attack db schedule daily 07:00

2. **即時データベース更新**
   サーバーの攻撃データベースがセキュリティデバイスのデータベースより新しいという通知を受信したとき、次の操作を行います。

   exec attack-db update

手動更新

Manual Update オプションを使用すると、最初にブラウザを使用してシグネチャパッケージをローカルディレクトリまたは TFTP サーバーディレクトリにダウンロードできます。それから、シグネチャパッケージをセキュリティデバイスに、WebUI（ローカルディレクトリから）または CLI（TFTP サーバーディレクトリから）を使用してロードします

注： 即時データベース更新を実行する前に、**exec attack-db check** コマンドを実行してサーバーの攻撃オブジェクトデータベースがセキュリティデバイスのデータベースより新しいかどうか調べることができます。

この例（図 49 を参照）では、手動で最新のシグネチャパッケージをローカルディレクトリ「C:\netscreen\attacks-db」（WebUI を使用してデータベースをロードする場合）または C:\Program Files\TFTP Server（CLI を使用してロードする場合）に保存します。それから、ローカルディレクトリのデータベースをセキュリティデバイスにロードします。

注： シグネチャパッケージをダウンロードした後で、ローカルサーバーで公開して他のセキュリティデバイスがアクセスできるように設定できます。この場合他のデバイスの管理者は、データベースサーバー URL を新しい場所の URL に変更する必要があります。Configuration > Update > Attack Signature ページの Database Server フィールドに新しい URL を入力するか、CLI コマンド :**set attack db server** *url_string* を実行します。

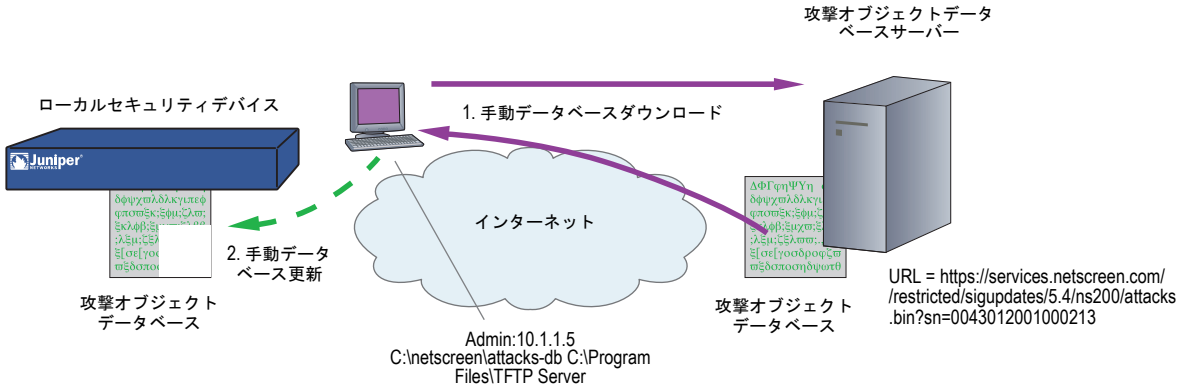
自動更新の場合、セキュリティデバイスは次の要素を URL に自動で追加します。

- セキュリティデバイスのシリアルナンバー
- このデバイスで動作する ScreenOS のメジャーバージョン番号
- プラットフォームタイプ

DI シグネチャを手動で更新するときは、これらの要素を自分で追加する必要があります。この例では、シリアルナンバーは 0043012001000213、ScreenOS のバージョンは 5.4、プラットフォームは NetScreen-208 (ns200) です。したがって、URL は次のようになります。

https://services.netscreen.com/restricted/sigupdates/5.4/ns200/attacks.bin?sn=0043012001000213

図 49: DI シグネチャの手動更新



1. シグネチャパッケージのダウンロード

ローカルサーバーにシグネチャパッケージを保存するには、ブラウザのアドレスフィールドに次の URL を入力します。定義済みのシグネチャパッケージおよび対応する URL のリストについては、123 ページの表 6 を参照してください。

https://services.netscreen.com/restricted/sigupdates/5.4/ns200/attacks.bin?sn=0043012001000213

attacks.bin をローカルディレクトリ C:\netscreen\attacks-db (WebUI でロードする場合) または自分の TFTP サーバーディレクトリ C:\Program Files\TFTP Server (CLI を使用してロードする場合) に保存します。

2. シグネチャパッケージの更新

WebUI

Configuration > Update > Attack Signature: 次のように入力してから **OK** をクリックします。

Deep Inspection Signature Update:
Load File: **C:\netscreen\attacks-db\attacks.bin** を入力します。

もしくは

Browse をクリックしてそのディレクトリへ移動し、**attacks.bin** を選択してから **Open** をクリックします。

サーバー、クライアント、またはワーム保護のシグネチャパッケージをダウンロードする場合は、該当するファイル名を入力します。

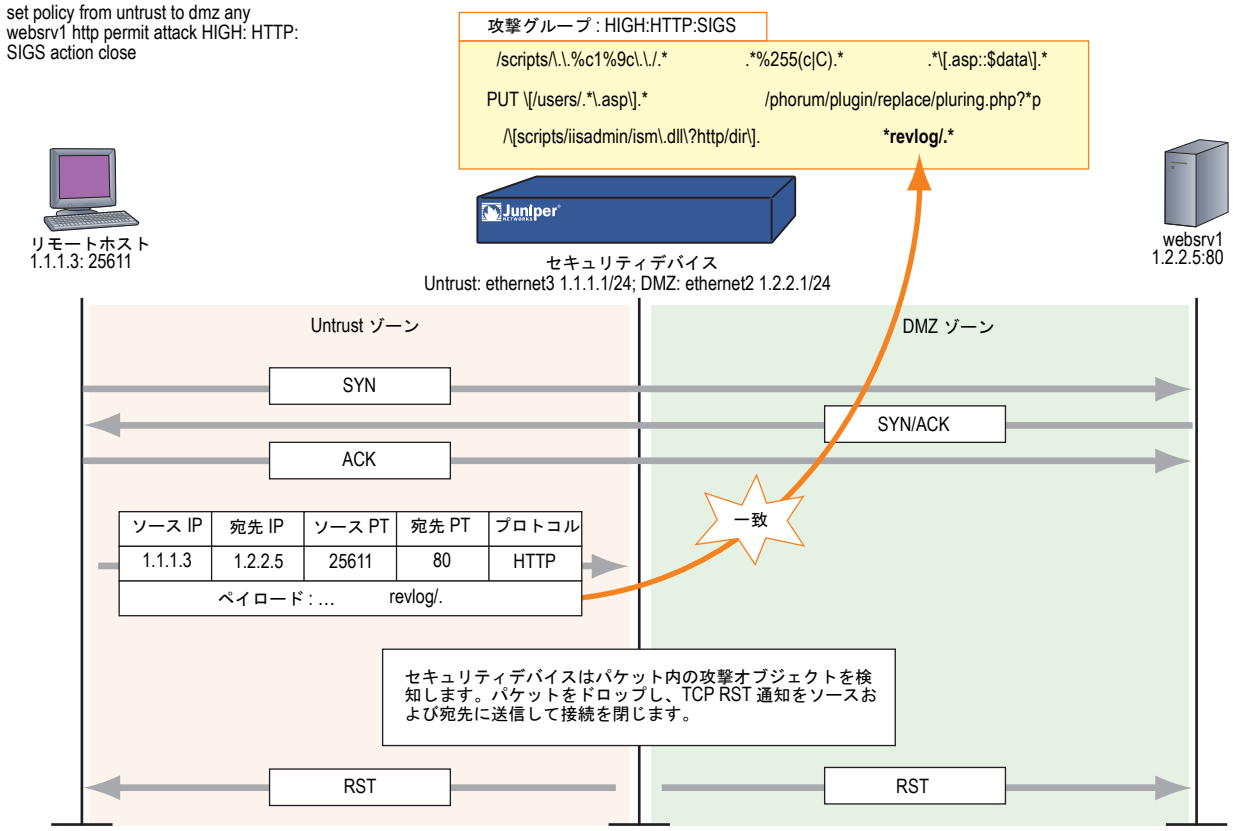
CLI

save attack-db from tftp 10.1.1.5 attacks.bin to flash

攻撃オブジェクトとグループ

攻撃オブジェクトはステートフルシグネチャ、ストリームシグネチャ (NetScreen-5000 シリーズの場合)、およびプロトコルアノーマリのことをいい、セキュリティデバイスはこれらを使用して、ネットワーク上の 1 基または複数のホストを危機にさらす攻撃を検知します。攻撃オブジェクトは、プロトコルタイプ別、さらに重大度別にグループ分けされています。DI (徹底監視) をポリシーに追加すると、デバイスはポリシーが許可するトラフィックで、参照する攻撃オブジェクトグループ (複数グループ可) 中のパターンと一致するパターンがあるかどうかを調べます。

図 50: 攻撃オブジェクトとグループ



ポリシーの DI コンポーネント内で参照する攻撃オブジェクトグループのターゲットは、ポリシーが許可するサービスタイプと同じでなければなりません。たとえば、ポリシーが SMTP トラフィックを許可する場合、攻撃オブジェクトグループは SMTP トラフィックの攻撃を標的にする必要があります。次のポリシーは、有効な構成例を示します。

set policy id 2 from trust to untrust any any **smtp** permit attack **CRIT:SMTP:SIGS** action close

次のポリシーは、SMTP トラフィックを許可していますが攻撃オブジェクトグループを POP3 トラフィックとしているため誤りです。

set policy id 2 from trust to untrust any any **smtp** permit attack **CRIT:POP3:SIGS** action close

2 番目のポリシーは構成が誤りであり、実装すると、セキュリティデバイスは SMTP トラフィックで見つかるはずのない POP3 攻撃オブジェクトを検査して不要なリソースを費やしてしまいます。ポリシー 2 が SMTP および POP3 トラフィックを許可する場合は、DI コンポーネントが SMTP 攻撃オブジェクト、POP3 攻撃オブジェクト、またはこの両方を調べるように構成できます。

set group service **grp1**
set group service **grp1** add **smtp**
set group service **grp1** add **pop3**
set policy id 2 from trust to untrust any any **grp1** permit attack **CRIT:SMTP:SIGS** action close
set policy id 2 attack **CRIT:POP3:SIGS** action close

サポートされているプロトコル

DI (徹底監視) モジュールは、次のプロトコルやアプリケーションに対するステートフルシグネチャ攻撃オブジェクトやプロトコルアノーマリ攻撃オブジェクトをサポートしています。

表 7: 基本ネットワークプロトコル

プロトコル	ステートフルシグネチャ	プロトコルアノーマリ	定義
DNS	はい	はい	DNS (Domain Name System) とは、ドメイン名と IP アドレスの対応 (例えば www.juniper.net は 207.17.137.68) を管理するデータベースシステムです。
FTP	はい	はい	FTP (File Transfer Protocol) とは、ネットワークを介してコンピュータ間でファイルをやり取りするためのプロトコルです。
HTTP	はい	はい	HTTP (Hypertext Transfer Protocol、ハイパーテキスト転送プロトコル) とは、主として Web サーバーから Web クライアントに情報を転送するためのプロトコルです。
IMAP	はい	はい	IMAP (Internet Mail Access Protocol) とは、受け取った電子メールを蓄積し、検索サービスを提供するためのプロトコルです。ユーザーは電子メールをローカル側にダウンロードしても、IMAP サーバー側に残しておいても構いません。
NetBIOS	はい	はい	NetBIOS (Network Basic Input Output System) とは、ユーザーのワークステーションにあるアプリケーションが、NetBEUI、SPX/IPX、TCP/IP などのネットワークトランスポートによって提供されるアクセスネットワークサービスにアクセスするのを可能にするアプリケーションインターフェースです。
POP3	はい	はい	POP3 (Post Office Protocol, version 3) とは、受け取った電子メールをいったん蓄積しておき、要求に応じてユーザー側に転送するためのプロトコルです。
SMTP	はい	はい	SMTP (Simple Mail Transfer Protocol、簡易メール転送プロトコル) とは、メールサーバー間で電子メールを転送するためのプロトコルです。
Chargen	はい	はい	Chargen (Character generator) プロトコル。
DHCP	はい	はい	DHCP (Dynamic Host Configuration Protocol、動的ホスト構成プロトコル) は、サーバーを利用してホスト (稼動中のクライアント) の重要なネットワークパラメータを制御する目的で使用されます。DHCP は、BOOTP と下位互換性があります。
Discard	はい	はい	Discard (破棄) プロトコルは、実用的なデバッグおよび測定のツールです。廃棄サービスは、受信するデータを単純に廃棄します。

プロトコル	ステートフルシグネチャ	プロトコルアノーマリ	定義
Echo	はい	はい	Echo (エコー) プロトコルは、テストおよび測定の目的で使用されるインターネットプロトコルです。ホストは、TCP または UDP ポート 7 のいずれかで Echo プロトコルをサポートしているサーバーに接続できます。一旦接続が確立すると、サーバーが受信するすべてのデータを送り返します。
Finger	はい	はい	Finger User Information Protocol は、リモートユーザー情報プログラムへのインターフェースを提供する簡易プロトコルです。
Gopher	はい	はい	Gopher は、分散型の文書検索用に設計されたインターネットプロトコルです。
ICMP	はい	はい	ICMP (Internet Control Message Protocol、インターネット制御メッセージプロトコル) は、IP と密接に一体化している必須のプロトコルです。IP パケットで配信される ICMP メッセージは、ネットワーク操作に関連する帯域外メッセージに使用されます。
IDENT	はい	はい	識別プロトコルは、特定の TCP 接続のユーザー ID を判別する手を提供します。
LDAP	はい	はい	LDAP (Lightweight Directory Access Protocol、軽量ディレクトリアクセスプロトコル) は、情報ディレクトリにアクセスするためのプロトコルセットです。
LPR	はい	はい	ラインプリンタスプーラ
NFS	はい	はい	NFS (Network File System、ネットワークファイルシステム) プロトコルは、ネットワークの共有ファイルに透過的なリモートアクセスを提供します。NFS プロトコルは、異なるマシン、オペレーティングシステム、ネットワークアーキテクチャ、トランスポートプロトコル間でも移動できるように設計されています。
NNTP	はい	はい	NNTP (Network News Transfer Protocol、ネットワークニュース転送プロトコル) は、信頼できるストリームベースのニュースの伝送を使用したニュース項目の配布、問い合わせ、取得、掲載用のプロトコルを指定します。
NTP	はい	はい	NTP (Network Time Protocol、ネットワークタイムプロトコル) と SNTP (Simple Network Time Protocol、簡易ネットワークタイムプロトコル) は、コンピュータのクライアントまたはサーバーの時刻を別のサーバーまたは参照用の時間ソース (ラジオ受信機、衛星放送受信機、またはモデム) に同期化させる目的で使用されます。
Portmapper	はい	はい	Port Mapper Program Protocol は、RPC プログラムとバージョン番号をトランスポート固有のポート番号にマッピングします。
RADIUS	はい	はい	RADIUS (Remote Authentication Dial In User Service、リモート認証ダイヤルインユーザーサービス) は、多数の ISP (Internet Service Provider、インターネットサービスプロバイダ) で使用される認証およびアカウンティングシステムです。
rexec	はい	はい	rexec (Remote Execution、遠隔実行)。
rlogin	はい	はい	ユーザーがインターネットホストに接続され、ネイティブユーザーインターフェースを使用する場合に、rlogin (リモートログイン) が行われます。
rsh	はい	はい	rsh (Remote Shell、リモートシェル)。
RTSP	はい	はい	RTSP (Real Time Streaming Protocol、リアルタイムストリーミングプロトコル) は、リアルタイムプロパティを使用してデータの配信を制御するクライアント / サーバー用のアプリケーションレベルのプロトコルです。連続メディア (音声やビデオなど) の 1 回または複数回の同期ストリームを確立し、制御します。

プロトコル	ステートフルシグネチャ	プロトコルアノーマリ	定義
SNMPTRAP	はい	はい	SNMP (Simple Network Management Protocol、簡易ネットワーク管理プロトコル) は、SNMP TRAP 操作を使用して、ネットワークマネージャに情報を送信する SNMP アプリケーションです。
SSH	はい	はい	SSH (Secure Shell、セキュアシェル) プロトコルは、安全でないネットワーク上のセキュアリモートログインおよびその他のセキュアネットワークサービス用のプロトコルです。
SSL	はい	はい	SSL (Secure Sockets Layer、セキュアソケットレイヤ) は、暗号システムを使用して、インターネット経由で秘密文書を送信するためのプロトコルです。
SYSLOG	はい	はい	システムロギングプロトコルは、ネットワークにイベント通知メッセージを伝送する目的で使用されます。
Telnet	はい	はい	Telnet プロトコルは、TCP/IP ネットワークのターミナルエミュレーションプログラムです。このプロトコルを使用すると、ネットワーク上の他のサーバーと通信を行うことができます。
TFTP	はい	はい	TFTP (Trivial File Transfer Protocol、トリビアルファイル転送プロトコル) は、ファイルを転送するための簡易プロトコルです。TFTP は UDP (User Datagram Protocol、ユーザーデータグラムプロトコル) を使用し、セキュリティ機能は提供しません。
VNC	はい	はい	VNC (Virtual Network Computing) は、別のコンピュータを遠隔から制御するデスクトッププロトコルです。
Whois	はい	はい	Network Directory Service Protocol (ネットワークディレクトリサービスプロトコル) は、ネットワーク全体のディレクトリサービスをインターネットユーザーに提供するクエリ / 応答サーバーに基づいた TCP トランザクションです。

表 8: インスタントメッセージアプリケーション

プロトコル	ステートフルシグネチャ	プロトコルアノーマリ	定義
AIM	はい	はい	AIM (America Online Instant Messaging) とは、America Online が提供するインスタントメッセージサービスです。
MSN Messenger	はい	はい	MSN Messenger (Microsoft Network Messenger) は、Microsoft が提供するインスタントメッセージサービスです。
Yahoo! Messenger	はい	はい	Yahoo! Messenger は、Yahoo! が提供するインスタントメッセージサービスです。
IRC	はい	はい	IRC (Internet Relay Chat) はテキストベースのプロトコルで、サーバーに接続することができるソケットプログラムの中でも最もシンプルなクライアントです。

表 9: P2P (ピアツーピア) ネットワークアプリケーション

プロトコル	ステートフルシグネチャ	プロトコルアノーマリ	定義
BitTorrent	はい	なし	BitTorrent は P2P ファイル配布ツールで、同じファイルを多人数のグループに効率的に配布できるよう、ダウンロードした人がほかの人にアップロードする機能が組み込まれています。
DC (Direct Connect)	はい	なし	DC (Direct Connect) は P2P ファイル共有アプリケーションです。DC ネットワークはハブを使ってユーザーグループ間を接続します。多くの場合、ある一定の記憶容量やファイルを共有する必要があります。多くのハブに、特定分野の話題のために割り当てた領域があって、少人数のコミュニティーを構築できるようになっています。
eDonkey	はい	なし	eDonkey は分散型 P2P ファイル共有アプリケーションで、MFTP (Multisource File Transfer Protocol) を利用しています。eDonkey ネットワークには、クライアント用とサーバー用の 2 種類のアプリケーションがあります。クライアントはネットワークに接続してファイルを共有します。サーバーはクライアントどうしが連絡を取り合うハブの役割を果たします。
Gnutella	はい	はい	Gnutella は P2P ファイル共有プロトコル / アプリケーションで、中央サーバーがない点が特徴です。Gnutella プロトコルを使っている他のアプリケーションとして、BearShare、Limewire、Morpheus、ToadNode などがあります。
KaZaa	はい	なし	KaZaa は分散型の P2P ファイル共有アプリケーションで、FastTrack プロトコルを使います。主として MP3 ファイルの共有のために使われています。
MLdonkey	はい	なし	MLdonkey は P2P クライアントアプリケーションで、さまざまなプラットフォーム上で動作し、BitTorrent、DC、eDonkey、FastTrack (KaZaa その他)、Gnutella、Gnutella2 など多くの P2P ネットワークにアクセスできます。
Skype	はい	なし	Skype は無料の P2P インターネット電話サービスで、インターネットなどの TCP/IP ネットワークを介して通話ができます。
SMB	はい	はい	SMB (Server Message Block) はファイルやプリンタなどの資源をコンピュータ間で共有するためのプロトコルです。SMB は NetBIOS プロトコル上で動作します。
WinMX	はい	なし	WinMX は P2P ファイル共有アプリケーションで、クライアントは同時に複数のサーバーに接続できます。

注 : ここに挙げた P2P アプリケーションはほとんどが独自のプロトコルで動作します。

表 10: アプリケーションレイヤーゲートウェイ (ALG)

プロトコル	ステートフルシグネチャ	プロトコルアノーマリ	定義
MSRPC	はい	はい	MSRPC (Microsoft-Remote Procedure Call) とは、リモートコンピュータ上でプロセスを実行するための機構です。

セキュリティデバイスが http://help.juniper.net/sigupdates/english にアクセスすると、すべての定義済み攻撃オブジェクトグループの内容と定義済み攻撃オブジェクトの説明を見ることができます。ブラウザを開き、次のいずれかの URL をアドレスフィールドに入力してください。

http://help.juniper.net/sigupdates/english/AIM.html
http://help.juniper.net/sigupdates/english/DNS.html
http://help.juniper.net/sigupdates/english/FTP.html
http://help.juniper.net/sigupdates/english/GNUTELLA.html
http://help.juniper.net/sigupdates/english/HTTP.html
http://help.juniper.net/sigupdates/english/IMAP.html
http://help.juniper.net/sigupdates/english/MSN.html
http://help.juniper.net/sigupdates/english/NBDS.html
http://help.juniper.net/sigupdates/english/NBNAME.html
http://help.juniper.net/sigupdates/english/POP3.html
http://help.juniper.net/sigupdates/english/SMTP.html
http://help.juniper.net/sigupdates/english/MSRPC.html
http://help.juniper.net/sigupdates/english/SMB.html
http://help.juniper.net/sigupdates/english/YMSG.html

上記の各 URL は、特定のプロトコルに対して、（重度によってグループ分けされた）事前定義された全攻撃オブジェクトリストを持つ HTML ページにリンクします。攻撃オブジェクトの説明を表示するには、その名前をクリックしてください。

ステートフル署名

攻撃シグネチャとは、ある特定の脆弱性不正利用 (エクスプロイト) が進行しているときに存在するパターンです。このシグネチャは、たとえば 1 つのアドレスが大量のパケットを別のアドレスの別ポートナンバーへ送信する場合 (9 ページの「ポートスキャン」を参照) といったレイヤ 3 や 4 のトラフィックパターンであったり、不正な URL 文字列が 1 つの HTTP または FTP パケットのデータペイロードに現れるといったテキストパターンであったりします。この文字列は、特定のコードのセグメントであったりパケットヘッダー内の特定の値であったりもします。しかしテキストパターンを検索する場合、セキュリティデバイスの DI (徹底監視) モジュールはシグネチャを単にパケット内で探すだけではありません。シグネチャをパケットの特定の部分内 (フラグメント化やセグメント化されていても) や、セッション期間の特定の時間に送信されたパケット内、そして接続のイニシエータまたは受信側によって送信されたパケット内で探します。

注 : DI モジュールは正規表現をサポートしているため、パターンを探す際にワイルドカードを使用できます。そのため、1 つの攻撃シグネチャ定義を複数の攻撃パターン変形体に適用できます。正規表現に関するより詳細な情報は、159 ページの「正規表現」を参照してください。

DI モジュールはテキストパターンを調べるとき、参加者の役割をクライアントかサーバーであると考え、セッションの状態を監視して、攻撃者がパターンを使用する目的である脆弱性不正利用 (エクスプロイト) に関係した要素だけに検索をしぼります。文脈情報を使用してより詳細なパケット検査を行うと、誤検出つまり “false positives” (誤検出) を大きく減らし、不必要なプロセスを回避することができます。「ステートフルシグネチャ」という言葉は、参加者の役割とセッションの状態というコンテキストの中でシグネチャを探すという概念を表わしています。

シグネチャが発生するコンテキストを考慮することの利点を理解するには、EXPN Root 攻撃の検知を有効にしたときに DI モジュールがパケットを調べる様子に注目してください。攻撃者は EXPN Root 攻撃を使用して、メールサーバーのメーリングリストを展開し、脅威にさらします。EXPN Root 攻撃を検知するた

め、セキュリティデバイスはシグネチャ「expn root」を SMTP (簡易メール転送プロトコル) セッションの制御部内で探します。デバイスは制御部のみを調べます。理由は、制御部が攻撃を発生し得る唯一の場所だからです。“expn root”がセッションの他の場所に発生しても、これは攻撃にはなりません。

シグネチャ “expn root”は、単純なテキストパケットシグネチャ検出技術を使用して、これが SMTP 接続のデータ部分、つまり E メールメッセージの本文に現れた場合もアラームを起動します。たとえばあなたが同僚に EXPN Root 攻撃に関するメールを出すと、単純なパケットシグネチャ検出ではこれを攻撃と見なします。ステートフルシグネチャを使用すると、DI モジュールは、攻撃を示すテキスト文字列と無害なテキスト文字列を見分けることができます。

注 : 定義済みのステートフルシグネチャ攻撃オブジェクトがあるプロトコルのリストは、131 ページの「サポートされているプロトコル」を参照してください。

TCP ストリームシグネチャ

ステートフルシグネチャと同様、TCP ストリームシグネチャは、脆弱性不正利用 (エクスプロイト) が進行中の場合に存在するパターンです。しかし、DI モジュールはトラフィックのステートフル署名を調べるとき、特定のコンテキスト内でしか探しません。DI モジュールはトラフィックの TCP ストリームシグネチャを調べる場合、コンテキストにかまわずに調べます。2 種類のシグネチャ間のもう 1 つの違いは、ステートフル署名が事前定義またはユーザー定義可能であるのに対し、TCP ストリームシグネチャはかならずユーザー定義である点です。ストリームシグネチャ攻撃オブジェクトを攻撃オブジェクトグループに追加すると、DI を適用するポリシー内でこのグループが参照可能になります (TCP ストリームシグネチャの詳細については、162 ページの「TCP ストリームシグネチャ攻撃オブジェクト」を参照してください。)

注 : TCP ストリームシグネチャは、ハイエンドシステムでのみ定義できます。

ストリームシグネチャは、プロトコルから独立しているので、トラフィックの照合がより柔軟になります。ストリームシグネチャは、プロトコルデコーダが検査できないトラフィックを調べることができます。ただし、この柔軟性は、パフォーマンスとリソースの消費量に影響します。

ストリームシグネチャはリソースを消費し、パフォーマンスに影響するので、慎重に使用する必要があります。一方、Stream256 シグネチャの動作は同じですが、ストリーム全体を照合するのではなく、先頭 256 バイトのストリームだけを照合するので、リソースの消費量とパフォーマンスの影響が少なくなります。

プロトコルアノーマリ (プロトコル異常)

プロトコルアノーマリを探し出す攻撃オブジェクト は、RFC および共通 RFC 拡張で定義された標準から外れたトラフィックを検出します。シグネチャ攻撃オブジェクトを使用する場合は、定義済みパターンを使用するか新しいパターンを作成するため、既知の攻撃しか検出しません。プロトコルアノーマリ検出は、新しい攻撃やテキストパターンで定義できない攻撃を捕らえる場合に特に便利です。

注 : 定義済みのプロトコルアノーマリ攻撃オブジェクトがあるプロトコルのリストは、131 ページの「サポートされているプロトコル」を参照してください。

攻撃オブジェクトグループ

定義済み攻撃オブジェクトグループは、特定プロトコルの攻撃オブジェクトで構成されます。プロトコルごとに、攻撃オブジェクトグループはプロトコルアノーマリとステートフル署名に分けられ、それから重大度別に大まかに体系化されています。攻撃オブジェクトグループには 3 つの重大度レベルがあり、Critical、High、Medium です。

- **Critical (クリティカル):** 検出を回避しようとしたりネットワークデバイスの故障を引き起こそうとしたり、システムレベルの権限獲得を試みる脆弱性不正利用 (エクスプロイト) と一致する攻撃オブジェクトが含まれます。
- **High (高):** サービスを阻害しようとしたり、ネットワークデバイスへのユーザーレベルのアクセス権を獲得しようとしたり、それまでにデバイスにロードされた「トロイの木馬」を作動させようとする脆弱性不正利用と一致する攻撃オブジェクトが含まれます。
- **Medium (中):** ディレクトリ巡回や情報リークを経て重要情報へアクセスしようとするスパイ活動を検知する脆弱性不正利用と一致する攻撃オブジェクトが含まれます。
- **Low (低):** クリティカルでない情報を取得する、あるいはツールを使ってネットワークをスキャンしようと試みる脆弱性不正利用 (エクスプロイト) と一致する攻撃オブジェクトが含まれます。
- **Info (情報):** URL、DNS 検索失敗、SNMP のパブリックコミュニティ文字列、ピアツーピア (P2P) パラメータなどを含む、正常で害のないトラフィックと一致する攻撃オブジェクトが含まれます。通知攻撃オブジェクトを使用して、自分のネットワークに関する情報を入手できます。

重大度レベルの変更

攻撃オブジェクトグループはプロトコルと重大度レベル (クリティカル、High、Medium) に類別されていますが、各攻撃オブジェクトにはそれぞれの重大度レベルがあります。critical, high, medium, low, info. これらの攻撃オブジェクト重大度レベルは、イベントログエントリの重大度レベルへ次のように対応します。

表 11: 攻撃オブジェクト重大度レベル

攻撃オブジェクト重大度レベル　マップ先	イベントログエントリ重大度レベル
Critical	Critical
High	Error
Medium	Warning
Low	Notification
Info	Information

たとえばセキュリティデバイスが重大度レベル「Medium」の攻撃を検知すると、イベントログの中に現れる対応エントリの重大度レベルは「Warning」になります。

ポリシー内で参照される 1 つ以上の攻撃オブジェクトグループ内で、すべての攻撃オブジェクトのデフォルト重大度レベルを上書きすることが可能です。ポリシーレベルで上書きするには、既存ポリシーのコンテキストを入力してからこのポリシーが参照するすべての攻撃オブジェクトグループに新しい重大度レベルを割り当てます。

次に、ポリシー内で参照される攻撃オブジェクトグループの重大度レベルを WebUI および CLI で変更する方法を示します。

WebUI

Policies > Edit (既存ポリシーの場合): 次の操作を行って **OK** をクリックします。

> Deep Inspection: Severity ドロップダウンリストで重大度オプションを選択して、**OK** をクリックします。

CLI

```
device-> set policy id number
device(policy: number)-> set di-severity { info | low | medium | high | critical }
```

各攻撃オブジェクトの重大度レベルを最初の設定に戻すには、ポリシーのコンテキストを再度入力して

WebUI

Policies > Edit (既存ポリシーの場合): 次の操作を行って **OK** をクリックします。

> Deep Inspection: Severity ドロップダウンリストの中の **Default** を選択して、**OK** をクリックします。

CLI

```
device-> set policy id number
device(policy: number)-> unset di-severity
```

例 : P2P の徹底監視

この例では、Trust ゾーンに属するどのホストからでも、Untrust ゾーンに属するホストとの間で、HTTP、DNS、Gnutella サービスを使ってピアツーピア (P2P) セッションを起動できるように設定します。次にこのトラフィックに対して徹底監視 (DI) を適用して、次の攻撃オブジェクトグループの定義に従い、ステートフルシグネチャおよびプロトコルアノーマリを検査します。

- HIGH:HTTP:SIGS
- INFO:GNUTELLA:ANOM
- INFO:HTTP:SIGS

注 : セキュリティ保護のため、Untrust ゾーンに属するホストから、Trust ゾーンに属するホストとの間で P2P セッションを起動することを許可するポリシーは定義しません。

セキュリティデバイスは、シグネチャや異常な動作を検知すると、接続を切断し、クライアントに TCP RST を送ってセッションを閉じます。また、攻撃があった旨をログに記録することもできます。デフォルト状態では、記録するようになっています。

注 : セキュリティデバイスが実行できる各種の攻撃アクションについて詳しくは、141 ページの「攻撃アクション」を参照してください。検知した攻撃のログ記録について詳しくは、152 ページの「攻撃のログ出力」を参照してください。

WebUI

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), Any
Service: DNS

> **Multiple** をクリックし、**GNUTELLA** および **HTTP** を選択してから、**OK** をクリックして基本ポリシー構成ページに戻ります。

Action: Permit

> **Deep Inspection** をクリックし、次のように入力し、**Add** をクリックして各攻撃オブジェクトグループを追加します。その後 **OK** をクリックして基本ポリシー構成ページに戻ります。

Severity: Default
Group: HIGH:HTTP:SIGS
Action: Close Client
Log: (**選択**)
Severity: Default
Group: INFO:GNUTELLA:ANOM
Action: Close Client
Log: (**選択**)
Severity: Default
Group: INFO:HTTP:SIGS
Action: Close Client
Log: (**選択**)

CLI

```
set policy id 1 from trust to untrust any any dns permit attack
HIGH:HTTP:SIGS action close-client
set policy id 1
device(policy:1)-> set service gnutella
device(policy:1)-> set service http
device(policy:1)-> set attack INFO:GNUTELLA:ANOM action close-client
device(policy:1)-> set attack INFO:HTTP:SIGS action close-client
device(policy:1)-> exit
save
```

注 : 検知した攻撃のログ出力はデフォルトで有効になっているので、CLI コマンドで改めて設定する必要はありません。

攻撃オブジェクトの無効化

ポリシー中で攻撃オブジェクトグループを参照していれば、セキュリティデバイスはそのポリシーを適用するトラフィックについて、当該グループに属するいずれかの攻撃オブジェクトに合致するパターンがないかどうか検査します。しかしある攻撃オブジェクトが正当なトラフィックをしばしば攻撃と誤認識する (false-positive) ようであれば、これを無効にする必要があるでしょう。この攻撃オブジェクトが独自に作成したものであれば、単にこれが属する攻撃オブジェクトグループから削除するだけで構いません。しかし定義済みの攻撃オブジェクトは、定義済み攻撃オブジェクトグループから削除することができないようになっています。この場合、攻撃オブジェクトを無効化するのが最善の解決法になります。

なお、定義済み攻撃オブジェクトが無効になるのは、実際に無効にしたルートシステムまたは仮想システム (vsys) の範囲内に限ります。例えばルートシステム内で無効にしても、他の仮想システム内で自動的に無効になる、ということはないのです。同様に、ある vsys で無効にしても、他の vsys では有効なままです。

注 : 攻撃オブジェクトを無効にしてもスループットが改善されるということはありません。

攻撃オブジェクトを無効にするには、次のように操作してください。

WebUI

Objects > Attacks > Predefined 無効にしたい攻撃オブジェクトの **Configure** 列にあるチェックボックスをオフにします。

CLI

set attack disable *attack_object_name*

無効にした攻撃オブジェクトを再び有効にしたい場合は、次のように操作します。

WebUI

Objects > Attacks > Predefined 有効にしたい攻撃オブジェクトの **Configure** 列にあるチェックボックスをオンにします。

CLI

unset attack disable *attack_object_name*

攻撃アクション

セキュリティデバイスは攻撃を検知すると、これに合致する攻撃が属する攻撃オブジェクトグループで指定されたアクションを実行します。アクションとしては、より安全度の高い処理から順に、次のようなものがあります。

- **Close** (接続を切断して RST をクライアントとサーバーへ送信します)

注 : クライアントは常にセッションのイニシエータであり、つまりポリシーの中ではソースアドレスとなります。サーバーは常に受信側、つまり宛先アドレスとなります。

TCP 接続の場合に選択します。セキュリティデバイスは接続をドロップして、TCP RST をクライアント (ソース) とサーバー (宛先) へ送信します。RST 通知の送信は信頼性に劣るため、RST をクライアントとサーバーの両方に送ることにより、少なくとも一方が RST を取得してセッションを閉鎖する確立が高くなります。

- **Close Server** (接続を切断して RST をサーバーに送信します。)

  アントラステッドクライアントから保護されたサーバーへのインバウンド TCP 接続の場合に選択します。クライアントが攻撃を仕掛けようとすると、セキュリティデバイスは接続をドロップし、TCP RST をサーバーにのみ送信することで、クライアントを放置している間にサーバーはリソースをクリアします。

- **Close Client** (接続を切断して RST をクライアントに送信します。)

  保護されたクライアントからアントラステッドサーバーへのアウトバウンド TCP 接続の場合に選択します。たとえば、サーバーが不正な URL 文字列を送信すると、セキュリティデバイスは接続をドロップして、RST をクライアントにのみ送信することで、サーバーを放置している間にクライアントはリソースをクリアします。

- **Drop** (RST をどこにも送信しないで接続を切断します。)

  UDP 、または DNS など TCP 以外の接続の場合に使用します。セキュリティデバイスはセッション内のすべてのパケットをドロップしますが、TCP RST は送信しません。

- **Drop Packet** (特定パケットをドロップしますが、接続は切断しません。)

  これを選択すると、攻撃シグネチャやプロトコルアノーマリが存在するパケットをドロップしますが、セッション自体は終了しません。これは、奇形のパケットをドロップするがセッション全体は中断しない場合に選択します。たとえば、セキュリティデバイスが AOL プロキシから攻撃シグネチャやプロトコルアノーマリを検知した場合、すべてをドロップすると AOL サービスすべてが中断されます。そのため、パケットだけをドロップすれば問題のパケットが停止し、他のすべてのパケットはフローを停止しません。

- **Ignore** (攻撃シグネチャやアノーマリの検出後、セキュリティデバイスはログエントリを作成し、接続の残りのチェックを中止 (あるいは無視) します。)

セキュリティデバイスは攻撃シグネチャやプロトコルアノーマリを検知すると、イベントログエントリを作成しますが接続そのものは切断しません。これは、徹底監視 (DI) 実装の初期設定段階における偽陽性を微調整する場合に選択します。また、サービスが非標準プロトコルアクティビティに対して標準ポート番号を使用する場合、たとえば Yahoo Messenger が非 SMTP トラフィックに対してポート 25 (SMTP ポート) を使用する場合に選択します。セキュリティデバイスは、(ログが偽陽性で一杯にならないように) 1 セッションにつき発生を 1 回記録しますが、実行するアクションはありません。

- **None** (アクションなし)

  これは、DI 実装の初期設定段階で攻撃タイプを最初に認識した場合に便利です。セキュリティデバイスは攻撃シグネチャやプロトコルアノーマリを検知すると、エントリをイベントログに作成しますが、トラフィック自体にアクションを実行しません。セキュリティデバイスはそのセッションで後に続くトラフィックのチェックを続行し、他の攻撃シグネチャやアノーマリを検知するとログエントリを作成します。

攻撃オブジェクトグループを複数用意して、それぞれ異なるアクションを設定し、同じポリシーから参照することもできます。同時に複数の攻撃を検知し、それが別々の攻撃オブジェクトグループに属する場合、セキュリティデバイスはその中で最も重大度の高いアクションを実行します。

例 : 攻撃アクション ー Close Server、Close、Close Client

この例では、Trust、Untrust、および DMZ の 3 つのゾーンがあります。すでに攻撃の解析が終了し、次の 3 つのポリシーが必要であるとの結論が出されています。

- **ポリシー ID 1:** Untrust ゾーン内のあらゆるアドレスから DMZ 内の Web サーバー (websrv1 および websrv2) への HTTP、HTTPS、PING、および FTP-GET トラフィックを許可します。

  ポリシー ID 1 の攻撃設定 :

  - CRITICAL:HTTP:ANOM, CRITICAL:HTTP:SIGS
  - HIGH:HTTP:ANOM, HIGH:HTTP:SIGS
  - MEDIUM:HTTP:ANOM, MEDIUM:HTTP:SIGS
  - CRITICAL:FTP:SIGS
  - 攻撃オブジェクトグループに設定するアクション (すべて共通): Close Server
  - ロギング : 有効 (デフォルト設定)

  接続を停止して TCP RST 通知を保護された Web サーバーのみに送信することを選択するため、これらのサーバーはセッションを終了してリソースをクリアできます。攻撃の送信元は Untrust ゾーンであると予想しています。

- **ポリシー ID 2:** Trust ゾーン内のあらゆるアドレスから DMZ 内の Web サーバー (websrv1 および websrv2) への HTTP、HTTPS、PING、および FTP トラフィックを許可します。

  ポリシー ID 2 の攻撃設定 :

  - CRITICAL:HTTP:ANOM, CRITICAL:HTTP:SIGS
  - HIGH:HTTP:ANOM, HIGH:HTTP:SIGS
  - MEDIUM:HTTP:ANOM, MEDIUM:HTTP:SIGS
  - CRITICAL:FTP:SIGS
  - 攻撃オブジェクトグループに設定するアクション (すべて共通): Close
  - ロギング : 有効 (デフォルト設定)

  接続を停止して TCP RST 通知を保護されたクライアントとサーバーの両方へ送信することを選択するため、これらのサーバーとクライアントはどちらも、攻撃の重大度レベルに関わらずセッションを終了してそれぞれのリソースをクリアできます。

- **ポリシー ID 3:** Trust ゾーン内のあらゆるアドレスから Untrust ゾーン内のあらゆるアドレスへの FTP-GET、HTTP、HTTPS、PING トラフィックを許可します。

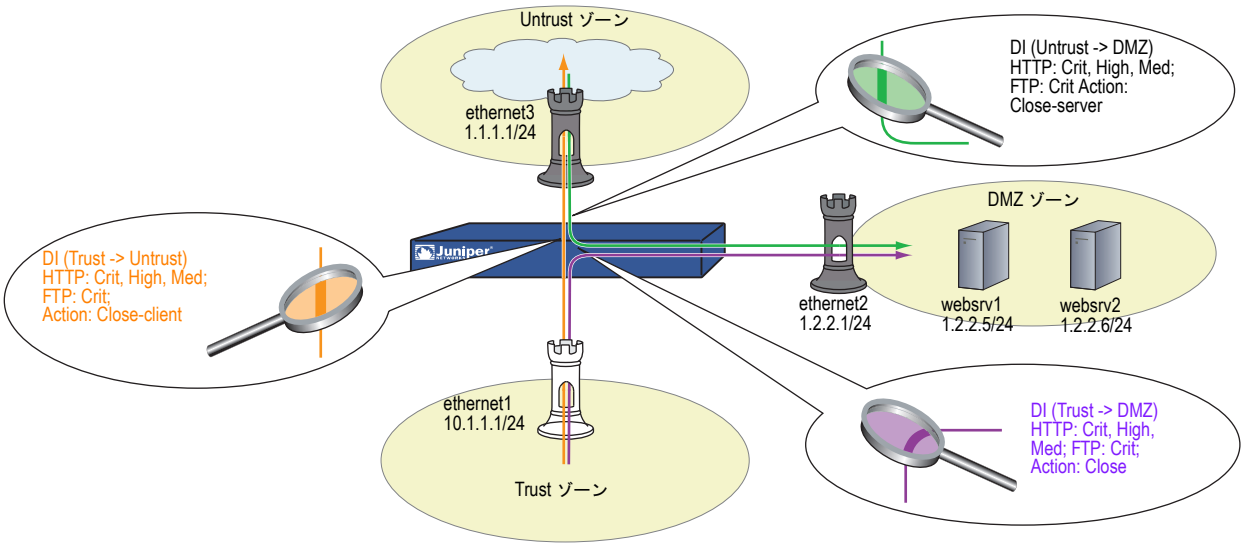
  ポリシー ID 3 の攻撃設定 :

  - CRITICAL:HTTP:ANOM, CRITICAL:HTTP:SIGS
  - HIGH:HTTP:ANOM, HIGH:HTTP:SIGS
  - MEDIUM:HTTP:ANOM, MEDIUM:HTTP:SIGS
  - CRITICAL:FTP:SIGS
  - 攻撃オブジェクトグループに設定するアクション (すべて共通): Close Client
  - ロギング : 有効 (デフォルト設定)

  接続を停止して TCP RST 通知を保護されたクライアントに送信することを選択するため、これらのクライアントはセッションを終了してリソースをクリアできます。この場合、攻撃の送信元は HTTP または FTP のアントラステッドサーバーであると予想しています。

これらのポリシーは HTTP、HTTPS、Ping、FTP-Get または FTP を許可していますが、セキュリティデバイスは DI を HTTP および FTP トラフィックだけに作動させます。すべてのゾーンは、trust-vr ルーティングドメインにあります。

図 51: DI 攻撃アクション



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24

   次のように入力してから **OK** をクリックします。

   Interface Mode: NAT
   Service Options:
   Management Services: (すべて選択)
   Other services: Ping

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

   Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

   Zone Name: DMZ
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.2.2.1/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: websrv1
IP Address/Domain Name:
IP/Netmask: (選択), 1.2.2.5/32
Zone: DMZ

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: websrv2
IP Address/Domain Name:
IP/Netmask: (選択), 1.2.2.6/32
Zone: DMZ

3. Route

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

4. ポリシー ID 1

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), websrv1

> **Multiple** をクリックし、**websrv2** を選択してから、**OK** をクリックして基本ポリシー構成ページに戻ります。

Service: HTTP

> **Multiple** をクリックし、**FTP-GET**、**HTTPS**、**PING** を選択してから **OK** をクリックして基本ポリシー構成ページに戻ります。

Action: Permit

> **Deep Inspection** をクリックし、次のように入力し、**Add** をクリックして各攻撃オブジェクトグループを追加します。その後 **OK** をクリックして基本ポリシー構成ページに戻ります。

Group: CRITICAL:HTTP:ANOM
Action: Close Server
Log: (選択)
Group: CRITICAL:HTTP:SIGS
Action: Close Server
Log: (選択)
Group: HIGH:HTTP:ANOM
Action: Close Server
Log: (選択)

Group: HIGH:HTTP:SIGS
Action: Close Server
Log: (選択)
Group: MEDIUM:HTTP:ANOM
Action: Close Server
Log: (選択)
Group: MEDIUM:HTTP:SIGS
Action: Close Server
Log: (選択)
Group: CRITICAL:FTP:SIGS
Action: Close Server
Log: (選択)

5. **ポリシー ID 2**

Policies > (From: Trust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), websrv1

> **Multiple** をクリックし、**websrv2** を選択してから、**OK** をクリックして基本ポリシー構成ページに戻ります。

Service: HTTP

> **Multiple** をクリックし、**FTP-GET**、**HTTPS**、**PING** を選択してから **OK** をクリックして基本ポリシー構成ページに戻ります。

Action: Permit

> **Deep Inspection** をクリックし、次のように入力し、**Add** をクリックして各攻撃オブジェクトグループを追加します。その後 **OK** をクリックして基本ポリシー構成ページに戻ります。

Group: CRITICAL:HTTP:ANOM
Action: Close
Log: (選択)
Group: CRITICAL:HTTP:SIGS
Action: Close
Log: (選択)
Group: HIGH:HTTP:ANOM
Action: Close
Log: (選択)
Group: HIGH:HTTP:SIGS
Action: Close
Log: (選択)
Group: MEDIUM:HTTP:ANOM
Action: Close
Log: (選択)
Group: MEDIUM:HTTP:SIGS
Action: Close
Log: (選択)
Group: CRITICAL:FTP:SIGS
Action: Close
Log: (選択)

6. ポリシー ID 3

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), Any
Service: HTTP

> **Multiple** をクリックし、**FTP-GET**、**HTTPS**、**PING** を選択してから **OK** をクリックして基本ポリシー構成ページに戻ります。

Action: Permit

> **Deep Inspection** をクリックし、次のように入力し、**Add** をクリックして各攻撃オブジェクトグループを追加します。その後 **OK** をクリックして基本ポリシー構成ページに戻ります。

Group: CRITICAL:HTTP:ANOM
Action: Close Client
Log: (選択)
Group: CRITICAL:HTTP:SIGS
Action: Close Client
Log: (選択)
Group: HIGH:HTTP:ANOM
Action: Close Client
Log: (選択)
Group: HIGH:HTTP:SIGS
Action: Close Client
Log: (選択)
Group: MEDIUM:HTTP:ANOM
Action: Close Client
Log: (選択)
Group: MEDIUM:HTTP:SIGS
Action: Close Client
Log: (選択)
Group: CRITICAL:FTP:SIGS
Action: Close Client
Log: (選択)

CLI

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 manage
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet2 zone dmz
set interface ethernet2 ip 2.1.1.1/24
```

2. アドレス

```
set address dmz websrv1 1.2.2.5/32
set address dmz websrv2 1.2.2.6/32
```

3. **Route**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

4. **ポリシー ID 1**
   set policy id 1 from untrust to dmz any websrv1 http permit attack
   CRITICAL:HTTP:ANOM action close-server
   set policy id 1
   device(policy:1)-> set dst-address websrv2
   device(policy:1)-> set service ftp-get
   device(policy:1)-> set service https
   device(policy:1)-> set service ping
   device(policy:1)-> set attack CRITICAL:HTTP:SIGS action close-server
   device(policy:1)-> set attack HIGH:HTTP:ANOM action close-server
   device(policy:1)-> set attack HIGH:HTTP:SIGS action close-server
   device(policy:1)-> set attack MEDIUM:HTTP:ANOM action close-server
   device(policy:1)-> set attack MEDIUM:HTTP:SIGS action close-server
   device(policy:1)-> set attack CRITICAL:FTP:SIGS action close-server
   device(policy:1)-> exit

5. **ポリシー ID 2**
   set policy id 2 from trust to dmz any websrv1 http permit attack
   CRITICAL:HTTP:ANOM action close
   set policy id 2
   device(policy:2)-> set dst-address websrv2
   device(policy:2)-> set service ftp
   device(policy:2)-> set service https
   device(policy:2)-> set service ping
   device(policy:2)-> set attack CRITICAL:HTTP:SIGS action close
   device(policy:2)-> set attack HIGH:HTTP:ANOM action close
   device(policy:2)-> set attack HIGH:HTTP:SIGS action close
   device(policy:2)-> set attack MEDIUM:HTTP:ANOM action close
   device(policy:2)-> set attack MEDIUM:HTTP:SIGS action close
   device(policy:2)-> set attack CRITICAL:FTP:SIGS action close
   device(policy:2)-> exit

6. **ポリシー ID 3**
   set policy id 3 from trust to untrust any any http permit attack
   CRITICAL:HTTP:ANOM action close-client
   set policy id 3
   device(policy:3)-> set service ftp-get
   device(policy:3)-> set service https
   device(policy:3)-> set service ping
   device(policy:3)-> set attack CRITICAL:HTTP:SIGS action close-client
   device(policy:3)-> set attack HIGH:HTTP:ANOM action close-client
   device(policy:3)-> set attack HIGH:HTTP:SIGS action close-client
   device(policy:3)-> set attack MEDIUM:HTTP:ANOM action close-client
   device(policy:3)-> set attack MEDIUM:HTTP:SIGS action close-client
   device(policy:3)-> set attack CRITICAL:FTP:SIGS action close-client
   device(policy:3)-> exit
   save

ブルートフォース攻撃アクション

典型的なブルートフォース攻撃は、ネットワークにアクセスするときに、さまざまなソースポートまたは IP を使用して大量のトラフィックを送信することによって行われます。将来の攻撃を効率的に防ぐために、ScreenOS では、ポリシーの各攻撃グループに IP アクションを関連付けることができます。

ブルートフォース攻撃は、DI 対応のプロトコルに設定されたしきい値に基づいて検出されます。たとえば、以下のとおりです。

set di service *protocol-name value*

DI アクションは別として、ブルートフォース攻撃アクションは、**IP action** コマンドを使用して、設定した期間、指定したターゲットに対して設定されます。セキュリティデバイスがブルートフォース攻撃を検出した場合、実行するアクションを次の中から選択します。

- Notify: セキュリティデバイスはイベントを記録しますが、タイムアウト設定に指定された期間、ターゲット定義に一致するそれ以降のトラフィックに対してアクションを実行しません。
- Block: セキュリティデバイスはイベントを記録し、タイムアウト設定に指定された期間、ターゲット定義に一致するそれ以降のすべてのトラフィックをドロップします。
- Close: セキュリティデバイスはイベントを記録し、タイムアウト設定に指定された期間、ターゲット定義に一致するそれ以降のすべてのトラフィックをドロップし、ソースアドレスと宛先アドレスに TCP トラフィックのリセット (RST) を送信します。

ブルートフォース攻撃オブジェクト

表 12 に、ScreenOS 5.4 のブルートフォース攻撃オブジェクトと IP アクションと連携して使用できるしきい値のパラメータを示します。

表 12: ブルートフォース攻撃オブジェクト

ブルートフォース攻撃名	パラメータ
HTTP Brute Force Login Attempt	failed_logins
HTTP Brute Search Attempt	brute_search
IMAP Brute Force Login Attempt	failed_logins
LDAP Brute Force Login Attempt	failed_logins
MS-RPC IsSystemActive request flood	設定不能 (試行回数 32)
MS-SQL Login Brute Force	設定不能 (試行回数 4)
POP3 Brute Force Login Attempt	failed_login
RADIUS Brute Force Authentication Attempt	failed_auth
SMB Brute Force Directory Create/Delete	設定不能 (試行回数 200)
SMB Brute Force Login Attempt	failed_login
FTP Brute Force Login Attempt	failed_login
Telnet Brute Force Login Attempt	failed_login
VNC Brute Force Login Attempt	failed_login

ブルートフォース攻撃ターゲット

ターゲットオプションは、セキュリティデバイスがパケットをブルートフォース攻撃の一部かどうか確認するために照合する必要がある要素セットを指定します。指定したタイムアウト期間中に到着する IP パケットの指定の要素セットは、後続のパケットが同じ攻撃の一部として確認されるように、セキュリティデバイスがブルートフォース攻撃の一部として検出したパケットの要素セットと一致する必要があります。デフォルトのターゲット定義は、Serv です。表 13 に表示されている次のいずれかのターゲット定義を選択できます。

表 13: ターゲットオプション

ターゲットオプション	照合要素
Serv	ソース IP、宛先 IP、宛先ポート、プロトコル
Src-IP	ソース IP アドレス
Zone-Serv	ソースセキュリティゾーン、宛先 IP、宛先ポート番号、プロトコル
Dst-IP	宛先 IP アドレス
Zone	ソースセキュリティゾーン (ingress インターフェースがバインドされるセキュリティゾーン。すなわち、攻撃パケットが発生したソースセキュリティゾーン)

ブルートフォース攻撃のタイムアウト

タイムアウトとは、ブルートフォース攻撃検出の後の期間で、セキュリティデバイスが指定されたターゲットパラメータに一致するパケットに対して IP アクションを実行します。デフォルトのタイムアウトは、60 秒です。

例 1

この例では、既存の DI アクション以外に、IP アクションをポリシーの各グループに設定します。以下の CLI コマンドは、ブルートフォース攻撃オブジェクト (HTTP Brute Force Login Attempt または HTTP Brute Force Search) を 45 秒間ブロックします。HIGH:HTTP:ANOM 攻撃グループの他のすべての攻撃が **close** の DI アクションで設定されています。

ScreenOS のこのリリースでは、サーバーからクライアントへのシグネチャ攻撃を構成する場合のみ、S2C HTTP プロトコルデコードは実行されます。ポリシーで HTTP サーバーからクライアントへのシグネチャ攻撃を構成する場合、サーバーからクライアントへのアノーマリ攻撃（HTTP:Brute-Force）が検出されます。次の例では、HTTP:HIGH:SIGS が、サーバーからクライアントへのシグネチャ攻撃をしています。そのため、ポリシーに HTTP:HIGH:ANOM と共に HTTP:HIGH:SIGS を追加します。

CLI

```
device> get attack group HIGH:HTTP:ANOM
GROUP "HIGH:HTTP:ANOM" is pre-defined.It has the following members
ID     Name
1674 HTTP:INVALID:INVLD-AUTH-CHAR
1675 HTTP:INVALID:INVLD-AUTH-LEN
1711 HTTP:OVERFLOW:HEADER
1713 HTTP:OVERFLOW:INV-CHUNK-LEN
1717 HTTP:OVERFLOW:AUTH-OVFLW
5394 HTTP:EXPLOIT:BRUTE-FORCE
5395 HTTP:EXPLOIT:BRUTE-SEARCH
device> set policy id 1 from Untrust to DMZ Any Any Any permit attack
    MEDIUM:HTTP:ANOM action none
device> set policy id 1 from Untrust to DMZ Any Any Any permit attack
    MEDIUM:HTTP:HIGH:SIGS action none
device> set policy id 1
device(policy:1)-> set attack HIGH:HTTP:ANOM action close ip-action block
    target dst-ip timeout 45
```

設定された攻撃グループにブルートフォース攻撃のプロトコルアノーマリが存在しない場合、IP アクションは実施されません。

例 2

この例では、設定した期間、指定したホストからの各攻撃グループに対して IP アクションを関連付けます。

```
set policy id 1 from trust to untrust any any any permit attack POP3 BRUTE FORCE
    Login Attempt action close ip-action notify target serv timeout 60
```

例 3

この例では、FTP ブルートフォースのログイン試行回数に対するデフォルトのしきい値は、8 回 / 分です。ユーザーのアカウント名とパスワードを調べるために、IP アドレスが 192.168.2.2 のユーザーが FTP ブルートフォースのログイン試行を 10.150.50.5 の FTP サーバーに対して行う場合、攻撃者が 1 分内に 8 回、FTP ログインしようとすると検出されます。

「serv」のターゲットで、120 秒間、IP アクションが「Block」に設定されている場合、192.168.2.2 (送信元 IP) から TCP (プロトコル) で 10.150.50.5 (宛先 IP) のポート 21 (宛先ポート) に送信されたトラフィックが 120 秒間ブロックされます。

一部の IP アクションのターゲットは、別のポリシーに一致するトラフィックに影響する場合があります。

攻撃のログ出力

検知した攻撃のログ出力は、攻撃グループごと、ポリシーごとに、有効 / 無効を切り替えることができます。したがって、同じポリシーの中で複数の攻撃グループを適用し、そのうち必要なものについてのみ、検知した攻撃をログ出力するよう設定できるのです。

デフォルトではログ出力が有効になっています。緊急度が低く、特に注意を払わなくても構わないと判断した攻撃については、ログ出力を無効にしてもよいでしょう。こうすることにより、重大な攻撃があったのに膨大なログの中に埋もれてしまっていて気がつかない、といった事故を防ぐことができます。

例 : 攻撃グループごとにログ出力を無効化

この例では、次の 5 つの攻撃グループをポリシーから参照しますが、1 つめと 2 つめのみログ出力するよう設定します。

- HIGH:IMAP:ANOM
- HIGH:IMAP:SIGS
- MEDIUM:IMAP:ANOM
- LOW:IMAP:ANOM
- INFO:IMAP:ANOM

このポリシーは、Trust ゾーンに属するホストから、DMZ に属する mail1 というメールサーバーに向かう IMAP トラフィックに適用されます。上記 5 つのグループに属する、定義済みの IMAP 攻撃オブジェクトに合致する攻撃を検知すると、セキュリティデバイスは接続を閉鎖 (close) します。しかしログは、1 つめまたは 2 つめのグループに属する攻撃オブジェクトに合致した場合にのみ出力します。

WebUI

1. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: mail1
   IP Address/Domain Name:
   IP/Netmask: (選択する),1.2.2.10/32
   Zone: DMZ

2. ポリシー

Policies > (From: Trust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), mail1
Service: IMAP
Action: Permit

> **Deep Inspection** をクリックし、次のように入力し、**Add** をクリックして各攻撃オブジェクトグループを追加します。その後 **OK** をクリックして基本ポリシー構成ページに戻ります。

Group: HIGH:IMAP:ANOM
Action: Close
Log: (**選択**)

Group: HIGH:IMAP:SIGS
Action: Close
Log: (**選択**)

Group: MEDIUM:IMAP:ANOM
Action: Close
Log: (**オフ**)

Group: LOW:IMAP:ANOM
Action: Close
Log: (**オフ**)

Group: INFO:IMAP:ANOM
Action: Close
Log: (**オフ**)

CLI

1. アドレス

```
set address dmz mail1 1.2.2.10/32
```

2. ポリシー

```
device-> set policy id 1 from trust to dmz any mail1 imap permit attack
    HIGH:IMAP:ANOM action close
device-> set policy id 1
device(policy:1)-> set attack HIGH:IMAP:SIGS action close
device(policy:1)-> set attack MEDIUM:IMAP:ANOM action close
device(policy:1)-> unset attack MEDIUM:IMAP:ANOM logging
device(policy:1)-> set attack LOW:IMAP:ANOM action close
device(policy:1)-> unset attack LOW:IMAP:ANOM logging
device(policy:1)-> set attack INFO:IMAP:ANOM action close
device(policy:1)-> unset attack INFO:IMAP:ANOM logging
device(policy:1)-> exit
device-> save
```

顧客サービスとアプリケーションのマッピング

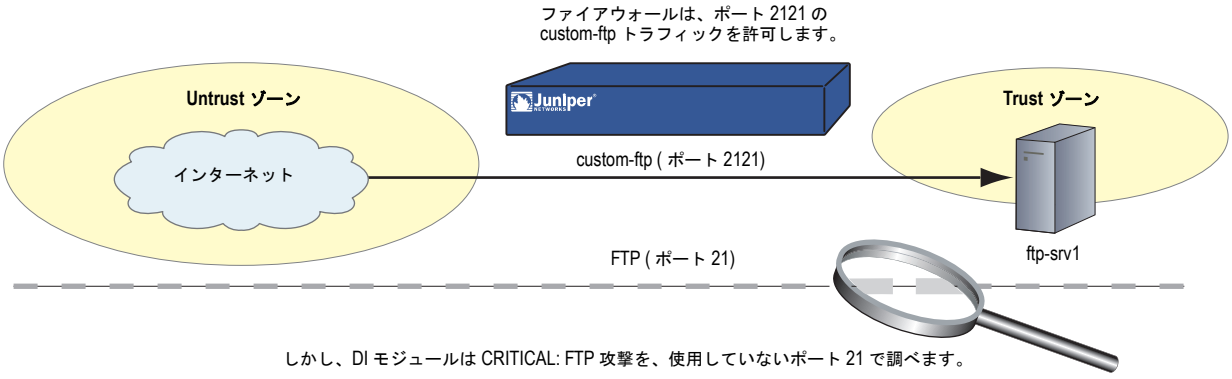
顧客サービスを徹底監視 (DI) コンポーネントをもつポリシー内で使用する場合、DI モジュールが適切に機能するようにその顧客サービス上で実行しているアプリケーションを明示的に指定する必要があります。たとえば、非標準ポート番号 2121 (図 52 を参照) 上で稼動する FTP の顧客サービスを作成する場合、ポリシー内でこの顧客サービスを次のように参照します。

```
set service ftp-custom protocol tcp src-port 0-65535 dst-port 2121-2121
set policy id 1 from untrust to trust any ftp-srv1 custom-ftp permit
```

ただし、DI コンポーネントを追加するポリシーが顧客サービスを参照する場合、このアプリケーションは非標準のポート番号を使用しているため DI モジュールが認識できません。

```
set policy id 1 from untrust to trust any ftp-srv1 custom-ftp permit attack
    CRITICAL:FTP:SIGS action close-server
```

図 52: 顧客サービスのマッピング



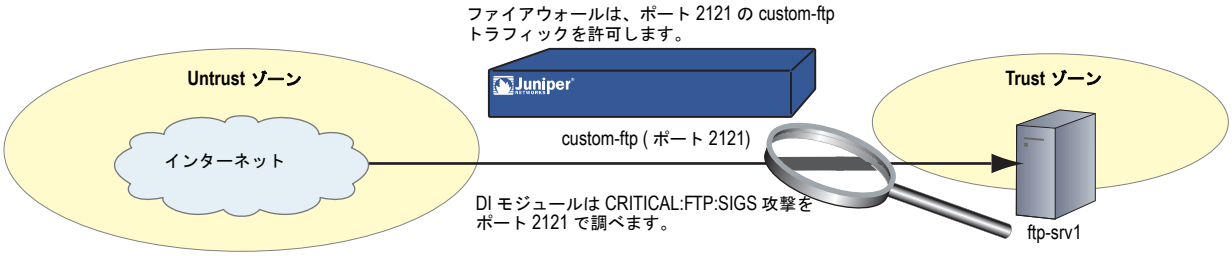
この問題を回避するため、FTP アプリケーションがポート 2121 で稼動していることを DI モジュールに知らせる必要があります (図 53 を参照)。本質的には、アプリケーション層のプロトコルをトランスポート層の特定ポートナンバーへマッピングする必要があります。そのためには、ポリシーレベルのバインディングを行います。

```
set policy id 1 application ftp
```

FTP アプリケーションを顧客サービス custom-ftp にマッピングし、DI がポリシーの中で FTP トラフィックを CRITICAL:FTP:SIGS 攻撃オブジェクトグループ内で定義された攻撃の有無について調べ、そのポリシーが custom-ftp を参照するように構成すると、DI モジュールはポート 2121 でその検査を実行します。

```
set policy id 1 from untrust to trust any ftp-srv1 custom-ftp permit attack
    CRITICAL:FTP:SIGS action close-server
set policy id 1 application ftp
```

図 53: 顧客サービスの攻撃オブジェクトグループへのマッピング



例 : アプリケーションと顧客サービスのマッピング

この例では、宛先ポート 8080 を使用する「HTTP1」という名の顧客サービスを定義します。Untrust ゾーンのあらゆるアドレスから DMZ ゾーンの「server1」という名の Web サーバーへの HTTP1 トラフィックを許可するポリシーのために、HTTP アプリケーションを顧客サービスにマップします。次に、8080 番ポートで待ち受ける HTTP トラフィックに対して、DI (徹底監視) を適用します。このポリシーに対する DI 設定は次のとおりです。

- 攻撃オブジェクトグループ :
  - CRITICAL:HTTP:ANOM, CRITICAL:HTTP:SIGS
  - HIGH:HTTP:ANOM, HIGH:HTTP:SIGS
  - MEDIUM:HTTP:ANOM, MEDIUM:HTTP:SIGS
- 攻撃オブジェクトグループに設定するアクション (すべて共通): Close Server
- ロギング : 有効 (デフォルト設定)

WebUI

1. **顧客サービス**
   Policy > Policy Elements > Services > Custom > New: 次のように入力してから **OK** をクリックします。

   Service Name: HTTP1
   Transport Protocol: TCP (選択)
   Source Port Low: 0
   Source Port High: 65535
   Destination Port Low: 8080
   Destination Port High: 8080

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: server1
   IP Address/Domain Name:
   IP Address/Netmask: 1.2.2.5/32
   Zone: DMZ

3. **ポリシー**
   Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Any
   Destination Address:
   Address Book Entry: (選択), server1
   Service: HTTP1
   Application: HTTP
   Action: Permit

   > **Deep Inspection** をクリックし、次のように入力し、**Add** をクリックして各攻撃オブジェクトグループを追加します。その後 **OK** をクリックして基本ポリシー構成ページに戻ります。

   Group: CRITICAL:HTTP:ANOM
   Action: Close Server
   Log: (選択)

   Group: CRITICAL:HTTP:SIGS
   Action: Close Client
   Log: (選択)

   Group: HIGH:HTTP:ANOM
   Action: Close Client
   Log: (選択)

   Group: HIGH:HTTP:SIGS
   Action: Close Client
   Log: (選択)

   Group: MEDIUM:HTTP:ANOM
   Action: Close Client
   Log: (選択)

   Group: MEDIUM:HTTP:SIGS
   Action: Close Client
   Log: (選択)

CLI

1. **顧客サービス**
   set service HTTP1 protocol tcp src-port 0-65535 dst-port 8080-8080

2. **アドレス**
   set address dmz server1 1.2.2.5/32

3. **ポリシー**
   device-> set policy id 1 from untrust to dmz any server1 HTTP1 permit attack CRITICAL:HTTP:ANOM action close-server
   device-> set policy id 1
   device(policy:1)-> set attack CRITICAL:HTTP:SIGS action close-server
   device(policy:1)-> set attack HIGH:HTTP:ANOM action close-server
   device(policy:1)-> set attack HIGH:HTTP:SIGS action close-server
   device(policy:1)-> set attack MEDIUM:HTTP:ANOM action close-server
   device(policy:1)-> set attack MEDIUM:HTTP:SIGS action close-server
   device(policy:1)-> exit
   device-> set policy id 1 application http
   save

例 : HTTP を悪用する攻撃に関するアプリケーションとサービスの対応づけ

HTTP を悪用した、よく知られている攻撃の中に、TCP の 8000 番ポートを狙うものがあります。この資料の執筆時点では、徹底監視 (DI) 攻撃オブジェクトデータベースに、これに当てはまる 2 種類の攻撃が登録されています。

- 3656, App: HP Web JetAdmin Framework Infoleak

  DOS:NETDEV:WEBJET-FW-INFOLEAK (攻撃オブジェクトグループ MEDIUM:HTTP:SIGS 内)

- 3638, App: HP Web JetAdmin WriteToFile Vulnerability

  DOS:NETDEV:WEBJET-WRITETOFILE (攻撃オブジェクトグループ CRITICAL:HTTP:SIGS 内)

しかしデフォルトでは、ScreenOS は HTTP が 80 番ポートを使うものと想定しています。したがってポート 8000 に対する TCP トラフィックがあっても、セキュリティデバイスは HTTP と認識しません。従って、DI エンジンはこれらの攻撃に対してそのような HTTP トラフィックをスキャンせず、発生した場合にも検出できません。ただし、ポート 8000 を使用して、顧客サービスへのアプリケーションとして HTTP をマッピングしている場合を除きます。

この例では、非標準ポート 8000 を HTTP に対応づけて、上記のような攻撃を検知できるようにします。

注 : HTTP に限らず、非標準ポートを使ってサービスを提供している場合、DI エンジンで攻撃を検知するためには、ポート番号とサービスとの対応づけが必要です。

WebUI

1. **顧客サービス**
   Policy > Policy Elements > Services > Custom > New: 次のように入力してから **OK** をクリックします。

   Service Name: HTTP2
   Transport Protocol: TCP (選択)
   Source Port Low: 0
   Source Port High: 65535
   Destination Port Low: 8000
   Destination Port High: 8000

2. **ポリシー**
   Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   　　Address Book Entry: (選択), Any
   Destination Address:
   　　Address Book Entry: (選択), Any
   Service: HTTP2
   Application: HTTP
   Action: Permit

> **Deep Inspection** をクリックし、次のように入力し、**Add** をクリックして各攻撃オブジェクトグループを追加します。その後 **OK** をクリックして基本ポリシー構成ページに戻ります。

Group: CRITICAL:HTTP:SIGS
Action: Close
Log: (選択)

Group: MEDIUM:HTTP:SIGS
Action: Close
Log: (選択)

CLI

1. **顧客サービス**
   set service HTTP2 protocol tcp src-port 0-65535 dst-port 8000-8000
2. **ポリシー**
   device-> set policy id 1 from untrust to dmz any any HTTP2 permit attack CRITICAL:HTTP:SIGS action close
   device-> set policy id 1
   device(policy:1)-> set attack MEDIUM:HTTP:SIGS action close
   device(policy:1)-> exit
   device-> set policy id 1 application http
   save

カスタマイズした攻撃オブジェクトとグループ

新しい攻撃オブジェクトおよびオブジェクトグループを定義すれば、徹底監視 (DI) アプリケーションがニーズに最も合うようにカスタマイズできます。攻撃オブジェクトは、ステートフル署名にすることも、(NetScreen-5000 では) TCP ストリームシグネチャにすることもできます。また、パラメータ設定により、定義済みのプロトコルアノーマリ攻撃オブジェクトを変更することも可能です。

ユーザー定義のステートフルシグネチャ攻撃オブジェクト

FTP、HTTP、および SMTP のステートフル署名攻撃オブジェクトを作成できます。攻撃オブジェクトを作成するときは、次の手順を実行します。

- 攻撃オブジェクトに名前を付けます。(ユーザー定義の攻撃オブジェクトはすべて“CS:”で始めます。)
- DI 検索のコンテキストを設定します (攻撃オブジェクトを作成する際に使えるコンテキストの一覧は、A ページ の「ユーザー定義シグネチャのコンテキスト」を参照してください)。
- シグネチャを定義します。(159 ページの「正規表現」に、シグネチャの定義に使える正規表現を解説します)。
- 攻撃オブジェクトに重大度レベルを割り当てます。(重大度レベルについては、137 ページの「重大度レベルの変更」を参照してください。)

次に、ユーザー定義攻撃オブジェクトを、ポリシーで使用するためにユーザー定義攻撃オブジェクトグループに加える必要があります。

注 : ユーザー定義攻撃オブジェクトグループに加えることができるのは、ユーザー定義攻撃オブジェクトのみです。定義済み攻撃オブジェクトとユーザー定義攻撃オブジェクトは、同じ攻撃オブジェクトグループ内で一緒にできません。

正規表現

シグネチャのテキスト文字列を入力するときは、通常文字の英数字文字を入力して文字と文字の完全一致を探したり、正規表現を使用して文字セットに可能な限り一致するよう検索範囲を広げることができます。ScreenOS は、表 14 に表示される次の正規表現に対応しています。

表 14: ScreenOS でサポートされる正規表現

目的	メタ文字	例	意味
直接バイナリ一致 (8 進数)[1]	\O*octal_number*	\0162 一致文字 : 162	この 8 進数 162 に完全一致です。
直接バイナリ一致 (16 進数)[2]	\X*hexadecimal_number*\X	\X01 A5 00 00\X 一致文字 : 01 A5 00 00	次の 4 つの 16 進数に完全一致です : 01 A5 00 00
大文字小文字を区別しない一致	\[*characters*\]	\[cat\] 一致文字 : ■ Cat, cAt, caT ■ CAt, CaT, CAT ■ cat, cAt	cat の文字で一致し、各文字の大文字小文字の区別を無視します。
あらゆる文字に一致	.	c . t 一致文字 : ■ cat, cbt, cct, … czt ■ cAt, cBt, cCt, … cZt ■ c1t, c2t, c3t, … c9t	c- あらゆる文字 -t に一致します。
直前の文字が 1 度だけではなく、0 回または複数回出現する場合に一致	*	a*b + c 一致文字 : ■ bc ■ bbc ■ abc ■ aaabbbbc	0 個、1 個または複数個の a、その後に 1 個または複数個の b、その後に 1 個の c が続く文字列に一致します。
直前の文字が 1 回または複数回出現する場合に一致	+	a + b + c 一致文字 : ■ abc ■ aabc ■ aaabbbbc	1 個または複数個の a、その後に 1 個または複数個の b、その後に 1 個の c が続く文字列に一致します。
直前の文字が 0 回または 1 回出現する場合に一致	?	drop-?packet 一致文字 : ■ drop-packet ■ droppacket	drop-packet と droppacket のどちらでも一致します。
グループ式	( )		

目的	メタ文字	例	意味
すぐ前の文字とすぐ後の文字のどちらか — は ( ) と共に使用	|	(drop | packet) 一致文字 : ■ drop ■ packet	drop と packet のどちらでも一致します。
文字範囲	[*start-end*]	[c-f]a(d | t) 一致文字 : ■ cad, cat ■ dad, dat ■ ead, eat ■ fad, fat	最初の文字が c、d、e、または f で始まり、真ん中の文字が a、最後の文字が d または t の文字列すべてに一致します。
すぐ後の文字を否定	[^*character*]	[^0-9A-Z] 一致文字 : a, b, c, d, e, … z	小文字に一致します。

1.8 進数は、0 ～ 7 までの数字のみ使用する 8 進法です。
2.16 進数は、通常の数字 0 ～ 9、および 10 進数で 10 ～ 15 にあたる 16 進数を表わす文字 A ～ F を使用する、16 進法です。

例 : ユーザー定義のステートフル署名攻撃オブジェクト

この例では、FTP サーバー、Web サーバー、メールサーバーが DMZ ゾーンにあります。ユーザー定義のシグネチャオブジェクトに対する次の攻撃オブジェクトを、表 15 に表示されているように定義します。

表 15: ユーザー定義のステートフルシグネチャ攻撃オブジェクト

オブジェクト名	処理
cs:ftp-stor	FTP サーバーに誰かがファイルを入れるのを阻止する
cs:ftp-user-dm	dmartin のログイン名を持つユーザーの FTP アクセスを拒否する
cs:url-index	あらゆる HTTP 要求の中で定義済み URL を持つ HTTP パケットを阻止する
cs:spammer	「spam.com」のあらゆる E メールアドレスからの E メールを阻止する

次にこれらのオブジェクトを 泥 MZ DIi という名前のユーザー定義攻撃オブジェクトグループの中に組み入れ、このグループを Untrust ゾーンから DMZ ゾーン内のサーバーへのトラフィックを許可するポリシーで参照します。

WebUI

1. **攻撃オブジェクト 1: ftp-stor**
   Objects > Attacks > Custom > New: 次のように入力してから **OK** をクリックします。

   Attack Name: cs:ftp-stor
   Attack Context: FTP Command
   Attack Severity: Medium
   Attack Pattern: STOR

2. **攻撃オブジェクト 2: ftp-user-dm**
   Objects > Attacks > Custom > New: 次のように入力してから **OK** をクリックします。

   Attack Name: cs:ftp-user-dm
   Attack Context: FTP User Name
   Attack Severity: Low
   Attack Pattern: dmartin

3. **攻撃オブジェクト 3: url-index**
   Objects > Attacks > Custom > New: 次のように入力してから **OK** をクリックします。

   Attack Name: cs:url-index
   Attack Context: HTTP URL Parsed
   Attack Severity: High
   Attack Pattern: .*index.html.*

4. **攻撃オブジェクト 4: spammer**
   Objects > Attacks > Custom > New: 次のように入力してから **OK** をクリックします。

   Attack Name: cs:spammer
   Attack Context: SMTP From
   Attack Severity: Info
   Attack Pattern: .*@spam.com

5. **攻撃オブジェクトグループ**
   Objects > Attacks > Custom Groups > New: 次のグループ名を入力し、次のカスタム攻撃オブジェクトを移動してから **OK** をクリックします。

   Group Name: CS:DMZ DI

   cs:ftp-stor を選択し、< < ボタンを使ってアドレスを Available Members 列から Selected Members 列へ移動します。

   cs:ftp-user-dm を選択し、< < ボタンを使ってアドレスを Available Members 列から Selected Members 列へ移動します。

   cs:url-index を選択し、< < ボタンを使ってアドレスを Available Members 列から Selected Members 列へ移動します。

   cs:spammer を選択し、< < ボタンを使ってアドレスを Available Members 列から Selected Members 列へ移動します。

6. **ポリシー**
   Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   　　Address Book Entry: (**選択**), Any
   Destination Address:
   　　Address Book Entry: (**選択**), Any
   Service: HTTP

> **Multiple** をクリックし、**FTP** を選択してから、**OK** をクリックして基本ポリシー構成ページに戻ります。

Action: Permit

> **Deep Inspection** をクリックし、次のように入力し、**Add** をクリックして各攻撃オブジェクトグループを追加します。その後 **OK** をクリックして基本ポリシー構成ページに戻ります。

Group: CS:DMZ DI
Action: Close Server
Log: (選択)

CLI

1. **攻撃オブジェクト 1: ftp-stor**
   set attack cs:ftp-stor ftp-command STOR severity medium
2. **攻撃オブジェクト 2: ftp-user-dm**
   set attack cs:ftp-user-dm ftp-username dmartin severity low
3. **攻撃オブジェクト 3: url-index**
   set attack cs:url-index http-url-parsed index.html severity high
4. **攻撃オブジェクト 4: spammer**
   set attack cs:spammer smtp-from .*@spam.com severity info
5. **攻撃オブジェクトグループ**
   set attack group “CS:DMZ DI”
   set attack group “CS:DMZ DI” add cs:ftp-stor
   set attack group “CS:DMZ DI” add cs:ftp-user-dm
   set attack group “CS:DMZ DI” add cs:url-index
   set attack group “CS:DMZ DI” add cs:spammer
6. **ポリシー**
   set policy id 1 from untrust to dmz any any http permit attack “CS:DMZ DI” action close-server
   set policy id 1
   device(policy:1)-> set service ftp
   device(policy:1)-> exit
   save

TCP ストリームシグネチャ攻撃オブジェクト

ステートフルシグネチャは、FTP ユーザー名や SMTP ヘッダーフィールドのように、特定アプリケーション内でコンテキストに基づいています。TCP ストリームシグネチャはパターンをあらゆる種類の TCP トラフィック内で、使用しているアプリケーションプロトコルに関係なく探します。

注 : TCP ストリームシグネチャは、NetScreen-5000 シリーズシステムでのみ定義できます。

定義済みの TCP ストリームシグネチャ攻撃オブジェクトがないため、自分で定義する必要があります。シグネチャ攻撃オブジェクトを作成するときは、次のコンポーネントを定義します。

- 攻撃オブジェクト名 (すべてのユーザー定義攻撃オブジェクトは “CS:” で始めて下さい)。
- オブジェクトタイプ (“stream”)
- パターン定義
- 重大度レベル

図 54: TCP ストリームシグネチャ攻撃オブジェクトの例



例 : ユーザー定義のストリームシグネチャ攻撃オブジェクト

この例では、ストリームシグネチャオブジェクト .*satori.* を定義します。CS:A1 の名前を付けて、重大度レベルを Critical に定義します。ポリシーは攻撃オブジェクトグループしか参照できないため、CS:Gr1 という名のグループを作成し、定義したオブジェクトをこのグループに追加します。最後に CS: Gr1 を参照するポリシーを定義し、さらにこのポリシーを適用するトラフィックの中に定義したパターンが出現した場合に接続の切断とクライアントへの TCP RST 送信をセキュリティデバイスに命令するようこのポリシーを定義します。

WebUI

1. **ストリームシグネチャ攻撃オブジェクト**
   Objects > Attacks > Custom > New: 次のように入力してから **OK** をクリックします。

   Attack Name: CS:A1
   Attack Context: Stream
   Attack Severity: Critical
   Attack Pattern: .*satori.*

2. **ストリームシグネチャ攻撃オブジェクトグループ**
   Objects > Attacks > Custom Groups > New: 次のように入力してから **OK** をクリックします。

   Group Name: CS:Gr1

   Available Members 列の **CS:A1** を選択してから < < をクリックして Selected Members 列へ移動します。

3. **ポリシー**
   Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Any
   Destination Address:
   Address Book Entry: (選択), Any

Service: ANY
Action: Permit

> **Deep Inspection** をクリックし、次のように入力し、**Add** をクリックして各攻撃オブジェクトグループを追加します。その後 **OK** をクリックして基本ポリシー構成ページに戻ります。

Group: CS:Gr1
Action: Close Client
Log: (選択)

CLI

1. **ストリームシグネチャ攻撃オブジェクト**
   set attack “CS:A1” stream “.*satori.*” severity critical
2. **ストリームシグネチャ攻撃グループ**
   set attack group “CS:Gr1”
   set attack group “CS:Gr1” add “CS:A1”
3. **ポリシー**
   set policy from trust to untrust any any any permit attack CS:Gr1 action close-client save

プロトコルアノーマリパラメータの構成

プロトコルアノーマリ攻撃オブジェクトのパラメータは変更可能です。Juniper ではプロトコルアノーマリ攻撃オブジェクトを、RFC で定義されている標準的なプロトコルやその一般的な拡張に基づいて定義しています。個別の実装にそって定義しているわけではありません。あるプロトコルアノーマリ攻撃オブジェクトを適用したとき、正当なトラフィックを攻撃と誤認識することが多いようであれば、パラメータを適宜変更して、正しく認識するよう調整するとよいでしょう。

注 : 設定可能なパラメータの一覧は、*ScreenOS CLI Reference Guide: IPv4 Command Descriptions* の **di** コマンドを参照してください。

例 : パラメータの変更

この例では、次のパラメータの値を増やして、デフォルト状態よりも誤認識を減らします。

プロトコルパラメータ	デフォルト	新しい
SMB - 分毎のログイン失敗最大数	4 回	8 回
Gnutella - TTL (生存時間) ホップの最大数	8 ホップ	10 ホップ

また、次のパラメータの値を減らして、デフォルト状態では攻撃と認識し損なう場合でも、正しく検知できるようにします。

プロトコルパラメータ	デフォルト	新しい
AOL Instant Messenger (AIM) - OFT (OSCAR File Transfer) ファイル名の最大長 ただし OSCAR とは Open System for Communication in Real-time の略で、AIM クライアントが使うプロトコルです。	10,000 バイト	5,000 バイト
AOL Instant Messenger - FLAP フレームの最大長 (常に 6 バイトの FLAP ヘッダー + データ) OSCAR は FLAP プロトコルを使って接続し、AIM クライアントとのチャネルを開きます。	10,000 バイト	5,000 バイト

WebUI

注 : プロトコルアノーマリパラメータの変更には CLI を使う必要があります。

CLI

```
set di service smb failed_logins 8
set di service gnutella max_ttl_hops 10
set di service aim max_flap_length 5000
set di service aim max_oft_frame 5000
save
```

否定

攻撃オブジェクトは、通常、悪意による異常な動作を検知するためのパターンとして使います。しかしこれとは逆に、問題のない、正当な動作を表すパターンとしての使い方も可能です。この場合、あるパターンに合致しないトラフィックがあれば、問題があると判断することになります。攻撃オブジェクトをこのように使う場合、検知の論理を「否定」する必要があります。

攻撃オブジェクト否定の有効な使い方の例としては、正しいユーザー名とパスワードを与えたもの以外のログインをブロックする、というものがあります。正当でないユーザー名とパスワードをすべて定義するのは困難ですが、逆に正しい組み合わせだけを定義し、それ以外のものを攻撃と判断するのは容易です。つまり、ある攻撃オブジェクトに合致するもの以外を攻撃と見なす、ということです。

例 : 攻撃オブジェクトの否定

この例 (図 55 を参照) では、2 つの攻撃オブジェクトを定義します。ひとつは FTP サーバーにログインできる正しいユーザー名を指定したもの、もうひとつは正しいパスワードを設定したものです。こうしておいて、攻撃オブジェクトの否定を適用すると、セキュリティデバイスは設定された以外のユーザー名とパスワードによるログインをすべてブロックするようになります。

例では次のような条件を想定します。

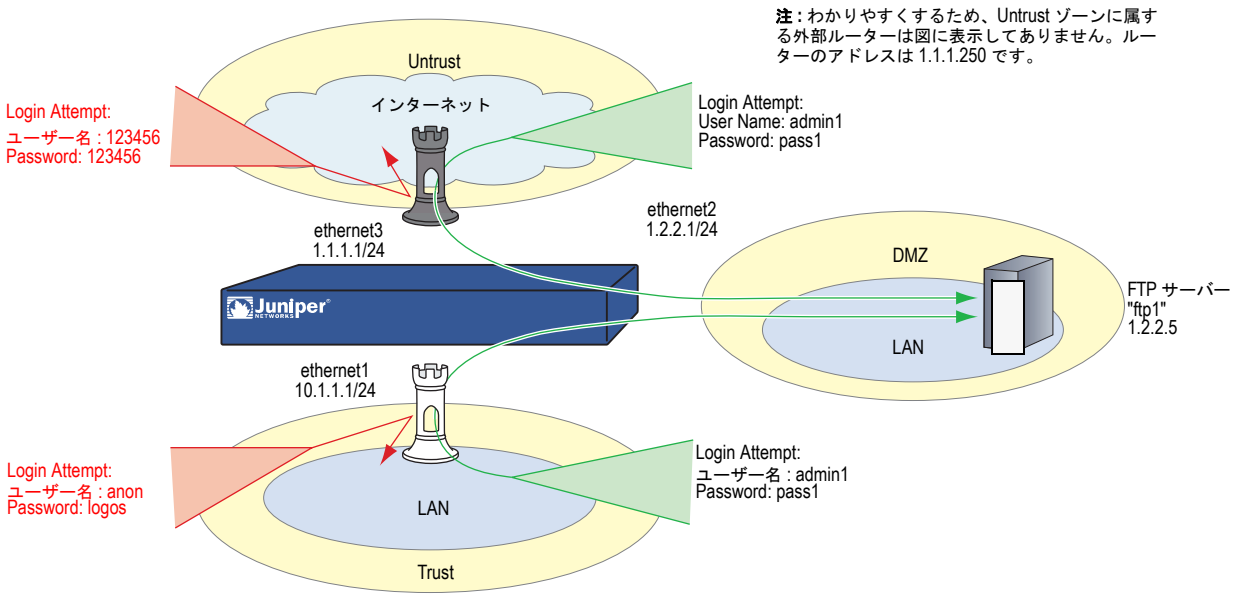
- 正当なユーザー名は *admin1*、そのパスワードは *pass1* です。
- FTP サーバーは DMZ ゾーンにあり、そのアドレスは 1.2.2.5 です。サーバー名は *ftp1* です。
- Untrust ゾーンおよび Trust ゾーンに属するホストからサーバーへの FTP トラフィックを徹底監視します。
- セキュリティゾーンはすべて trust-vr ルーティングドメインにあります。

次の 2 つの攻撃オブジェクトを作成します。

- 攻撃オブジェクト 1:
  - Name: CS:FTP1_USR_OK
  - Negation: enabled
  - Context: ftp-username
  - Pattern: admin1
  - Severity: high
- 攻撃オブジェクト 2:
  - Name: CS:FTP1_PASS_OK
  - Negation: enabled
  - Context: ftp-password
  - Pattern: pass1
  - Severity: high

この 2 つのオブジェクトを *CS:FTP1_LOGIN* という攻撃オブジェクトグループに登録します。次に、Trust ゾーンおよび Untrust ゾーンに属するホストから、DMZ にある ftp1 への FTP トラフィックを許可する、2 つのポリシーからこのグループを参照するようにします。

図 55: 攻撃オブジェクトの否定



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24

   次のように選択してから **OK** をクリックします。

   Interface Mode: NAT (選択)

注 : デフォルトでは、Trust ゾーンにバインドされたどのインターフェースも NAT モードになっています。そのため、Trust ゾーンにバインドされたインターフェースではこのオプションはすでに有効にしています。

Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

Zone Name: DMZ
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.2.2.1/24

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: ftp1
   IP Address/Domain Name:
   IP/Netmask: (選択), 1.2.2.5/32
   Zone: DMZ

3. **攻撃オブジェクト 1: CS:FTP1_USR_OK**
   Objects > Attacks > Custom > New: 次のように入力してから **OK** をクリックします。

   Attack Name: CS:FTP1_USR_OK
   Attack Context: ftp-username
   Attack Severity: High
   Attack Pattern: admin1
   Pattern Negation: (選択)

4. **攻撃オブジェクト 2: CS:FTP1_PASS_OK**
   Objects > Attacks > Custom > New: 次のように入力してから **OK** をクリックします。

   Attack Name: CS:FTP1_PASS_OK
   Attack Context: ftp-password
   Attack Severity: High
   Attack Pattern: pass1
   Pattern Negation: (選択)

5. **攻撃オブジェクトグループ**
   Objects > Attacks > Custom Groups > New: 次のグループ名を入力し、次のカスタム攻撃オブジェクトを移動してから **OK** をクリックします。

   Group Name: CS:FTP1_LOGIN

   CS:FTP1_USR_OK を選択し、< < ボタンを使ってアドレスを Available Members 列から Selected Members 列へ移動します。

   CS:FTP1_PASS_OK を選択し、< < ボタンを使ってアドレスを Available Members 列から Selected Members 列へ移動します。

6. **ルート**
   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選択)
   Interface: ethernet3
   Gateway IP Address: (選択), 1.1.1.250

7. ポリシー

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), ftp1
Service: FTP
Action: Permit

> **Deep Inspection** をクリックし、次のように入力し、**Add** をクリックして各攻撃オブジェクトグループを追加します。その後 **OK** をクリックして基本ポリシー構成ページに戻ります。

Group: CS:FTP1_LOGIN
Action: 破棄
Log: (選択)

Policies > (From: Trust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), ftp1
Service: FTP
Action: Permit

> **Deep Inspection** をクリックし、次のように入力し、**Add** をクリックして各攻撃オブジェクトグループを追加します。その後 **OK** をクリックして基本ポリシー構成ページに戻ります。

Group: CS:FTP1_LOGIN
Action: 破棄
Log: (選択)

CLI

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet2 zone dmz
set interface ethernet2 ip 1.2.2.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. アドレス

```
set address dmz ftp1 1.2.2.5/32
```

3. 攻撃オブジェクト

```
set attack CS:FTP1_USR_OK ftp-username not admin1 severity high
set attack CS:FTP1_PASS_OK ftp-password not pass1 severity high
set attack group CS:FTP1_LOGIN
set attack group CS:FTP1_LOGIN add CS:FTP1_USR_OK
set attack group CS:FTP1_LOGIN add CS:FTP1_PASS_OK
```

4. **Route**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

5. **ポリシー**
   set policy from untrust to dmz any ftp1 ftp permit attack CS:FTP1_LOGIN action drop
   set policy from trust to dmz any ftp1 ftp permit attack CS:FTP1_LOGIN action drop
   save

HTTP コンポーネントの細分ブロッキング

Juniper Networks セキュリティデバイスは、HTTP を経て送信された ActiveX コントロール、Java アプレット、.zip ファイル、および .exe ファイルを選択的に阻止できます。これらのコンポーネントがネットワークのセキュリティにもたらす危険性とは、信頼できない者がこれらのコンポーネントを読み込んで保護されたネットワーク内のホストのアプリケーションを制御可能にしてしまうということです。

セキュリティゾーン内でこれらのコンポーネントのブロッキングを有効にすると、セキュリティデバイスはこのセキュリティゾーンと接続したインターフェースに届くすべての HTTP ヘッダーを調べます。ヘッダーでリストされたコンテンツ形式は、ターゲットとするコンポーネントがパケットペイロード内にあることを示しているかどうかを調べます。コンテンツ形式が Java、.exe、または .zip でありセキュリティデバイスがこれらの HTTP コンポーネント形式をブロックするよう構成されていれば、デバイスはそのパケットをブロックします。コンテンツ形式に特定のコンポーネント形式でなく「octet stream」のみがリストされる場合、デバイスはペイロード内のファイル形式を調べます。ファイル形式が Java、.exe、または .zip であり、デバイスがこれらのコンポーネント形式をブロックするよう構成されていれば、デバイスはそのパケットをブロックします。

ActiveX コントロールのブロッキングを有効にすると、デバイスはペイロードにあるすべてのタイプの HTTP コンポーネントを含むすべての HTTP パケットをブロックします (ActiveX コントロール、Java アプレット、.exe ファイル、または .zip ファイルなど)。

注 : ActiveX ブロッキングを有効にすると、セキュリティデバイスは Java アプット、.exe ファイル、および .zip ファイルを、これらが ActiveX コントロールに含まれていてもいなくてもブロックします。

ActiveX コントロール

Microsoft ActiveX テクノロジは、Web 設計者が動的で対話式 Web ページを作成するためのツールを提供します。ActiveX コントロールは、異なるプログラム同士による情報のやりとりを可能にするコンポーネントです。たとえば、ActiveX を導入することでブラウザはスプレッドシートを開いたり、バックエンドデータベースの中にある自分の個人アカウントを表示することができます。ActiveX コンポーネントには、Java アプレットや .exe ファイル、.zip ファイルなど別のコンポーネントが含まれることもあります。

ActiveX 対応の Web サイトを開くと、ActiveX コントロールをコンピュータにダウンロードするよう求めるメッセージが表示されます。Microsoft は、ダウンロード可能な ActiveX コードを証明した企業やプログラマの名前を表示するポップアップメッセージを提供しています。このコードの供給元を信頼できる方は、このコントロールのダウンロードへ進むことができます。供給元を信頼できない方は、ダウンロードを辞退できます。

ActiveX コントロールをコンピュータにダウンロードすると、コントロールの作成者がこのコントロールに実行させようとしたあらゆることをこのコンピュータは実行できます。これが不正なコードであれば、ハードディスクを再フォーマットしたり、すべてのファイルを削除したり、個人的な E メールを上司へ送信するなどのことができます。

Java アプレット

ActiveX と同様に、Java アプレットも Web ページが他のプログラムと情報をやり取りできるようにすることでその機能を向上させます。Java アプレットは、使用しているコンピュータの Java 仮想マシン (VM) にダウンロードします。Java の初期バージョンでは、仮想マシンに Java アプレットとコンピュータの他のリソースがやりとりできるようにする機能はありませんでした。Java 1.1 から、これらの制限事項のいくつかは緩和され、機能が向上しています。その結果、Java アプレットは現在仮想マシン外部のローカルリソースにアクセスできます。攻撃者は Java アプレットをプログラミングして仮想マシン外部を操作できるため、ActiveX コントロールと同様のセキュリティ脅威をもたらします。

EXE ファイル

Web 上で入手した実行ファイル (.exe 拡張子の付いたファイル) をダウンロードして実行する場合、そのファイルが汚染されていないという保証はありません。この実行ファイルをダウンロードしたサイトが信頼できるサイトであっても、このサイトからのダウンロード要求を嗅ぎ付けた何者かがあなたの要求をキャッチして、不正なコードが入った .exe ファイルに改ざんして返すという可能性があります。

ZIP ファイル

zip ファイル (.zip 拡張子の付いたファイル) は、圧縮したファイルを 1 つ以上含むファイルの形式です。.exe ファイルをダウンロードすることの危険性は .exe ファイルに関する前のセクションで説明しましたが、.zip ファイルはいくつもの .exe ファイルを含むことができるためそのまま .zip ファイルにも当てはまります。

例 : Java アプレットと .exe ファイルのブロッキング

この例では、Untrust ゾーンインターフェースに届きパケット内に Java アプレットと .exe ファイルが含まれるあらゆる HTTP トラフィックをブロックします。

WebUI

Screening > Screen (Zone: Untrust): **Block Java Component** および **Block EXE Component** を選択して、**Apply** をクリックします。

CLI

```
set zone untrust screen component-block jar
set zone untrust screen component-block exe
save
```

第 6 章

侵入探知と阻止

通常、*ファイアウォール*と呼ばれる侵入防止システム（IDP）は、ネットワークトラフィック中の攻撃を検出し防止するのに使用されます。ファイアウォールは、周囲および境界を保護しますが、許可されたトラフィックは、検知するようにファイアウォールが設計されていない攻撃を隠すことができます。

Juniper Networks 侵入検出・予防（IDP）技術は、ネットワークのインラインに配備されると、攻撃を検知し防止できます。IPS 単独の場合と異なり、IDP は、複数の方式を使用して、ネットワークに対する攻撃を検知し、攻撃者がアクセスポリシーを得し、損害を与えるのを妨げます。IDP は、不正なパケットや接続を、攻撃がネットワークに侵入する前に除去できます。IDP は、誤検知を削減し、本当に不正なトラフィックだけを検知し停止するように設計されています。また、パッシブなスニッファーとしても IDP を配備できます。その機能は、従来の IPS に似ていますが、精度および扱いやすさが向上しています。

本章のセクションは、以下のようになります。

- 174 ページの「IDP 対応のセキュリティデバイス」
- 175 ページの「IDP 対応デバイスでのトラフィックフロー」
- 176 ページの「侵入探知と阻止の構成」
- 184 ページの「セキュリティポリシーの構成」
- 185 ページの「IDP ルールベースの使用」
- 187 ページの「ファイアウォールルールで IDP を使用可能にする」
- 189 ページの「IDP ルールの構成」
- 202 ページの「免除ルールの構成」
- 207 ページの「バックドアルールの構成」
- 212 ページの「IDP 攻撃オブジェクトの構成」
- 230 ページの「デバイスをスタンドアロンの IDP デバイスとして構成する」
- 234 ページの「IDP の管理」

IDP 対応のセキュリティデバイス

ScreenOS は、限られたセキュリティデバイスだけで IDP 機能をサポートします。限られたセキュリティデバイスにインストールされたオプションのコンポーネントである、セキュリティモジュールが、IDP 機能を提供するからです。

ファイアウォールまたは仮想プライベートネットワーク（VPN）機能だけを持ったセキュリティデバイスを購入した場合、次を行うことにより、デバイスを IDP 対応のシステムにアップグレードできます。

- Advanced および IDP の両ライセンスキーのインストール
- ブートローダーのアップグレード
- IDP 対応バージョンの ScreenOS のインストール
- システムメモリのアップグレード
- セキュリティモジュールのインストール

注： IDP ライセンスキーをインストールすると、ScreenOS 徹底監視（DI）機能は使用できなくなります。

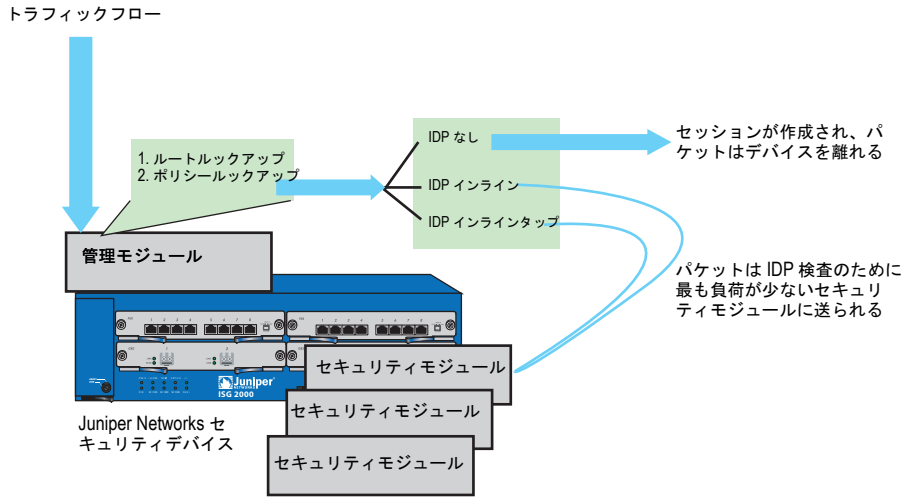
IDP 機能を含むデバイスをアップグレードする方法は、*ISG 2000 and ISG 1000 Field Upgrade* ドキュメントを参照してください。

IDP 対応のセキュリティデバイスは、インターネットとユーザーのプライベートネットワークの間のトラフィックを遮断するだけでなく、アプリケーションレベルのセキュリティを提供する、ファイアウォール /VPN/IDP が完全に統合されたセキュリティシステムとして使用できます。また、プライベートネットワークの重要なセグメントを保護するためのスタンドアロンの IDP システムとしても、このデバイスを使用できます。詳細については、230 ページの「デバイスをスタンドアロンの IDP デバイスとして構成する」を参照してください。

IDP 対応デバイスでのトラフィックフロー

このセクションでは、IDP 対応セキュリティデバイスでのパケットフローについて説明します。デバイスの ASIC プロセッサはパケットを受信し、セッションテーブルをチェックして、マッチが見つからない場合、管理モジュールへパケットを転送します。図 56 は、管理モジュールからセキュリティモジュールまでのパケットフローを示します。管理モジュールは、ファイアウォールポリシーに対してパケットをチェックします。IDP が有効な場合、トラフィックは、パケットについての IDP 分析を実行する、最も負荷が少ないセキュリティモジュールに転送されます。

図 56: セキュリティデバイスのトラフィックフロー



デュアル CPU から構成される各セキュリティモジュールは、自身のセッションテーブルを維持しています。デュアル CPU により、各セキュリティモジュールは、モジュール当たり IDP の 2 つのインスタンスを実行できます。**get sm status** コマンドは、各セキュリティモジュールのデュアル CPU を表示します（179 ページ を参照）。

インラインタップモード構成では、IDP セキュリティモジュールは、トラフィックをパッシブに監視できます。インラインタップモードでは、内部タップは、IDP 処理のためにセキュリティモジュールへトラフィックフローの各パケットのコピーを送ります。同時に、ASIC モジュールはインラインのトラフィック上でファイアウォール /VPN 処理を実行します。

攻撃オブジェクトが検出された場合、セッションテーブルをクリアするため、"close" オプションで TCP リセットが行われます。ルールに一致する各攻撃に対して、現在の攻撃パケットまたは接続を無視する、ドロップする、または閉じるという選択ができます。攻撃オブジェクトが見つかると、どのアクションを実行するかについての詳細は、197 ページの「アクションの定義」を参照してください。

侵入探知と阻止の構成

このセクションでは、セキュリティデバイス上で IDP を構成する 3 つの基本的な例を示します。

- 177 ページの「例 1: IDP の基本構成」
- 180 ページの「例 2: アクティブ / パッシブフェールオーバー向けの IDP の構成」
- 182 ページの「例 3: アクティブ / アクティブフェールオーバー向けの IDP の構成」

構成の前に

デバイス上で IDP を構成し始める前に、次の点を確認する必要があります。

- 構成するセキュリティデバイスが IDP 対応である。詳細については、174 ページの「IDP 対応のセキュリティデバイス」を参照してください。
- 管理ステーションに NetScreen-Security Manager（NSM）システムをインストールし構成している。

注： ScreenOS の CLI または WebUI を使用して、基本的なデバイスの構成を実行できますが、セキュリティデバイスで IDP を構成し管理するため、NSM が必要です。

NetScreen-Security Manager は、統合ポリシー管理を提供します。各セキュリティデバイスは、ネットワークで許可されるトラフィックのタイプおよびトラフィックがネットワーク内部で処理される方法を定義するルールを含んだ、1 つのセキュリティポリシーにリンクされています。

- そのデバイス用のセキュリティポリシーがあるわけです。NetScreen-Security Manager で提供されているデフォルトのセキュリティポリシーを使用できます。または、デバイスのファイアウォール /VPN 機能について、カスタムセキュリティポリシーを作成できます。

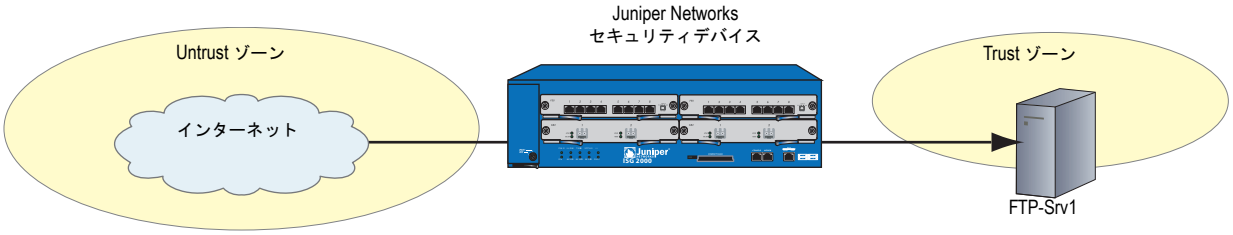
例 1: IDP の基本構成

この例では、Juniper Networks デバイスは、ファイアウォール /VPN/IDP の機能を備えています。構成を始める前に、174 ページの「IDP 対応のセキュリティデバイス」で説明したように、デバイスが IDP 対応であることを確認してください。図 57 で示したようにデバイスをセットアップして、次を行います。

1. ネットワークコンポーネントを物理的に接続します。

2. CLI、WebUI または NetScreen-Security Manager UI を使用して、IDP が保護するネットワークコンポーネントを追加します。

図 57: 基本的な IDP 用のデバイスのセットアップ



これらのコンポーネントは、ルータ、サーバー、ワークステーション、サブネットワークなどの、ユーザーのネットワークに接続されたオブジェクトでもかまいません。NetScreen-Security Manager では、これらのネットワークコンポーネントは*アドレスオブジェクト*として表現されます。複数のアドレスオブジェクトを表す、アドレスオブジェクト*グループ*を作成することもできます。アドレスオブジェクトの作成に関する詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。

3. そのデバイスに適切なファイアウォールルールで IDP（デフォルトはインラインモード）を使用可能にします。

   この手順は、CLI、Web UI または NetScreen-Security Manager UI を使用して実行できます。CLI コマンドを下に示します（NSM を使用した構成は、187 ページの「ファイアウォールルールで IDP を使用可能にする」を参照してください）。

```
device-> get policy
Total regular policies 5, Default deny.
ID From     To       Src-address  Dst-address  Service  Action State   ASTLCB
9 Trust     Untrust  Any          Any          MAIL     Permit  enabled --X-X
4 blade1    dmz2     Any          Any          ANY      Permit  enabled --X-X
6 dmz2      blade1   Any          Any          ANY      Permit  enabled --X-X
10 Untrust  Trust    Any          MIP(172.24.~ HTTP     Permit  enabled --X-X
                                               HTTPS
device-> get policy id 4
name: "none" (id 4), zone blade1 -> dmz2,action Permit, status "enable
src "Any", dst "Any", serv "ANY"
Policies on this vpn tunnel: 0
nat off, Web filtering: disabled
vpn unknown vpn, policy flag 00010000, session backup: on
policy IDP mode: disable
traffic shapping off, scheduler n/a, serv flag 00
log yes, log count 0, alert no, counter no(0) byte rate(sec/min) 0/0
total octets 0, counter(session/packet/octet) 0/0/0
```

```
No Authentication
No User, User Group or Group expression set
device-> set policy id 4
device (policy:4)-> set idp
device(policy:4)-> exit
device-> get policy id 4
policy IDP mode: inline
```

4. Netscreen-Security Manager UI を使用して、デバイスを追加します。

   デバイスの追加には、次を行います。

   a. **Device Manager > Security Devices > +** (**Device**) を選択します。

   b. デバイス名を入力して、**Next** をクリックします。

   c. デバイスの IP アドレスを入力して、**Finish** をクリックします。

   新しいデバイスが、セキュリティデバイスのリストに表示されます。

5. デバイスのセキュリティポリシーを確認します。

   そのデバイスにセキュリティポリシーがあることを確認します。デフォルトのセキュリティポリシーを使用できます。あるいは、デバイスがファイアウォール /VPN/IDP 統合デバイスとして配備されている場合、デバイスのファイアウォール /VPN 機能用のカスタムセキュリティポリシーを作成できます。詳細については、184 ページの「セキュリティポリシーの構成」を参照してください。NSM を使用したセキュリティポリシーの構成に関する詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。

6. デバイスをインポートします。

   デバイスのインポートには、追加したデバイスを右クリックして、**Import device** を選択します。デバイスをインポートすると、デバイスを管理するため、セキュリティポリシー情報がデバイスから NSM サーバーにコピーされます。インポートされたポリシーは、NSM の **Security Policy** に表示されます。

   NSM を使用したデバイスの追加および構成に関する詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。他の構成設定には、動作モード、管理パスワード、ゾーンインターフェースの割り当て、およびデフォルトルートの構成などがあります。

7. そのデバイスのセキュリティポリシーに IDP ルールを追加し構成します。

   デバイスのセキュリティポリシーに IDP ルールを含めよう構成します。デバイスで構成を更新すると、IDP ルールの追加または変更を含むセキュリティポリシー全体が、デバイスにインストールされます。IDP ルールの有効および構成に関する詳細については、189 ページの「IDP ルールの構成」を参照してください。

注 : スタンドアロンの IDP システムとしてデバイスを使用している場合、全トラフィックを IDP ルールと照合するように指定する、簡単なファイアウォールルールを構成する必要があります。詳細については、230 ページの「デバイスをスタンドアロンの IDP デバイスとして構成する」を参照してください。

8. セキュリティデバイスにセキュリティポリシーを割り当てます。

9. 次のコマンドを使用して、トラフィックのフローを許可し、IDP セッションを表示します。

device->get sm status

SM	CPU	aval	ena	Sess_cnt	
1	1	1		10	セキュリティモジュール 1
2	1	1		8	
3	0	1		0	セキュリティモジュール 2
4	0	1		0	
5	0	1		0	セキュリティモジュール 3
6	0	1		0	

上のコマンドは、デバイスにインストールされた 1 つのセキュリティモジュール（SM1 および SM2）を示します。CPU 列は、セキュリティモジュール 2 および 3 が、デバイスにインストールされていないことを示します。各セキュリティモジュールの 2 つの CPU の状況は、別々の行に表示されます。

デバイスの管理モジュールは、トラフィックを処理し、次に IDP 検査のためにセキュリティモジュールへトラフィックを転送します。そのトラフィックには、セキュリティモジュールの 2 つの CPU の間でロードバランシングを行います（**Sess_Cnt** 列を参照）。デバイスに複数のセキュリティモジュールがある場合、管理モジュールは、セキュリティモジュール間でトラフィックのロードバランシングを行います。

注 : デバイスに複数のセキュリティモジュールをインストールしてあり、1 つのモジュールが機能しない場合、IDP セッションは、次のセキュリティモジュールに自動的に転送されます。

10. NetScreen-Security Manager サーバーの攻撃オブジェクトデータベースを定期的に更新します。

    詳細については 234 ページの「IDP の管理」を参照してください。

例 2: アクティブ/ パッシブフェールオーバー向けの IDP の構成

この例では、高可用性（HA）ペアでセキュリティデバイスをセットアップし、ネットワークデザインから潜在的な障害発生ポイントを取り除きます。図 58 は、アクティブ / パッシブなフェールオーバー用に IDP を構成するためのデバイスのセットアップを示しています。2 台のデバイスはアクティブ / パッシブ構成になっています。すなわち、1 次デバイスはアクティブで、ファイアウォールおよび VPN のすべての活動を処理し、バックアップはパッシブで、1 次デバイスがダウンした時に処理を引き継ぐために待機します。

図 58: アクティブ / パッシブフェールオーバー向けの IDP の構成

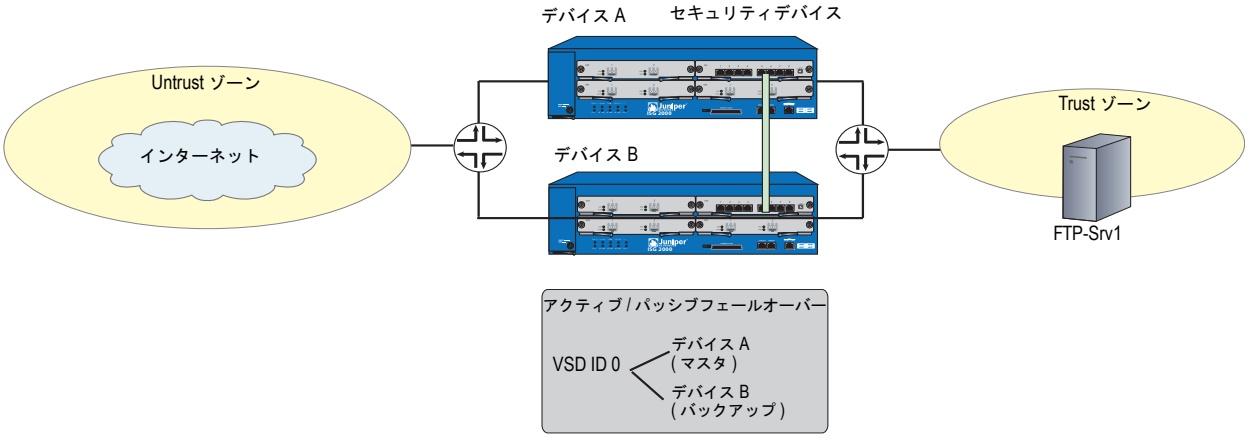


図 58 で示したようにデバイスをセットアップして、次を行います。

1. 177 ページの「例 1: IDP の基本構成」で説明したように、デバイス A およびデバイス B を IDP 用に構成します。

2. トラフィックフローが連続して流れるように、2 台のセキュリティデバイスを配線し、2 台のうち 1 台を 1 次デバイス、もう 1 台をバックアップとして、冗長クラスタを構成します。

   デバイス A の e1/x からデバイス B の e1/x へ配線します。同様に、e2/x インターフェースを配線します。2 つのデバイスの配線、バックアップデバイスを管理するための管理 IP アドレスのセットアップ、または HA ペアの一方で冗長スイッチをセットアップすることによる、他の潜在的な障害発生ポイントの削除に関する詳細については、*第 11 部、高可用性を参照してください。*

3. HA インターフェースを構成します。

   HA インターフェースを持つゾーンを指定します。e1/x および e2/x を HA ゾーンにバインドします。両デバイスで、Trust ゾーンインターフェースの管理 IP アドレスを設定します。

4. アクティブ / パッシブ NSRP（NetScreen Redundancy Protocol）クラスタを構成します。

各デバイスを NSRP クラスタ ID 0 に割り当てます。デバイスが NSRP クラスタのメンバになると、その物理インターフェースの IP アドレスが、仮想セキュリティデバイス（VSD）グループ ID 0 の仮想セキュリティインターフェース（VSI）の IP アドレスに自動的になります。各 VSD メンバのデフォルトの優先順位は 100 です。ユニット ID の高い方のデバイスが、VSD グループの 1 次デバイスになります。VSD について詳しくは、*第 11 部、高可用性*を参照してください。

たとえば、各デバイスで次を入力して、NSRP クラスタを構成します。

a. NSRP クラスタおよび VSD グループにデバイスを追加します。

```
set nsrp cluster id 0
```

b. 自動ランタイムオブジェクト（RTO）同期を使用可能にします。

```
set nsrp rto sync all
```

c. デバイスがモニタするポートを選択します。

デバイスが、モニタしているポートの 1 つでネットワーク接続の消失を検知すると、デバイスフェールオーバーが発生します。

```
set nsrp rto-mirror sync
set nsrp monitor interface ethernet1
set nsrp monitor interface ethernet3
set nsrp cluster id 0
save
```

初期の NSRP 構成では、0 に最も近い優先順位番号を持つ VSD グループメンバが、1 次デバイスになります。(デフォルトは 100 です。) デバイス A とデバイス B の優先順位値が同じ場合は、MAC アドレスの大きい方のデバイスが 1 次デバイスになります。

1 次デバイスは、そのすべてのネットワークおよび構成の設定と現在のセッションの情報をバックアップに設定同期します。バックアップデバイスは、パッシブですが、1 次デバイスから取得する情報を使って、その同期を維持しています。1 次デバイスに障害が発生した場合は、バックアップが 1 次デバイスに昇格し、トラフィックの処理を引き継ぎます。

注 : 同期は、ファイアウォールセッションについてだけ維持されます。ステートフルフェールオーバーは、IDP セッションでは起こりません。

例 3: アクティブ/ アクティブフェールオーバー向けの IDP の構成

この例では、Route モードまたは NAT（ネットワークアドレス変換）モードでセキュリティデバイスをセットアップし、冗長クラスタのセキュリティデバイスが、その間で分配されたトラフィックを共有しアクティブであるように構成します。このため、図 59 に示すように、NSRP を使用して 2 つの VSD グループを作成します。デバイス A は、VSD グループ 1 の 1 次デバイスおよび VSD グループ 2 のバックアップとして機能します。デバイス A は、VSD グループ 2 の 1 次デバイスおよび VSD グループ 1 のバックアップとして機能します。アクティブ / アクティブ設定では、シングルポイント障害は発生しません。

図 59: アクティブ / アクティブフェールオーバー向けの IDP の構成

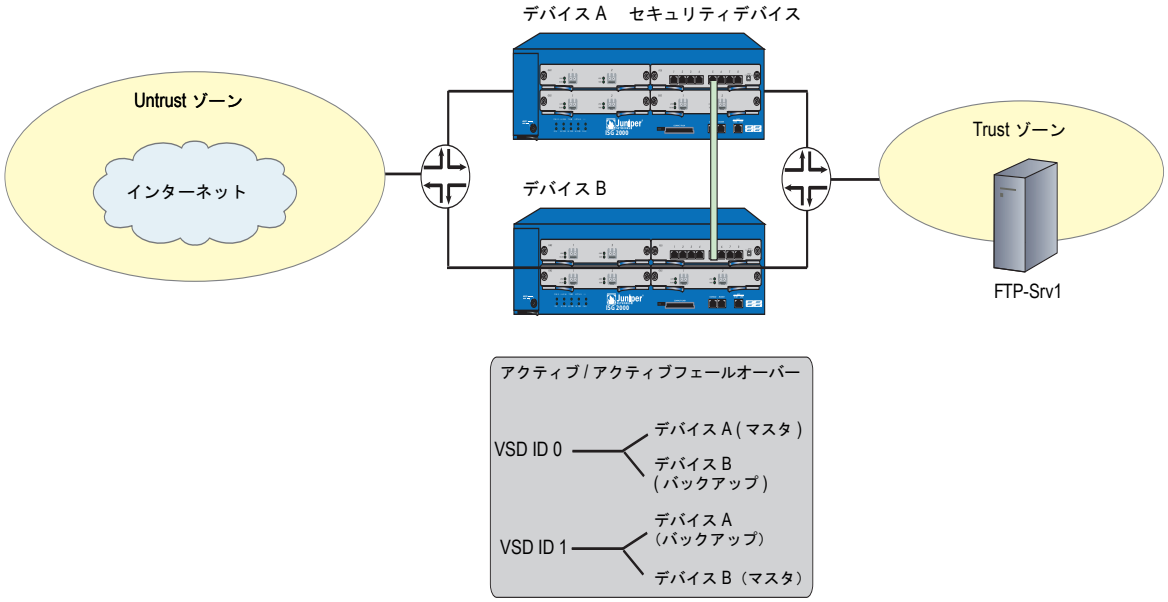


図 59 で示したようにデバイスをセットアップして、次を行います。

注： 同じ数のセキュリティモジュールを両方のデバイスにインストールするよう推奨しました。

1. 177 ページの「例 1: IDP の基本構成」で説明したように、デバイス A およびデバイス B を IDP 用に構成します。

2. トラフィックフローが連続するように、2 台のセキュリティデバイスを冗長クラスタに配線および構成します。

   デバイス A の e1/x からデバイス B の e1/x へ配線します。同様に、e2/x インターフェースを配線します。2 つのデバイスの配線、バックアップデバイスを管理するための管理 IP アドレスのセットアップ、または HA ペアの一方で冗長スイッチをセットアップすることによる、他の潜在的な障害発生ポイントの削除に関する詳細については、*第 11 部、高可用性*を参照してください。

3. HA インターフェースを構成します。

   HA インターフェースを持つゾーンを指定します。e1/x および e2/x を HA ゾーンにバインドします。両デバイスで、Trust ゾーンインターフェースの管理 IP アドレスを設定します。

4. アクティブ / アクティブ NSRP クラスタを構成します。

   デバイス A とデバイス B は、同じ NSRP クラスタおよび VSD グループ 0 のメンバです。アクティブ / アクティブフェールオーバー用に、別の VSD グループ、グループ 1 を作成します。

   1. デバイス A の優先順位を、グループ 0 では 1 に割り当て、グループ 1 ではデフォルトの優先順位（100）に割り当てます。

   2. デバイス B の優先順位を、グループ 1 では 1 に割り当て、グループ 0 ではデフォルトの優先順位（100）に割り当てます。

   両方の VSD グループで、1 次デバイスの優先使用オプションを使用可能にし、優先使用抑制時間を 10 秒に設定します。両方のデバイスがアクティブの場合、デバイス A は必ずグループ 1 の 1 次デバイスとなり、デバイス B は必ずグループ 2 の 1 次デバイスとなります。

   デバイス A

```
set nsrp vsd-group id 0 priority 1
set nsrp vsd-group id 0 preempt hold-down 10
set nsrp vsd-group id 0 preempt
set nsrp vsd-group id 1
save
```

   デバイス B

```
set nsrp vsd-group id 1 priority 1
set nsrp vsd-group id 1 preempt hold-down 10
set nsrp vsd-group id 1 preempt
save
```

   2 つの VSD グループの作成について詳しくは、*第 11 部、高可用性*を参照してください。

   デバイス A およびデバイス B は、それぞれネットワークと VPN のトラフィックの 50% を受信します。デバイス A に障害が発生した場合は、デバイス B が VSD グループ 1 の 1 次デバイスになりますが、依然として VSD グループ 2 のマスタでもあるため、トラフィックの 100% を処理します。

注 : 同期は、ファイアウォールセッションについてだけ維持されます。ステートフルフェールオーバーは、IDP セッションでは起こりません。

セキュリティポリシーの構成

セキュリティポリシーは、管理対象のデバイスがどうネットワークトラフィックを処理するかを定義します。NetScreen-Security Manager では、複数のセキュリティポリシーを構成できます。しかし、1 つのデバイスが 1 度に複数のアクティブなセキュリティポリシーを持つことはできません。複数のデバイスに同じセキュリティポリシーをインストールすることも、ネットワーク内の各デバイスに個別のセキュリティポリシーをインストールすることもできます。

セキュリティポリシーについて

セキュリティポリシーの各命令は、*ルール*と呼ばれます。セキュリティポリシーは、複数のルールを含むことができます。セキュリティポリシーを定義するためのルールの集合である、*ルールベース*にルールを作成します。各セキュリティポリシーには、Zone および Global ファイアウォールルールベースが含まれており、これらは削除できません。セキュリティポリシーの他のルールベース、Multicast、IDP、Exempt、および Backdoor は、追加や削除ができます。しかし、1 つのポリシーには、同じタイプのルールベースの複数のインスタンスを含めることはできません。全ルールベースをまとめた各セキュリティポリシーは、最大 40,000 件のルールを含むことができます。

このセクションでは、IDP、Exempt、および Backdoor ルールベースについて説明します。Zone と Global ファイアウォールルールベース、およびマルチキャストルールベースに関する詳細については、*NetScreen-Security Manager Administrator's Guide* のセキュリティポリシーの構成に関する情報を参照してください。

注： ScreenOS WebUI および CLI では、セキュリティポリシーは、ソース、宛先、ゾーン、方向、およびサービスを定義する 1 つステートメントです。NetScreen-Security Manager では、これらの同じステートメントが*ルール*と呼ばれ、セキュリティポリシーはルールの集合になっています。

セキュリティポリシーの管理

セキュリティポリシー内では、次のように各ルールベースのルールを管理できます。

- ルールがネットワークトラフィックに適用される順序の決定
- ルールの使用不可
- ソースアドレスまたは宛先アドレスの否定（ScreenOS 5.x デバイスだけ）
- セキュリティポリシーの確認
- セキュリティポリシーの結合

注： 2 つのポリシーを 1 つに結合すると、IDP、Exempt、および Backdoor の各ルールベースは含まれていません。

セキュリティポリシーの管理に関する詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。

セキュリティポリシーのインストール

1 つ以上のルールベースにルールを構築して、セキュリティポリシーを作成した後、そのポリシーを特定の管理対象のデバイスに割り当てたり、確認、インストールできます。セキュリティポリシーのインストールに関する詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。

IDP ルールベースの使用

ファイアウォールルール（ゾーン内またはグローバル）がネットワークトラフィックを許可した後、既知の攻撃についてそのトラフィックをさらに検査するよう、デバイスに指示できます。NetScreen-Security Manager は、次の IDP ルールベースをサポートしています。

- **IDP:** このルールベースは、攻撃オブジェクトを使用して既知および未知の攻撃を検知することにより、攻撃からネットワークを保護します。Juniper Networks は、IDP ルールで使用できる、定義済みの攻撃オブジェクトを提供しています。また、自分のカスタム攻撃オブジェクトを構成することもできます。詳細については、212 ページの「IDP 攻撃オブジェクトの構成」を参照してください。

注 : Juniper Networks は、新しく発見された攻撃に対応するため、定義済み攻撃オブジェクトを定期的に更新します。攻撃オブジェクトの更新に関する詳細については、234 ページの「IDP の管理」を参照してください。

- **Exempt:** このルールベースは、IDP ルールベースと連携して、不必要なアラームが生成されるのを防ぎます。このルールベース中のルールを構成して、既知の 誤検知を除外したり、または IDP ルールとの照合から特定のソース、宛先またはソース / 宛先のペアを除外します。トラフィックが IDP ルールベースのルールに適合する場合、IDP は、指定したアクションを実行する前に、そのトラフィックを Exempt ルールベースと照合しようと試みます。

- **Backdoor Detection:** このルールベースは、システムへの無許可のアクセスを容易にする、ホストコンピュータにインストールされたメカニズムからネットワークを保護します。攻撃者は、システムに損害を与える際、通常は（トロイの木馬などの）バックドアをインストールして、将来の攻撃を行いやすくします。攻撃者がバックドアプログラムに情報を送信したり、バックドアプログラムから情報を取得すると、IDP が検知でき対話型のトラフィックが生成されます。

Zone、Global、および Multicast ルールベースなど、全ルールベースのルールがまとまって、セキュリティポリシーを作成します。IDP ルールベースのルールをデバイスが処理、実行するよう指示するには、ファイアウォールルールの IDP を使用可能にする必要があります。187 ページの「ファイアウォールルールで IDP を使用可能にする」を参照してください。

注 : NetScreen-Security Manager にデバイスをインポートした場合、インポートされたデバイスの構成には、IDP、Exempt、または Backdoor ルールベースが含まれません。

IDP ルールベースの役割ベースの管理

NetScreen-Security Manager の役割ベースの管理（RBA）では、IDP ルールベースの表示や編集の権限を与えるカスタム役割を、個々の管理者について作成できます。RBA に関する詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。IDP ルールベースに基づいた役割に対して、表示や編集の機能を割り当てることができます。たとえば、ファイアウォールルールベースを表示、編集できる管理者は IDP および Backdoor ルールベースだけを表示できるように、指定できます。

デフォルトでは、定義済みの役割である、システム管理者およびドメイン管理者は、全ルールベースを表示および編集できます。また、読取専用システム管理者および読取専用ドメイン管理者は、ルールベースの表示しかできません。新しい役割を作成すると、New Role ダイアログボックスで、管理者が IDP または Backdoor ルールベースを表示または編集できるかどうか、指定できます。

オブジェクトの IDP ルール向け構成

オブジェクトとは、ルールに適用できる再使用可能な論理エンティティのことです。作成した各オブジェクトは、オブジェクトタイプ用のデータベースに追加されます。以下のタイプのオブジェクトを使用できます。

- **アドレスオブジェクト**は、ホストマシンやサーバー、サブネットなどのネットワークコンポーネントを表しています。セキュリティポリシールールでアドレスオブジェクトを使用して、保護したいネットワークコンポーネントを指定します。

注： アドレスオブジェクトデータベースに各オブジェクトを作成しなければなりません。デフォルトのアドレスオブジェクトはありません。

アドレスオブジェクトの作成に関する詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。

- **サービスオブジェクト**は、TCP、UDP、RPC および ICMP のような、トランスポートレイヤプロトコルを使用するネットワークサービスを表します。ルールでサービスオブジェクトを使用して、攻撃がネットワークにアクセスするために使用するサービスを指定します。NetScreen-Security Manager には、定義済みサービスオブジェクトが含まれています。これは、業界標準のサービスに基づくサービスオブジェクトのデータベースです。定義済みサービスオブジェクトに含まれていないサービスオブジェクトを追加する必要がある場合、カスタムサービスオブジェクトを作成できます。サービスオブジェクトの作成に関する詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。

- **IDP 攻撃オブジェクト**は、既知および未知の攻撃を表します。IDP には、Juniper Networks が定期的に更新する定義済み攻撃オブジェクトデータベースが含まれています（234 ページの「IDP の管理」を参照）。ユーザーのネットワークに固有の攻撃を検出するため、カスタム攻撃シグネチャを追加することもできます。（212 ページの「IDP 攻撃オブジェクトの構成」を参照してください。）

セキュリティポリシーテンプレートの使用

新しいセキュリティポリシーを作成するとき、次のオプションがあります。

- デフォルトのファイアウォールルールを含むセキュリティポリシーを作成します。
- 定義済みのテンプレートを選択します。
- 既存のセキュリティポリシーを新しいポリシーにコピーします。このポリシーは変更できます。

テンプレートとは、セキュリティポリシーを作成するときに出発点として使用できる、特定のルールベースタイプのルールの集合のことです。テンプレートの一覧は、*NetScreen-Security Manager Administrator's Guide* を参照してください。

ファイアウォールルールで IDP を使用可能にする

全ルールベースのルールがまとまって、セキュリティポリシーを作成します。セキュリティデバイスは、次の順に各ルールベースのルールを処理し実行します。

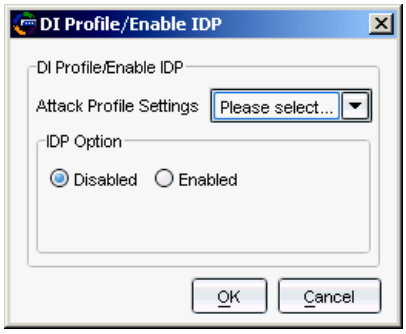
1. ゾーンベースのファイアウォール
2. グローバルなファイアウォール
3. マルチキャスト
4. IDP
5. 除外
6. バックドア

ゾーンベースのまたはグローバルなファイアウォールルールで IDP を使用可能にすると、ファイアウォールルールに適合するトラフィックは、IDP ルールベースと照合されます。

注 : ファイアウォールアクションは **permit** でなければなりません。デバイスが拒否するトラフィックには IDP を使用可能にすることができません。

ファイアウォールルールで IDP を使用可能にするには、ゾーンベースのまたはグローバルなファイアウォールの Rule Options 列をクリックして、次に **DI Profile/Enable IDP** 選択します。図 60 のように、DI Profile/Enable IDP ダイアログボックスが表示されます。

図 60: DI Profile/Enable IDP ダイアログボックス



注： これらの攻撃プロファイル設定は、ファイアウォール /VPN デバイスの徹底監視（DI）機能にだけ適用されます。デバイスに IDP ライセンスをインストールすると、DI はそのデバイスでは使用不可になります。

IDP を使用可能にする

デフォルトでは、IDP オプションは無効です。ファイアウォールルールに適合するトラフィックに IDP を使用可能にするには、**Enable** を選択します。IDP を使用可能にするとき、IDP 機能が、セキュリティポリシーがインストールされるデバイスで、インラインモードで動作するか、またはインラインタップモードで動作するかを選択することもできます。

注： ターゲットデバイスのファイアウォールルールで IDP を使用可能にしない場合は、引き続きそのデバイスの IDP ルールを構成できます。しかし、デバイスでセキュリティポリシーを更新すると、IDP ルールを適用できなくなります。

インラインモードまたはインラインタップモードの指定

ターゲットデバイスの IDP は、次の 2 つのモードの 1 つで動作できます。

- **inline** モードでは、IDP は、ネットワーク上のトラフィックの進路の中にあり、攻撃を検知しブロックできます。たとえば、インターネットとエンタープライズ LAN、WAN または DMZ のような特別なゾーンの間のファイアウォール /VPN/IDP 統合機能をセキュリティデバイスに配備できます。これはデフォルトモードです。

- **inline tap** モードでは、IDP は、パケットのコピーを受信します。その一方で、元のパケットはネットワークで転送されます。IDP は、パケットのコピーを検査し、問題になりそうな点があれば、フラグを立てます。IDP のパケットの検査は、ネットワーク上のパケットの転送に影響しません。

注： IDP 対応のデバイスをインラインに配備しなければなりません。スイッチの外部 TAP または SPAN ポートへ、インラインタップモードのデバイスは接続できません。

デバイスのセキュリティポリシーの一部として IDP モードを指定します。

IDP ルールの構成

IDP ルールベースは、悪意のある活動を識別するために攻撃オブジェクトを使用し、次に攻撃を妨害するアクションを行うことにより、攻撃からネットワークを保護します。多くの IDP ルールを構成して、性能の問題が発生しないように注意します。

IDP ルールを作成するときは、次の事項を指定します。

- 次の特性を使用して、IDP が攻撃を監視するネットワークトラフィックのタイプ。
  - **From Zone/To Zone:** 全トラフィックはソースゾーンから宛先ゾーンへと流れます。ソースまたは宛先には、どのゾーンでも選択できます。ただし、そのゾーンは、ルールの Install On 列で選択したセキュリティデバイスについて有効でなければなりません。また、ゾーン例外を使用して、各デバイスについて、独自の **to** および **from** ゾーンを指定できます。
  - **Source IP:** ネットワークトラフィックが発生するソース IP アドレス。任意の IP アドレスから発生するネットワークトラフィックをモニタするため、これを "any" に設定できます。また、指定したアドレス以外の全ソースを指定するため、"negate" を指定できます。
  - **Destination IP:** ネットワークトラフィックが送信される宛先 IP アドレス。任意の IP アドレスに送信されるネットワークトラフィックをモニタするため、これを「any」に設定できます。また、指定したアドレス以外の全宛先を指定するため、「negate」を指定できます。
  - **Service:** 宛先 IP アドレスがサポートするアプリケーションレイヤプロトコル。
  - **Terminate Match:** デフォルトでは、IDP ルールベースのルールは*非ターミナル*です。IDP は、ルールベースの全ルールを検討し、適合をすべて実行します。ルールを*ターミナル*に指定できます。IDP が、ターミナルルールで指定されたソース、宛先、およびサービスによる適合に遭遇すると、その接続の以後のルールは検査しません。トラフィックは、ターミナルルールで指定された攻撃と照合する必要がないことに注意します。ターミナルルールが表示される位置はルールベースの最上部近くで、同じトラフィックが一致する他ルールの前にする必要があります。ターミナルルールを指定するときは注意が必要です。

    196 ページの図 70 を参照してください。また、Terminate Match をチェックすると、Terminate Match Rule (Rule Shadowing) より下のルールは評価されないことに注意してください。

    Terminate Match をチェックしていない場合、複数イベントのロギング / マッチングが発生し、1 つの攻撃でログに複数のエントリが作成されて、複数のアクションが行われます。
- モニタしているネットワークトラフィックで IDP に照合させたい攻撃。各攻撃は*攻撃オブジェクト*として定義されます。これは、攻撃の既知のパターンを表します。モニタしているネットワークトラフィックで、この既知のパターンの攻撃に遭遇すると常に、攻撃オブジェクトはマッチします。攻撃オブジェクトは、カテゴリ別、オペレーティングシステム別、重大度別、または個別に追加できます。

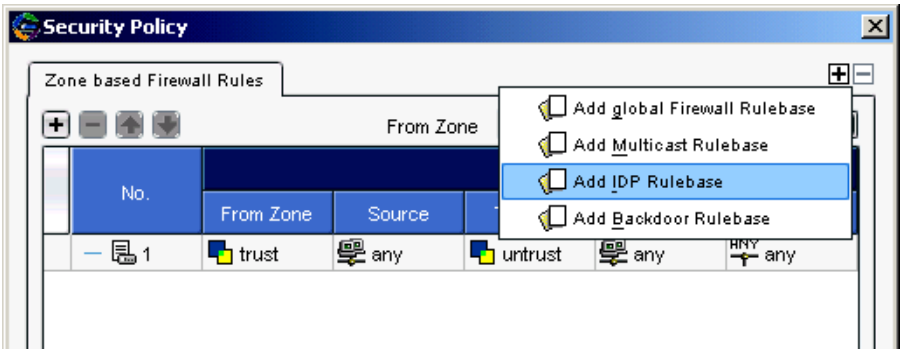
- モニタしているトラフィックが、ルールの攻撃オブジェクトとマッチすると、IDP が行うアクション。以下を指定できます。
  - **Action:** 現在の接続に対して IDP に実行させたいアクション。
  - **IP Actions:** 同じ IP アドレスを使用する将来の接続に対して IDP に実行させたいアクション。
  - **Notification: none** を選択するか、ロギングを使用可能にして、ネットワークに適切なロギングオプションを選択します。
  - **Severity:** 選択した攻撃オブジェクトのデフォルトの重大度設定を使用するか、自分のルール専用の重大度を選択します。

IDP ルールベースの追加

IDP ルールベースのルールを構成すること前に、次の手順を使用して、セキュリティポリシーに IDP ルールベースを追加する必要があります。

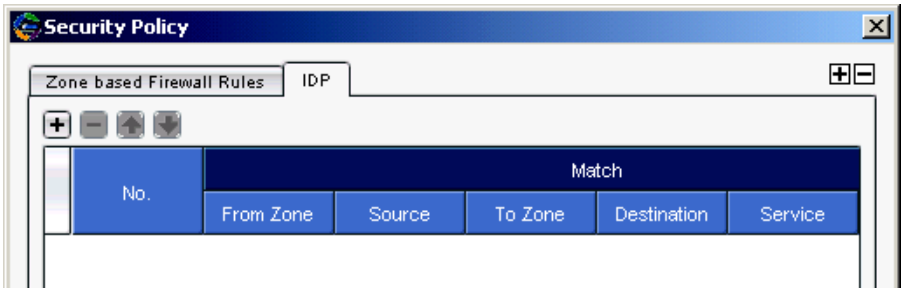
1. メインナビゲーションツリーで、**Security Policies** を選択します。Security Policy ウィンドウのポリシー名をダブルクリックするか、またはポリシー名をクリックして、Edit アイコンを選択することにより、セキュリティポリシーを開きます。
2. Security Policy ウィンドウの右上角にある Add アイコンをクリックして、**Add IDP Rulebase** を選択します。図 61 を参照してください。

図 61: IDP ルールベースの追加



IDP ルールベースのタブが表示されます。図 62 を参照してください。

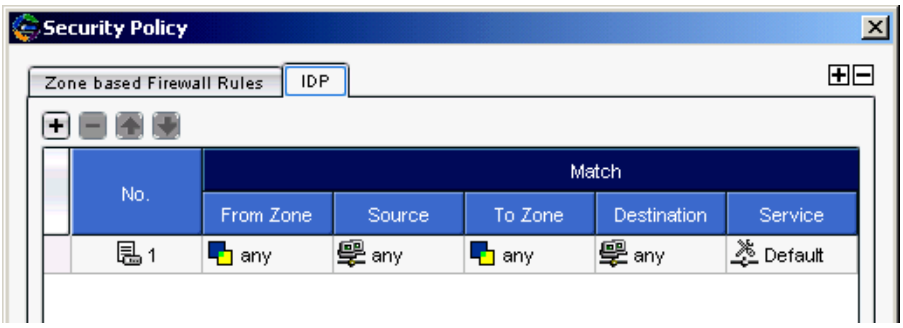
図 62: 追加した IDP ルールベース



3. IDP ルールを構成するには、Security Policy ウィンドウの左側にある Add アイコンをクリックします。

   デフォルトの IDP ルールが表示されます。必要に応じて、このルールを変更できます。図 63 を参照してください。

図 63: 追加した IDP ルール



トラフィックとのマッチング

IDP ルールを作成するとき、攻撃がないか IDP にモニタさせたいネットワークトラフィックのタイプを指定しなければなりません。これらの特性には、トラフィックを発信または受信するネットワークコンポーネントおよびトラフィックが通過するファイアウォールゾーンが含まれます。

From Zone、Source、To Zone、Destination、Service の各 Match 列は、IDP ルールベースの全ルールに必要です。Terminate Match を選択すると、ルールをターミナルとして指定できます。IDP が、ターミナルルールの他の Match 列に適合するトラフィックに遭遇した場合、ルールベースの他のルールは検査されません。適合したトラフィックは、ターミナルルールで指定された攻撃と照合する必要がありません。（詳細については、195 ページの「ターミナルルール」を参照してください。）

次のセクションでは、IDP ルールの Match 列を詳しく説明します。

ソースゾーンおよび宛先ゾーン

ソースと宛先に複数のゾーンを選択できます。ただし、これらのゾーンは、ポリシーをインストールするセキュリティデバイスで利用可能でなければなりません。任意のゾーンから発生する、または任意のゾーンが宛先となる、ネットワークトラフィックをモニタするため、ソースゾーンまたは宛先ゾーンに「any」を指定できます。

注： セキュリティデバイスにカスタムゾーンを作成できます。ソースゾーンおよび宛先ゾーンを選択できるゾーンのリストには、NetScreen-Security Manager が管理する全デバイス用に構成された、定義済みゾーンとカスタムゾーンが含まれています。したがって、セキュリティポリシーをインストールするデバイスに適用可能なゾーンだけを選択します。

ソースおよび宛先アドレスオブジェクト

NetScreen-Security Manager システムでは、アドレスオブジェクトは、ホスト、ネットワーク、サーバーなどの、ネットワーク上のコンポーネントを表すために使用されます。通常、ネットワーク上のサーバーなどのデバイスは、送られてきた攻撃の宛先 IP であり、対話型攻撃の場合は発信元 IP になっている可能性があります（対話型攻撃の詳細は、207 ページの「バックドアルールの構成」を参照してください）。任意の IP アドレスから発生するネットワークトラフィックをモニタするため、「any」を指定できます。また、除外されたオブジェクト以外のソースまたは宛先をすべて指定するため、Source または Destination 列に示されたアドレスオブジェクトを「否定」することもできます。

IDP ルールを作成する前（*NetScreen-Security Manager Administrator's Guide* を参照）、または IDP ルールの作成または編集の間に、アドレスオブジェクトを作成できます。アドレスオブジェクトを選択または構成するには、ルールの Source または Destination 列のいずれかを右クリックして、**Select Address** を選択します。**Select Source Addresses** ダイアログボックスで、既に作成されたアドレスオブジェクトを選択するか、または新しいホスト、ネットワーク、またはグループオブジェクトを作成するために Add アイコンをクリックします。

例：ソースと宛先の設定

あなたの内部ネットワークを標的とする攻撃の着信を検出したいとします。From Zone を **Untrust** に設定し、Source IP を **any** に設定します。To Zone を **dmz** および **trust** に設定します。攻撃から保護したいホストまたはサーバーを表すアドレスオブジェクトを Destination IP に選択します。

ルールは、図 64 の例のようになります。

図 64: 設定したソースと宛先

No.	Match			
	From Zone	Source	To Zone	Destination
1	untrust	any	dmz trust	Internal Network

例：複数のソースおよび宛先の設定

ネットワークとネットワークの間の攻撃を検出したいとします。Source および Destination に複数のアドレスオブジェクトを選択します。

ルールは、図 65 の例のようになります。

図 65: 設定した複数のソースと宛先ネットワーク

No.	Match			
	From Zone	Source	To Zone	Destination
1	untrust	Europe Users Europe Email Server Europe Workstation	dmz trust	Internal Network Security Team Network Administrator

攻撃のソースと宛先の定義を具体的にすればするほど、偽陽性は少なくなります。

サービス

サービスとは、データがネットワーク上を移動するときどのような構造をとるかを定義するアプリケーションレイヤプロトコルです。あなたが自分のネットワーク上でサポートするサービスは、攻撃者があなたのネットワークを攻撃するために使用するのと同じサービスであるため、どのサービスが宛先 IP によってサポートされるかを指定して、ルールをより効率化できます。

注： すべてのサービスは、トランスポートレイヤプロトコルを使用してデータを転送します。IDP には、TCP、UDP、RPC、および ICMP のトランスポートレイヤプロトコルを使用するサービスが備わっています。

サービスオブジェクトは、ネットワーク上で実行するサービスを表します。NetScreen-Security Manager には、業界標準のサービスに基づく、定義済みサービスオブジェクトが含まれています。ルールでこれらのサービスオブジェクトを使用して、攻撃がネットワークにアクセスするために使用するサービスを指定します。また、定義済みサービスに含まれていないプロトコルを表すために、カスタムサービスオブジェクトを作成できます。サービスオブジェクトの構成に関する詳細については、*NetScreen-Security Manager Administrator's Guide* のオブジェクトの構成に関する情報を参照してください。

Service 列では、IDP が照合するトラフィックのサービスを選択します。

- **Default** を選択して、Attacks 列で選択した攻撃オブジェクトが指定するサービスを確定します。攻撃オブジェクトを Attack 列で選択すると、その攻撃オブジェクトに関連付けられたサービスは、ルールのデフォルトサービスになります。正確なサービスを確認するには、攻撃オブジェクトの詳細を表示します。
- すべてのサービスを設定するには **Any** を選択します。
- 定義されたサービスオブジェクトのリストから特定のサービスを選ぶには、**Select Service** を選択します。

例：デフォルトサービスの設定

FTP サーバーを FTP 攻撃から防御したいとします。サービスを Default に設定し、FTP バッファオーバーフロー試行を検出する攻撃オブジェクトを追加します。ルールの Service コラムは “Default”と表示されたままですが、実際にはルールは TCP-FTP のデフォルトサービスを使用します。これは、攻撃オブジェクトで指定されたものです。

ルールは、図 66 の例のようになります。

図 66: 設定したデフォルトサービス

Match						Action	Attacks
From Zone	Source	To Zone	Destination	Service	Terminate Ma...		
untrust	any	dmz trust	FTP Server	Default	☑	None	FTP - Critical

例：特定のサービスの設定

ユーザーのメールサーバーは POP3 および SMTP 接続をサポートしていますが、IMAP 接続はサポートしていません。メールサーバーを攻撃するために利用できるサービスとして、POP3 と SMTP のサービスオブジェクトを設定します。IMAP はサポートされていないので、IMAP サービスオブジェクトは追加する必要がありません。

ルールは、図 67 の例のようになります。

図 67: 設定した特定のサービス

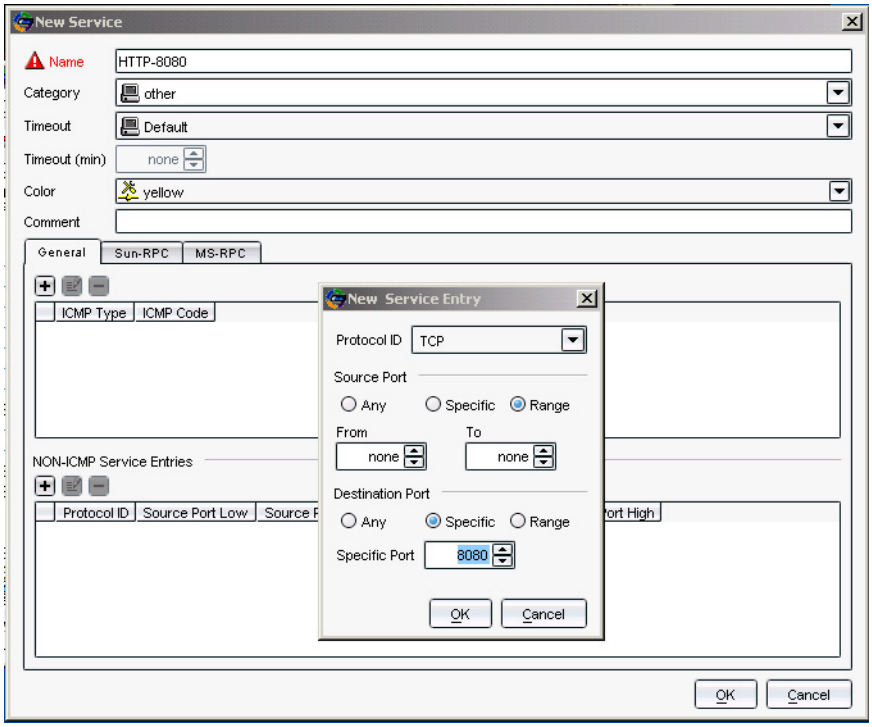


非標準ポートのサービスをサポートしている場合、デフォルト以外のサービスを選択する必要があります。

例：非標準サービスの設定

あなたは HTTP サービスに非標準ポート (8080) を使用しています。Object Manager を使用して、ポート 8080 にカスタムサービスオブジェクトを作成します。

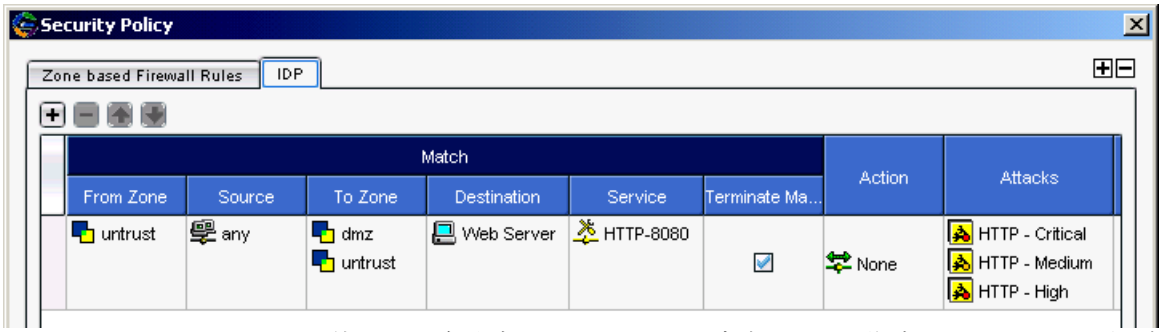
図 68: 非標準サービスオブジェクトの追加



このサービスオブジェクトを自分のルールに追加し、TCP/80 のデフォルトサービスを持つ HTTP 攻撃オブジェクトをいくつか追加します。IDP は、指定されたサービスである HTTP-8080 をデフォルトの代わりに使用し、HTTP 攻撃の一致をポート 8080 の TCP トラフィックで探します。

ルールは、図 69 の例のようになります。

図 69: 設定した非標準サービス



ルールで使用する自分専用のサービスオブジェクトを作成できます。たとえば、非標準ポートを使用するプロトコルのサービスオブジェクトを作成できます。ただし、攻撃オブジェクトを、これらの攻撃オブジェクトが使用しないプロトコルに一致させることはできません。

ターミナルルール

通常の IDP ルール照合アルゴリズムは、ルールベースの上の方から始めて、ソース、宛先、およびサービスとマッチするルールベースの全ルールについて、トラフィックをチェックします。ターミナルルールは、この通常のルール照合アルゴリズムの例外です。マッチが、ソース、宛先、およびサービスのターミナルのルールで発見されると、IDP は、同じソース、宛先、およびサービスについては、それ以後のルールをチェックしません。トラフィックが、一致ルールの攻撃オブジェクトとマッチするかどうかは、関係ありません。

以下の目的でターミナルルールを使用できます。

- 同じソースおよび宛先について、異なる攻撃には異なるアクションを設定する。これは、次のセクション 「例 : ターミナルルールの設定」のルール 3 および 6 で説明します。
- 既知の信頼できるソースから送出されたトラフィックを無視する。通常、このタイプのターミナルルールのアクションは None（なし）です。これは、次のセクション 「例 : ターミナルルールの設定」のルール 1 で説明します。
- 特定の攻撃のセットにのみ脆弱なサーバーへ送られるトラフィックを無視する。通常、このタイプのターミナルルールのアクションは「接続を除去」です。

ターミナルルールを定義するときは注意が必要です。ターミナルルールが不適切な場合、ネットワークが攻撃に対して無防備になる場合があります。トラフィックはターミナルルールのソース、宛先、およびサービスに一致すると、たとえターミナルルール内の攻撃オブジェクトと一致しなくても、後に続くルールと比較されないことを忘れないでください。ターミナルルールを使用するのは、ある種のトラフィックを特定の攻撃オブジェクトのセットについて調べる場合だけにしてください。ソースと宛先の両方に any を使用するターミナルルールには特に注意してください。

ターミナルルールが現れる位置はルールベースの最上部近くで、同じトラフィックが一致する他ルールの前にする必要があります。ルールをターミナルに設定するには、ルールを作成または変更したとき、Security Policy ウィンドウの Terminate Match 列でボックスを選択します。

注： 多くの場合、ターミナルルールの代わりに除外ルールを使用できます。ターミナルルールよりも除外ルールを構成する方が、簡単で明快かもしれません。202 ページの「免除ルールの構成」を参照してください。

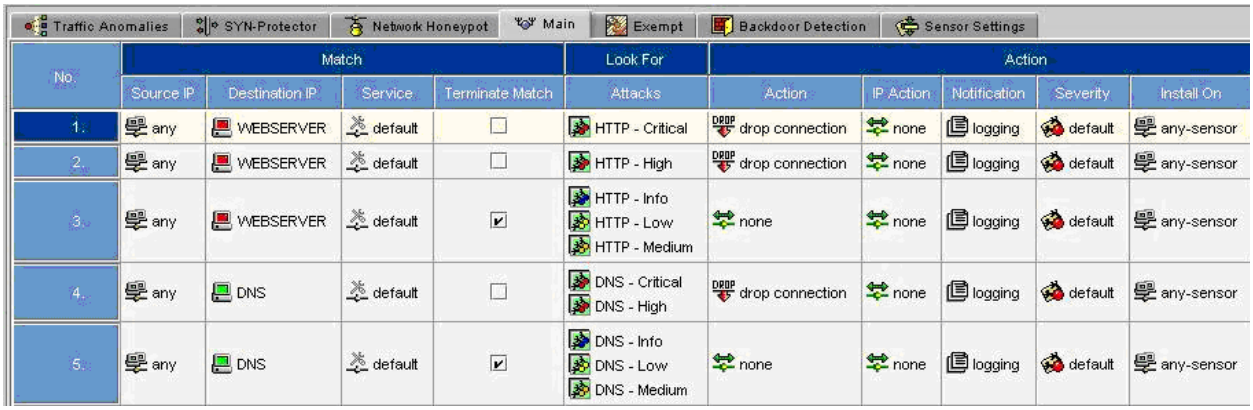
例：ターミナルルールの設定

下に示された IDP ルールベースの例では、ルール 1、3、4、および 5 がターミナルルールとして設定されます。

- ルール 1 は、トラフィックのソース IP が、既知のトラステッドネットワークであるセキュリティネットワークから送出されたものである場合、照合アルゴリズムを終了します。このルールが一致すると、IDP はそのセキュリティネットワークからのトラフィックを無視して、セッションでの不正なデータの監視を中断します。
- ルール 3 と 6 は、宛先 IP が、企業またはヨーロッパの電子メールサーバーである場合、異なる攻撃に異なるアクションを設定します。ルール 3 は、攻撃が SMTP コンテキスト Confidential を使用する電子メールであると、照合アルゴリズムを終了します。ルール 6 は、攻撃が SMTP 攻撃であると、サーバーを閉じます。
- ルール 4 は､宛先が Web サーバーであり攻撃が Critical または High の HTTP 攻撃であると、照合アルゴリズムを終了します。このルールによって、IDP は Web サーバーに対して最も重要な HTTP 攻撃を除去しますが、接続の照合は継続しません。
- ルール 5 は、ソースが内部ネットワークであり攻撃が Critical、High、または Medium のトロイの木馬であると、照合アルゴリズムを終了します。このルールによって、IDP はクライアントとサーバーの両方を閉じますが、接続の照合は継続しません。

Service 列のデフォルト（196 ページの図 70 を参照）は、ルールの攻撃オブジェクトのサービスバインディングに基づいて、ルールが動的に構築されることを意味しています。ルールのサービスバインディングを表示するには、攻撃を右クリックして、**View Services** を選択します。HTTP Critical のような幅広いカテゴリを選択している場合でも、View Services を使って詳細を確認します。

図 70: ターミナルルールの設定



アクションの定義

セキュリティポリシーのルールに一致する攻撃に対して、どのアクションを実行するのか、IDP に指定できます。ルールに一致する各攻撃に対して、現在の攻撃パケットまたは接続を無視する、ドロップする、または閉じるという選択ができます。このルールが起動されると、IDP は接続に対してアクションを実行できます。

IDP が Drop Packet に構成されており、TCP 攻撃を発見すると、セキュリティモジュールが、後続するパケットが攻撃であることを管理モジュールに通知します。このため、IDP アクションの重大度は、より高い Drop Connection に更新されます。

パケットが複数のルールアクションをトリガーする場合、デバイスは最も重大なアクションを適用します。たとえば、パケットが diffserv マーキングを受け破棄されようルールが命じると、パケットは破棄されます。

表 16 は、IDP ルールに指定できるアクションを示します。

表 16: IDP ルールのアクション

Action	解説
None	IDP は接続に対してアクションを行いません。「なし」のアクションを含むルールが一致した場合、対応するログレコードはログビューアのアクションコラムに「accept (承認)」を表示します。
Ignore	攻撃の一致が見つかった場合、IDP は、以後の検査についてフローを無視します。通常、このアクションの選択は避けてください。 注記 : このアクションは、攻撃を無視するという意味ではありません。
Diffserv Marking	示されたサービス区別値を攻撃のパケットに割り当て、それらを正常に渡します。ルールベースのこのアクションを選択すると表示されるダイアログでサービス区別値を設定します。 diffserv マーキングは、攻撃として検出された最初のパケットには適用されず、その後のパケットに適用されることに注意してください。マーキングには、タップモードへの影響または NSRP 使用時の影響はありません。
Drop Packet	IDP は、適合するパケットが宛先に到達する前にそのパケットをドロップしますが、接続は閉じません。このアクションは、UDP トラフィックのように、スプーフィングの傾向があるトラフィック中の攻撃のパケットを除去するために使用してください。このようなトラフィックに対して接続をドロップすると、サービス拒否が発生し、正当なソース IP アドレスからのトラフィックを受信できなくなる可能性があります。
Drop Connection	IDP は、その接続と関連付けられたパケットをすべてドロップします。このアクションを使用して、スプーフィングするタイプでないトラフィックの接続を除去します。
Close Client and Server	IDP は接続を閉じて、RST パケットをクライアントとサーバーの両方へ送ります。IDP がインラインタップモードで動作している場合、IDP は、RST パケットをクライアントとサーバーの両方へ送りますが、接続は閉じません。
Close Client	IDP はクライアントへの接続を閉じますが、サーバーへの接続は閉じません。
Close Server	IDP はサーバーへの接続を閉じますが、クライアントへの接続は閉じません。

IDP ルールのアクションに関する詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。

攻撃オブジェクトの設定

攻撃オブジェクトは、接続内の不正な活動のあるパターンを表し、攻撃を検出する方法です。各攻撃オブジェクトは、ネットワークを侵害するために使われる既知または未知の攻撃を検出します。攻撃オブジェクトの詳細については、212 ページの「IDP 攻撃オブジェクトの構成」を参照してください。

攻撃オブジェクトを自分のルールに個別にまたはグループで追加できます。攻撃オブジェクトは次のようにまとめられています。

- **Attack List** は、カスタム攻撃オブジェクトを含む、全攻撃オブジェクトのアルファベット順のリストです。
- **Dynamic Attack Group** には、定義済みおよびカスタム攻撃グループが含まれます。

ルールに攻撃オブジェクトを追加するには、ルールの Attacks 列を右クリックして、**Select Attacks** を選択します。Add Attacks ダイアログボックスが表示されます。

攻撃オブジェクトを個別に追加する

Attack List では、ルールに 1 つ以上の具体的な攻撃オブジェクトを選択できます。Attack List には、アルファベット順に攻撃オブジェクトが表示されています。また、NetScreen-Security Manager の統合検索機能を使用して、攻撃オブジェクト名に特定の単語または文字列を使用できます。検索機能の使用に関する詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。

攻撃オブジェクトおよびカスタム攻撃オブジェクトおよびグループの作成に関する詳細については、212 ページの「IDP 攻撃オブジェクトの構成」を参照してください。

攻撃オブジェクトのカテゴリ別の追加

IDP は、攻撃オブジェクトを定義済みのサービスカテゴリグループに分類します。サービスとは、データがネットワーク上を移動するときどのような構造をとるかを定義する、アプリケーションレイヤプロトコルです。

システムを攻撃するためには、攻撃者は、そのシステムでサポートされるプロトコルを使用しなければなりません。したがって、システムを保護するルールを作成すると、ルールで保護しているアドレスオブジェクトによって使用されるカテゴリだけを選択しなければなりません。

例 : 攻撃オブジェクトのサービス別の追加

使用している Web サーバーでは、拡張的なファイル転送に FTP および HTTP を使用しているとします。FTP および HTTP カテゴリグループを選択して、これらのサービスを使用するすべてのトラフィックを注意して監視してください。

ルールのカテゴリグループ全体を選択したくない場合、重大度によって攻撃オブジェクトを選択できます。

攻撃オブジェクトのオペレーティングシステム別の追加

IDP は、定義済みのオペレーティングシステムについて攻撃オブジェクトをグループ化します。これは、ネットワーク上の特定のデバイスに最も危険な攻撃オブジェクトを選択するのに役立ちます。BSD、Linux、Solaris、または Windows を選択できます。

ルールのオペレーティングシステムグループ全体を選択したくない場合、重大度によって攻撃オブジェクトを選択できます。

重大度別攻撃オブジェクトの追加

IDP は、5 つの重大度レベルを定義し、各レベルに IDP アクションおよび通知の推奨セットが付属しています（表 17 を参照）。重大度レベルをルールの Attack 列に追加し、Action 列で重大度レベルの推奨アクションを選択できます。（選択できるアクションの詳細については、197 ページの「アクションの定義」を参照してください。）また、Notifications 列では、重大度レベルに推奨される通知を選択できます。（選択できる通知の詳細については、201 ページの「通知の設定」を参照してください。）

注： 重要なアドレスオブジェクトや攻撃されやすい標的を守るために、複数の重大度レベルを使用して最大の防御機能を備えてください。

表 17 は、IDP 重大度レベルをその推奨アクションおよび通知と示しています。

表 17: 重大度レベルおよび推奨アクションと通知

重大度レベル	解説	推奨アクション	推奨通知
Critical	攻撃は、IPS から逃れる、マシンをクラッシュする、またはシステムレベルの権限を得ようと試みます。	Drop Packet Drop Connection	ロギング 警報
Major	攻撃は、サービスのクラッシュ、サービス拒否の実行、トロイの木馬のインストールまたは使用、ホストへのユーザーレベルのアクセス権獲得を試みます。	Drop Packet Drop Connection	ロギング 警報
Minor	攻撃は、重要な情報をディレクトリ巡回や情報リークを経て取り出そうとします。	None	ロギング
Warning	攻撃は、重要でない情報を得たり、ネットワークをスキャンしようとします。これらは、現在では廃れてしまった攻撃で、（しかしおそらくは無害な）トラフィックでもあります。	None	ロギング
Info	攻撃は、通常の無害なトラフィックであり、URL、DNS ルックアップエラー、および SNMP 公開コミュニティ文字列が含まれます。通知攻撃オブジェクトを使用して、自分のネットワークに関する情報を入手できます。	None	なし

IP アクションの設定

セキュリティポリシーを Expanded モードで表示した場合だけ、IP Action 列が表示されます。セキュリティポリシーの表示を Compact モードから Expanded モードに変更するには、**View > Expanded Mode** を選択します。

現在のネットワークトラフィックがルールに一致すると、IDP は IP アクションを、同じ IP アドレスを使用する将来のネットワークトラフィックに対して実行できます。IP アクションは、他のアクションと同じで、IDP に接続のドロップや終了を指示します。しかし、現在あなたは攻撃者の IP アドレスもわかっているため、攻撃者を指定された時間遮断することができます。攻撃者があなたのネットワークへ即座に再接続できなければ、もっと簡単な標的に攻撃をしかけるでしょう。

IP アクションを普通のアクションやロギングと一緒に使用して、自分のネットワークを保護してください。ルールではまず、現在の不正な接続を検出してアドレスオブジェクトに到達できないようにするアクションを構成します。次に、そのルールの IP Action 列を右クリックして、**Configure** を選択し、Configure IP Action ダイアログボックスを表示します。攻撃者の IP アドレスからの将来の不正な接続を防ぐため、IP アクションを使用可能にし構成します。

IP アクションの選択

各 IP アクションオプションごとに、IP アクションは IDP システムによって生成されます。IP アクションは、指定されたタスクを実行するよう IDP に指示します。次のいずれかを選択します。

- **IDP Notify**: IDP は将来のトラフィックに対してアクションを起こしませんが、イベントをログします。これがデフォルトです。
- **IDP Drop**: IDP は、Blocking Options ボックスの基準に一致する将来の接続を遮断します。
- **IDP Close**: IDP は、Blocking Options ボックスの基準に一致する接続を閉じます。

ブロッキングオプションの選択

各ブロッキングオプションは、Actions ボックスで設定された基準に従います。ブロッキングオプションは、攻撃トラフィックの次の一致をベースにすることができます。

- **Source**、**Destination**、**Destination Port** および **Protocol**: IDP は、攻撃トラフィックのソース、宛先、宛先ポート、およびプロトコルに基づいて、将来のトラフィックを遮断します。これがデフォルトです。
- **Source**: IDP は、攻撃トラフィックのソースに基づいて、将来のトラフィックを遮断します。
- **Destination**: IDP は、攻撃トラフィックの宛先に基づいて、将来のトラフィックを遮断します。
- **From Zone**、**Destination**、**Destination Port** および **Protocol**: IDP は、攻撃トラフィックのソースゾーン、宛先、宛先ポート、およびプロトコルに基づいて、将来のトラフィックを遮断します。
- **From Zone**: IDP は、攻撃トラフィックのソースゾーンに基づいて、将来のトラフィックを遮断します。

ロギングオプションの設定

IDP が、ルールと一致する攻撃トラフィックを検知して、IP アクションを開始すると、IDP は、IP アクションに関する情報をログに記録したり、ログビューアで警報を作成できます。デフォルトでは、ロギングオプションは設定されていません。

タイムアウトオプションの設定

トラフィックの一致後に IP アクションを有効にしておきたい秒数を設定できます。永続的な IP アクションについては、デフォルトのタイムアウト値は 0 です。

通知の設定

初めてセキュリティポリシーを設計するときは、攻撃のデータをすべてログに記録し、ポリシーを無制限に実行したくなるものです。しかし、これはすべきでありません。攻撃オブジェクトには、通知のみを行うものや、誤検知や冗長ログを生成できるものがあります。データが過剰になると、重要なものを見逃す可能性があります。セキュリティポリシーの生成するログレコードが多すぎると、攻撃の発見が遅れたり、何百ものログ記録を調べるためにセキュリティの抜け穴を見逃してしまうため、ネットワークのセキュリティに有害なことを忘れないでください。過剰なロギングは、IDP の処理能力、性能、および使用可能なディスク領域にも影響を及ぼします。良いセキュリティポリシーは、ネットワーク上の重要なセキュリティイベントだけがすべて記録されるログを生成します。

ロギングの設定

Configure Notification ダイアログボックスで、**Logging** を選択して、**OK** をクリックします。ルールが一致するごとに、IDP システムはログレコードを作成してログビューアに表示します。

攻撃のロギングにより、ログビューアにリアルタイムで表示できるログレコードが作成されます。より重大な攻撃については、警告フラグをログレコードに立てることができます。

あるルールの攻撃をログするには、ルールの Notification 列を右クリックして、**Configure** を選択します。Configure Notification ダイアログボックスが表示されます。

警報の設定

Configure Notification ダイアログボックスで、**Alert** を選択して、**OK** をクリックします。**Alert** を選択してルールが一致すると、IDP は、一致したログレコードについて、警報フラグをログビューアの Alert 列にセットします。

パケットのロギング

ルールに一致したネットワークトラフィックの中のパケットを個々に記録するには、攻撃のパケットデータをキャプチャします。ネットワークの攻撃で使用されているパケットを見ることで、試みられている攻撃の範囲とその目的、攻撃が成功したかどうか、そしてネットワークに与えるあらゆる損害を判別できます。

注 : IDP 性能を向上させるには、攻撃後に受信したパケットだけをログします。

パケットキャプチャを有効にした複数ルールが同じ攻撃に一致すると、IDP は指定されたパケットの最大数をキャプチャします。たとえば、ルール 1 で攻撃の前後 10 パケットをキャプチャするように構成し、ルール 2 は攻撃の前後 5 パケットをキャプチャするよう構成したとします。両方のルールが同じ攻撃に適合した場合、IDP は攻撃の前後 10 パケットをキャプチャしようとします。

注： パケットキャプチャは、攻撃前後の 256 パケットまでに限られます。

重大度の構成

セキュリティポリシーを Expanded モードで表示した場合だけ、Severity 列が表示されます。セキュリティポリシーの表示を Compact モードから Expanded モードに変更するには、メニューバーから **View > Expanded Mode** を選択します。

IDP ルールベース内のルール単位で、攻撃に関する固有の重大度を変更できます。重大度レベルは、Default、Info、Warning、Minor、Major、または Critical に設定できます。

ルールの重大度を変更するには、ルールの Severity 列を右クリックして、重大度を選択します。

ターゲットの設定

IDP ルールベースのルールごとに、そのルールを使用して攻撃を検出および予防するセキュリティデバイスを選択できます。そのルールが属するセキュリティポリシーをインストールすると、ルールは、ルールベースの Install On 列で選択されたデバイス上でのみアクティブになります。

コメントの入力

Comments 列にルールに関する注釈を入力できます。Comments 列の情報は、ターゲットデバイスにプッシュされません。コメントを入力するには、Comments 列を右クリックして、**Edit Comments** を選択します。Edit Comments ダイアログボックスが表示されます。1024 文字以内のコメントを入力できます。

免除ルールの構成

免除ルールベースは、IDP ルールベースと連携します。免除ルールを作成する前に、まずは IDP ルールベースにルールを作成する必要があります。トラフィックが IDP ルールベースのルールと一致すると、IDP は、そのトラフィックを免除ルールベースと照合してから、指定されたアクションを実行したりイベントのログレコードを作成します。

注： IDP ルールベースを削除すると、免除ルールベースも削除されます。

免除ルールを使用するのは、次のような状況です。

- 誤検知または無関係のログレコードを生成する、1 つ以上の攻撃オブジェクトを含む、攻撃オブジェクトグループを IDP ルールが使用する場合。

- IDP ルールとの照合から、特定のソース、宛先またはソース / 宛先のペアを免除したい場合。これは、IDP が不必要なアラームを生成するのを防ぎます。

また、IDP ルールベースが、誤検知または無関係のログレコードを生成する、1 つ以上の攻撃オブジェクトを含む、静的または動的な攻撃オブジェクトグループを使用する場合も、免除ルールを使用できます。

免除ルールを作成するときは、次の事項を指定します。

- 免除するトラフィックのソースと宛先。任意のソースを起点とする、または任意の宛先へ送信されたネットワークトラフィックを免除するには、ソースまたは宛先を「any」に設定できます。また、指定したアドレス以外の全ソースまたは宛先を指定するため、「negate」も指定できます。

- 指定したソース / 宛先アドレスについて IDP に免除させる攻撃。免除ルールには、攻撃オブジェクトを最低 1 つ含める必要があります。

注： 免除ルールは、非ターミナルのルールベースです。つまり、IDP は、免除ルールベースの全ルールに対してトラフィックを照合し、すべての一致を実行しようとします。

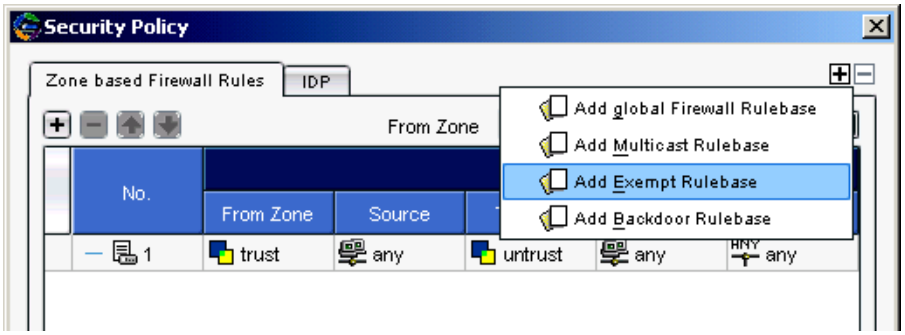
免除ルールベースの追加

免除ルールベースのルールを構成する前に、次の手順を使用して、セキュリティポリシーに免除ルールベースを追加する必要があります。

1. メインナビゲーションツリーで、**Security Policies** を選択します。Security Policies ウィンドウのポリシー名をダブルクリックするか、またはポリシー名をクリックして、Edit アイコンを選択することにより、セキュリティポリシーを開きます。

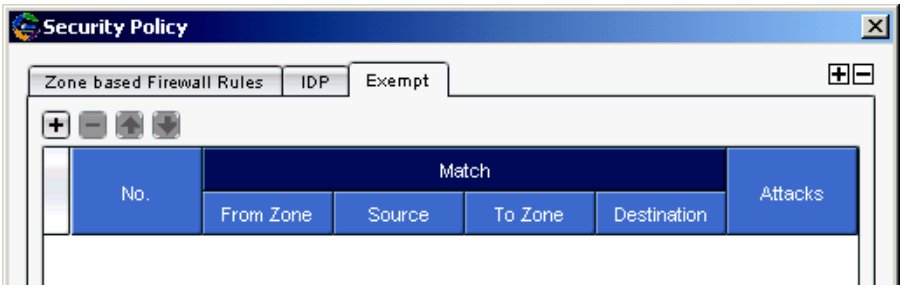
2. Security Policy ウィンドウの右上角にある Add アイコンをクリックして、**Add Exempt Rulebase** を選択します。

図 71: 免除ルールベースの追加



Add Exempt Rulebase タブが表示されます。

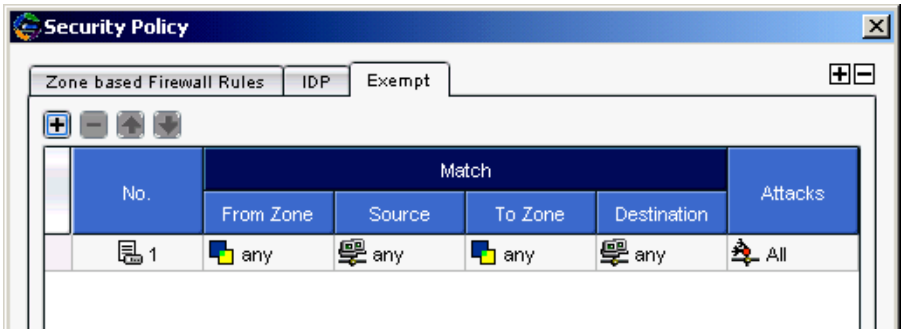
図 72: 追加された免除ルールベース



3. 免除ルールを構成するには、Security Policy ウィンドウの左側にある Add アイコンをクリックします。

   デフォルトの免除ルールが表示されます。必要に応じて、このルールを変更できます。

図 73: 追加された免除ルール



一致の定義

攻撃の検出を免除したいトラフィックを指定します。Match 列の From Zone、Source、To Zone、および Destination は、免除ルールベースの全ルールに必要です。

次のセクションでは、免除ルールの Match 列を詳しく説明します。

ソースゾーンおよび宛先ゾーン

ソースと宛先に複数のゾーンを選択できます。ただし、これらのゾーンは、ポリシーをインストールするデバイスで利用可能でなければなりません。任意のゾーンから発生する、または任意のゾーンが宛先となる、ネットワークトラフィックをモニタするため、ソースゾーンまたは宛先ゾーンに「any」を指定できます。

注： セキュリティデバイスにカスタムゾーンを作成できます。ソースゾーンおよび宛先ゾーンを選択できるゾーンのリストには、NetScreen-Security Manager が管理する全デバイス用に構成された、定義済みゾーンとカスタムゾーンが含まれています。したがって、セキュリティポリシーをインストールするデバイスに適用可能なゾーンだけを選択します。

ソースおよび宛先アドレスオブジェクト

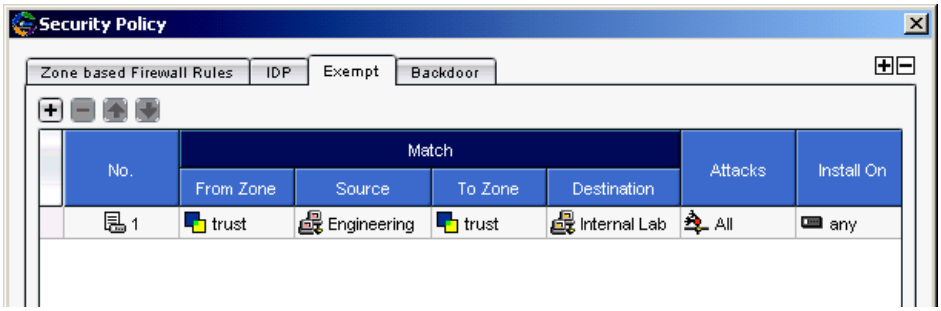
NetScreen-Security Manager システムでは、アドレスオブジェクトは、ホスト、ネットワーク、サーバーなどの、ネットワーク上のコンポーネントを表すために使用されます。任意の IP アドレスから発生するネットワークトラフィックをモニタするため、「any」を指定できます。また、除外されたオブジェクト以外のソースまたは宛先をすべて指定するため、Source または Destination 列に示されたアドレスオブジェクトを否定することもできます。

免除ルールを作成する前（*NetScreen-Security Manager Administrator's Guide* を参照）、または免除ルールの作成または編集の間に、アドレスオブジェクトを作成できます。アドレスオブジェクトを選択または構成するには、ルールの Source または Destination 列のいずれかを右クリックして、**Select Address** を選択します。Select Source Addresses ダイアログボックスで、既に作成されたアドレスオブジェクトを選択するか、または新しいホスト、ネットワーク、またはグループオブジェクトを作成するために Add アイコンをクリックします。

例：ソース / 宛先ペアの免除

パフォーマンスを向上して Internal Lab デバイスと Engineering デスクトップ間の偽陽性をなくすために、攻撃検出を免除したいとします。免除ルールは、図 74 のようになります。

図 74: ソースおよび宛先の免除



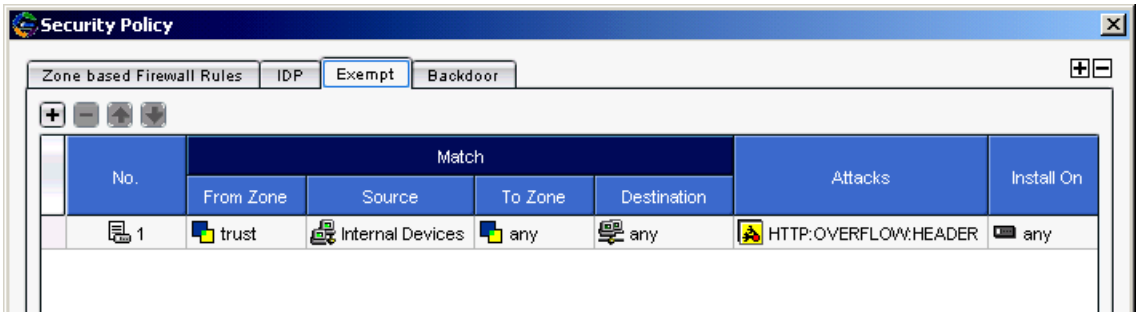
攻撃オブジェクトの設定

指定したソース / 宛先アドレスについて IDP に免除させたい攻撃を指定します。免除ルールには、攻撃オブジェクトを最低 1 つ含める必要があります。

例：特定の攻撃オブジェクトの免除

作成したセキュリティポリシーでは常に、HTTP BUFFER OVERFLOW 攻撃に偽陽性が生成されています。インターネットネットワーク上のヘッダーソース IP が自分の内部ネットワークであるときこの攻撃の攻撃検出を免除したいとします。免除ルールは、図 75 のようになります。

図 75: 攻撃オブジェクトの免除



ターゲットの設定

免除ルールベースのルールごとに、そのルールを使用して攻撃を検出および予防する IDP 対応デバイスを選択できます。そのルールが属するセキュリティポリシーをインストールすると、ルールは、ルールベースの Install On 列で選択されたデバイス上でのみアクティブになります。

コメントの入力

Comments 列にルールに関する注釈を入力できます。Comments 列の情報は、ターゲットデバイスにプッシュされません。コメントを入力するには、Comments 列を右クリックして、**Edit Comments** を選択します。Edit Comments ダイアログボックスが表示されます。1024 文字以内のコメントを入力できます。

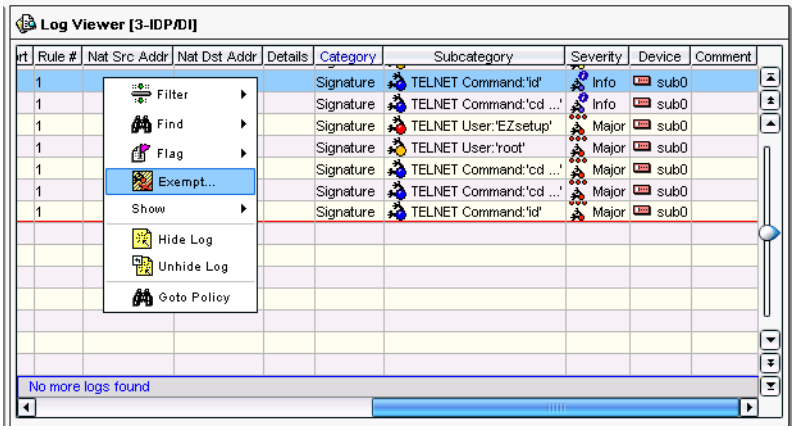
ログビューアから免除ルールを作成

また、NetScreen-Security Manager のログビューアからも、免除ルールベースにルールを直接作成できます。この方法を使用すると、偽陽性のログレコードを生成するルールをすばやく消去できます。（IDP ログの表示に関する詳細については、234 ページの「IDP の管理」を参照してください。ログビューアの使用に関する詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。）

ログビューアから免除ルールを作成するには、次の手順を行います。

1. ログビューアで IDP/DI ログを表示します。
2. 免除したい攻撃オブジェクトが含まれたログレコードを右クリックして、**Exempt** を選択します。

図 76: ログレコードルールの免除



ログレコードを生成したセキュリティポリシーの免除ルールベースが、ログエントリに関係する免除ルールとともに表示されます。ルールのソース、宛先および攻撃の設定は、ログレコードの情報に基づいて、自動的に記入されています。

注： ログビューアから免除ルールを作成したときに免除ルールベースがまだ存在しない場合、ルールベースが自動的に作成され、ルールが追加されます。

免除ルールベースに直接作成した他の免除ルールと同じ方法で、ログビューアから作成した免除ルールを変更、再順序付け、および結合することができます。

バックドアルールの構成

バックドアは、ホストコンピュータにインストールされた機構で、システムへの無許可アクセスを可能にします。すでにシステムに不正侵入している攻撃者は、バックドアを仕掛けてより簡単に攻撃できるようにしてしまいます。攻撃者がバックドアを操作するコマンドをタイプすると、双方向のトラフィックが生成されます。

既知のバックドアファイルや実行ファイルをホストシステムでスキャンするウィルス対策ソフトウェアとは異なり、IDP は、バックドアが使用されたときに発生する対話型のトラフィックを検出します。対話型のトラフィックが検出されると、IDP は IP アクションをその接続に対して実行して、攻撃者がネットワークをこれ以上侵害できないようにします。

バックドアルールを構成する場合は、以下の項目を指定します。

- モニタするトラフィックのソースおよび宛先アドレス。対話型の受信トラフィックを検出するには、Source を「any」、Destination を防御したいネットワークデバイスの IP アドレスに設定します。対話型の発信トラフィックを検出するには、Source を防御したいネットワークデバイスの IP アドレスに、Destination を「any」に設定します。
- Source または Destination が提供するサービス、および攻撃者がインストールし使用できる対話型サービス。

注： Telnet、SSH、RSH、NetMeeting または VNC を入れないでください。これらのサービスは正当にリモートシステムを制御するためしばしば利用され、これらを入れると誤検知が発生する場合があります。

- 対話型のトラフィックが検知された場合に、IDP が実行するアクション。Operation を 「detect」に設定します。多数のネットワークデバイスを対話型トラフィックから防御している場合は、これらのデバイスから来た承認された形式の対話型トラフィックを無視するルールを作成してから、これらのデバイスから来たすべての対話型トラフィックを検出する別のルールを作成できます。

注： バックドアルールベースは、ターミナルルールベースです。つまり、IDP がバックドアルールベースのルールに一致するトラフィックを見つけると、後続のルールは実行しません。

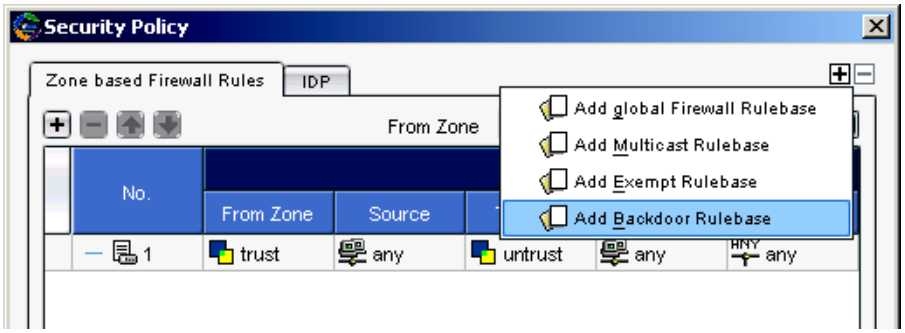
バックドアルールベースの追加

バックドアルールベースのルールを構成する前に、次の手順を使用して、セキュリティポリシーにバックドアルールベースを追加する必要があります。

1. メインナビゲーションツリーで、**Security Policies** を選択します。Security Policy ウィンドウのポリシー名をダブルクリックするか、またはポリシー名をクリックして、Edit アイコンを選択することにより、セキュリティポリシーを開きます。

2. バックドアルールベースを構成するには、Security Policy ウィンドウの右上角にある Add アイコンをクリックします（図 77 を参照）。

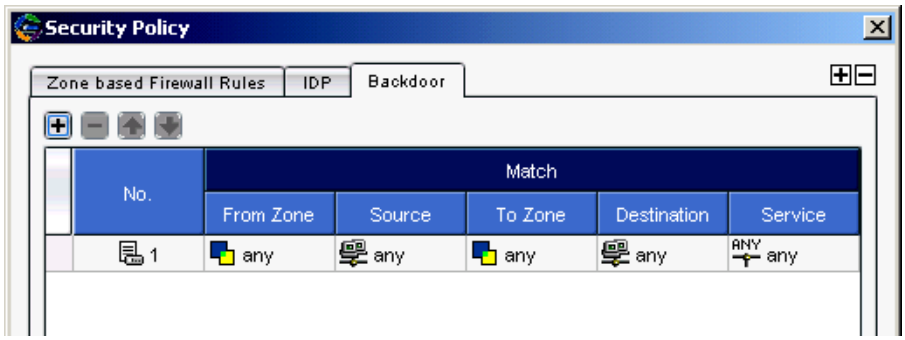
図 77: バックドアルールベースの追加



3. **Add Backdoor Rulebase** を選択します。

   デフォルトのバックドアルールが、図 78 のように表示されます。必要に応じて、このルールを変更できます。

図 78: 追加したバックドアルール



一致の定義

バックドアまたはトロイの木馬を指摘するために、IDP に監視させるトラフィックを指定します。Match 列の From Zone、Source、To Zone、Destination、および Service は、バックドアルールベースの全ルールに必要です。

次のセクションでは、バックドアルールの Match 列を詳しく説明します。

ソースゾーンおよび宛先ゾーン

ソースと宛先に複数のゾーンを選択できます。ただし、これらのゾーンは、ポリシーをインストールするセキュリティデバイスで利用可能でなければなりません。任意のゾーンから発生する、または任意のゾーンが宛先となる、ネットワークトラフィックをモニタするため、ソースゾーンまたは宛先ゾーンに「any」を指定できます。

注： セキュリティデバイスにカスタムゾーンを作成できます。ソースゾーンおよび宛先ゾーンを選択できるゾーンのリストには、NetScreen-Security Manager が管理する全デバイス用に構成された、定義済みゾーンとカスタムゾーンが含まれています。したがって、セキュリティポリシーをインストールするデバイスに適用可能なゾーンだけを選択します。

ソースおよび宛先アドレスオブジェクト

NetScreen-Security Manager システムでは、アドレスオブジェクトは、ホスト、ネットワーク、サーバーなどの、ネットワーク上のコンポーネントを表すために使用されます。通常、ネットワーク上のサーバーなどのデバイスは、送られてきた攻撃の宛先 IP であり、対話型攻撃の場合は発信元 IP になっている可能性があります。任意の IP アドレスから発生するネットワークトラフィックをモニタするため、「any」を指定できます。また、除外されたアドレスオブジェクト以外のソースまたは宛先をすべて指定するため、Source または Destination 列に示されたアドレスオブジェクトを否定することもできます。

バックドアルールを作成する前（*NetScreen-Security Manager Administrator's Guide* を参照）、またはバックドアルールの作成または編集の間に、アドレスオブジェクトを作成できます。アドレスオブジェクトを選択または構成するには、ルールの Source または Destination 列のいずれかを右クリックして、**Select Address** を選択します。Select Source Addresses ダイアログボックスで、既に作成されたアドレスオブジェクトを選択するか、または新しいホスト、ネットワーク、またはグループオブジェクトを作成するために **Add** アイコンをクリックします。

Services

対話型サービスオブジェクトを選択します。ソースまたは宛先 IP が供給するサービスだけでなく、供給されない対話式サービスも必ず含めてください。攻撃者はバックドアを使用してあらゆる双方向サービスをインストールできます。Telnet、SSH、RSH、NetMeeting または VNC を入れないでください。これらのサービスは正当にリモートシステムを制御するためしばしば利用され、これらを入れると誤検知が発生する場合があります。

操作の設定

Operation を **detect** または **ignore** に設定します。**detect** を選択した場合は、バックドアトラフィックが検出された場合に実行するアクションを選択します。多数のアドレスオブジェクトを対話型トラフィックから防御している場合は、これらのオブジェクトから来る承認された形式の対話型トラフィックを無視するルールを作成してから、これらのオブジェクトから来るすべての対話式トラフィックを検出する別のルールを作成できます。

アクションの設定

次の手順を使って、IDP が対話型トラフィックを検出した場合に実行するアクションを構成します。

表 18: バックドアルールのアクション

アクション	解説
Accept	IDP は対話式トラフィックを承認します。
Drop Connection	IDP は、RST パケットを送信側に送らずに対話型接続を除去し、トラフィックがその宛先に届かないようにします。このアクションを使用して、スプーフィングするタイプでないトラフィックの接続を除去します。
Close Client and Server	IDP は対話型の接続を閉じて、RST パケットをクライアントとサーバーの両方へ送ります。IDP がスニッファモードの場合、IDP は、RST パケットをクライアントとサーバーの両方へ送りますが、接続は閉じません。
Close Client	IDP は、クライアントへの対話型接続を閉じますが、サーバーへの対話型接続は閉じません。
Close Server	IDP は、サーバーへの対話型接続を閉じますが、クライアントへの対話型接続は閉じません。

通知の設定

初めてセキュリティポリシーを設計するときは、攻撃のデータをすべてログに記録し、ポリシーを無制限に実行したくなるものです。しかし、これはすべきでありません。攻撃オブジェクトには、通知のみを行うものや、誤検知や冗長ログを生成できるものがあります。データが過剰になると、重要なものを見逃す可能性があります。セキュリティポリシーの生成するログレコードが多すぎると、攻撃の発見が遅れたり、何百ものログ記録を調べるためにセキュリティの抜け穴を見逃してしまうため、ネットワークのセキュリティに有害なことを忘れないでください。過剰なロギングは、IDP の処理能力、性能、および使用可能なディスク領域にも影響を及ぼします。良いセキュリティポリシーは、ネットワーク上の重要なセキュリティイベントだけがすべて記録されるログを生成します。

ロギングの設定

Configure Notification ダイアログボックスで、**Logging** を選択して、**OK** をクリックします。ルールが一致するごとに、IDP システムはログレコードを作成してログビューアに表示します。

攻撃のロギングにより、ログビューアにリアルタイムで表示できるログレコードが作成されます。より重大な攻撃については、通知フラグをログレコードに表示するよう設定したり、電子メールによって直ちに通知させたり、攻撃に応じて IDP にスクリプトを実行させたり、ログレコードにアラームフラグを表示するよう設定したりできます。セキュリティポリシーの攻撃通知を各自のセキュリティニーズに合わせて微調整することを目標にしてください。

あるルールの攻撃をログするには、ルールの Notification 列を右クリックして、**Configure** を選択します。Configure Notification ダイアログボックスが表示されます。

警報の設定

Configure Notification ダイアログボックスで、**Alert** を選択して、**OK** をクリックします。Alert を選択してルールが一致すると、IDP は、一致したログレコードについて、警報フラグをログビューアの Alert 列にセットします。

パケットのロギング

ルールに一致したネットワークトラフィックの中のパケットを個々に記録するには、攻撃のパケットデータをキャプチャします。ネットワークの攻撃で使用されているパケットを見ることで、試みられている攻撃の範囲とその目的、攻撃が成功したかどうか、そしてネットワークに与えるあらゆる損害を判別できます。

注 : IDP 性能を向上させるには、攻撃後のパケットだけをログします。

パケットキャプチャを有効にした複数ルールが同じ攻撃に一致すると、IDP は指定されたパケットの最大数をキャプチャします。たとえば、ルール 1 で攻撃の前後 10 パケットをキャプチャするように構成し、ルール 2 は攻撃の前後 5 パケットをキャプチャするよう構成したとします。両方のルールが同じ攻撃に適合した場合、IDP は攻撃の前後 10 パケットをキャプチャしようとします。

注 : パケットキャプチャは、攻撃前後の 256 パケットまでに限られます。

重大度の構成

バックドアルールベース内のルール単位で、攻撃に固有の重大度を変更できます。重大度は、Default、Info、Warning、Minor、Major、または Critical に設定できます。

ルールの重大度を変更するには、Severity 列を右クリックして、重大度を選択します。

ターゲットの設定

バックドアルールベースのルールごとに、そのルールを使用して攻撃を検出および予防するセキュリティデバイスを選択できます。そのルールが属するセキュリティポリシーをインストールすると、ルールは、ルールベースの Install On 列で選択されたデバイス上でのみアクティブになります。

コメントの入力

Comments 列にルールに関する注釈を入力できます。Comments 列の情報は、ターゲットデバイスにプッシュされません。コメントを入力するには、Comments 列を右クリックして、**Edit Comments** を選択します。Edit Comments ダイアログボックスが表示されます。1024 文字以内のコメントを入力できます。

IDP 攻撃オブジェクトの構成

攻撃オブジェクトは、攻撃者がネットワークに損害を与えるために使用できる、既知の攻撃のパターンを持っています。攻撃オブジェクトは、単体では動作しません。ルールの一部になってから、既知の攻撃を検出したり、ユーザーのネットワークに不正なトラフィックが入るのを防いだりできます。IDP ルールで攻撃オブジェクトを使用するには、セキュリティポリシーに IDP ルールベースを追加してから、そのルールベースに IDP ルールを追加します。184 ページの「セキュリティポリシーの構成」を参照してください。

注： IDP は、IDP 対応のセキュリティデバイスでだけサポートされます。

IDP 攻撃オブジェクトのタイプ

セキュリティポリシーでは、ネットワークに対する攻撃を検出するためデバイスが使用する攻撃オブジェクトを選択できます。攻撃が検出されると、そのデバイスが、ログビューアに表示される攻撃ログエントリを生成します。詳細については、189 ページの「IDP ルールの構成」を参照してください。

NetScreen-Security Manager は、次の 3 タイプの IDP 攻撃オブジェクトをサポートします。

- シグネチャ攻撃オブジェクト
- プロトコルアノーマリ攻撃オブジェクト
- 複合攻撃オブジェクト

次のセクションで、各攻撃オブジェクトのタイプを詳しく説明します。

シグネチャ攻撃オブジェクト

攻撃 *シグネチャ*とは、ある攻撃に常に存在するパターンを指します。その攻撃が存在すると、攻撃シグネチャも存在します。IDP は、*ステートフルシグネチャ*を使用して、攻撃を検出します。ステートフルシグネチャは、標準のシグネチャより具体的です。ステートフルシグネチャを使って、IDP は、攻撃の実行に使用される特定のプロトコルまたはサービス、攻撃の方向と流れ、および攻撃が生じるコンテキストをさがすことができます。ScreenOS は、攻撃オブジェクトに、サービス、コンテキストなどの情報と攻撃パターンを組み合わせて入れています。攻撃のコンテキストが定義され、攻撃が生じなかったネットワークトラフィックの大部分を除去するので、ステートフルシグネチャでは誤検知がほとんど生じません。

プロトコルアノーマリ攻撃オブジェクト

プロトコルアノーマリ攻撃オブジェクトは、使用されている特定のプロトコルのルールの集合に従って、接続内の異常または曖昧なメッセージを検知します。RFC および一般的な RFC 拡張が定義する場合の多い、プロトコル標準からの逸脱を発見することによって、プロトコルアノーマリ検出は機能しま。ほとんどの合法トラフィックは、確立されているプロトコルに忠実です。忠実でないトラフィックは、IPS を回避するなど、特定の目的のために攻撃者が作成したアノーマリを生成します。

複合攻撃オブジェクト

複合攻撃オブジェクトは、単一のオブジェクトに、複数のシグネチャやプロトコルアノーマリを組み合わせたものです。トラフィックが、複合攻撃オブジェクトに一致するには、組み合わされたシグネチャやプロトコルアノーマリすべてに一致する必要があります。また、シグネチャやアノーマリが一致する順番も指定できます。複合攻撃オブジェクトを使用してセキュリティポリシールールをより詳細にすると、誤検知を減らして検出の正確性を向上できます。

複合攻撃オブジェクトは、どのようなイベントが起きればトラフィックが攻撃として識別されるかについて、非常に具体的に指定できます。たとえば、FTP セッションで特定のユーザーのログインが失敗した場合にのみ、対応したい場合があります。

定義済み IDP 攻撃オブジェクトおよびグループの表示

Juniper Networks は、既知の攻撃についてトラフィックを照合するため、セキュリティポリシーで使用できる定義済み攻撃オブジェクトおよび攻撃オブジェクトグループを提供しています。Juniper Networks は定期的に定義済み攻撃オブジェクトおよびグループを更新します。定義済み攻撃オブジェクトの作成、編集、削除はできませんが、セキュリティポリシーで使用できる攻撃オブジェクトのリストは更新できます。改訂された攻撃オブジェクトおよびグループは、NetScreen-Security Manager GUI サーバーにダウンロードされる、攻撃データベース更新の一部として利用可能です。攻撃データ更新に関する詳細については、234 ページの「IDP の管理」を参照してください。

定義済み攻撃オブジェクトおよびグループを表示するには、次の手順を実行します。

1. Object Manager で、**Attack Objects > IDP Objects** をクリックします。IDP Objects ダイアログボックスが表示されます。

2. Predefined Attacks または Predefined Attack Groups タブをクリックして、定義済み攻撃オブジェクトおよびグループを表示します。

定義済み攻撃の表示

Predefined Attacks タブは、すべての攻撃を表形式で表示し、それには次の情報が含まれています。

- 攻撃オブジェクトの名前
- 攻撃の重大度。critical、major、minor、warning、info
- カテゴリ

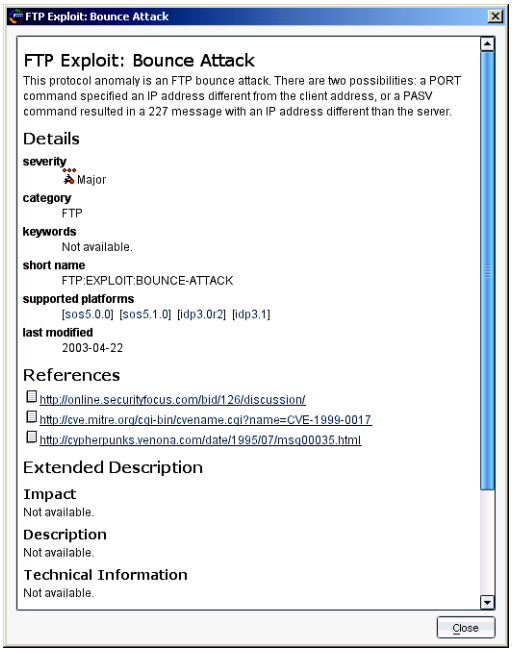
- 攻撃のキーワード
- CVE 番号。これは、Common Vulnerabilities and Exposures データベースに登録されている攻撃の番号を識別するためのものです。
- Bugtraq 番号。これは、Security Focus Bugtraq データベースに登録されている同種の攻撃を識別します。

最初、攻撃オブジェクトは、カテゴリ名別にアルファベット順で表示されますが、コラム見出しをクリックすると、別の順序で攻撃を表示できます。

定義済み攻撃オブジェクトを使用するルールをすべて確認するには、攻撃オブジェクトを右クリックして、**View Usages** を選択します。

攻撃オブジェクトの詳細な説明を表示するには、攻撃をダブルクリックします。

図 79: 攻撃ビューア



定義済みグループの表示

Predefined Attack Group タブに次の定義済み攻撃グループが表示されます。

- **Recommended** - Juniper Networks が深刻な脅威であると考える全攻撃オブジェクトをカテゴリごとに一覧にしたリスト。
  - **Attack Type** は、攻撃オブジェクトをタイプ（アノーマリまたはシグネチャ）別にグループ分けします。各タイプでは、攻撃オブジェクトは重大度別にグループ分けされます。
  - **Category** は、攻撃オブジェクトを定義済みカテゴリ別にグループ分けします。各カテゴリ内では、攻撃オブジェクトは重大度別にグループ分けされます。

- **Operating System** は、BSD、Linux、Solaris または Windows といった、適用されるオペレーティングシステム別に攻撃オブジェクトをグループ分けします。各オペレーティングシステムでは、攻撃オブジェクトはサービスおよび重大度別にグループ分けされます。

- **Severity** は、攻撃に割り当てられた重大度別に攻撃オブジェクトをグループ分けします。IDP には、Info、Warning、Minor、Major、Critical という、5 つの重大度レベルがあります。各重大度内では、攻撃オブジェクトはカテゴリ別にグループ分けされます。

定義済み攻撃オブジェクトグループを使用するルールをすべて確認するには、攻撃オブジェクトグループを右クリックして、**View Usages** を選択します。

攻撃オブジェクトの詳細な説明を表示するには、攻撃をダブルクリックします。

定義済みグループに関する詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。

カスタム IDP 攻撃オブジェクトの作成

新しい攻撃を検知したり、あるいは、ユーザーのネットワーク独自のニーズを満たすため、カスタム攻撃オブジェクトを作成できます。

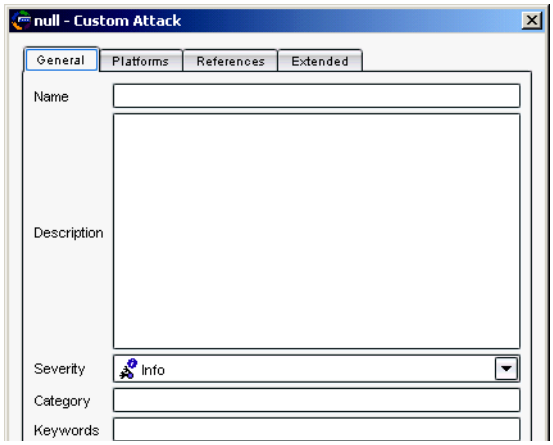
カスタム攻撃オブジェクトを作成するには、次の手順を実行します。

1. Object Manager で、**Attack Objects > IDP Objects** をクリックします。IDP Objects ダイアログボックスが表示されます。

2. **Custom Attacks** タブをクリックします。

3. **Add** アイコンをクリックします。Custom Attack ダイアログボックスが、General タブが選択された状態で表示されます。

図 80: Custom Attack ダイアログボックス



a. 攻撃の名前を入力します。この名前を使用して、UI に攻撃オブジェクトを表示します。攻撃名に攻撃が使用するプロトコルを含めたい場合があります。

b. 攻撃の説明を入力します。説明は、攻撃の詳細を示します。新しい攻撃オブジェクトを作成するとき、説明の入力はオプションです。しかし、攻撃に関する重要な情報を覚えておくのに役立ちます。例として、定義済み攻撃の攻撃の説明を表示します。定義済み攻撃に関する詳細を表示するには、213 ページの「定義済み攻撃の表示」を参照してください。

c. この攻撃の重大度を、Info、Warning、Minor、Major、または Critical から選択します。クリティカル攻撃は最も危険な攻撃で、多くの場合サーバーをクラッシュさせたりネットワークの制御権を奪おうとしたりします。通知の攻撃は最も危険度が低く、通常はネットワーク管理者が自分のセキュリティシステムのセキュリティホールを発見するために使用します。

d. この攻撃のカテゴリを入力します。定義済みのカテゴリを使用したり、新しいカテゴリを定義できます。

e. 後で見つけるのに役立つ、この攻撃のキーワードを 1 つ以上入力します。キーワードとは、ログレコードの攻撃オブジェクトを表示するため使用される一意の識別子です。キーワードは、攻撃や攻撃オブジェクトに関連した重要な単語を示します。

f. この攻撃オブジェクトを危険度が最も高いグループに入れたい場合は、チェックボックスをチェックしてください。その後、動的なグループにこの攻撃オブジェクトを追加すると、推奨された攻撃オブジェクトだけを含むかどうか指定できます。推奨された攻撃オブジェクトに関する詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。

4. Custom Attack ダイアログボックスの Platforms タブをクリックして、攻撃の検出が行われるセキュリティプラットフォームを指定します。

a. Add アイコンをクリックします。Custom Attack ダイアログボックスが表示されます。

b. 攻撃の検出が行われるプラットフォームを選択します。

c. 攻撃のタイプを、Signature、Protocol Anomaly、または Compound Attack から選択します。次に、**Next** をクリックします。

新しい攻撃オブジェクトを構成している場合、攻撃オブジェクトエディタに指示に従って、具体的なタイプの攻撃を構成します。

- シグネチャ攻撃オブジェクトについては、次のセクション、「シグネチャ攻撃オブジェクトの作成」を参照してください。
- プロトコルアノーマリ攻撃オブジェクトについては、213 ページの「プロトコルアノーマリ攻撃オブジェクト」を参照してください。
- 複合攻撃オブジェクトについては、213 ページの「複合攻撃オブジェクト」を参照してください。

シグネチャ攻撃オブジェクトの作成

Custom Attack ダイアログボックスでシグネチャ攻撃を構成するには、次の手順を実行します。

1. 次の手順を実行して、攻撃の汎用パラメータを構成します。

   - **False-Positives** は、セキュリティポリシーで使用された時に攻撃オブジェクトが誤検知を行う頻度（Unknown、Rarely、Occasionally、Frequently）を示します。デフォルトでは、すべての複合攻撃オブジェクトは Unknown に設定されています。ネットワークトラフィックに応じて IDP システムを微調整しながら、この設定を変更し、誤検知の追跡に役立てることができます。

   - **Service Binding** では、攻撃がネットワークに入るために使用するプロトコルを選択できます。選択したプロトコルによっては、さらにフィールドが表示される場合があります。以下のプロトコルタイプを指定できます。

     - **Any** では、IDP は、すべてのサービスでシグネチャを照合します（攻撃は、複数のサービスを使用して、ネットワークを攻撃できます）。

     - **IP**（プロトコル番号を指定）では、IDP は、指定した IP プロトコルタイプについてシグネチャを照合します。

     - **TCP**（ポートの範囲を指定）では、IDP は、指定した TCP ポートについてシグネチャを照合します。

     - **UDP**（ポートの範囲を指定）では、IDP は、指定した UDP ポートについてシグネチャを照合します。

     - **ICMP**（ID を指定）では、IDP は、指定した ICMP ID についてシグネチャを照合します。

     - **RPC**（プログラム番号を指定）では、IDP は、指定したリモートプロシージャコール プログラム番号についてシグネチャを照合します。

     - **Service**（サービスを指定）では、IDP は、指定したサービスについてシグネチャを照合します。

   - **Time Binding** では、IDP は、ある期間にわたって連続する同じ攻撃を検出できます。**Time Binding** を選択した場合、攻撃オブジェクトに 1 分間バインドされる次の属性を指定できます。

     - **Scope** は、攻撃のカウントを、同じソース IP アドレス、同じ宛先 IP アドレスまたはピアから来ている攻撃について行うかを指定します。**Source** を選択すると、宛先 IP アドレスに関係なく、IDP は、指定された回数分、ある IP ソースアドレスからの攻撃を検出します。**Destination** を選択すると、ソース IP アドレスに関係なく、IDP は、指定された回数分、ある宛先 IP アドレスに対する攻撃を検出します。**Peer** を選択すると、IDP は、指定された回数分、ソースおよび宛先 IP アドレス間での攻撃を検出します。

     - **Count** は、イベントをトリガーされる前に、指定した範囲内で IDP が攻撃を検出する回数を指定します。

2. **Next** をクリックします。

3. シグネチャ攻撃の検出パラメータを構成します。

   - 攻撃パターンは検出する攻撃のシグネチャです。シグネチャとは、ある攻撃に常に存在するパターンを指します。その攻撃が存在すると、シグネチャも存在します。新しいシグネチャ攻撃オブジェクトを作成するときは、攻撃を分析してパターン（コードのセグメント、URL、パケットヘッダーの値など）を検出し、そのパターンを使用してシグネチャを作成してください。入力したパターンを否定することもできます。

     表 19 は、攻撃パターンで使用できる正規表現を示します。

表 19: 攻撃パターンの表現

正規表現	解説
\0<*8- 進数*>	直接バイナリ一致
\X<*16- 進数*>\X	直接バイナリ一致
\[< *文字セット* >\]	大文字と小文字を区別しない一致
.	すべての記号と一致
*	0 個以上の記号と一致
+	1 個以上の記号と一致
?	0 個または 1 個の記号と一致
( )	表現のグループ化
|	代替を表す。通常は ( ) と使用。
[< *開始* >-< *終了*>]	文字範囲
[^< *開始* >-< *終了*>]	範囲の否定。

   - **Offset** は、IDP が攻撃を捜す指定されたサービスコンテキストからの出発点となります。オフセットがない場合、**None** を指定できます。ある場合は、10 進値を指定できます。

   - **Context** は、特定のアプリケーションレイヤプロトコルで、IDP が攻撃を捜すべき場所を定義します。シグネチャ攻撃オブジェクトを作成するときは、できればサービスコンテキストを選択してください。サービスコンテキストは非常に具体的なため、偽陽性を検出する確率が非常に低くなります。ただし、サービスコンテキストを選択すると、以前に Service Binding 汎用パラメータで指定したプロトコルは無効になります。

     表 20 は、攻撃に使用できるサービスコンテキストを示しています。

表 20: シグネチャ攻撃のサービスコンテキスト

Service	解説	RFC
AIM	AOL インスタントメッセンジャー	
DHCP	動的ホスト設定プロトコル	2131, 2132
DNS	ドメイン名システム	1034, 1035
Finger	Finger 情報プロトコル	1128
FTP	ファイル転送プロトコル	959

Service	解説	RFC
Gnutella	Gnutella	
Gopher	Gopher	1436
HTTP	ハイパーテキスト転送プロトコル	2616
IMAP	インターネットメッセージアクセスプロトコル	2060
IRC	インターネットリレーチャット	2810, 2811, 2812, 2813
LDAP	軽量ディレクトリアクセスプロトコル	2251, 2252, 2253, 3377
LPR	ラインプリンタプロトコル	1179
MSN	Microsoft インスタントメッセンジャー	
NBNAME/ NBDS	NetBios ネームサービス	1001, 1002
NFS	ネットワークファイルシステム	
NNTP	ネットワークニュース転送プロトコル	977
NTP	ネットワークタイムプロトコル	1305
POP3	ポストオフィスプロトコル、バージョン 3	1081
RADIUS	リモート認証ダイヤルインユーザーサービス	2865, 2866, 2867, 2868, 3575
REXEC		
RLOGIN	リモートログイン (rlogin)	1258, 1282
RSH	リモートシェル (rsh)	
RUSERS		
SMB	サーバーメッセージブロック	
SMTP	簡易メール転送プロトコル	821
SNMP	簡易ネットワーク管理プロトコル	1067
SNMPTRAP	SNMP トラップ	1067
SSH	セキュアシェル	所有権
SSL	セキュアソケットレイヤー	
Telnet	Telnet TCP プロトコル	854
TFTP	簡易ファイル転送プロトコル	783
VNC	仮想ネットワークコンピューティング	
YMSG	Yahoo! Messenger	

- **Direction** では、攻撃の接続方向が定義されます。
  - **Client to Server** は、クライアントからサーバーへのトラフィックのみで攻撃を検出します。
  - **Server to Client** は、サーバーからクライアントへのトラフィックのみで攻撃を検出します。
  - **Any** は、いずれの方向の攻撃も検出します。
- **Flow** では、攻撃の接続フローを Control、Auxiliary、または Both に定義します。

4. **Next** をクリックします。
5. そのシグネチャ攻撃のヘッダー照合情報を構成します。ヘッダー照合の構成により、IDP は、次のプロトコルのヘッダー情報についてだけ、パターンマッチを捜してパケットを探索するように指定できます。
   - インターネットプロトコル (IP)
     - **Type-of-service**: オペランド（なし、=、!、>、<）および 10 進数を指定します。
     - **Total length**: オペランド（なし、=、!、>、<）および 10 進数を指定します。
     - **ID**: オペランド（なし、=、!、>、<）および 10 進数を指定します。
     - **Time-to-live**: オペランド（なし、=、!、>、<）および 10 進数を指定します。
     - **Protocol**: オペランド（なし、=、!、>、<）および 10 進数を指定します。
     - **Source**: 攻撃を行っているデバイスの IP アドレスを指定します。
     - **Destination**: 攻撃の対象の IP アドレスを指定します。
     - **Reserved Bit**: IP フラグが設定されていてもいなくても（**none**）、フラグが設定されている場合だけ（**set**）、またはフラグが設定されていない場合だけ（**unset**）、IDP が、パターンマッチを捜すように指定します。
     - **More Fragments**: IP フラグが設定されていてもいなくても（**none**）、フラグが設定されている場合だけ（**set**）、またはフラグが設定されていない場合だけ（**unset**）、IDP が、パターンマッチを捜すように指定します。
     - **Don't Fragment**: IP フラグが設定されていてもいなくても（**none**）、フラグが設定されている場合だけ（**set**）、またはフラグが設定されていない場合だけ（**unset**）、IDP が、パターンマッチを捜すように指定します。

- TCP（伝送制御プロトコル）
  - **Source Port**: 攻撃しているデバイスのポート番号。
  - **Destination Port**: 攻撃の対象のポート番号。
  - **Sequence Number**: パケットのシーケンス番号。この番号はデータシーケンス全体におけるデータの位置を識別します。
  - **ACK Number**: パケットの ACK 番号。この番号は次のシーケンス番号を識別します。このフィールドをアクティブにするには ACK フラグを設定する必要があります。
  - **Header Length**: TCP ヘッダーのバイト数。
  - **Window Size**: TCP ウィンドウサイズのバイト数。
  - **Urgent Pointer**: パケット内のデータが緊急であることを示します。このフィールドをアクティブにするには URG フラグを設定する必要があります。
  - **Data Length**: データペイロードのバイト数。SYN、ACK、および FIN パケットではこのフィールドを空白にする必要があります。

  また、次の TCP フラグオプションで **none**、**set**、または **unset** を指定できます。
    - **URG**: set にすると、パケットデータが緊急であることを緊急フラグが示します。
    - **ACK**: set にすると、確認応答フラグがパケットの受信を確認します。
    - **PSH**: set にすると、受信者がシーケンスの残りのパケットを待たずに現在のシーケンスの全データを宛先アプリケーション (ポート番号で識別) に設定すべきであることをプッシュフラグが示します。
    - **RST**: set にすると、リセットフラグが TCP 接続をリセットし、既存のシーケンスのパケットはすべて廃棄されます。
    - **FIN**: set にすると、パケット転送が完了し接続を終了できることを終了フラグが示します。
- ユーザーデータグラムプロトコル (UDP)
  - **Source Port**: 攻撃しているデバイスのポート番号。オペランド（なし、=、!、>、<）および 10 進数を指定します。
  - **Destination Port**: 攻撃の対象のポート番号。オペランド（なし、=、!、>、<）および 10 進数を指定します。
  - **Data Length**: データペイロードのバイト数。オペランド（なし、=、!、>、<）および 10 進数を指定します。

- インターネット制御メッセージプロトコル
  - **ICMP Type**: 要求 / 応答の機能を識別する 1 次コード。
  - **ICMP Code**: 設定されたタイプの要求 / 応答の機能を識別する 2 次コード。
  - **Sequence Number**: パケットのシーケンス番号。この数値はシーケンス全体における要求 / 応答の位置を識別します。
  - **ICMP ID**: ID 番号は、宛先システムが要求と応答を関連付けるのに使用する一意の値です。
  - **Data Length**: データペイロードのバイト数。

6. **Finish** をクリックします。

プロトコルアノーマリ攻撃の作成

次の手順を実行して、Custom Attack ダイアログボックスでプロトコルアノーマリ攻撃を構成します。

1. 攻撃の汎用パラメータを構成します。

   - **False-Positives** は、セキュリティポリシーで使用された時に攻撃オブジェクトが誤検知を行う頻度（**Unknown**、**Rarely**、**Occasionally**、**Frequently**）を示します。IDP システムをネットワークトラフィックに適するよう微調整するときに、この設定を変更すると、誤検知を追跡するのに役立ちます。

   - **Anomaly** では、既知のプログラムアノーマリのリストから、プロトコルアノーマリを選択できます。NetScreen-Security Manager は、次のプロトコルのアノーマリを検出します。

AIM	DHCP	IDENT	RUSERS	TFTP
FINGER	CHARGEN	IMAP	Gnutella	RLOGIN
FTP	DISCARD	IP Packet	Gopher	RPC
HTTP	DNS	POP3	IRC	RSH
ICMP	ECHO	REXEC	MSN	RTSP
MSN	LPR	NFS	VNC	NNTP
SNMP	SMTP	SMB	SNMP TRAP	YMSG
TCP セグメント	SYSLOG	SSH	TELNET	

   - **Time Binding** では、IDP は、指定した期間にわたって連続する同じ攻撃を検出できます。**Time Binding** を選択した場合、攻撃オブジェクトに 1 分間バインドされる次の属性を指定できます。
     - **Scope** は、攻撃のカウントを、同じソース IP アドレス、同じ宛先 IP アドレスまたはピアから来ている攻撃について行うかを指定します。**Source** を選択すると、宛先 IP アドレスに関係なく、IDP は、指定された回数分、ある IP ソースアドレスからの攻撃を検出します。**Destination** を選択すると、ソース IP アドレスに関係なく、IDP は、

指定された回数分、ある宛先 IP アドレスに対する攻撃を検出します。**Peer** を選択すると、IDP は、指定された回数分、ソースおよび宛先 IP アドレス間での攻撃を検出します。

- **Count** は、イベントがトリガーされる前に、指定された範囲内で攻撃を検出する回数を指定します。

2. **Finish** をクリックします。

複合攻撃の作成

カスタム複合攻撃オブジェクトを作成するときは、次に注意します。

- 複合攻撃オブジェクトのメンバはすべて、FTP、Telnet、YMSG、TCP/80 など同じサービス設定やサービスバインディングを使用する必要があります。
- 定義済み、またはカスタムのシグネチャ攻撃オブジェクトは、複合攻撃オブジェクトに追加できません。その代わり、複合攻撃オブジェクト内に直接シグネチャを指定します。この場合は、サービス（またはサービスバインディング）、サービスコンテキスト、攻撃パターン、および方向などの詳細を含めます。プロトコルアノーマリ攻撃オブジェクトは複合攻撃オブジェクトに追加できます。
- 複合攻撃オブジェクトのメンバとして、プロトコルアノーマリ攻撃オブジェクトやシグネチャを 2 ～ 32 個追加できます。ただし、すべてのメンバは同じサービス設定やサービスバインディングを使用する必要があります。

次の手順を実行して、Custom Attack ダイアログボックスで複合攻撃を構成します。

1. 攻撃の汎用パラメータを構成します。
   - **False-Positives** は、セキュリティポリシーで使用された時に攻撃オブジェクトが誤検知を行う頻度（**Unknown**、**Rarely**、**Occasionally**、**Frequently**）を示します。デフォルトでは、すべての複合攻撃オブジェクトは、**Unknown** に設定されています。IDP システムをネットワークトラフィックに適するよう微調整するときに、この設定を変更すると、誤検知を追跡するのに役立ちます。
   - **Service Binding** では、攻撃がネットワークに入るために使用するプロトコルを選択できます。選択したプロトコルによっては、さらにフィールドが表示される場合があります。以下のプロトコルタイプを指定できます。
     - **Any** では、IDP は、すべてのサービスでシグネチャを照合します（攻撃は、複数のサービスを使用して、ネットワークを攻撃できます）。
     - **IP**（プロトコル番号を指定）では、IDP は、指定した IP プロトコルタイプのシグネチャを照合します。
     - **TCP**（ポートの範囲を指定）では、IDP は、指定した TCP ポートについてシグネチャを照合します。
     - **UDP**（ポートの範囲を指定）では、IDP は、指定した UDP ポートについてシグネチャを照合します。

- **ICMP**（ID を指定）では、IDP は、指定した ICMP ID についてシグネチャを照合します。
- **RPC**（プログラム番号を指定）では、IDP は、指定したリモートプロシージャコール プログラム番号についてシグネチャを照合します。
- **Service**（サービスを指定）では、IDP は、指定したサービスについてシグネチャを照合します。

- **Time Binding** では、IDP は、指定した期間にわたって連続する同じ攻撃を検出できます。**Time Binding** を選択した場合、攻撃オブジェクトに 1 分間バインドされる次の属性を指定できます。
  - **Scope** は、攻撃のカウントを、同じソース IP アドレス、同じ宛先 IP アドレスまたはピアから来ている攻撃について行うかを指定します。**Source** を選択すると、宛先 IP アドレスに関係なく、IDP は、指定された回数分、ある IP ソースアドレスからの攻撃を検出します。**Destination** を選択すると、ソース IP アドレスに関係なく、IDP は、指定された回数分、ある宛先 IP アドレスに対する攻撃を検出します。**Peer** を選択すると、IDP は、指定された回数分、ソースおよび宛先 IP アドレス間での攻撃を検出します。
  - **Count** は、イベントがトリガーされる前に、指定された範囲内で攻撃を検出する回数を指定します。

2. **Next** をクリックします。
3. 次の手順を実行して、複合攻撃メンバを構成します。
   - **Scope** は、照合を単一セッションで行うか、または 1 つのセッション内の複数のトランザクションを横断して行うことができるかどうかを指定します :
     - **Session** を選択すると、同一セッション内でオブジェクトの一致が複数回可能になります。
     - **Transaction** を選択すると、同一セッション内で発生する複数のトランザクションでオブジェクトの一致が行えます。
   - 1 つのセッションまたはトランザクションで複合攻撃を複数回一致させる場合は、**Reset** を選択します。**Reset** に設定すると、1 つのセッションやトランザクション内で複数の一致が可能になります。
   - **Ordered Match** を使用して、シグネチャやプロトコルアノーマリの各メンバを指定した順序で照合する複合攻撃オブジェクトを作成します。順序指定一致を使用しない場合でも、複合攻撃オブジェクトは、すべてのメンバで照合する必要がありますが、攻撃やプロトコルアノーマリは任意の順序で出現できます。

次のセクションで説明するように、複合攻撃にシグネチャ攻撃オブジェクトやプロトコルアノーマリ攻撃オブジェクトを追加できます。

複合攻撃オブジェクトへのシグネチャの追加

1. 複合攻撃オブジェクトに攻撃パターンを追加するには、Add アイコンをクリックして、**Signature** を選択します。New Member ダイアログボックスが表示されます。

2. 複合攻撃オブジェクトの新しく作成されたシグネチャメンバをダブルクリックします。攻撃パターン設定を構成します。

   - **DFA Pattern**: IDP が一致させるパターンを指定します。新規シグネチャ攻撃オブジェクトの作成時と同じように、攻撃パターンを構築します。

     指定したパターンを照合から除外するには、Negate チェックボックスを選択します。

   - **Context:** IDP がパターンを検索するコンテキストを指定します。コンテキストには、指定したサービスに該当するコンテキストだけが表示されます。サービスバインディング **any** を選択した場合は、使用できるサービスコンテキストがパケットと先頭パケットのみに制限されます。

   - **Direction**: IDP がどちらの方向に流れているトラフィックでパターンの一致検索を行うのか、あるいはクライアントからサーバー、またはサーバーからクライアントに流れるトラフィックで一致検索を行うのかを指定します。

     方向を決定する前に、トラフィックを検討します。Juniper Networks は、性能を考慮して、クライアントからサーバーへの方向を推奨します。サーバーからクライアントを選択し、攻撃オブジェクトのリスクが、クライアントからサーバーの方が低い場合、デバイスに負担がかかります。

3. **OK** をクリックする。

複合攻撃オブジェクトへのプロトコルアノーマリの追加

1. 複合攻撃オブジェクトにプロトコルアノーマリを追加するには、Add アイコンをクリックして、**Anomaly** を選択します。New Member ダイアログボックスが表示されます。

2. アノーマリを選択します。

3. **OK** をクリックする。

複合攻撃オブジェクトからのメンバの削除

メンバのシグネチャやアノーマリを削除するには、リストからメンバを選択し Delete アイコンをクリックします。そのアイテムを削除してもよいか確認するウィンドウが表示されます。**OK** をクリックする。

カスタム攻撃オブジェクトの編集

カスタム攻撃オブジェクトを変更するには、IDP Objects ダイアログボックスの Custom Attacks タブでオブジェクトをダブルクリックします。Custom Attacks ダイアログボックスが現れ、General および Platforms タブで以前に構成した情報が表示されます。References タブおよび Extended タブにオプション情報を入力できます。必要な変更を入力したら、**Apply** をクリックします。ダイアログボックスを閉じるには、**OK** をクリックします。

カスタム攻撃オブジェクトの削除

カスタム攻撃オブジェクトを削除するには、IDP Objects ダイアログボックスの Custom Attacks タブでオブジェクトを右クリックして、**Delete** を選択します。そのアイテムを削除してもよいか確認するウィンドウが表示されます。**OK** をクリックする。

カスタム IDP 攻撃グループの作成

IDP システムには、何百もの定義済み攻撃オブジェクトがあります。また、さらにカスタム攻撃オブジェクトを作成できます。セキュリティポリシールールを作成すると、攻撃オブジェクトを個々に、または定義済み攻撃グループやカスタム攻撃グループごとに追加できます。セキュリティポリシーを整理するため、攻撃オブジェクトをグループに分けることができます。

指定したグループまたは攻撃オブジェクトだけを含む*静的グループ*、または指定した基準に基づく攻撃オブジェクトを含む*動的グループ*を作成できます。

静的グループの構成

静的グループには、特定の攻撃オブジェクトまたはグループが有限個含まれています。静的グループには、*定義済み*静的グループと*カスタム*静的グループの 2 種類があります。

定義済み静的グループには、次のメンバを含めることができます。

- 定義済み攻撃オブジェクト
- 定義済み静的グループ
- 定義済み動的グループ

カスタム静的グループには、定義済み静的グループと同じメンバに加えて、次のメンバを含めることができます。

- カスタム攻撃オブジェクト
- カスタム動的グループ
- 他のカスタム静的グループ

静的グループを使用して、次を行います。

- ネットワークが被害を受けやすいことがわかっている攻撃の集合を定義する。
- グループカスタム攻撃オブジェクト
- 通知攻撃オブジェクトの集合を定義し、ネットワークの状況を把握しておくために使用する。

静的グループでメンバを変更するには、グループ内の攻撃オブジェクトを手動で追加したり削除したりしなければならないため、静的グループは動的グループよりもメンテナンスの手間がかかります。ただし、静的グループの中に動的グループを含めると、一部の攻撃オブジェクトを自動的に更新できます。たとえば、定

義済み攻撃オブジェクトグループ Operating System は、BSD、Linux、Solaris、および Windows という、4 つの定義済み静的グループを含んでいる、静的グループです。BSD グループは、攻撃データベース更新中に攻撃オブジェクトを追加できる、定義済み動的グループ BSD-Services-Critical を含んでいます。

カスタム静的グループを作成するには、次を行います。

1. Object Manager で、**Attack Objects > IDP Objects** をクリックします。IDP Objects ダイアログボックスが表示されます。

2. Custom Groups タブをクリックします。

3. Add アイコンをクリックして、**Add Static Group** を選択します。New Static Group ダイアログボックスが表示されます。

4. 静的グループの名前と説明を入力します。グループアイコンの色を選択します。

5. 静的グループに攻撃またはグループを追加するには、Attacks/Group リストから攻撃またはグループを選択して、**Add** をクリックします。

6. **OK** をクリックする。

動的グループの構成

動的グループには、グループに指定された基準に基づいて自動的に追加または削除される、攻撃オブジェクトの動的な集合を含んでいます。たとえば、攻撃データベース更新は、グループ基準に基づいて、動的グループから攻撃オブジェクトを追加または削除できます。これで、既存のセキュリティポリシーで使用する必要があるかどうかを判断するのに、個々の新しいシグネチャを確認する必要がなくなります。

定義済みまたはカスタム動的グループには、攻撃オブジェクトを入れることができますが、攻撃グループを入れることはできません。動的グループのメンバは、定義済み攻撃オブジェクトでもカスタム攻撃オブジェクトでもかまいません。

次の手順を実行して、カスタム動的グループを作成します。

1. Object Manager で、**Attack Objects > IDP Objects** をクリックします。IDP Objects ダイアログボックスが表示されます。

2. Custom Groups タブをクリックします。

3. Add アイコンをクリックして、**Add Dynamic Group** を選択します。New Dynamic Group ダイアログボックスが表示されます。

4. 静的グループの名前と説明を入力します。グループアイコンの色を選択します。

5. Filters タブで、Add アイコンをクリックして、次のいずれかを選択します。

   - **Add Products Filter** は、攻撃に脆弱なアプリケーションに基づいて、攻撃オブジェクトを追加します。

   - **Add Severity Filter** は、攻撃の重大度に基づいて、攻撃オブジェクトを追加します。

注： 定義済み攻撃オブジェクトはすべて、Juniper Networks によって重大度が割り当てられています。ただし、この設定はユーザーのネットワークの必要に合わせて編集できます。

- **Add Category Filter** は、カテゴリに基づいて攻撃オブジェクトを追加します。
- **Add Last Modified Filter** は、最終変更日に基づいて攻撃オブジェクトを追加します。
- **Add Recommended Filter** は、動的なグループに対する最も深刻な脅威であると指定された攻撃だけを含んでいます。将来、Juniper Networks は、深刻な脅威であると考える攻撃だけを Recommended (推奨) に指定します。これらの設定は新しい攻撃オブジェクトのアップデートで更新されます。さらに、カスタム攻撃オブジェクトを Recommended (推奨) であるかないか指定できます。Recommended (推奨) アクションに関する詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。

フィルタは 1 つずつ作成します。各条件を追加すると IDP はその条件を各攻撃オブジェクトの属性と比較し、一致しない攻撃オブジェクトがあると、すぐにフィルタリングして削除します。作成したフィルタの属性に一致する攻撃オブジェクトが 1 つもない場合、動的グループにメンバがないことを警告するメッセージが表示されます。

一致攻撃オブジェクトのリストから、ネットワークで誤検知が発生したり、ネットワークが脆弱でない攻撃を検知する攻撃オブジェクトを排除できます。

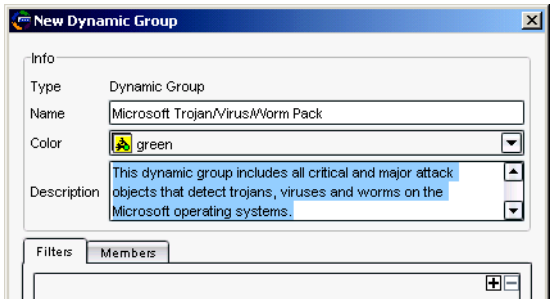
注： 動的グループには、他のグループ（定義済み、静的、または動的）を含めることはできません。ただし、静的グループのメンバとして動的グループを含めることはできます。

例：動的グループの作成

次の手順を実行して、動的グループを作成します。

1. Custom Attack Groups タブで、Add アイコンをクリックして、**Add Dynamic Group** を選択します。New Dynamic Group ダイアログボックスが表示されます。
2. グループの名前と説明を入力します。グループアイコンの色を選択します。

図 81: 新しい動的グループ



3. Filters タブで Add アイコンをクリックして、どの攻撃オブジェクトをグループに入れておくかを決めるフィルタを追加します。

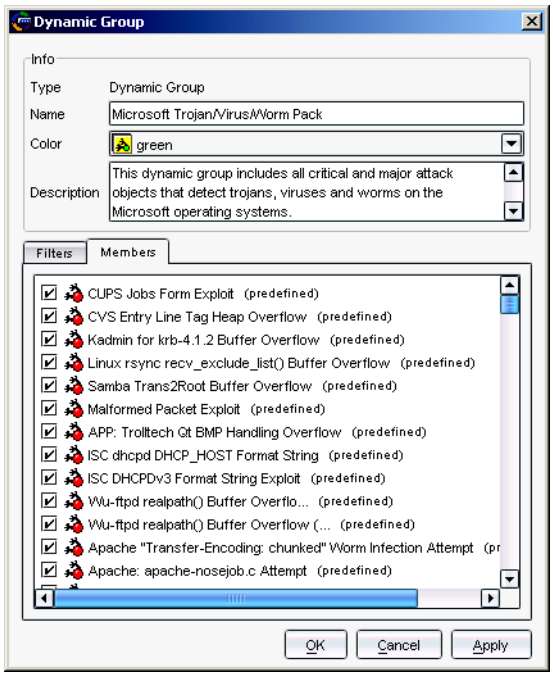
   a. **Add a Products** フィルタは、Microsoft Windows オペレーティングシステムすべてに対する攻撃を検知する攻撃オブジェクトを追加します。

   b. **Add a Severity** フィルタは、重大度レベルが Critical または Major の攻撃オブジェクトを追加します。

   IDP は、攻撃オブジェクトデータベース全体にすべてのフィルタを自動的に適用して、定義した条件に適合する攻撃オブジェクトを識別します。そして、一致するオブジェクトをグループのメンバとして追加します。

4. グループのメンバを表示するには、図 82 に示すように Members タブをクリックします。

図 82: 新しい動的グループメンバ



5. **OK** をクリックして、動的グループを保存します。

動的グループの更新

満足のいくグループの条件とそのメンバが作成できたら、そのグループをセキュリティポリシーで使用します。次に攻撃オブジェクトを更新したときに、次のタスクが自動的に実行されます。

- 新しい攻撃オブジェクトについては、各攻撃オブジェクトの定義済み属性と動的グループの各条件が比較され、一致する攻撃オブジェクトが追加されます。
- 更新された攻撃オブジェクトについては、動的グループの条件を満たさなくなった攻撃オブジェクトが削除されます。また、更新された攻撃オブジェクトについて、他の動的グループの条件を満たすようになっているか判断され、必要に応じてそれらのグループにその攻撃オブジェクトが追加されます。
- 削除された攻撃オブジェクトについては、動的グループからその攻撃オブジェクトが削除されます。

動的グループは手動で編集することもでき、新規フィルタを追加したり既存のフィルタを調整したりして、希望どおりのタイプの攻撃オブジェクトを作成できます。セキュリティポリシー内からも動的グループグループを編集できます(184 ページの「セキュリティポリシーの構成」を参照)。

カスタム攻撃グループの編集

カスタム攻撃グループを変更するには、IDP Objects ダイアログボックスの Custom Attack Groups タブでグループをダブルクリックします。Static Group または Dynamic Group ダイアログボックスが現れ、以前に構成した情報が表示されます。必要な変更を入力して、**Apply** をクリックします。ダイアログボックスを閉じるには、**OK** をクリックします。

カスタム攻撃グループの削除

カスタム攻撃グループを削除するには、IDP Objects ダイアログボックスの Custom Attack Groups タブでグループを右クリックして、**Delete** を選択します。そのアイテムを削除してもよいか確認するウィンドウが表示されます。**OK** をクリックする。

デバイスをスタンドアロンの IDP デバイスとして構成する

IDP 対応デバイスは、プライベートネットワークの重要なセグメントを保護する、スタンドアロンの IDP セキュリティシステムとしても配備できます。たとえば、セキュリティデバイス が、既にインターネットとプライベートネットワークの間のトラフィックをアクティブにスクリーニングしているとします（デバイスには、オプションで、このトラフィックを検査するのに徹底監視機能を使用できるものがあります)。しかし、メールサーバーのような内部システムを、他の点ではトラステッドなネットワークにあるユーザーマシンから生じる攻撃から、保護する必要が依然としてあります。この場合、ファイアウォール機能ではなく、IDP を提供するセキュリティシステムが必要です。

このセクションでは、セキュリティデバイスを構成し、スタンドアロンの IDP 機能を提供する方法を説明します。

注： Juniper Networks は、統合ファイアウォール /VPN 機能のない IDP 機能を提供する、スタンドアロンの IDP 装置を提供しています。IDP 対応のファイアウォール /VPN デバイスだけでなく、これらの装置も NetScreen-Security Manager システムを使用して管理できます。

IDP を使用可能にする

IDP を使用可能にするには、適用可能なゾーン間のトラフィックが IDP ルールベースと照合されるように指定するセキュリティポリシーのファイアウォールルールを構成する必要があります。このファイアウォールルールを非常に簡単にすることができます。全サービスについて全ソースから全宛先へのトラフィックをすべて照合できるようにします。

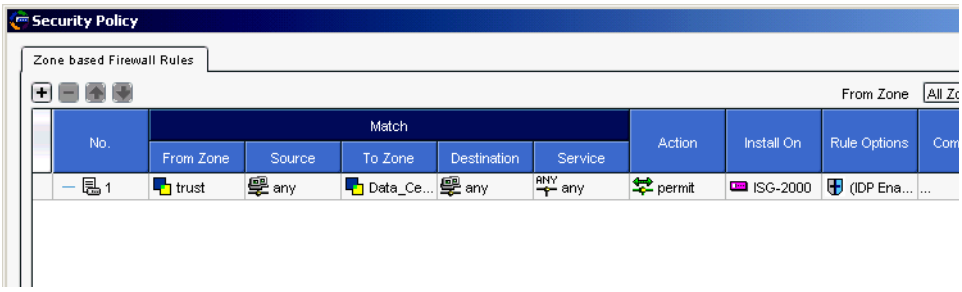
1. 任意のサービスについて任意のソースから任意の宛先へのトラフィックを許可する、ファイアウォールルールを作成します。
2. ファイアウォールルールの Rule Options 列を右クリックして、**DI Profile/Enable IDP** を選択します。
3. DI Profile/Enable IDP ダイアログボックスで、ボタンをクリックして IDP を使用可能にし、**OK** を選択します。
4. 必要に応じて IDP ルールベースを作成し、IDP ルールを構成します。

IDP ルールを含むセキュリティポリシーの構成に関する詳細については、184 ページの「セキュリティポリシーの構成」を参照してください。

例：スタンドアロンの IDP 用のファイアウォールルールの構成

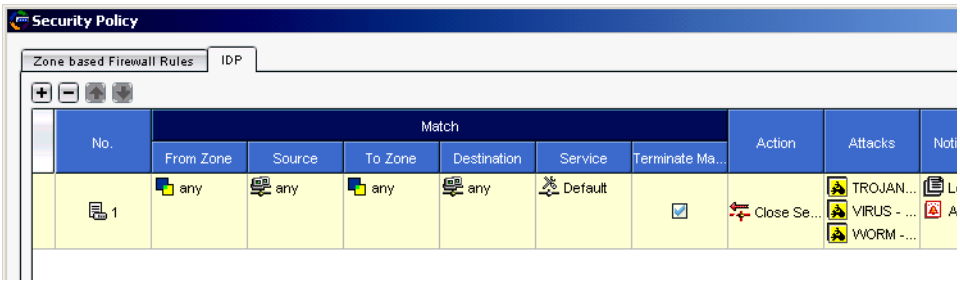
この例では、ネットワークの Trust ゾーンとカスタム Data_Center ゾーンの間のスタンドアロンの IDP セキュリティシステムとして、IDP/ ファイアウォール /VPN デバイスを配備しています。あなたの企業のファイル、メール、およびデータベースの各サーバーは、Data_Center ゾーンにあります。Data_Center ゾーンにあるサーバーにアクセスできるよう、Trust ゾーンのユーザーに許可を与えたいのですが、一方で、Trust ゾーンのユーザーマシンに不注意から侵入した可能性がある攻撃からサーバーを保護する必要もあります。図 83 に示すように、Trust ゾーンから Data_Center ゾーンへのファイアウォールルールを作成して、任意のサービスについて任意のソースから任意の宛先へのトラフィックを許可します。また、Rule Options 列で IDP を使用可能にします。

図 83: スタンドアロンの IDP のファイアウォールルール



次に、図 84 に示すように、セキュリティポリシーが Data_Center ゾーンにあるサーバーに対する攻撃を検出するように、IDP ルールベースを追加し構成する場合もあります。

図 84: スタンドアロンの IDP の IDP ルール



役割ベースの管理の構成

NetScreen-Security Manager の役割ベース管理（RBA）では、スーパー管理者（superadmin）が、スタンドアロンの IDP デバイス用にカスタムの役割および管理者を作成できます。これにより、IDP の管理者に、IDP 機能の構成および管理に特有のタスクだけを実行する権限が与えられます。IDP 管理者は、デバイスの構成を作成、編集、削除、表示、または更新する必要はありません。NetScreen-Security Manager UI にログインすると、IDP 管理者には、IDP に適用可能なメニューおよびオプションだけが表示されます。

例 : IDP 専用管理者の構成

この例では、スーパー管理者が、カスタム役割および IDP 管理者を作成します。IDP 管理者は、スタンドアロンの IDP デバイスでの IDP の構成および管理に特有のタスクだけを実行できます。

1. superadmin として、グローバルドメインにログインします。メニューバーから、**Tools > Manage Administrators and Domains** を選択します。

2. Roles タブをクリックし、Add アイコンをクリックして、**IDP_Only** という名前の役割を作成します。次のような IDP の構成および管理に特有のタスクを選択します。

   - 攻撃の更新
   - ポリシーの作成、表示、編集、削除
   - バックドアルールベースおよび IDP ルールベースの作成、表示、編集、削除
   - ファイアウォールルールベースの表示
   - 共用オブジェクトおよびグループの作成、編集、削除

   IDP 管理者に役立つかもしれない他のタスクを選択します。たとえば、ジョブやシステムステータスモニタを表示するオプションを選択できます。

3. New Role ダイアログボックスで **OK** をクリックして、Manage Administrators and Domains ダイアログボックスに戻ります。

4. Administrators タブをクリックし、Add アイコンをクリックして、**IDP_Administrator** という名前の管理者を作成します。New Admin ダイアログボックスが、General タブが選択された状態で表示されます。

5. Name フィールドに **IDP_Administrator** を入力します。管理者の連絡先情報を入力できます。

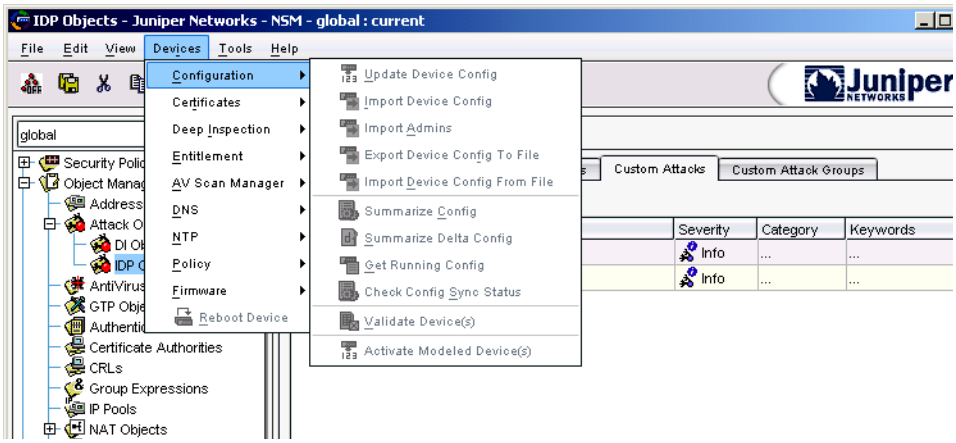
6. Authorization タブをクリックします。管理者の権限付与方式およびローカルのパスワードを選択します。

7. Permissions タブをクリックし、Add アイコンをクリックして、この管理者に役割 **IDP_Only** を選択します。

8. **OK** をクリックして、New Select Role and Domains ダイアログボックスを閉じます。**OK** をクリックして New Admin ダイアログボックスを閉じます。**OK** をクリックして、Manage Administrators and Domains ダイアログボックスを閉じます。

スタンドアロンの IDP デバイス用の管理者が、**IDP_Administrator** として NetScreen-Security Manager にログインできるようになりました。ログイン時に、図 85 に示すように、NetScreen-Security Manager UI は、このユーザー用の制限されたナビゲーションツリーおよびメニューオプションを表示します。UI が、ナビゲーションツリーで、セキュリティポリシーおよびオブジェクトマネージャのオプションだけを表示していることに注意してください。このユーザーは、Devices > Configuration オプションを利用できません。

図 85: IDP_Administrator 用の UI 表示



IDP の管理

このセクションでは、IDP 対応のデバイスでの IDP 管理について説明します。

攻撃データベース更新

Juniper Networks は、Juniper のウェブサイトにおいて、ダウンロードファイルの形で、攻撃データベース更新を定期的に提供しています。攻撃データベース更新には、次を含むことができます。

- 新しいまたは変更された、定義済み IDP 攻撃オブジェクトおよびグループ
- 徹底監視（DI）機能が使用する、新しいまたは変更されたシグネチャ
- セキュリティデバイスで実行する、IDP エンジンの更新

新しい攻撃データベース更新では、バージョン番号が 1 だけ増えます。Juniper Networks ウェブサイトから、あるバージョンの攻撃データベース更新をダウンロードすると、NetScreen-Security Manager は、その攻撃データベース更新のバージョン番号を格納します。ダウンロードした最後の更新より新しい更新が利用できるか、チェックできます。

攻撃データベース更新のダウンロード

攻撃データベース更新は、NetScreen-Security Manager GUI サーバーにダウンロードされます。次の手順を実行して、攻撃データベース更新ファイルをダウンロードします。

1. メニューバーから、**Tools > View/Update NSM Attack Database** を選択します。Attack Update Manager ウィザードが表示されます。
2. Attack Update Manager の指示に従って、NetScreen-Security Manager GUI サーバーに攻撃データベース更新ファイルをダウンロードします。

注： Juniper Networks の Web サイトは、デフォルトでは New Preferences ダイアログボックスに設定されています。**Tools > Preferences** を選択して、Web サイトにアクセスします。GUI サーバーがインターネットにアクセスできる必要があります。

更新された攻撃オブジェクトの使用

定義済み IDP 攻撃オブジェクトまたはグループは作成、編集、または削除できません。しかし、NetScreen-Security Manager GUI サーバーにインストールされた攻撃オブジェクトデータベースは更新できます。定義済み IDP 攻撃オブジェクトおよびグループへの更新は、次を含むことができます。

- 既存の攻撃オブジェクトの新しい説明または重大度
- 新しい攻撃オブジェクトまたはグループ
- 古くなった攻撃オブジェクトの削除

更新された IDP 攻撃オブジェクトおよびグループを GUI サーバーにダウンロードすると、更新の新しい攻撃オブジェクトは、セキュリティポリシーの IDP ルールベースで選択できます。管理対象のデバイスにセキュリティポリシーをインストールすると、IDP ルールでそのデバイス用に使用されている攻撃オブジェクトだけが、GUI サーバーからデバイスへプッシュされます。

注 : DI 機能では、更新されたシグネチャがすべて、管理対象のデバイスにプッシュされます。管理対象のデバイスでの DI 用の攻撃オブジェクトデータベースの更新に関する詳細については、*NetScreen-Security Manager Administrator's Guide* を参照してください。

IDP エンジンの更新

IDP エンジンは、ファイアウォール /VPN デバイス上で動作する、動的に変化可能なファームウェアです。デバイスで IDP エンジンを更新できる方法が 2 つあります。

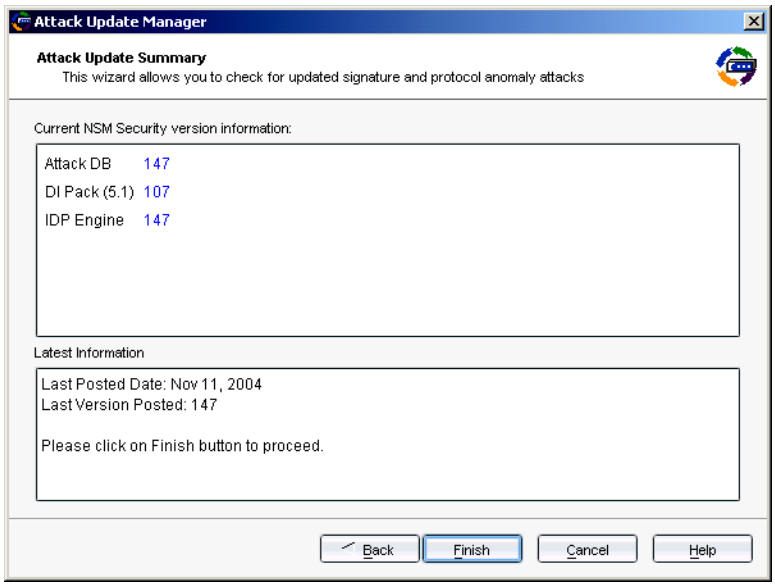
- IDP/ ファイアウォール /VPN デバイスのファームウェアをアップグレードする時、アップグレードされたファームウェアは通常、新バージョンの ScreenOS および新しいバージョンの IDP エンジンに更新されています。(セキュリティデバイスのファームウェアのアップグレードについては、*NetScreen-Security Manager Administrator's Guide* を参照してください。)
- GUI サーバーの攻撃データベース更新から、管理対象のデバイスの IDP エンジンを更新できます。攻撃データベース更新の方が、ファームウェアのリリースより頻繁に行われる場合が多いので、攻撃データベース更新には、最新のファームウェアリリースよりも新しいバージョンの IDP エンジンが含まれている場合があります。たとえば、攻撃データベース更新に、更新された IDP エンジンとしか使用できない、更新 IDP 攻撃オブジェクトが含まれている可能性があります。

次の手順を実行して、デバイスで現在動作している IDP エンジンのバージョンを表示します。

1. **Tools > View/Update NSM Attack Database** を選択します。Attack Update Manager ウィザードが表示されます。
2. **Next** をクリックします。

   Attack Update Summary は、図 86 に示すように、GUI サーバーにダウンロードされている現行バージョン、および Juniper Networks から利用可能な最新バージョンに関する情報を表示します。

図 86: 攻撃更新サマリー



3. 最新の攻撃データベース更新をダウンロードするには **Finish** をクリックします。Attack Update Manager を終了するには、**Cancel** をクリックします。

デバイスの IDP エンジンを更新するには、次を行います。

1. **Devices > IDP Detector Engine > IDP Detector Engine** を選択します。Change Device Sigpack ダイアログボックスが表示されます。

注： セキュリティデバイスにインストールする IDP エンジンのバージョンは、デバイスで動作しているファームウェアのバージョンと互換性を持っている必要があります。デバイスの IDP エンジンのバージョンを下げることはできません。

---

2. **Next** をクリックして、IDP エンジン更新をインストールしたい管理対象デバイスを選択します。

3. Change Device Manager の指示に従って、選択したデバイスの IDP エンジンを更新します。

注： デバイスの IDP エンジンの更新には、デバイスの再起動は必要ありません。

IDP ログの表示

攻撃オブジェクトが IDP ルールでマッチすると、IDP ログエントリが NetScreen-Security Manager のログビューアに表示されます。次の手順を実行して、ログビューアに IDP ログエントリを受信します。

1. 希望する重大度設定を持つログエントリを NetScreen-Security Manager へ送信するよう、デバイスを使用可能にします。

   a. Device Manager で、そのデバイスのデバイス構成を開きます。

   b. デバイスナビゲーションツリーで、**Report Settings > General > NSM** を選択します。

   c. NetScreen-Security Manager にログしたい重大度設定を選択します。

   d. **OK** をクリックする。

2. デバイスにインストールされたセキュリティポリシーで、IDP の検出およびロギングを使用可能にします。セキュリティポリシーで IDP ロギングを構成する詳細については、184 ページの「セキュリティポリシーの構成」を参照してください。

IDP アラームログエントリがログビューアに現れ、次の列を表示します。

- Source and Destination Address（ソースアドレスと宛先アドレス）
- Action
- プロトコル
- Category (Anomaly、Custom、または Signature)（カテゴリ（アノーマリ、カスタム、またはシグネチャ））
- Subcategory（サブカテゴリ）
- Severity
- Device

第 7 章

不審なパケット属性

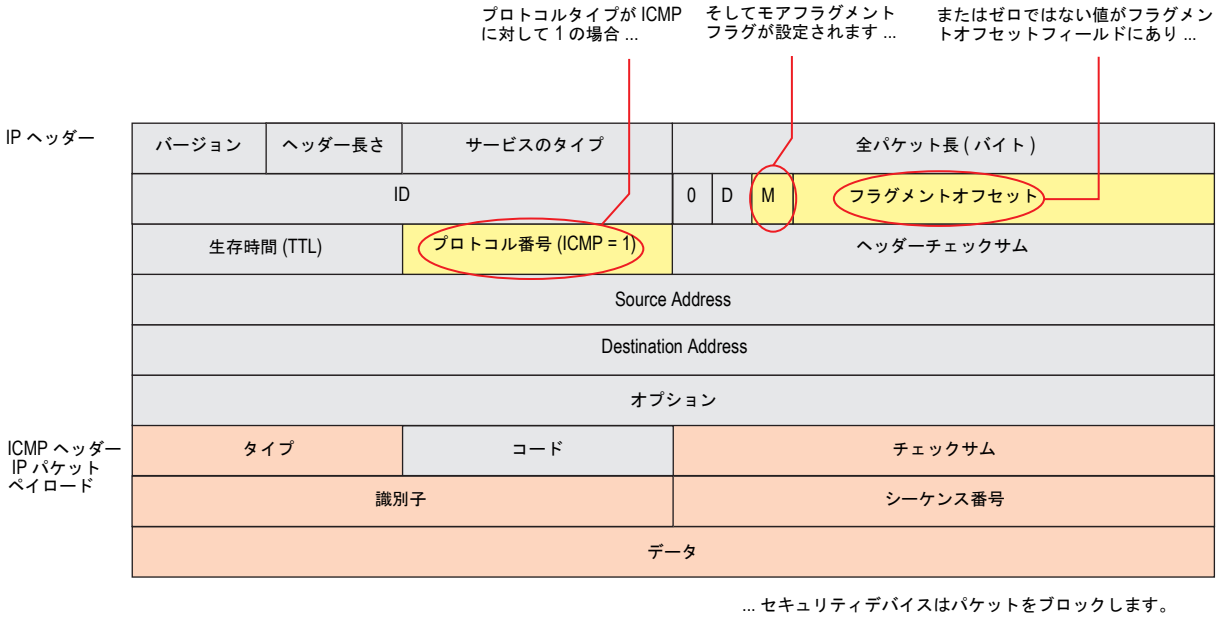
本編の他の章で示したように、攻撃者は偵察やサービス拒否 (DoS) 攻撃を行うパケットを巧妙に作成することがあります。作成されたパケットがどのような動作を行うか明確でないこともありますが、巧妙に作り上げられたということから、何らかの悪意のある用途に使用されるものと予想されます。この章で示すすべての SCREEN オプションは、脅威となるおそれのある次のような不審なパケットを阻止します。

- 240 ページの「ICMP フラグメント」
- 241 ページの「ラージ ICMP パケット」
- 242 ページの「不良 IP オプション」
- 243 ページの「不明のプロトコル」
- 244 ページの「IP パケットフラグメント」
- 245 ページの「SYN (周期) フラグメント」

ICMP フラグメント

ICMP (インターネット制御メッセージプロトコル) では、エラーレポートおよびネットワーク探査機能が利用できます。ICMP パケットに含まれるメッセージはきわめて短いため、ICMP パケットをフラグメント化する合理的な理由はありません。ICMP パケットがフラグメント化を必要となるほど大きい場合は、何らかの間違いがあると考えられます。ICMP Fragment Protection SCREEN オプションを使用可能にした場合、セキュリティデバイスは、More Fragments フラグを設定された、またはオフセットフィールドに示されたオフセット値をもつ ICMP パケットをブロックします。

図 87: ICMP フラグメントのブロック



フラグメント化した ICMP パケットをブロックするには、次のいずれかを行います。ここで指定するゾーンは、フラグメント化した要素が発生したセキュリティゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): **ICMP Fragment Protection** を選択してから、**Apply** をクリックします。

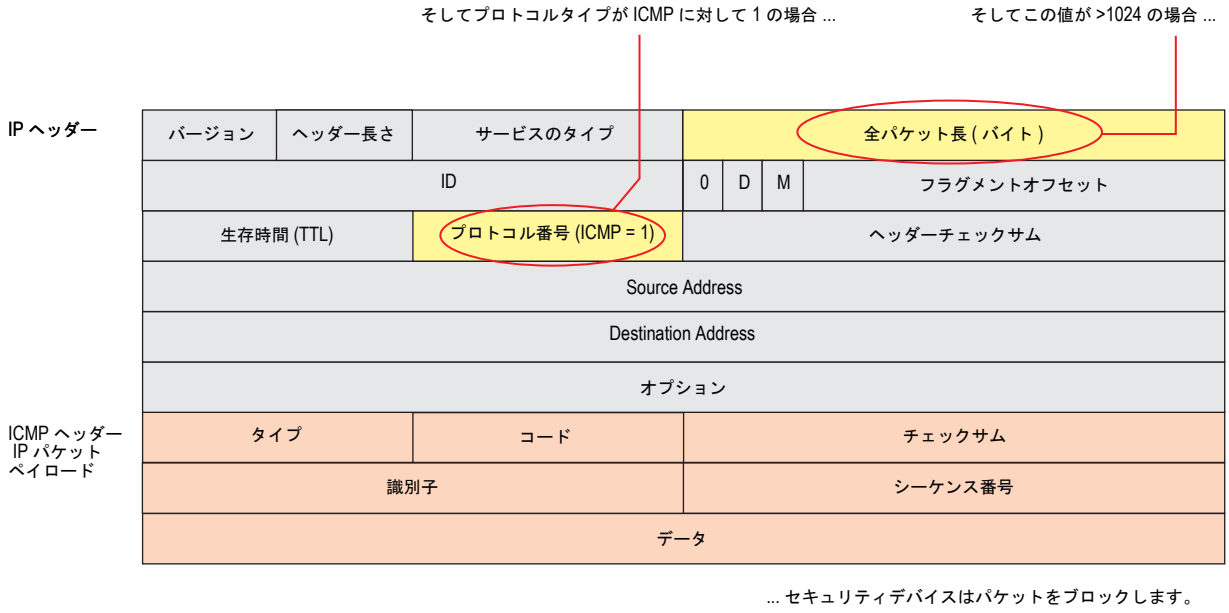
CLI

set zone *zone* screen icmp-fragment

ラージ ICMP パケット

240 ページの「ICMP フラグメント」で説明したように、ICMP (インターネット制御メッセージプロトコル) では、エラーレポートおよびネットワーク探査機能が利用できます。ICMP パケットに含まれるメッセージはきわめて短いため、ICMP パケットをフラグメント化する合理的な理由はありません。ICMP パケットが異常に長い場合は、何らかの間違いがあると考えられます。たとえば、Loki プログラムは隠れたメッセージを伝送するためのチャンネルとして、ICMP を使用します。ICMP パケットが存在すると、Loki エージェントとして動作する故障したコンピュータが現れることがあります。また、その他の不審なアクティビティを示すこともあります。

図 88: ラージ ICMP パケットのブロック



Large Size ICMP Packet Protection SCREEN オプションを使用可能にすると、セキュリティデバイスは 1024 バイトを超える長さの ICMP パケットをチェックしてドロップします。

ラージ ICMP パケットをブロックするには、次のいずれかを行います。ここで指定するゾーンは、ICMP パケットが発生したセキュリティゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): **Large Size ICMP Packet (Size > 1024) Protection** を選択してから、**Apply** をクリックします。

CLI

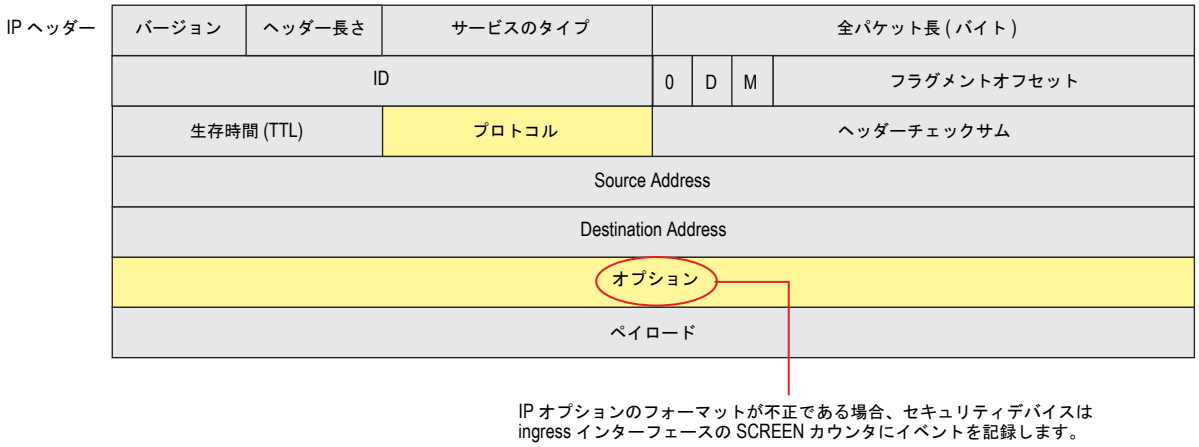
set zone *zone* screen icmp-large

不良 IP オプション

インターネットプロトコル規格の RFC 791、*Internet Protocol* では、特定のルーティング制御、診断ツール、およびセキュリティを提供する 8 つのオプションのセットが指定されています。本来、これらのオプションは正当な目的で使用するように考案されたものですが、不正な目的に悪用する方法も考え出されてきました (攻撃者が IP オプションから開始する攻撃の概要については、10 ページの「IP オプションを使用したネットワーク偵察」を参照してください)。

意図的にまたは偶然に、攻撃者は IP オプションを不正に構成し、フィールドが不完全または不恰好となることがあります。パケットの作成者の意図にかかわらず、不正なフォーマット化は、目的とする受信側にとっては異常で、有害となります。

図 89: 不正にフォーマット化された IP オプション



Bad IP Option Protection SCREEN オプションを使用可能にした場合、IP パケットヘッダー内の何らかの IP オプションが不正にフォーマットされていると、セキュリティデバイスはパケットをブロックします。セキュリティデバイスは、イベントログにイベントを記録します。

不正なフォーマットの IP オプションを持つ IP パケットを検出しブロックするには、次のいずれかを行います。ここで指定するゾーンは、パケットが発生したセキュリティゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): **Bad IP Option Protection** を選択してから、**Apply** をクリックします。

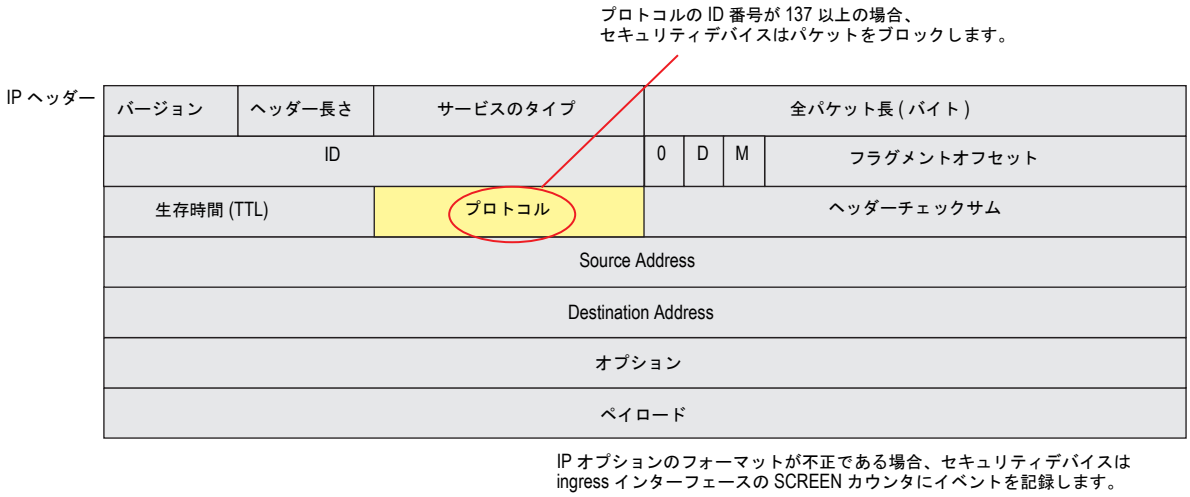
CLI

set zone *zone* screen ip-bad-option

不明のプロトコル

137 以上の ID 番号を持つこれらの プロトコルタイプは、この時点では未使用で未定義です。プロトコルが未定義であるために、不明のプロトコルが正当か不正であるかを事前に知ることができなくなります。ご利用のネットワークで 137 以上の ID 番号を持つ非標準プロトコルが使用されていない限り、保護されたネットワークにそのような不明の要素が侵入するのをブロックするのが慎重な方策となります。

図 90: 不明のプロトコル



Unknown Protocol Protection SCREEN オプションを使用可能にした場合、プロトコルフィールドに 137 以上のプロトコル ID 番号が含まれる際には、セキュリティデバイスはパケットをブロックします。

不明のプロトコルを使用するパケットをドロップするには、次のいずれかを行います。ここで指定するゾーンは、パケットが発生したセキュリティゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): **Unknown Protocol Protection** を選択してから、**Apply** をクリックします。

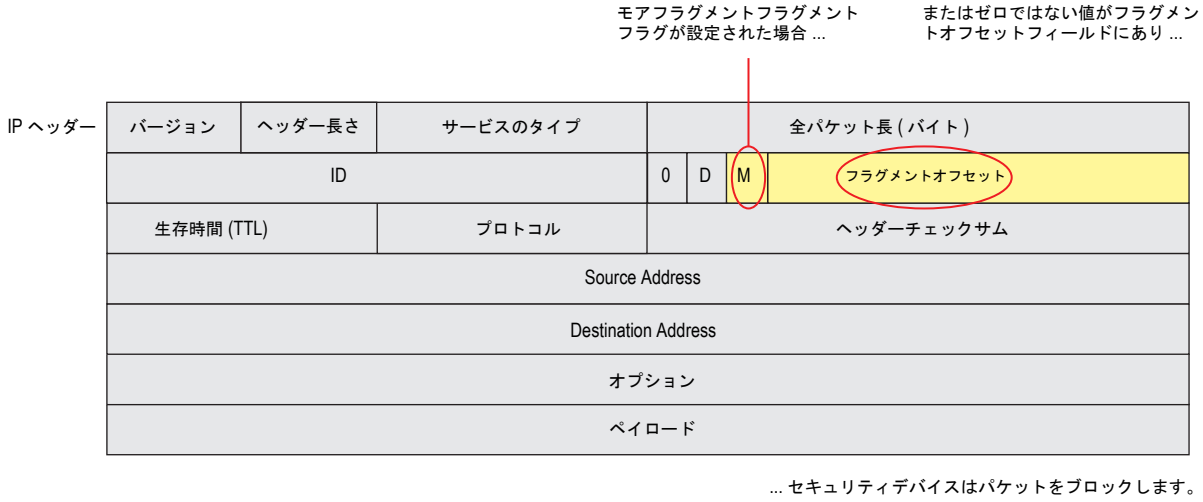
CLI

set zone *zone* screen unknown-protocol

IP パケットフラグメント

パケットが異なるネットワークを移動するにつれて、各ネットワークの MTU (最大伝送ユニット) に基づいて、パケットをさらに小さな部分 (フラグメント) へ分割する必要が生じることがあります。IP フラグメントには、特定の IP スタックインプリメンテーションの脆弱性を利用するように攻撃者が意図したものが含まれることがあります。被害者がこうしたパケットを受信すると、パケットの不正な処理からシステム全体のクラッシュなど、さまざまな程度で被害が生じます。

図 91: IP パケットフラグメント



セキュリティデバイスを有効にして、セキュリティゾーンの IP フラグメントを拒否した場合、デバイスは、そのゾーンにバインドされたインターフェースで受信するすべての IP パケットフラグメントをブロックします。

フラグメント化した IP パケットをドロップするには、次のいずれかを行います。ここで指定するゾーンは、フラグメント化した要素が発生したセキュリティゾーンです。

WebUI

Screening > Screen (Zone: ゾーン名を選択): **Block Fragment Traffic** を選択してから、**Apply** をクリックします。

CLI

set zone *zone* screen block-frag

SYN (周期) フラグメント

IP (インターネットプロトコル) は、TCP (伝送制御プロトコル) を起動する IP パケットの TCP SYN セグメントをカプセル化します。このパケットの目的は接続を開始して応答の際に SYN/ACK セグメントを呼び出すことであるため、通常、SYN セグメントにはデータは全く含まれていません。この IP パケットは小さいため、フラグメント化を行う正当な理由はありません。フラグメント化された SYN パケットは正常ではなく、疑う必要があります。慎重を期すなら、保護されたネットワークにそのような要素が侵入するのをブロックします。

SYN Fragment Detection SCREEN オプションを使用可能にすると、パケットがフラグメント化され、SYN フラグが TCP ヘッダーに設定されていることが IP ヘッダーから明らかとなった場合に、セキュリティデバイスはそのパケットを検出します。セキュリティデバイスは、ingress インターフェースの SCREEN カウンタリストにイベントを記録します。

SYN フラグメントを含むパケットをドロップするには、次のいずれかを行います。ここで指定するゾーンは、パケットが発生したセキュリティゾーンです。

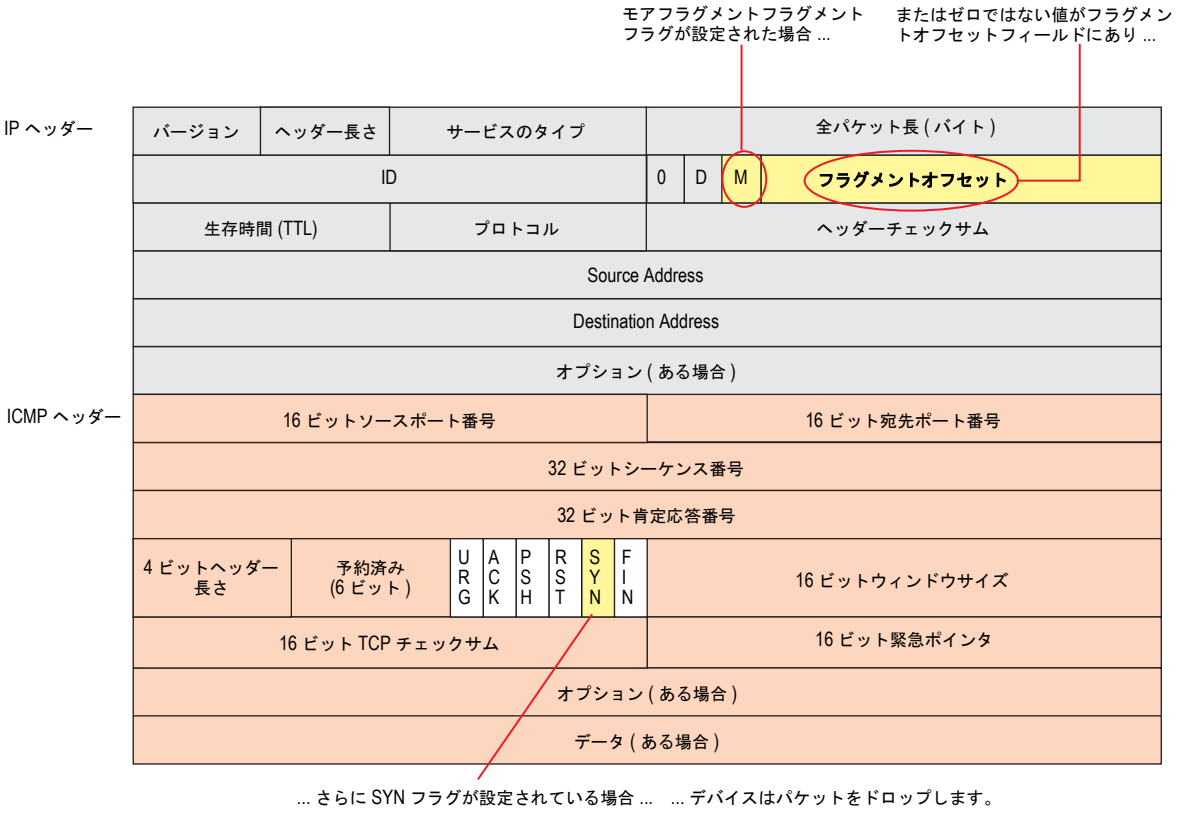
WebUI

Screening > Screen (Zone: ゾーン名を選択): **SYN Fragment Protection** を選択してから、**Apply** をクリックします。

CLI

set zone *zone* screen syn-frag

図 92: SYN (周期) フラグメント



付録 A

ユーザー定義シグネチャのコンテキスト

コンテキストとは、DI (徹底監視) モジュールが攻撃オブジェクトパターンと一致するシグネチャを探すパケット内の場所の定義です。ステートフルなシグネチャ攻撃オブジェクトを定義する際、以下に挙げるようなコンテキストを自由に使って記述できます。なお、攻撃オブジェクトは、ユーザー定義の攻撃オブジェクトグループに登録しなければ、ポリシーに記述して適用することはできません。

注 : ユーザー定義攻撃オブジェクトグループに加えることができるのは、ユーザー定義攻撃オブジェクトのみです。定義済み攻撃オブジェクトとユーザー定義攻撃オブジェクトは、同じ攻撃オブジェクトグループ内で一緒にできません。

DI モジュールはトラフィックの TCP ストリームシグネチャを調べる場合、コンテキストにかまわずに調べます。TCP ストリームシグネチャはパターンをあらゆる種類の TCP トラフィック内で、使用しているアプリケーションプロトコルに関係なく探します。ストリームシグネチャは、NetScreen-500 と NetScreen-2000 シリーズシステムでのみ定義されます。ただし、Stream256 は先頭 256 バイトのデータ内でパターンを検索します。

表 21: ユーザー定義シグネチャのコンテキスト

プロトコル	コンテキスト	説明 (この位置にあるデータの内容)
AIM	aim-chat-room-desc	AIM (アメリカオンライン インスタント メッセンジャー) または ICQ (I Seek You) セッションで使われる、チャットルームの説明
	aim-chat-room-name	AIM または ICQ セッションで使われる、チャットルームの名前
	aim-get-file	ユーザーがピアから転送するファイルの名前
	aim-nick-name	AIM または ICQ ユーザーのニックネーム
	aim-put-file	ユーザーがピアに転送するファイルの名前
	aim-screen-name	AIM または ICQ ユーザーのスクリーンネーム
DNS	dns-cname	DNS (ドメイン名システム) の問い合わせや応答に使われる CNAME (標準名)。RFC 1035、*Domain Names － Implementation and Specification* の定義にもとづく
FTP	ftp-command	FTP コマンド。RFC 959、*File Transfer Protocol (FTP)* の定義にもとづく
	ftp-password	FTP セッションのログイン用パスワード
	ftp-pathname	FTP コマンドの引数として指定するディレクトリ名またはファイル名
	ftp-username	FTP サーバーにログインするユーザー名
Gnutella	gnutella-http-get-filename	Gnutella クライアントが検索を試みるファイル名

プロトコル	コンテキスト	説明 (この位置にあるデータの内容)
HTTP	http-authorization	HTTP（HyperText Transfer Protocol、ハイパーテキスト転送プロトコル）の基本認証ヘッダー “Authorization” を復号化して得られるユーザー名とパスワード。RFC 1945、*HyperText Transfer Protocol ― HTTP/1.0* にもとづく
	http-header-user-agent	HTTP 要求のヘッダー内、user-agent フィールドの内容 (どのブラウザーを使ってウェブサイトにアクセスしているかをあらわす情報)
	http-request	HTTP 要求
	http-status	HTTP 応答のステータス行 (接続状態をクライアントに通知するための、3 桁の数字。例えば 401 は「Unauthorized」、404 は「Not found」を表す)
	http-text-html	HTTP トランザクション中の本体部分、すなわち HTML (HyperText Markup Language) で記述されたテキスト
	http-url	HTTP 要求に記述された URL (ユニフォームリソースロケータ) を、データストリーム中に現れるとおりに転記したもの
	http-url-parsed	HTTP 中の URL をユニコード文字列から「正規化」形式の文字列に複合化したもの
	http-url-variable-parsed	HTTP-GET 要求に現れる、URL 中の変数を復号化したもの。CGI (Common Gateway Interface) アプリケーションに渡される変数
IMAP	imap-authenticate	IMAP (Internet Mail Access Protocol) の AUTHENTICATE コマンドに与えられた引数。IMAP クライアントがサーバーに対して提示する認証機構の種類を表す。KERBEROS_V4、GSSAPI (RFC 1508、*Generic Security Service Application Program Interface* を参照)、SKEY など IMAP について詳しくは、RFC 1730、*Internet Message Access Protocol - Version 4*、RFC 1731、*IMAP4 Authentication Mechanisms* を参照してください。
	imap-login	IMAP の LOGIN コマンドに現れるユーザー名またはプレーンテキストパスワード
	imap-mailbox	IMAP の SELECT コマンドに現れるメールボックス名文字列
	imap-user	IMAP の LOGIN コマンドに現れるユーザー名
MSN Messenger	msn-display-name	MSN (Microsoft Network) インスタントメッセージのセッションで使われる表示用ユーザー名
	msn-get-file	クライアントがピアからダウンロードするファイルの名前
	msn-put-file	クライアントがピアに送信するファイルの名前
	msn-sign-in-name	MSN インスタントメッセージのユーザーのスクリーンネーム (ログイン名)
POP3	pop3-auth	POP3 (Post Office Protocol, version 3) セッションの AUTH コマンド。POP3 について詳しくは、RFC 1939、*Post Office Protocol ― Version 3* を参照してください。
	pop3-header-from	SMTP セッションの「To:」ヘッダーの文字列
	pop3-header-line	POP3 トランザクションに現れる電子メールのヘッダーの内容
	pop3-header-subject	SMTP セッションの「To:」ヘッダーの文字列
	pop3-header-to	SMTP セッションの 「To:」ヘッダーの文字列
	pop3-mime-content-filename	POP3 セッションに現れる、MIME (Multipurpose Internet Mail Extensions) 形式の添付ファイル名
	pop3-user	POP3 セッションのユーザー名
SMB	smb-account-name	SMB (Server Message Blocks) セッションの SESSION_SETUP_ANDX 要求に現れる SMB アカウント名
	smb-connect-path	SMB セッションの TREE_CONNECT_ANDX 要求に現れる接続パス
	smb-connect-service	SMB セッションの TREE_CONNECT_ANDX 要求に現れる接続サービス名
	smb-copy-filename	SMB セッションの COPY 要求に現れるファイル名
	smb-delete-filename	SMB セッションの DELETE 要求に現れるファイル名
	smb-open-filename	SMB セッションの NT_CREATE_ANDX と OPEN_ANDX 要求に現れるファイル名

プロトコル	コンテキスト	説明 (この位置にあるデータの内容)
SMTP	smtp-from	SMTP (Simple Mail Transfer Protocol) セッションの「MAIL FROM」コマンド行に現れる文字列。RFC 2821、*Simple Mail Transfer Protocol* の定義にもとづく
	smtp-header-from	SMTP セッションの「To: 」ヘッダーに現れる文字列
	smtp-header-line	SMTP セッションのヘッダーに現れる文字列
	smtp-header-subject	SMTP セッションの「To: 」ヘッダーに現れる文字列
	smtp-header-to	SMTP セッションの 「To: 」ヘッダーに現れる文字列
	smtp-mime-content-filename	SMTP セッションに現れる、MIME (Multipurpose Internet Mail Extensions) 形式の添付ファイル名
	smtp-rcpt	SMTP セッションの「RCPT TO」コマンド行に現れる文字列
	stream256	再アセンブリされ正規化された TCP データストリームの先頭 256 バイト
Yahoo! Messenger	ymsg-alias	Yahoo! Instant Messaging ユーザーのニックネーム
	ymsg-chatroom-message	Yahoo! Instant Messaging チャットルームで名
	ymsg-chatroom-name	Yahoo! Instant Messaging チャットルーム名
	ymsg-nickname	Yahoo! Instant Messaging ユーザのニックネーム
	ymsg-p2p-get-filename-url	Yahoo! Instant Messaging におけるピアのダウンロード元マシン上のファイルの場所
	ymsg-p2p-put-filename-url	Yahoo! Instant Messaging におけるピアのダウンロード先マシン上のファイルの場所

索引

数字

3 方向ハンドシェイク 36

A

ActiveX コントロール、ブロッキング 170
ALG 59
AV オブジェクト
　タイムアウト 89
AV スキャン 62–87
　FTP 72
　HTTP 73
　HTTP キープアライブ 85
　HTTP トリックリング 85
　IMAP 75
　MIME 75
　POP3 75
　SMTP 77
　解凍 90
　クライアントあたりの AV リソース 83
　購読 80
　故障モード 83
　ファイル拡張子 91

C

Chargen 131

D

DDoS 29
DHCP 131
DI (徹底監視) 138–162
　カスタムシグネチャ 159–162
　攻撃アクション 141–148
　攻撃オブジェクトデータベース 122–129
　顧客サービス 154–158
　正規表現 159–160
DNS 131
DoS
　OS 指定 52–55
　セッションテーブルフラッ 18, 30
　ネットワーク 36–51
　ファイアウォール 30–35
DoS 攻撃 29–55
drop-no-rpf-route 20

E

exe ファイル、ブロッキング 171

F

FIN スキャン 15
Finger 132

G

Gopher 132

H

HTTP
　キープアライブ 85
　コンポーネントのブロッキング 170–171
　セッションタイムアウト 33
　トリックリング 85

I

ICMP 132
　フラグメント 240
　ラージパケット 241
IDENT 132
IDP
　インラインモードまたはインラインタップモードの指定 188
　基本設定 176
　デバイスのスタンドアロン IDP 用の構成 230
　ファイアウォールルールで使用可能にする 187
IDP エンジン
　更新 235
IDP エンジンの更新 235
IDP 攻撃オブジェクト 186
IDP 対応システム 174
IDP モード 188

IDP ルール 189
IDP 攻撃オブジェクトの構成 186
IP アクションの構成 200
Match 列の構成 191
アクションの構成 197
アドレスオブジェクトの構成 186
攻撃の構成 198
攻撃の重大度の構成 202
構成 191
コメントの入力 202, 206, 212
サービスオブジェクトの構成 186
サービスの構成 193
ソースおよび宛先の構成 192
ターゲットの構成 202
ターミナルルールの構成 195
通知の構成 201
IDP ルールベース
概要 189
種類 185
セキュリティポリシーへの追加 190
役割ベースの管理 186
IP
パケットフラグメント 244
IP オプション 10–11
record route 11
stream ID 11
timestamp 11
ストリクトソースルート 11, 24–26
セキュリティ 10, 11
ソースルート 24
属性 10–11
不正なフォーマットの 242
ルーズソースルート 10, 24–26
IP スプーフィング 19–24
Layer 2 ..... 20, 23
Layer 3 ..... 19, 21
drop-no-rpf-route 20

J

Java アプレット、ブロッキング 171

L

LDAP 132
LPR スプーラ 132

M

America Online Instant MessagingAmerica Online Instant Messaging
AIM を参照
Microsoft Network Instant MessengerMicrosoft Network Instant Messenger
MSN Instant Messenger を参照
Microsoft-Remote Procedure CallMicrosoft-Remote Procedure Call
MS-RPC を参照
MIME、AV スキャン 75
MS-RPCMS-RPC 134

N

NetBIOSNetBIOS 134
NFS 132
NNTP 132
NSRP
VSD グループ 183
NTP 132

P

P2PP2P 134
BitTorrentBitTorrent 134
DC 134
eDonkeyeDonkey 134
FastTrackFastTrack 134
Gnutella 134
KaZaa 134
MLdonkeyMLdonkey 134
SkypeSkype 134
SMB 134
WinMXWinMX 134
Ping of Death 52

R

RADIUS 132
record route IP option 11
rexec 132
RFC
793, *793、Transmission Control Protocol* 13
791, *Internet Protocol* 10
1038, *Revised IP Security Option* 10
rlogin 132
rsh 132
RTSP 132

S

SCREEN
IP スプーフィング 19–24
SYN フラッド 36–42
Server Message BlockServer Message Block
SMB を参照
SMB
NetBIOSNetBIOS 134
SNMPTRAP 133
SSH 133
SSL 133
stream ID IP オプション 11
SurfControl 99, 108
SYN および FIN フラグセット 12
SYN クッキー 47

SYN チェック 16, 16–19
セッションテーブルフラッ....18
セッションの中断....17
調査ホール....18
非対称ルーティング....17
SYN フラグメント 245
SYN フラッド 36–42
SYN クッキー 47
宛先しきい値....41
アラームしきい値....40
キューサイズ....42
攻撃....36
攻撃しきい値....40
しきい値....37
ソースしきい値....41
タイムアウト....42
未知の MAC アドレスをドロップする 42
SYN-ACK-ACK プロキシフラッド....34
SYSLOG....133

T

TCP
ストリームシグネチャ....162
セッションタイムアウト....33
フラグのないパケット....14
Telnet 133
TFTP....133
timestamp IP オプション....11

U

UDP
セッションタイムアウト....34

V

VNC 133
VSD グループ....183

W

Web フィルタリング
SurfControl CPA サーバー 99
SurfControl SCFP....111
SurfControl サーバー....100
SurfControl サーバーポート....111
SurfControl サーバー名....111
URL カテゴリ 102
vsys ごとのサーバー 110
Websense サーバーポート....111
Websense サーバー名....111
キャッシュ....101
組み込み型....99
サーバー状態....114
通信タイムアウト....111
ブロックされた URL メッセージ....113
ブロック済み URL メッセージタイプ 113
プロファイル....104
プロファイルをポリシーに適用....106
リダイレクト型....108
ルーティング....114
Whois 133
WinNuke 攻撃....54

Y

Yahoo! Messenger....133

Z

zip ファイル、ブロッキング....171

あ

アグレッシブエージング 33–34
アプリケーションレイヤーゲートウェイ
ALG を参照

い

インスタントメッセージ....133
AIM....133
IRC....133
MSN Messenger....133
Yahoo! Messenger....133
インラインタップモード....188
インラインモード....188

え

エージェント、ゾンビ 29, 31
エコー 132

お

オブジェクト
攻撃オブジェクト....212
攻撃オブジェクト、カスタム....215
攻撃オブジェクト、シグネチャ....212
攻撃オブジェクト、プロトコルアノーマリ 213

オペレーティングシステム、ホストの探査.....12–15

か

解凍、AV スキャン.....90
回避.....15–26
監視.....3

く

攻撃オブジェクト
　シグネチャ.....212
クッキー、SYN.....47

こ

攻撃
　SYN フラッド.....36–42
　検出と防衛のオプション.....2–4
攻撃.....130
　DoS.....29–55
　IP パケットフラグメント.....244
　Ping of Death.....52
　SYN フラグメント.....245
　UDP フラッド.....50
　WinNuke.....54
　一般的な目的.....1
　セッションテーブルフラッ.....18, 30
　段階.....2
　ティアドロップ.....53
　未知のプロトコル.....243
　ラージ ICMP パケット.....241
　ランド.....51
攻撃アクション.....141–148
　close client.....141
　close server.....141
　drop.....141
　drop packet.....141
　ignore.....141
　なし.....142
　閉鎖.....141
攻撃オブジェクト.....119
　TCP ストリームシグネチャ.....162
　概要.....212
　再有効化.....140
　使用不可.....140
　ステートフルシグネチャ.....135
　ストリームシグネチャ.....136
　否定.....165
　ブルートフォース.....149
　プロトコルアノーマリ.....136
攻撃オブジェクトグループ
　重大度の変更.....137
　ヘルプ.....134
攻撃オブジェクト
　IDP.....186
　プロトコルアノーマリ.....213
　カスタム.....215
攻撃オブジェクトグループ.....137
　重大度レベル.....137
　ロギング.....152
　ポリシーで適用.....130
攻撃オブジェクトデータベース.....122–129
　自動更新.....125
　自動通知と手動更新.....126
　手動更新.....128
　即時更新.....124, 125
　デフォルト URL の変更.....128
攻撃データベース更新
　概要.....234
　ダウンロード.....234
攻撃オブジェクト
　プロトコルアノーマリ.....164
攻撃保護
　セキュリティゾーンレベル.....4
　ポリシーレベル.....4
高水準しきい値.....33
攻略
　攻撃を参照
故障モード.....83
コンテンツフィルタリング.....57–116

さ

サービス
　カスタム.....154
サービス拒否
　DoS を参照

し

しきい値
　高水準.....33
　低水準.....33
シグネチャパッケージ、DI.....122
侵入の検出と予防、定義済み.....173

す
スクリーン
- ACK フラグのない FIN、ドロップ 13
- ACK をもたない FIN 16
- ICMP 240
- ICMP フラッド 49
- IP オプション 10
- IP パケットフラグメント、ブロック 244
- Ping of Death 52
- SYN および FIN フラグセット 12
- SYN フラグメント、検出 245
- SYN-ACK-ACK プロキシフラッド 34
- UDP フラッド 50
- VLAN ゾーンおよび MGT ゾーン 3
- WinNuke 攻撃 54
- アドレススイープ 7
- ストリクトソースルート IP オプション、検出 .26
- ソースルート IP オプション、拒否する 26
- ティアドロップ 53
- フラグのない TCP パケット、検出 14
- 不良 IP オプション、ドロップ 242
- ポートスキャン 9
- 未知の MAC アドレスをドロップする 42
- 未知のプロトコル、ドロップ 243
- ラージ ICMP パケット、ブロック 241
- ランド攻撃 51
- ルーズソースルート IP オプション 26

ストリームシグネチャ 136
ストリクトソースルート IP オプション 11, 24–26

せ
正規表現 159–160
セキュリティ IP オプション 10, 11
セキュリティポリシー 184
- テンプレート 187
- ルール 184
- ルールベース 184
- ルールベースの実行 187

セッション制限 30–32
- 宛先ベース 31, 32
- ソースベース 30, 32

セッションタイムアウト
- HTTP 33
- TCP 33
- UDP 34

セッションテーブルフラッ 18, 30

そ
ゾンビエージェント 29, 31

た
探査
- オープンポート 9
- オペレーティングシステム 12, 15
- ネットワーク 7

ち
調査
- FIN スキャン 15
- IP オプション 10
- SYN および FIN フラグセット 12
- アドレススイープ 7
- フラグのない TCP パケット、検出 14
- ポートスキャン 9

て
ティアドロップ攻撃 53
偵察 7–26
低水準しきい値 33
徹底監視 (DI)
- 概要 118
- カスタム攻撃オブジェクト 158
- 攻撃オブジェクト 119
- 攻撃オブジェクトグループ 137, 152
- 攻撃オブジェクトの最有効化 140
- 攻撃オブジェクトの否定 165
- 攻撃オブジェクトの無効化 140
- コンテキスト I
- シグネチャパッケージ 122
- 重大度の変更 137
- ステートフルシグネチャ 135
- ストリームシグネチャ 136
- プロトコルアノーマリ 136
- ライセンスキー 120

テンプレート
- セキュリティポリシー 187

と
透過モード
- 未知の MAC アドレスをドロップする 42

動的パケットフィルタリング 3

は
破棄 131
パケット状態 3
- 監視 3
- シグネチャ 135

パターンで 136

バックドアルール.....207–212
Match 列の構成.....209
アクションの構成.....210
サービスの構成.....210
重大度の構成.....211
操作の構成.....210
ソースおよび宛先の構成.....209
ゾーンの構成.....209
ターゲットの構成.....211
バックドアルールベース
概要.....207
セキュリティポリシーへの追加.....208

ひ
ピアツーピア
P2P を参照
否定、DI (徹底監視).....165

ふ
ファイル拡張子、AV スキャン.....91
不正な URL からの保護.....58–61
フラグメントの再アセンブリ.....58–61
フラッド
SYN.....36–42, 47
UDP.....50
セッションテーブル.....30
ブルートフォース
攻撃アクション.....149
ブルートフォース攻撃オブジェクト.....149
プロトコルアノーマリ.....136
ALGALG.....134
P2P アプリケーション.....134
インスタントメッセージ.....133
基本ネットワークプロトコル.....131
サポートされているプロトコル.....131–135
パラメータ設定.....164

へ
URL ヘルプ.....134

ほ
ポートスキャン.....9
ポートマッパ.....132
ポリシー
コアセクション.....17, 120
コンテキスト.....122

み
未知のプロトコル.....243

め
免除ルール.....202–207
Match 列の構成.....204
攻撃の構成.....205
構成.....204
ソースおよび宛先の構成.....205
ゾーンの構成.....204
ターゲットの構成.....206
ログビューアからの構成.....206
免除ルールベース
概要.....202
セキュリティポリシーへの追加.....203

や
役割ベースの管理
IDP 専用管理者の構成.....232
IDP ルールベース.....186

ら
ライセンスキー
アドバンスモード.....120
攻撃パターンの更新.....120
ランド攻撃.....51

る
ルーズソースルート IP オプション.....10, 24–26

ろ
ロギング
攻撃オブジェクトグループ.....152
ログエントリ
IDP ルールで使用可能.....237
ログビューア
免除ルールの作成.....206

概念と用例
ScreenOS リファレンス ガイド

第 5 部 :
仮想プライベート ネットワーク

リリース 6.0.0、改訂 02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

品番 : 530-017771-01-JP, 改訂 02

Copyright Notice

Copyright © 2007 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

目次

本編について vii

ドキュメントの規則 viii
Web ユーザーインターフェースの規則 viii
コマンドラインインターフェースの規則 viii
ネーミング規則および文字タイプ ix
説明図の規則 x
技術ドキュメントおよびテクニカルサポート xi

第 1 章 インターネットプロトコルセキュリティ 1

VPN (仮想プライベートネットワーク) の紹介 2
IPSec の概念 3
モード 4
トランスポートモード 4
トンネルモード 4
プロトコル 6
認証ヘッダー 6
セキュリティペイロードのカプセル化 6
鍵管理 7
手動鍵 7
AutoKey IKE 7
セキュリティアソシエーション 8
トンネルネゴシエーション 8
フェーズ 1 9
メインモードとアグレッシブモード 9
Diffie-Hellman の鍵交換 10
フェーズ 2 11
完全転送機密保持 11
再生保護 12
IKE および IPSec パケット 12
IKE パケット 12
IPSec パケット 15

第 2 章 公開鍵暗号化 19

公開鍵暗号化序論 20
証明書を署名する 20
デジタル署名を確認する 20
公開鍵基盤 22
証明書および CRL 24
証明書を手動で要求する 25
証明書と CRL をロードする 28
CRL 設定を構成する 29
ローカル証明を自動で取得する 30

証明書および CRL（続き）
証明書の自動更新 33
鍵ペアの生成 33
OCSP (オンライン証明書ステータスプロトコル) 34
証明書取り消しチェック方法を指定する 35
ステータスチェック属性を表示する 35
オンライン証明書ステータスプロトコルレスポンダ URL を指定する 35
ステータスチェック属性を削除する 35
自己署名証明書 36
証明書の検証 37
自己署名証明書の手動作成 38
管理者定義の自己署名証明書を設定する 39
証明書の自動生成 42
自己署名証明書の削除 43

第 3 章 VPN (仮想プライベートネットワーク) のガイドライン 45

暗号オプション 46
サイトツーサイトの暗号オプション 46
ダイヤルアップ VPN オプション 53
ルートベーストンネルおよびポリシーベーストンネル 59
パケットフロー : サイトツーサイト VPN 61
トンネル構成のガイド 66
ルートベース VPN (仮想プライベートネットワーク) のセキュリティ検討事項 68
Null ルート 69
ダイヤルアップまたはリース回線 70
リース回線または Null ルートへの VPN フェールオーバー 71
おとりトンネルインターフェース 74
トンネルインターフェースの仮想ルーター 74
別のトンネルへの再ルーティング 75

第 4 章 サイト間 VPN (仮想プライベートネットワーク) 77

サイト間 VPN 構成 78
ルートベースのサイト間 VPN、AutoKey IKE 84
ポリシーベースのサイト間 VPN、AutoKey IKE 93
ルートベースのサイト間 VPN、動的ピア 99
ポリシーベースのサイト間 VPN、動的ピア 107
ルートベースのサイト間 VPN、手動鍵 116
ポリシーベースのサイト間 VPN、手動鍵 122
FQDN を使用した動的 IKE ゲートウェイ 127
エイリアス 128
FQDN を使用した AutoKey IKE ピアを設定する 129
アドレスがオーバーラップする VPN サイト 137
透過モード VPN 148

第 5 章 ダイヤルアップ仮想プライベートネットワーク 157

ダイヤルアップ 158
ポリシーベース ダイヤルアップ VPN、AutoKey IKE 159
ルートベース ダイヤルアップ VPN、動的ピア 164
ポリシーベース ダイヤルアップ VPN、動的ピア 171
ダイヤルアップ VPN ユーザー用の双方向性ポリシー 177

グループ IKE ID 182
証明書付きグループ IKE ID 182
ワイルドカードおよびコンテナ ASN1-DN IKE ID タイプ 184
グループ IKE ID（証明書）の作成 187
事前共有鍵を使用するグループ IKE ID の設定 191
共有 IKE ID 197

第 6 章 レイヤー 2 トンネリングプロトコル 205

L2TP について 205
パケットのカプセル化と脱カプセル化 208
カプセル化 208
脱カプセル化 209
L2TP パラメータの設定 211
L2TP と L2TP-Over-IPSec 213
L2TP 構成 213
L2TP-over-IPSec を構成する 218
双方向の L2TP-over-IPSec 226

第 7 章 高度な仮想プライベート ネットワーク機能 233

NAT-Traversal 234
NAT の精査 235
NAT デバイスのトラバース 237
UDP チェックサム 239
キープアライブパケット 240
イニシエータ / 受信側シンメトリー 240
NAT-Traversal を使用可能にする 241
NAT-Traversal との IKE ID の使用 242
VPN の監視 243
再入力および最適化オプション 244
ソースインターフェースおよび宛先アドレス 245
ポリシー考慮事項 246
VPN 監視機能の構成 247
SNMP VPN 監視オブジェクトおよびトラップ 255
1 つのトンネルインターフェースに対する複数のトンネル 256
ルートからトンネルへのマッピング 257
リモートピアのアドレス 259
手動および自動テーブルエントリ 260
手動テーブル入力 260
自動テーブル入力 261
オーバーラップするサブネットに対応する 1 つのトンネル インターフェースでの VPN の設定 262
自動ルートおよび NHTB テーブル エントリのバインディング 281
自動ルー テーブル エントリでの OSPF の使用方法 292
冗長 VPN ゲートウェイ 294
VPN グループ 295
監視機構 296
IKE ハートビート 296
DPD（デッド ピア検出） 297
IKE 復旧手順 298
TCP SYN-Flag チェック 300
冗長 VPN ゲートウェイの作成 300
VPN 対向の作成 306
ハブアンドスポーク方式 VPN の作成 313

第 8 章 AutoConnect 仮想プライベートネットワーク 323

概要 323
機能 324
NHRP メッセージ 324
ACVPN トンネルの開始 326
AC-VPN の構成 327
ネットワークアドレス変換 327
ハブでの構成 327
各スポークでの構成 328
例 328

索引 ..... IX-I

本編について

第 5 部: 仮想プライベート ネットワーク では、VPN （仮想プライベートネットワーク）の概念および ScreenOS VPN 固有の機能について説明します。

本編の章は、以下のようになります。

- 第 1 章「インターネットプロトコルセキュリティ」、では、IPSec (インターネットプロトコルセキュリティ) の要素、およびそれらの要素と VPN トンネリングとの関連性について紹介します。
- 第 2 章「公開鍵暗号化」、では、公開鍵暗号化、証明証の使用、および PKI （Public Key Infrastructure、公開鍵基盤）を背景とした CRL （Certificate Revocation List、証明書の取り消しリスト）の使用について紹介します。
- 第 3 章「VPN (仮想プライベートネットワーク) の ガイドライン」、では、VPN トンネリングについて説明します。
- 第 4 章「サイト間 VPN (仮想プライベートネットワーク)」、では、2 台の Juniper Networks セキュリティデバイス間のサイトツーサイト VPN トンネルの構成方法を説明します。
- 第 5 章「ダイヤルアップ仮想プライベート ネットワーク」、では、ダイヤルアップ VPN の設定方法を説明します。
- 第 6 章「レイヤー 2 トンネリングプロトコル」、では、L2TP （レイヤー 2 トンネリングプロトコル）について、および L2TP と L2TP-overIPSec の構成例を説明します。
- 第 7 章「高度な仮想プライベート ネットワーク機能」、では、NAT (Network Address Translation、ネットワークアドレス変換機能) トピック、VPN 監視、およびマルチトンネルを使用する VPN について説明します。
- 第 8 章「AutoConnect 仮想プライベートネットワーク」、では、セキュリティデバイスが必要に応じて AutoConnect VPN をセットアップできるように、ScreenOS が NHRP（ネクストホップレゾリューションプロトコル）メッセージをどのように使用するかを説明します。本章では、AC-VPN が使用される場合の典型的なシナリオの例を提供します。

ドキュメントの規則

このドキュメントは、次のセクションで説明されている規則を使用しています。

- viii ページの「Web ユーザーインターフェースの規則」
- viii ページの「コマンドラインインターフェースの規則」
- ix ページの「ネーミング規則および文字タイプ」
- x ページの「説明図の規則」

Web ユーザーインターフェースの規則

WebUI（Web ユーザーインターフェース）では、各作業の操作指示は、操作手順と構成設定値に分かれています。構成設定を入力できる WebUI ページを開くには、画面の左側にあるナビゲーション ツリーのメニュー項目をクリックして、そのページに移動します。先へ進むと、ナビゲーション パスが画面の上部に表示されます。各ページは角括弧で分離されています。

WebUI のパスおよびアドレスを定義するためのパラメータは、以下のとおりです。

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.2.2.5/32
Zone: Untrust

構成設定のオンラインヘルプを開くには、画面の左上にある疑問符（?）をクリックします。

ナビゲーションツリーにも、Help > Config Guide 構成ページがあり、セキュリティポリシーおよび IPSec （インターネットプロトコルセキュリティ）の構成に役立ちます。ドロップダウンメニューからオプションを選択して、そのページの指示に従います。構成設定のオンラインヘルプを開くには、左上にある **?** 文字をクリックします。

コマンドラインインターフェースの規則

次の規則は、例とテキストにおいて、コマンドラインインターフェース（CLI）コマンドの構文を示すために使用されます。

例においては、次のように使用されます。

- 角括弧 [ ] 内にあるものはすべてオプションです。
- 中括弧 { } 内にあるものはすべて必須です。
- 選択肢が複数ある場合、各選択肢はパイプ (|) で区切られています。例えば、次のように表示されます。

```
set interface { ethernet1 | ethernet2 | ethernet3 } manage
```

- 変数は*斜体*で表示されます。

  set admin user *name1* password *xyz*

テキストにおいては、コマンドは**太字**で、変数は*斜体*で表示されます。

注 : キーワード入力時には、単語を間違いなく識別できる数の文字を入力すれば十分です。**set admin user wheezer j12fmt54** というコマンドを入力する際には、**set adm u whee j12fmt54** と入力するだけで十分です。ただし、本編に記載されたコマンドはすべて本来の形式で記載されています。

ネーミング規則および文字タイプ

ScreenOS はオブジェクトの名前 (アドレス、管理ユーザー、認証サーバー、IKE ゲートウェイ、仮想システム、VPN トンネルおよびゾーンなど、ScreenOS 構成に定義されているもの) に関して、次の規則に従います。

- 名前文字列に 1 つまたは複数のスペースが含まれる場合、文字列全体を二重引用符で囲む必要があります。例 :

  set address trust “local LAN” 10.1.1.0/24

- 二重引用符で囲まれた文字列の先頭または末尾のスペースを取り除きます。たとえば、「 **local LAN** 」は「**local LAN**」となります。

- 連続した複数のスペースは、一つのスペースとして扱われます。

- CLI キーワードの多くはケースセンシティブではありませんが、名前文字列はケースセンシティブです。たとえば、「**local LAN**」は「**local lan**」とは異なります。

ScreenOS は、次の文字タイプをサポートします。

- 1 バイト文字セット (SBCS) およびマルチバイト文字セット (MBCS)。SBCS の例に、ASCII、欧州言語、およびヘブライ語があります。2 バイト文字セット (DBCS) とも呼ばれる MBCS の例に、中国語、韓国語、および日本語があります。

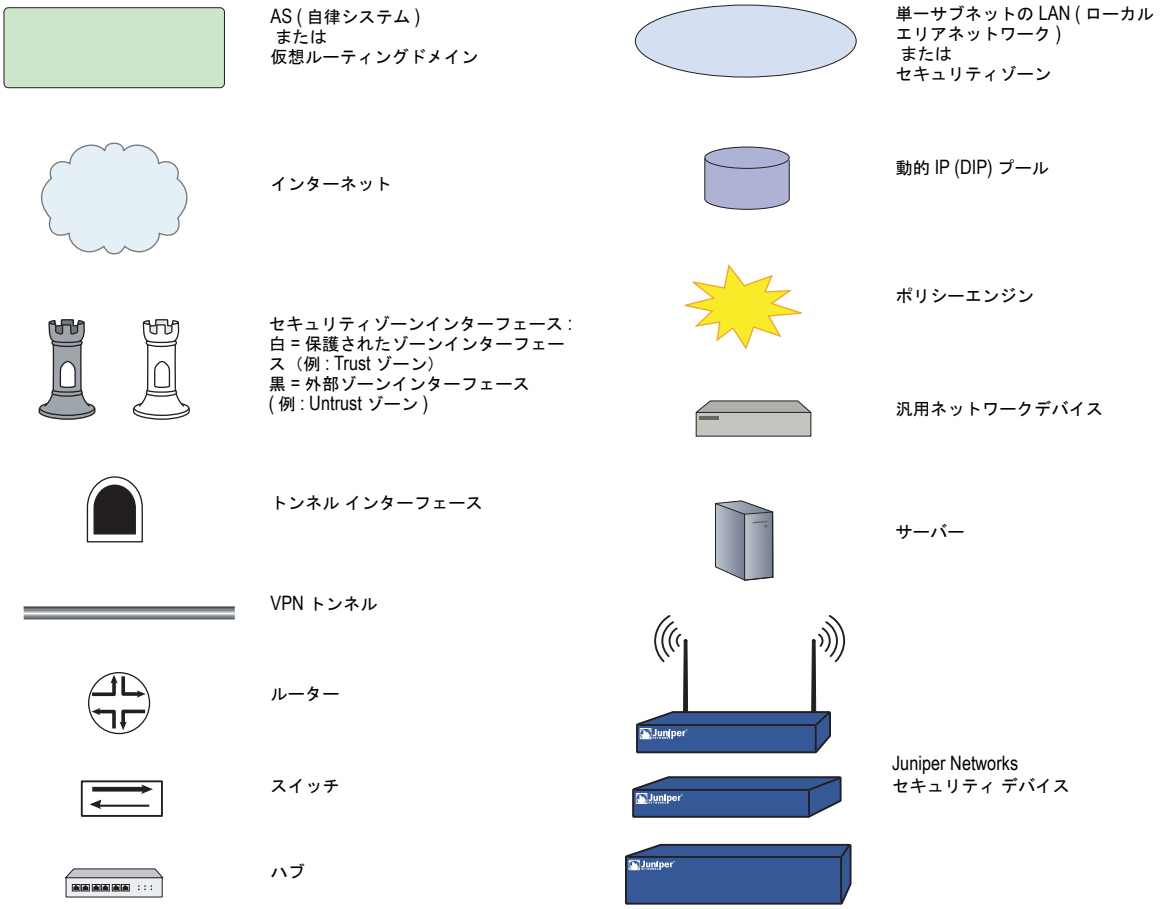
- ASCII 文字の 32（16 進数の 0x20）から 255（0xff)。ただし二重引用符 (“) は、スペースを含む名前文字列の先頭と末尾を示す特殊な意味をもつため、例外とします。

注 : コンソール接続では、SBCS のみがサポートされます。ご利用のブラウザがサポートする文字セットに応じて、WebUI は SBCS および MBCS の両方をサポートします。

説明図の規則

次の図は、本編を通して説明図に使用されている画像の基本的なものです。

図 1: 説明図の画像



技術ドキュメントおよびテクニカルサポート

Juniper Networks 製品のいずれかの技術ドキュメントを入手するには、www.juniper.net/techpubs/ をご覧になってください。

テクニカルサポートについては、http://www.juniper.net/customers/support/ にある Case Manager を使って事例サポートを開くか、1-888-314-JTAC (米国内) か 1-408-745-9500 (その他の国) までお問い合わせください。

本書に間違いや欠落があった場合は、techpubs-comments@juniper.net までお知らせください。

第 1 章

インターネットプロトコルセキュリティ

本章では、IPSec (インターネットプロトコルセキュリティ) の諸要素とそれらの VPN (仮想プライベートネットワーク) トンネリングとの関連性について紹介します。本章のセクションは、以下のようになります。

- 2 ページの「VPN (仮想プライベートネットワーク) の紹介」
- 3 ページの「IPSec の概念」
  - 4 ページの「モード」
  - 6 ページの「プロトコル」
  - 7 ページの「鍵管理」
  - 8 ページの「セキュリティアソシエーション」
- 8 ページの「トンネルネゴシエーション」
  - 9 ページの「フェーズ 1」
  - 11 ページの「フェーズ 2」
- 12 ページの「IKE および IPSec パケット」
  - 12 ページの「IKE パケット」
  - 15 ページの「IPSec パケット」

VPN (仮想プライベートネットワーク) の紹介

VPN (仮想プライベートネットワーク) は、インターネットのような公開された WAN (ワイドエリアネットワーク) 全域で各リモートコンピュータ間を安全に通信する手段を提供します。

VPN 接続は、2 つの LAN (ローカルエリアネットワーク)、あるいはリモートダイヤルアップユーザーと LAN を接続することができます。この 2 つのポイントを流れるトラフィックは、ルーター、スイッチ、および他のネットワーク設備などの共有リソースを通過します。これらの設備によって公開 WAN が構成されます。WAN の通過中、VPN 通信を安全に行うために、2 つの参加者は IPSec (IP セキュリティ) トンネルを作成します。

注 : *トンネル*の意味は、トランスポートでもトンネルモードでもありません (4 ページの「モード」を参照)。IPSec 接続を表します。

IPSec トンネルを構成するのは、トンネルの各端に 1 つずつある 1 組の 1 方向 SA (セキュリティアソシエーション) であり、これにより SPI (セキュリティパラメータインデックス)、宛先 IP アドレス、使用されるセキュリティプロトコル (認証ヘッダーまたはセキュリティペイロードのカプセル化) を指定します。

SPI の詳細については、8 ページの「セキュリティアソシエーション」を参照してください。IPSec セキュリティプロトコルの詳細については、6 ページの「プロトコル」を参照してください。

IPSec トンネルは、SA を介して以下のセキュリティ機能を供給することができます。

- プライバシー (暗号化パスワードを介して)
- コンテンツ保全性 (データ認証を介して)
- 送信側認証および一証明書を使用する場合一拒否不能 (データ発生元認証を介して)

使用されるセキュリティ機能は、ニーズによって異なります。IP パケットソースおよびコンテンツ保全性の認証だけが必要である場合、暗号化パスワードを適用することなく、そのパケットを認証できます。また、プライバシーの保護のみを重視する場合、認証メカニズムを適用することなくパケットを暗号化できます。オプションで パケットの暗号化と認証の両方を行うこともできます。多くのネットワークセキュリティデザイナーは、VPN トラフィックを暗号化し、認証し、再生保護することを選びます。

ScreenOS は、2 種の鍵作成メカニズムにより VPN トンネルを作成するために IPSec 技術をサポートします。

- 手動鍵
- 事前共有鍵または証明書付きの Autokey IKE

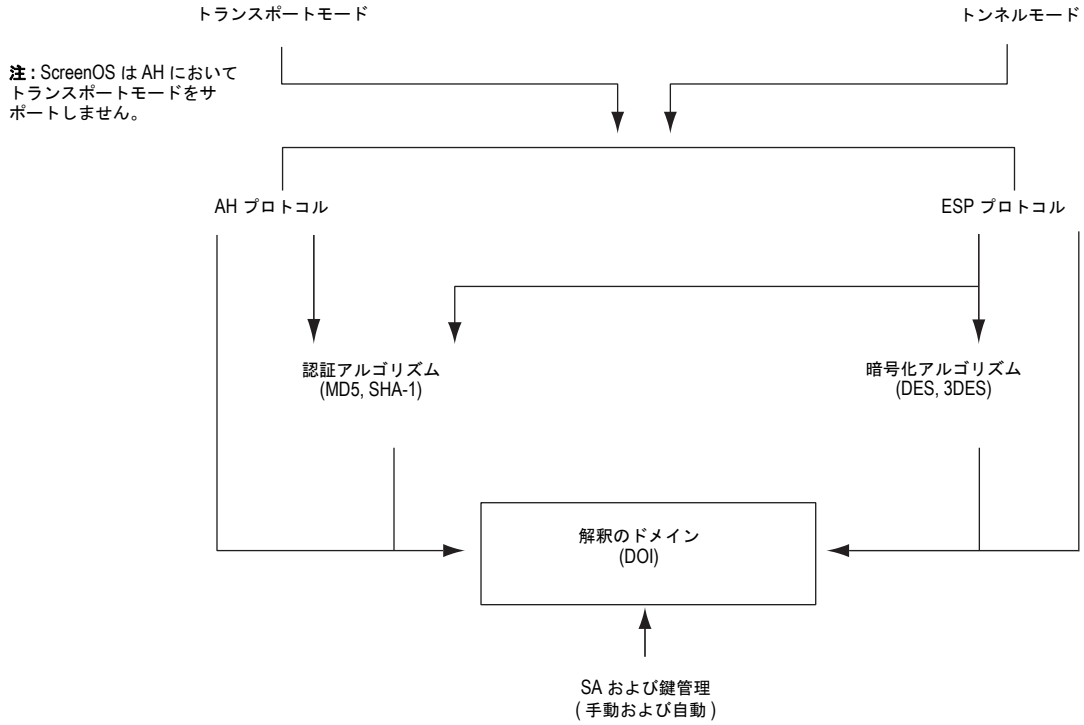
IPSec の概念

IPSec (IP セキュリティ) は、IP パケットレイヤーで暗号化して、通信を安全にするための関連プロトコルスイートです。IPSec は、2 つのモードと 2 つのメインプロトコルで構成されます。

- トランスポートおよびトンネルモード
- 認証を行うための AH (認証ヘッダー) プロトコル、および暗号化のため (および認証のため) の ESP (セキュリティペイロードのカプセル化)

IPSec はまた SA(セキュリティアソシエーション) と鍵配分の手動および自動ネゴシエーションの方法を提供します。このためのすべての属性が DOI (解釈ドメイン) に集められます。RFC 2407 および RFC 2408 を参照してください。

図 2: IPSec のアーキテクチャ



注 : IPSec DOI (解釈ドメイン) は、VPN トンネルのネゴシエーションを正常に行うために必要なすべてのセキュリティパラメータの定義が含むドキュメントです。基本的に、SA と IKE ネゴシエーションに必要とされるすべての属性に関する定義が含みます。

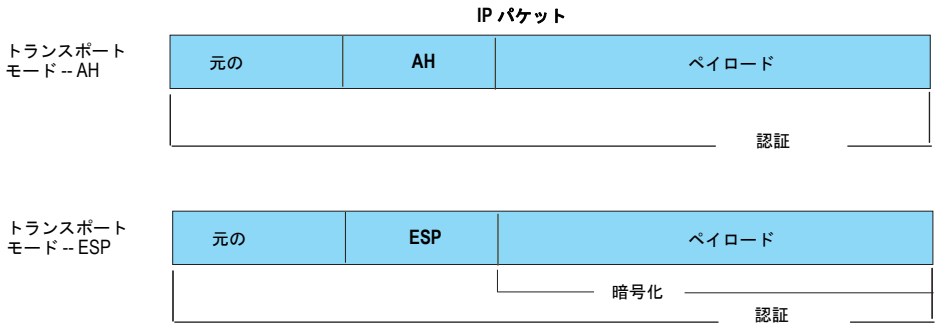
モード

IPSec は、トランスポートまたはトンネル、いずれかのモードで動作します。トンネルの両端がホストの場合、いずれかのモードを使用できます。少なくともトンネルの端点の 1 つがルーターやファイアウォールのようセキュリティゲートウェイの場合、トンネルモードを使用する必要があります。Juniper Networks セキュリティデバイスは、IPSec トンネルでは常にトンネルモードで、L2TP-over-IPSec トンネルでは常にトランスポートモードで動作します。

トランスポートモード

図 3 で示されるように、オリジナル IP パケットは、もう 1 つの IP パケット内ではカプセル化されません。パケット全体は (AH で) 認証され、ペイロードは (ESP で) 暗号化されます。オリジナルヘッダーは WAN を超えて送信されるので、プレーンテキストのままにします。

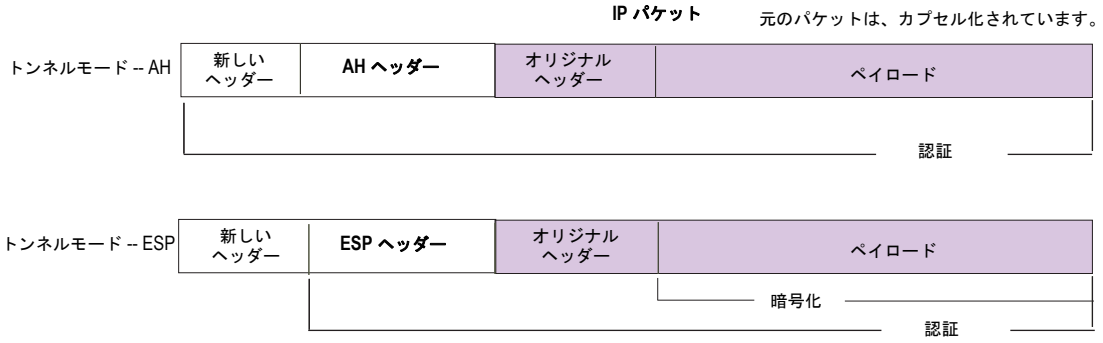
図 3: トランスポートモード



トンネルモード

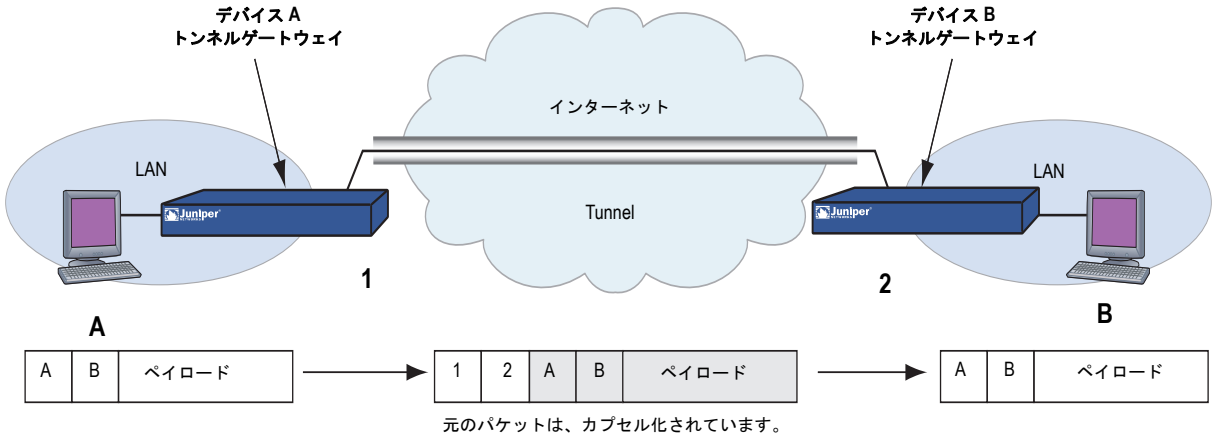
図 4 で示されるように、オリジナル IP パケット (ペイロードおよびヘッダー) 全体は、もう 1 つの IP ペイロード内にカプセル化され、新しいヘッダーが先頭に追加されます。オリジナルパケット全体は、暗号化、認証、または暗号化と同時に認証されます。AH で、AH および新しいヘッダーも認証されます。ESP で、ESP ヘッダーも認証できます。

図 4: トンネルモード



サイト間 VPN では、新ヘッダーに使用されるソースおよび宛先アドレスは、出力インターフェース (NAT あるいはルートモード) の IP アドレスか VLAN1 IP アドレス (透過モード) の IP アドレスです。カプセル化されているパケットのソースおよび宛先アドレスは、接続の最端点のアドレスです。

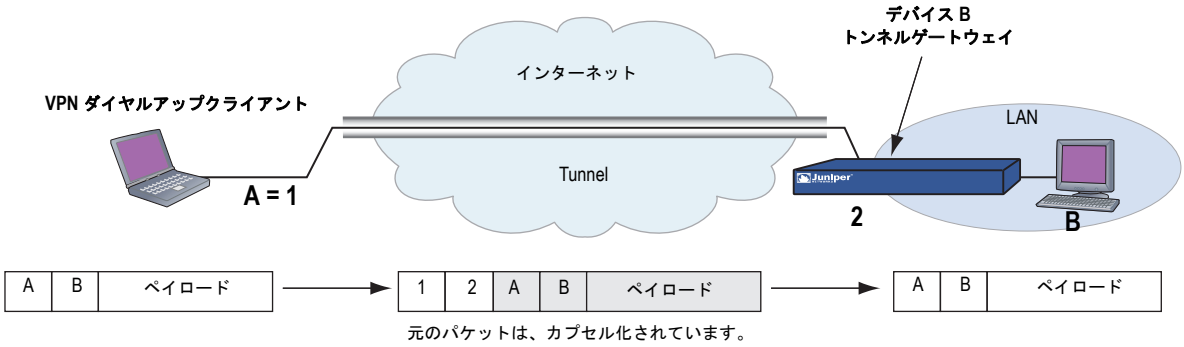
図 5: トンネルモードのサイト間 VPN



ダイヤルアップ VPN では、トンネルの VPN ダイヤルアップクライアント終端にはトンネルゲートウェイは全くありません。トンネルは、直接クライアントまで達します。この場合、ダイヤルアップクライアントから送信されるパケットでは新しいヘッダーとカプセル化された元のヘッダーはどちらも IP アドレスがクライアントのコンピュータと同じとなります。

注 : NetScreen-Remote など一部の VPN クライアントを使用すると、仮想内部 IP アドレスを定義することができます。この場合、仮想内部 IP アドレスはクライアントから送出されるトラフィックの元のパケットヘッダー内のソース IP アドレスであり、ISP がダイヤルアップクライアントに動的に割り当てる IP アドレスは外部ヘッダーのソース IP アドレスです。

図 6: トンネルモードのダイヤルアップ VPN



プロトコル

IPSec は、IP レイヤーの通信を安全にするために 2 つのプロトコルを使用します。

- AH (認証ヘッダー) ー IP パケットのソースを認証し、そのコンテンツの保全性を確認するためのセキュリティプロトコル
- ESP (セキュリティペイロードのカプセル化)ー IP パケット全体を暗号化する (およびそのコンテンツを認証する) ためのセキュリティプロトコル

認証ヘッダー

AH (認証ヘッダー) プロトコルは、パケットのコンテンツと発信元の信頼性および保全性を確認する手段を提供します。秘密鍵と MD5 あるいは SHA-1 ハッシュ機能のいずれかを使用して HMAC (ハッシュベースメッセージ認証コード) を経て計算されたチェックサムによってそのパケットを認証することができます。

- **MD5 (メッセージダイジェストバージョン 5)** ー任意に指定した長さのメッセージと 16 バイト鍵から、128 ビットハッシュ (*デジタル署名*あるいは *メッセージダイジェスト*とも呼ばれる) を生産するアルゴリズム。その結果生じるハッシュは、コンテンツおよびソースの信頼性と保全性を確認するために入力の指紋のように使用されます。
- **SHA-1 (セキュアハッシュアルゴリズム -1)** ー任意に指定した長さのメッセージと 20 バイト鍵から、160 ビットハッシュを生産するアルゴリズム。より大きなハッシュが生産されるため、一般に MD5 より安全とみなされます。計算処理が ASIC で行われるために、性能コストはごくわずかです。

注 : MD5 および SHA-1 ハッシングアルゴリズムの詳細は、RFC の 1321、2403 (MD5) と 2404 (SHA-1) を参照してください。HMAC については、RFC 2104 を参照してください。

セキュリティペイロードのカプセル化

ESP (セキュリティペイロードのカプセル化) プロトコルは、プライバシー (暗号化) およびソース認証とコンテンツ保全性 (認証) を保証するための手段を提供します。トンネルモードでの ESP は、IP パケット全体 (ヘッダーとペイロード) をカプセル化し、新規 IP ヘッダーを現在の暗号化済みパケットに追加します。この新規 IP ヘッダーは、ネットワークを通じて保護されたデータを送信するために必要な宛先アドレスを含みます。

ESP では、暗号化と認証、暗号化のみ、認証のみを行うことができます。暗号化パスワード用に、以下の暗号化アルゴリズムのいずれかを選択することができます。

- **DES (データ暗号化標準規格)** ー 56 ビット鍵による暗号化ブロックアルゴリズム
- **3DES (トリプル DES)** ー DES のより強力なバージョン。168 ビット鍵を使用して、3 つのラウンドでオリジナル DES アルゴリズムが適用されます。DES は、重要な性能保存を提供しますが、多くの機密性の高いデータ転送には適していないと考えられています。
- **AES (次世代標準暗号)** ー新たに制定された暗号化標準は、インターネットインフラワールドによって導入される場合に、他のネットワークセキュリティデバイスとでより大きな相互運用性を提供します。ScreenOS は、128 ビット、192 ビット、そして 256 ビット鍵による AES をサポートします。

認証には、MD5 と SHA-1 アルゴリズムのどちらを使用することができます。

注 : 認証に **NULL** を選択することもできますが、そのような状況下では IPSec が攻撃に弱くなることが分かっています。したがって、認証に **NULL** を選択するのはお勧めできません。

鍵管理

鍵の配布と管理は、VPN を正しく使用するために重要です。IPSec は、手動および自動の鍵配布方法をサポートします。

手動鍵

手動鍵を使用して、トンネルの両端の管理者はセキュリティパラメータのすべてを構成します。これは、ネットワークが小さくて変化がなく、鍵の配布、保守、追跡が難しくない場合に実行可能な技術です。しかし、手動鍵構成を遠くまで安全に配布するには、セキュリティの問題があります。鍵を直接手渡す場合を除いて、その鍵が転送中にまったく破損していないという確信を得ることはできません。また、その鍵を変えようとするたびに、その鍵を最初に配布した時と同じセキュリティ問題に直面してしまいます。

AutoKey IKE

非常に多数のトンネルをつくって管理しなければならない場合、すべての要素を手動で構成しなくてもよい方法が必要です。IPSec は、IKE (インターネット鍵交換) プロトコルを使用した鍵とセキュリティアソシエーションの自動的な生成とネゴシエーションをサポートします。ScreenOS では、そうした自動トンネルネゴシエーションを AutoKey IKE と呼び、事前共有鍵による AutoKey IKE と証明書による AutoKey IKE をサポートします。

事前共有鍵による AutoKey IKE

事前共有鍵を使用して IKE セッションで参加者を認証する AutoKey IKE では、双方が前もって事前共有鍵を構成して安全に交換する必要があります。この点では、安全な鍵配布の問題は手動鍵の場合と同じです。しかし、AutoKey は手動鍵と違って、いったん配布されると、所定の間隔で IKE プロトコルを使用してその鍵を自動的に変えることができます。鍵を頻繁に変えることでセキュリティも大きく向上し、また自動的に変更することで鍵管理の責任が少なくなります。ただし、鍵を変更するとトラフィックオーバーヘッドが増えるため、あまり頻繁に変更を行うとデータ伝送効率が低下してしまいます。

注 : 事前共有鍵は、両方の参加者が通信を始める前に持たなければならない暗号化と復号化両方のための鍵です。

証明書付き AutoKey IKE

AutoKey IKE ネゴシエーション中に参加者を認証するために証明書を使用する場合、各参加者は、公開 / 秘密鍵ペアを生成し、(19 ページの「公開鍵暗号化」を参照) 証明書を取得します。24 ページの「証明書および CRL」を参照してください。CA (認証局) の発行が両参加者に信頼される限り、参加者はピアの公開鍵を取り出し、ピアの署名を確認することができます。鍵と SA の追跡は全く必要ありません。IKE が自動的に行います。

注： 手動鍵と AutoKey IKE トンネルの例については、77 ページの「サイト間 VPN (仮想プライベートネットワーク)」を参照してください。

セキュリティアソシエーション

SA (セキュリティアソシエーション) は、通信チャンネルの保護で使用する方法とパラメータに関する VPN 参加者間の 1 方向の一致です。完全双方向通信は、各方向に 1 つずつで少なくとも 2 つの SA を必要とします。

SA は、以下の通信を保護するためのコンポーネントをまとめます。

- セキュリティアルゴリズムと鍵
- プロトコルモード (トランスポートまたはトンネル)
- 鍵管理方法 (手動鍵または AutoKey IKE)
- SA 寿命

アウトバウンド VPN トラフィックには、ポリシーが VPN トンネルと関連する SA を呼び出します。インバウンドトラフィックには、セキュリティデバイスがトリプレット （3 つ組）を使用して SA にチェックします。

- 宛先 IP
- セキュリティ プロトコル (AH または ESP)
- セキュリティパラメータインデックス (SPI) 値

トンネルネゴシエーション

手動鍵 IPSec トンネルの場合、すべての SA (セキュリティアソシエーション) パラメータがあらかじめ定義されているため、どの SA を使用するかをネゴシエートする必要はありません。実質的に、トンネルはすでに確立されています。トラフィックが、その手動鍵トンネルを使用するポリシーに適合する場合、あるいはルートにそのトンネルが含まれる場合、セキュリティデバイスは、設定されたとおりにデータを暗号化および認証し、そのデータを宛先ゲートウェイに転送するだけです。

AutoKey IKE IPSec トンネルを確立するためには、2 つのフェーズのネゴシエーションが必要になります。

- フェーズ 1 で、参加者は IPSec SA をネゴシエートする安全なチャネルを確立します。
- フェーズ 2 で、参加者はその後のユーザーデータの交換を暗号化して認証するための IPSec SA をネゴシエートします。

フェーズ 1

AutoKey IKE トンネルネゴシエーションのフェーズ 1 では、チャネルをどのように認証して保護するかについての提案を交換します。交換には、アグレッシブまたはメイン どちらのモードを使用しても、参加者は条件に合う次のようなセキュリティサービスについて提案を交わします。

- 暗号化アルゴリズム (DES および 3DES) と認証アルゴリズム (MD5 および SHA-1)。これらのアルゴリズムの詳細については、6 ページの「プロトコル」を参照してください。
- Diffie-Hellman グループ (10 ページの「Diffie-Hellman の鍵交換」を参照してください。)
- 事前共有鍵または RSA/DSA 証明書 (7 ページの「AutoKey IKE」を参照してください。)

フェーズ 1 ネゴシエーションは、トンネルの両端が、提案された フェーズ 1 セキュリティパラメータの少なくとも 1 セットを受け入れることに同意し、それらを処理すると終了します。Juniper Networks セキュリティデバイスはフェーズ 1 のネゴシエーション用に提案を 4 つまでサポートするため、受け入れる予定の鍵ネゴシエーション用のセキュリティパラメータの範囲をどこまで限定的にするかを定義できます。

ScreenOS が提供する定義済みフェーズ 1 の提案は、以下のとおりです。

- **Standard (標準):** pre-g2-aes128-sha と pre-g2-3des-sha
- **Compatible (互換):** pre-g2-3des-sha、pre-g2-3des-md5、pre-g2-des-sha、および pre-g2-des-md5
- **Basic (基本):** pre-g1-des-sha および pre-g1-des-md5

カスタムのフェーズ 1 提案を定義することもできます。

メインモードとアグレッシブモード

フェーズ 1 は、メインモードかアグレッシブモードのいずれかで行われます。2 つのモードの説明は以下のとおりです。

メインモード : 開始側と受信側は、以下のサービスを完成するために 3 つの双方向交換 (合計 6 つのメッセージ) を送信します。

- 第 1 交換、(メッセージ 1 および 2): 暗号化アルゴリズムと認証アルゴリズムを提案および承認します。
- 第 2 交換、(メッセージ 3 および 4): Diffie-Hellman 鍵交換を実行し、開始側と受信側はそれぞれ疑似乱数を提供します。
- 第 3 交換、(メッセージ 5 および 6): それぞれの身元 (ID) を送信して検証します。

第 3 のメッセージ交換で送信される情報は、第 1 と第 2 の交換で確立された暗号化アルゴリズムによって保護されます。したがって、参加者の身元が暗号化されずに送信されることはありません。

アグレッシブモード : 開始側と受信者が到達する目的は同じですが、両者の交換は 2 回だけで、メッセージ数は合計で 3 つです。

- 第 1 メッセージ : 開始側は SA を提案し、Diffie-Hellman 鍵交換を開始し、疑似乱数とその IKE ID を送信します。
- 第 2 メッセージ : 受信側は SA を承認し、開始側を認証して、疑似乱数とその IKE ID を送信し、証明書を使用している場合は受信側の証明書を送信します。
- 第 3 メッセージ : 開始側は受信側を認証し、交換を確認し、証明書を使用している場合は、開始側の証明書を送信します。

参加者の身元は 第 1 と第 2 のメッセージで暗号化されずに交換されるため、アグレッシブモードは身元保護を提供しません。

注 : ダイヤルアップ VPN ユーザーが事前共有鍵による AutoKey IKE トンネルをネゴシエートするときは、アグレッシブモードを使用する必要があります。ダイヤルアップ VPN ユーザーは、E メールアドレス、完全修飾ドメイン名 (FQDN)、または IP アドレスを IKE ID として使用できることにも注意してください。動的ピアは E メールアドレスと FQDN のどちらも使用できますが、IP アドレスは使用できません。

Diffie-Hellman の鍵交換

Diffie-Hellman (DH) 鍵交換を使用すると、参加者は共有秘密値を作成できます。この技術の強みは、通信路にて秘密値を露呈することなく、セキュアではない媒体上にその秘密値を作成することを許可するということにあります。5 つの Diffie-Hellman グループがあります (ScreenOS は、グループ 1、2、および 5 をサポートします)。各グループの計算で使用されるプライムモジュールの大きさは、以下のように異なります。

- **DH グループ 1:** 768 ビットモジュール
- **DH グループ 2:** 1024 ビットモジュール
- **DH グループ 5:** 1536 ビットモジュール

注 : DH グループ 1 のセキュリティ強度は低下しているため、使用は推奨していません。

モジュールサイズが大きくなるほど、生成した鍵の安全度は高まると考えられますが、モジュールサイズが大きいほど鍵生成プロセスにかかる時間は長くなります。各 DH グループのモジュールのサイズは異なるため、参加者は同じグループを使用することに合意する必要があります。

注 : フェーズ 1 ネゴシエーションで複数 (最大 4 つ) の提案を構成する場合、全ての提案で同じ Diffie-Hellman グループを使用してください。同じガイドラインが、フェーズ 2 ネゴシエーションの複数提案にも適用されます。

フェーズ 2

参加者は安全で認証されたチャネルを確立するとフェーズ 2 へ進み、そこでは IPSec トンネルを送信するデータを保護するために SA をネゴシエートします。

フェーズ 1 のプロセスと同様、参加者は提案を交換してどのセキュリティパラメータを SA で使用するかを決めます。フェーズ 2 の提案にも、ESP (セキュリティペイロードのカプセル化) と AH (認証ヘッダー) のどちらかのセキュリティプロトコルと、選択した暗号化および認証アルゴリズムが含まれます。PFS (完全転送機密保持) が必要であれば、この提案で Diffie-Hellman グループを指定することもできます。

フェーズ 1 で使用されたモードにかかわらず、フェーズ 2 は常にクイックモードで動作し、3 つのメッセージ交換を伴います。

Juniper Networks セキュリティデバイスはフェーズ 2 ネゴシエーションで提案を 4 つまでサポートしているため、受け入れるトンネルパラメータの範囲をどの程度限定的にするかを定義できます。ScreenOS は、再生保護 (Replay Protection) 機能も提供します。この機能を使用すると、パケットは常にシーケンス番号と共に送信されるため、ネゴシエーションを必要としません。シーケンス番号を確認するかしないかだけを選択します (再生保護の詳細は、12 ページの「再生保護」を参照してください)。

ScreenOS が提供する定義済みフェーズ 2 の提案は、以下のとおりです。

- **Standard (標準):** g2-esp-3des-sha および g2-esp-aes128-sha
- **Compatible (互換):** nopfs-esp-3des-sha、nopfs-esp-3des-md5、nopfs-esp-des-sha、および nopfs-esp-des-md5
- **Basic (基本):** nopfs-esp-des-sha および nopfs-esp-des-md5

カスタムのフェーズ 2 提案を定義することもできます。

フェーズ 2 では、ピアもプロキシ ID を交換します。プロキシ ID は、3 つの部分からなるタプルで、ローカル IP アドレス - リモート IP アドレス - サービスで構成されます。2 つのピアのプロキシ ID は一致しなければなりません。つまり、両ピアのプロキシ ID で指定されたサービスは同じでなければならず、一方のピアに指定されたローカル IP アドレスはもう一方のピアに指定されたリモート IP アドレスと同じでなければなりません。

完全転送機密保持

PFS (完全転送機密保持) はフェーズ 2 の鍵を導出するための方法で、この鍵はこれまでに説明した鍵から独立しており関係がありません。代わりに、フェーズ 1 提案が作成する鍵 (SKEYID_d 鍵) からすべてのフェーズ 2 鍵が導出されます。SKEYID_d 鍵は、最低限の CPU 処理でフェーズ 2 鍵を生成できます。不正パーティが SKEYID_d 鍵にアクセスすると、すべての暗号鍵は役に立たなくなってしまいます。

PFS は、各フェーズ 2 トンネルに対して、新規に起こす Diffie-Hellman 鍵交換を強要することによってこのセキュリティリスクに対処します。フェーズ 2 の再入力手順は、PFS を使用可能にすると時間が少し余計にかかりますが、PFS を使用することでより安全となります。

再生保護

再生攻撃が発生するのは、何者かが一連のパケットを傍受し、後でそれらのパケットを使用してシステムに大量の要求を送りつけて DoS (サービス拒否) を引き起こしたり、Trusted ネットワークに侵入するようなときです。再生保護機能によって、セキュリティデバイスはすべての IPSec パケットを調べて、以前に受信されているかどうかを確認できます。パケットが指定したシーケンス範囲外に達すれば、セキュリティデバイスはそのパケットを拒否します。

IKE および IPSec パケット

IPSec VPN トンネルには、主な要素が次の 2 つあります。

- **トンネルセットアップ :** ピアは、最初にセキュリティアソシエーション (SA) を確立し、ピア間のトラフィックを保護するパラメータを定義します。SA は、各終端の管理者が手動で定義するか、または IKE フェーズ 1 およびフェーズ 2 ネゴシエーションを通して動的に定義することができます。フェーズ 1 は、メインモードかアグレッシブモードのいずれかで動作します。フェーズ 2 は常にクイックモードで動作します。

- **適用されたポリシー :** IPSec は、トンネル設定中にピアが同意した SA で定義されたセキュリティパラメータを使用して、2 つのトンネル端点間で送信されるトラフィックを保護します。IPSec は、トランスポートまたはトンネル、いずれかのモードで適用できます。どちらのモードも、2 つの IPSec プロトコル ñ ESP (Encapsulating Security Payload) と AH (Authentication Header) に対応しています。

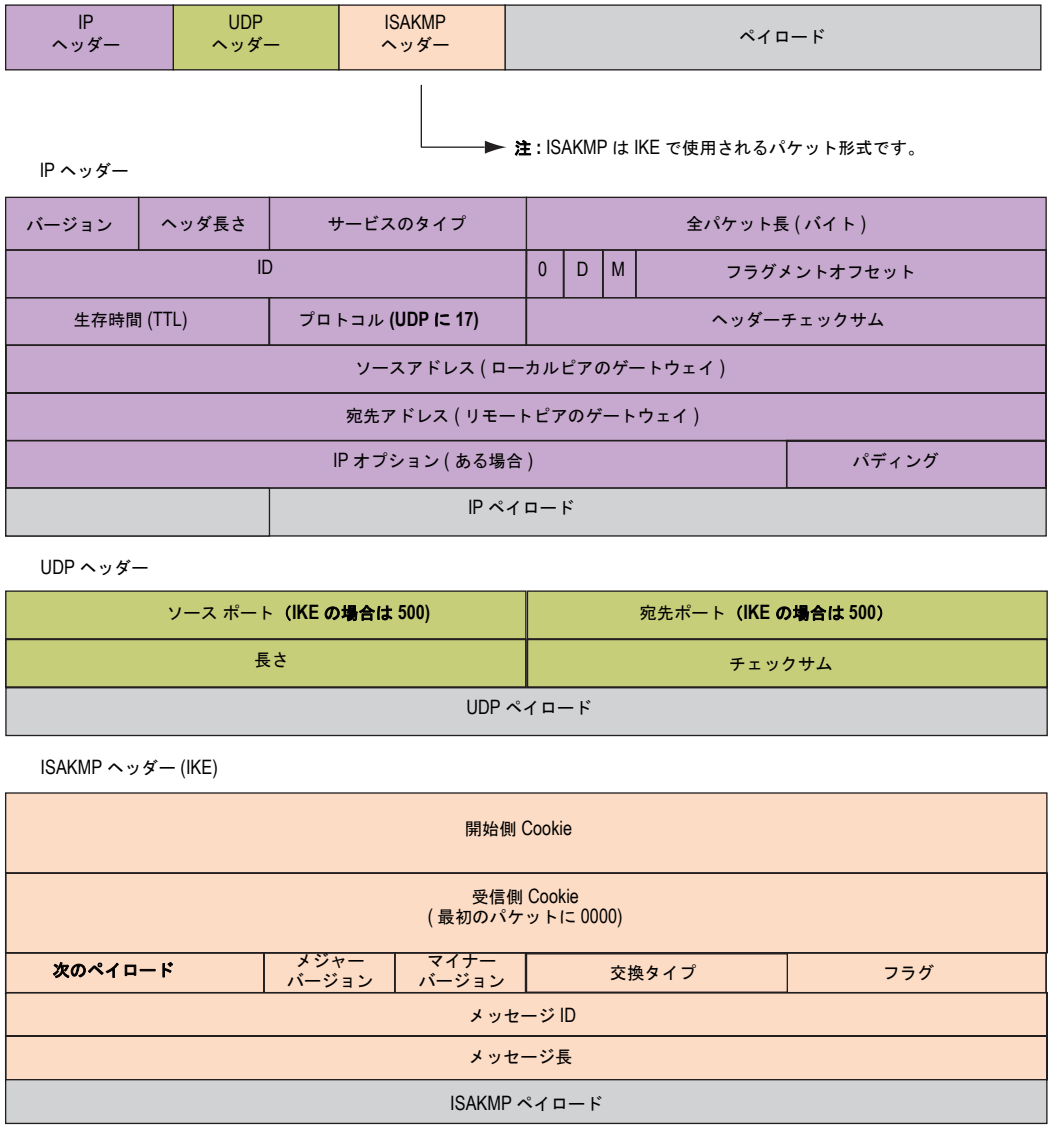
VPN トンネルの IKE および IPSec 段階でのパケット処理については、12 ページの「IKE パケット」および 15 ページの「IPSec パケット」を参照してください。それぞれ IKE と IPSec のパケットヘッダーについて説明があります。

IKE パケット

トンネルを必要としているセキュリティデバイスにクリアテキストパケットが到着し、そのトンネルのアクティブなフェーズ 2 SA がない場合、デバイスは IKE ネゴシエーションを開始します (そして、そのパケットをドロップします)。IP パケットヘッダーのソースと宛先のアドレスは、それぞれローカルおよびリモートの IKE ゲートウェイのアドレスとなります。IP パケットペイロードには、ISAKMP (Internet Security Association and Key Management Protocol) または IKE パケットをカプセル化している UDP セグメントがあります。フェーズ 1 とフェーズ 2 の IKE パケット形式は同じです。

注 : 最初の IP パケットがドロップされると、ソースホストが再送信します。通常、2 回目のパケットがセキュリティデバイスに到着するまでに、IKE ネゴシエーションは完了し、転送するまでの間、デバイスが、それ以降のセッション中の全パケットも含め、IPSec で保護しています。

図 7: (フェーズ 1 と 2 の IKE パケット)



次のペイロードフィールドには、以下のいずれかのペイロードタイプを示す数値を入力します。

- 0002 - SA ネゴシエーションペイロード。フェーズ 1 またはフェーズ 2 SA の定義が含まれています。
- 0004 - 提案ペイロード。フェーズ 1 またはフェーズ 2 の提案にできます。
- 0008 - 変換ペイロード。SA ペイロードでカプセル化された提案ペイロードでカプセル化されます。
- 0010 - KE (Key Exchange) ペイロード。Diffie-Hellman 公開値など鍵交換を実行するために必要な情報が含まれています。

- 0020 - Idx (識別番号) ペイロード。
  - フェーズ 1 では、IDii が開始側 ID を表し、IDir が受信側 ID を表します。
  - フェーズ 2 では、IDui が開始側ユーザー、IDur が受信側ユーザーを表します。

    ID には、FQDN、U-FQDN、IP アドレス、ASN.1_DN などの IKE ID タイプが入ります。
- 0040 - CERT (証明書) ペイロード。
- 0080 - CERT_REQ (証明書要求) ペイロード。
- 0100 - Hash (ハッシュ) ペイロード。特定のハッシュ関数のダイジェスト出力が含まれています。
- 0200 - SIG (署名) ペイロード。デジタル署名が含まれています。
- 0400 - Nonce (Nx) ペイロード。交換に必要な擬似乱数が含まれています。
- 0800 - 通知ペイロード。
- 1000 - ISAKMP 削除ペイロード。
- 2000 - ベンダー ID (VID) ペイロード。フェーズ 1 ネゴシエーションに含めることができます。NAT-T 対応の印として使用されます。

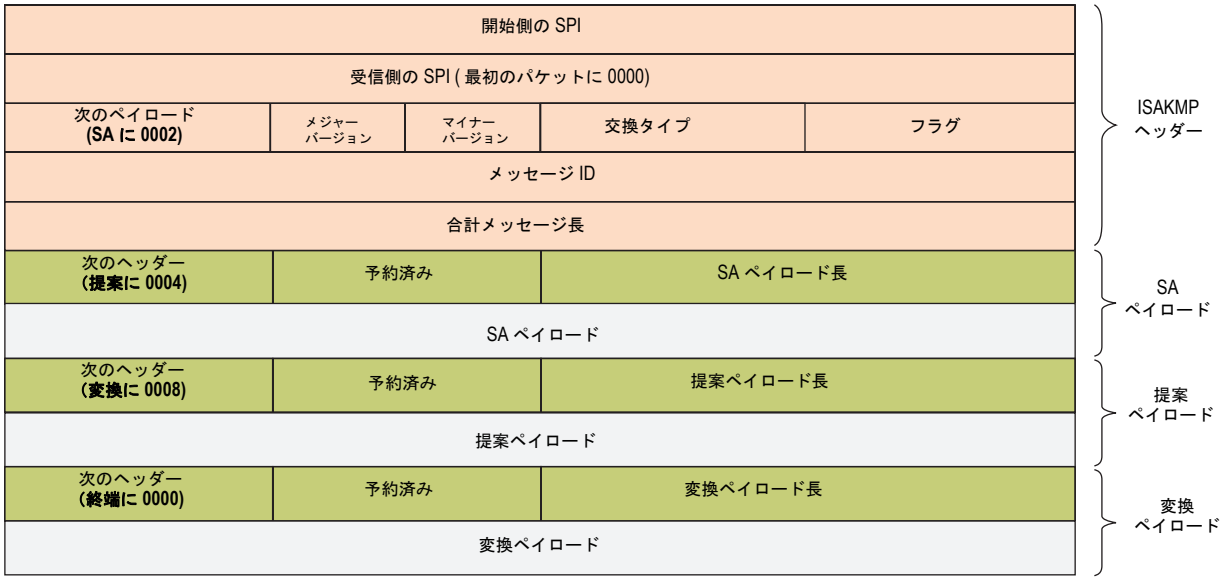
図 8 に示されるように、各 ISAKMP ペイロードは、次のような同一の汎用ヘッダーから開始します。

図 8: 汎用 ISAKMP ペイロードヘッダー

次のヘッダー	予約済み	ペイロード長 (バイト)
ペイロード		

次のヘッダーフィールドの値で示される、それ以降の各ペイロードタイプを繋げて、複数の ISAKMP ペイロードにすることができます。値 **0000** は最後の ISAKMP ペイロードを表します。15 ページの図 9 の例を参照してください。

図 9: 汎用 ISAKMP ペイロードの ISAKMP ヘッダー



IPSec パケット

IKE ネゴシエーションが完了し、2 つの IKE ゲートウェイがフェーズ 1 とフェーズ 2 セキュリティアソシエーション (SA) を確立すると、セキュリティデバイスは、ある IKE ゲートウェイの背後にあるホストが別のゲートウェイの背後にあるホストに送信する後続のクリアテキスト IP パケットに IPSec 保護を適用します (ポリシーがトラフィックを許可しているものと仮定します)。フェーズ 2 SA がトンネルモードで ESP (カプセル化されたセキュリティペイロード) を指定すると、パケットは下図のようになります。ここで、セキュリティデバイスは開始側のホストが送信する元のパケットに 2 つのヘッダーを追加します。

注 : ESP については、6 ページの「セキュリティペイロードのカプセル化」を参照してください。トンネルモードに関しては、4 ページの「トンネルモード」を参照してください。

図 10: IPSec パケット ó トンネルモードの ESP (カプセル化されたセキュリティペイロード)

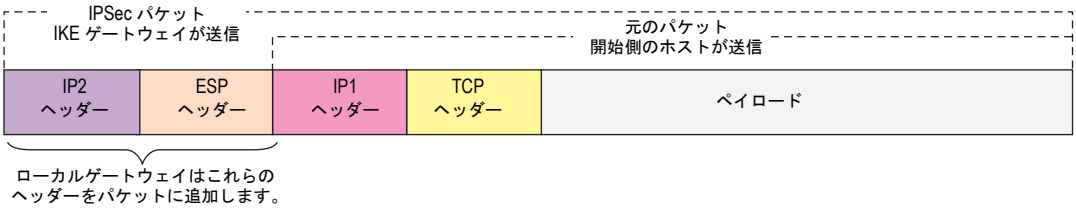
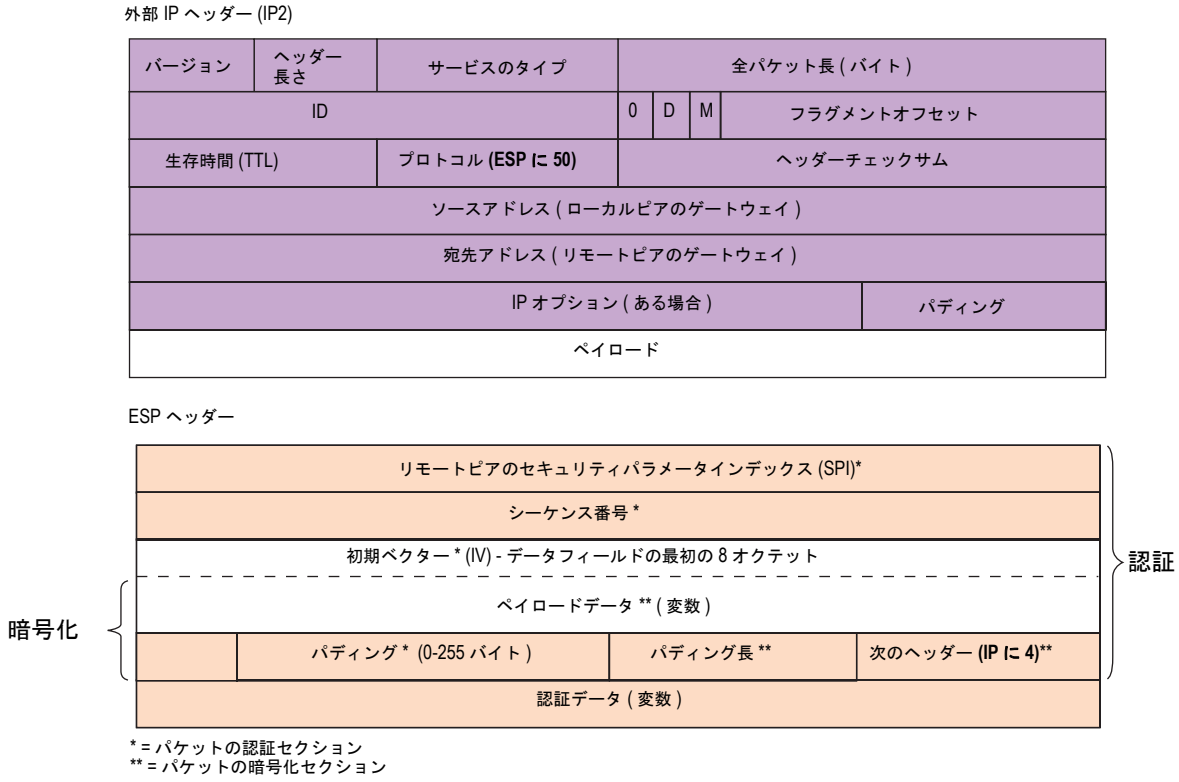


図 10 のように、開始側ホストが構築するパケットには、ペイロード、TCP ヘッダー、内部 IP ヘッダー (IP1) が含まれています。

セキュリティデバイスが追加する外部 IP ヘッダー (IP2) には、宛先 IP アドレスとしてリモートゲートウェイの IP アドレスとソース IP アドレスとしてローカルのセキュリティデバイスの IP アドレスが含まれています。さらに、セキュリティデバイスは、外部 IP ヘッダーと内部 IP ヘッダーの間に ESP ヘッダーも追加します。ESP ヘッダーには、リモートピアがパケットを受信すると、それを適切に処理するための情報が含まれています。16 ページの図 11 に示されています。

図 11: 外部 IP ヘッダー (IP2) と ESP ヘッダー



次のヘッダーフィールドは、ペイロードフィールドのデータタイプを示します。トンネルモードでは、この値は 4 となり、IP-in-IP であることを示しています。ESP がトランスポートモードに適用されると、この値は、TCP に 6、または UDP に 17 など、トランスポートレイヤープロトコルを示します。

図 12: 内部 IP ヘッダー (IP1) と TCP ヘッダー

内部 IP ヘッダー (IP1)

バージョン	ヘッダー長さ	サービスのタイプ	全パケット長 (バイト)					
ID			0	D	M	フラグメントオフセット		
生存時間 (TTL)		プロトコル (TCP に 6)	ヘッダーチェックサム					
ソースアドレス (開始側ホスト)								
宛先アドレス (受信側ホスト)								
IP オプション (ある場合)								パディング
ペイロード								

TCP ヘッダー

ソースポート								宛先ポート
シーケンス番号								
肯定応答番号								
ヘッダー長さ	予約済み	URG	ACK	PSH	RST	SYN	FIN	ウィンドウサイズ
チェックサム								緊急ポインタ
オプション (ある場合)								パディング
データ								

第 2 章

公開鍵暗号化

本章では、公開鍵暗号化と、PKI (公開鍵基盤) を背景とした認証と CRL (証明書取り消しリスト) の使用について紹介しています。本章の内容は、以下のようになります。

- 20 ページの「公開鍵暗号化序論」
  - 20 ページの「証明書を署名する」
  - 20 ページの「デジタル署名を確認する」
- 22 ページの「公開鍵基盤」
- 24 ページの「証明書および CRL」
  - 28 ページの「証明書と CRL をロードする」
  - 29 ページの「CRL 設定を構成する」
  - 30 ページの「ローカル証明を自動で取得する」
  - 33 ページの「証明書の自動更新」
- 34 ページの「OCSP (オンライン証明書ステータスプロトコル)」
  - 33 ページの「鍵ペアの生成」
  - 35 ページの「証明書取り消しチェック方法を指定する」
  - 35 ページの「オンライン証明書ステータスプロトコルレスポンダ URL を指定する」
- 36 ページの「自己署名証明書」
  - 35 ページの「ステータスチェック属性を削除する」
  - 38 ページの「自己署名証明書の手動作成」
  - 39 ページの「管理者定義の自己署名証明書を設定する」
  - 43 ページの「自己署名証明書の削除」

公開鍵暗号化序論

公開鍵暗号化では、公開鍵 / 秘密鍵ペアを使用してデータの暗号化と復号を行います。データ所有者が一般に公開するため、公開鍵により暗号化したデータは、機密保持、保護のため設定された対応秘密鍵によってのみ復号できます。たとえば Alice が Bob に暗号化したメッセージを送信したい場合、Alice は Bob の公開鍵でメッセージを暗号化して送信することができます。そしてメッセージを受け取った Bob は秘密鍵でメッセージを復号できことになります。

この逆、つまりデータを秘密鍵で暗号化し、対応する公開鍵で復号することもできます。これはデジタル署名の作成として知られています。たとえば Alice は自分がメッセージの送信者であることを表示したい場合、自分の秘密鍵でメッセージを暗号化して Bob に送信します。Bob は Alice の公開鍵でメッセージを復号し、このようにして Alice が本当に送信者であることを確認します。

公開鍵 / 秘密鍵ペアは、デジタル証明書を使用する際にも重要な役割を果たします。証明書を (CA が) 署名して、署名を (受信者が) 確認する手順は、次のように行われます。

証明書を署名する

1. 証明書を発行する CA (認証局) は、ハッシュアルゴリズム (MD5 か SHA-1) を使用して証明書をハッシュ処理し、ダイジェストを作成します。

2. 次に認証局はダイジェストを自分の秘密鍵で暗号化することで証明書を「署名」します。こうして作成されるのがデジタル署名です。

3. CA は今度はデジタル署名された証明書を、それを要求する者に送ります。

デジタル署名を確認する

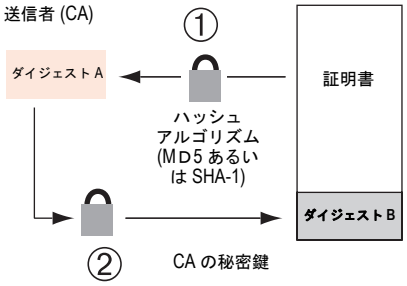
1. 受取側は証明書を受け取ると、同じハッシュアルゴリズム (MD5 か SHA-1) を証明書ファイルに適用して新たなダイジェストを作成します。

2. 受取側は CA の公開鍵を使用してデジタル署名を復号します。

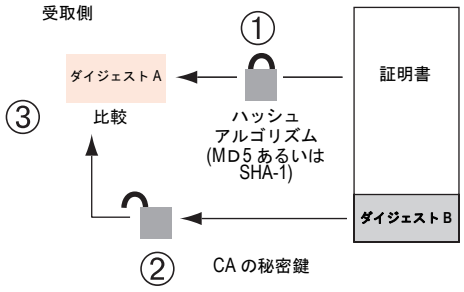
3. 受取側は、復号したダイジェストと作成したダイジェストとを比較します。2 つのダイジェストが一致すれば受取側は CA 署名の保全性を確認でき、ひいては付随する証明書の保全性を確認できることになります。

図 13: デジタル署名の確認

1. MD5 と SHA-1 のどちらかのハッシュアルゴリズムを使用して、CA は証明書からダイジェスト A を作成します。
2. CA は、自分の秘密鍵を使用して、ダイジェスト A を暗号化します。それがダイジェスト B、つまりデジタル署名です。
3. CA はデジタル署名された証明書を、それを要求する者へ送ります。



1. 受取側は、MD5 と SHA-1 のいずれかを使用して証明書からダイジェスト A を作成します。
2. 2. 次に CA の公開鍵を使用してダイジェスト B を復号します。
3. 受取側はダイジェスト A とダイジェスト B を比較し、両方が一致すれば証明書は不正変更されていないことがわかります。



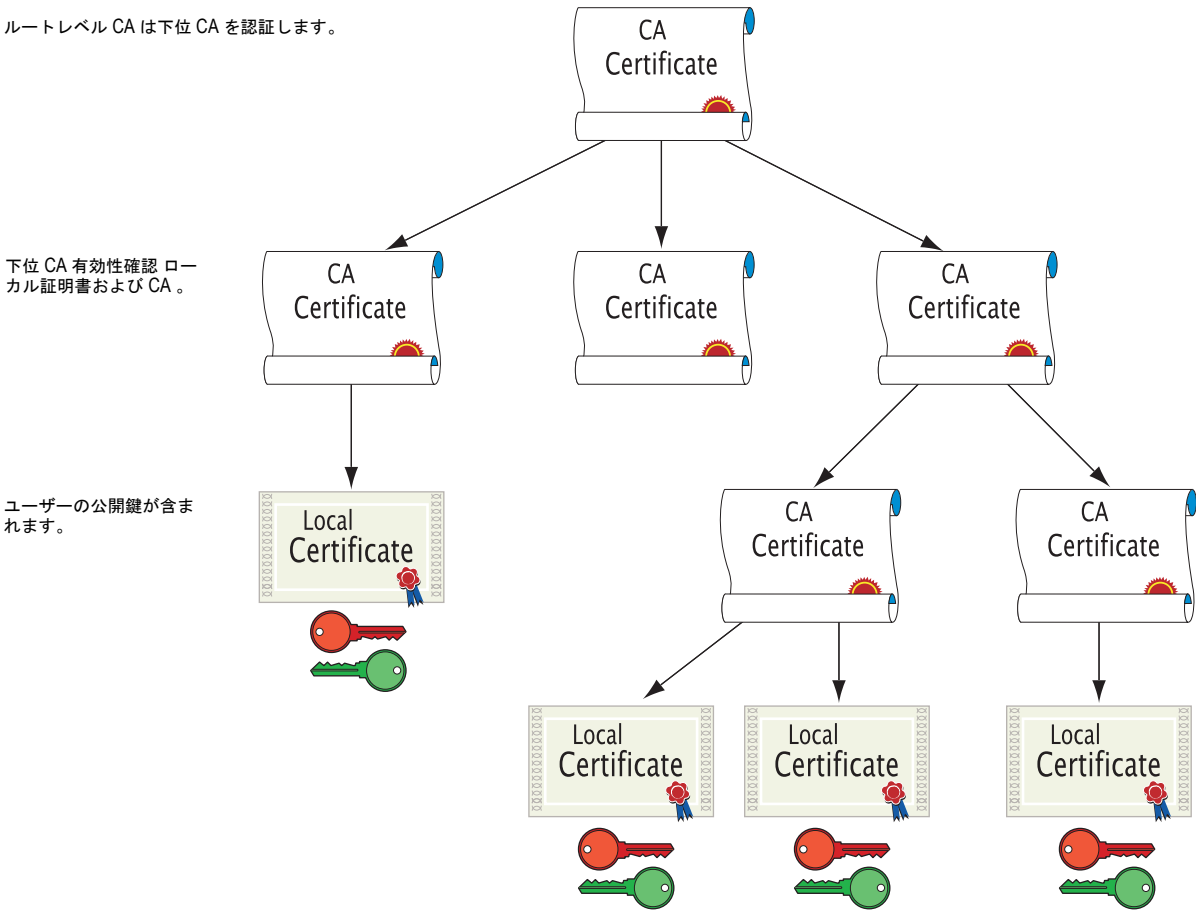
IKE セッションの参加者 2 人の間で送信されるメッセージをデジタル署名する手順もまったく同じように行われますが、次のような相違点があります。

- 送信者は CA 証明書からではなく IP パケットペイロードのデータからダイジェストを作成します。
- 一方受取側は CA ではなく送信者の公開鍵 / 秘密鍵ペアを使用します。

公開鍵基盤

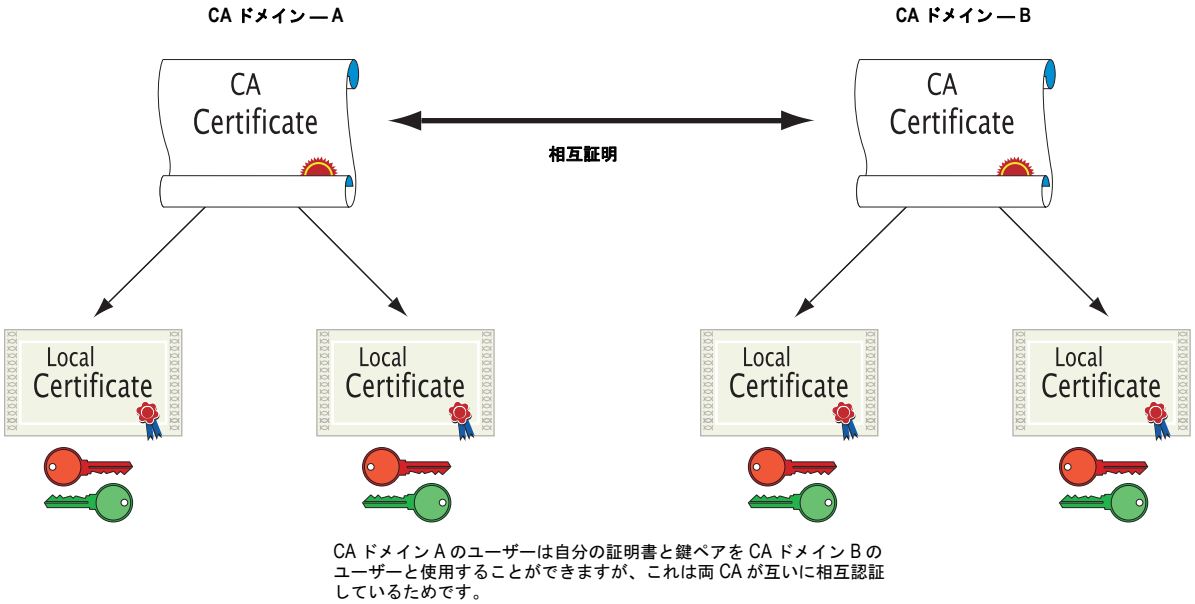
PKI (公開鍵基盤) という用語は、公開鍵暗号化の有効実施に必要なトラスト階層構造を意味しています。証明書の信頼性を確認するためには、ローカル証明書を発行から CA ドメインルート権限までさかのぼってその CA 証明パスを探知できなければなりません。

図 14: CA ドメインの PKI トラスト階層



証明書をある組織内のみで使用する場合、この組織は専用の CA ドメインを取得し、被雇用者間で本社認証を発行、有効性確認を実施することが可能です。また同組織がその後、他 CA ドメイン (他組織の被雇用者を所有する専用の CA ドメイン等) と証明交換実施を希望する場合、2 つの CA は相互証明を実施することができます。つまり相互に相手組織を信頼することに同意できるのです。この場合、PKI 構造は垂直方向ではなく、水平方向に拡大することになります。

図 15: 相互証明



PKI は、便利で実用的にするために、管理と実装を透過的にする必要があります。このため ScreenOS には、次の機能があります。

1. 証明書要求を作成すると、公開鍵 / 秘密鍵ペアを作成します。
2. この公開鍵を証明書要求の一部として送信用のテキスト PKCS10 ファイルの形で、CA (認証局) へ証明書登録のために供給します。
3. ローカル証明、CA 証明書、証明書の取り消しリスト (サブインターフェース CRL) をユニットへロード可能

注 : 認証局が通常は CRL を提供します。ユーザーは CRL をセキュリティデバイスへロードできますが、一度ロードすると見ることはできません。

CRL をオンラインで更新する間隔を指定することもできます。CRL (証明書の取り消しリスト) の詳細は、24 ページの「証明書および CRL」を参照してください。

4. IP セキュリティトンネルの確立時に、証明書を配布します。
5. PKI 階層内の CA 権限の 8 つのレベルを上に向かった証明書パス検証をサポートします。
6. PKCS #7 暗号化標準をサポートし、セキュリティデバイスは PKCS #7 封筒内にパッケージされた X.509 証明書と CRL を受け入れることができます。PKCS #7 に対応することで、1 つの PKI 要求内に複数の X.509 証明書を発行できます。これで CA が発行した全証明書の有効性を一度に確認できる PKI を構成することができます。

注 : ScreenOS は 7 キロバイトまでの PKCS #7 ファイルに対応しています。

7. LDAP または HTTP でのオンライン CRL 検索をサポートします。

証明書および CRL

デジタル証明書は、トラステッドサードパーティの言語を通じてユーザー識別、確認をする電子的手段で、いわゆる CA (認証局) として知られています。CA サーバーは独立した CA が所有して運営することも、あなたの組織が所有して運営することもでき、後者の場合はあなたが自分専用の CA になります。独立した CA を使用する場合は、その CA に CA と CRL サーバーのアドレス (証明書と証明書取り消しリストを取得するため) と、個人証明書要求の発行時に必要な情報を求める必要があります。あなたが自分の CA になる場合、これらの情報を自分で決定することになります。

注 : ScreenOS は以下の CA に対応しています。Baltimore、Entrust、Microsoft、Netscape、RSA Keon および Verisign。

ScreenOS には、AV (アンチウィルス) パターンファイルサーバーおよび DI (徹底監視) 攻撃オブジェクトデータベースサーバーからのダウンロードを認証するための CA 証明書が含まれています。AV パターンファイルサーバーの詳細は、**4**-62 ページの「ウィルス対策スキャン」を参照してください。DI 攻撃オブジェクトデータベースサーバーの詳細は、**4**-122 ページの「攻撃オブジェクトデータベースサーバー」を参照してください。

セキュア VPN 接続の確立時にデジタル証明書を使用して自分の身元を認証するには、最初に以下を実行します。

- セキュリティデバイスに鍵を作成し、CA へ送信して個人証明書 (*ローカル*証明書とも呼びます) をもらい、その証明書をセキュリティデバイスにロードします。
- 個人証明書を発行した CA の CA 証明書を取得し (基本的に、あなたを検証する CA の身元を検証して)、その CA 証明書をセキュリティデバイスにロードします。この作業は手動あるいは SCEP (簡易認証送受信プロトコル) を使用して自動で行うことができます。
- 証明書に CDP (証明書分布点) 拡張機能が含まれていない場合は、CRL を LDAP や HTTP で自動取得できません。CRL を手動で取り出してセキュリティデバイスにロードできます。

ビジネスの過程では、認証を無効にしなければならない場面が数度あることでしょう。認証の信頼性が失われる、証明書の所有者が会社を辞めた場合に認証を無効にしたいという場面がでてくるかもしれません。認証の取り消しおよび有効性の管理は、ローカル管理 (ソリューションが限定される)、1 日、1 ヶ月、1 年間隔でオンライン自動アクセスが可能な CA の CRL を参照、または CA 設定間隔のデフォルト値を使用することができます。

署名済みのデジタル証明書を手動方式で取得するには、次の手順を実行してください。

1. 公開鍵 / 秘密鍵のペアを作成します。
2. 認証要求に記入します。
3. 要求を自分の選んだ CA へ提出します。

4. 署名された証明書を受け取ったら、それをセキュリティデバイスへ CA 証明書と一緒にロードしてください。

これにより、次のアイテムがそろいます。

- セキュリティデバイス用のローカル証明は、各トンネル接続で自分の身元を認証するために使用します。
- CA 証明書 (公開鍵) は、ピアの証明書の検証に使用します。
- CRL (証明書の取り消しリスト) が CA 証明書に含まれていた場合は、CRL で無効証明書を識別します。

注 : CRL は認証局証明書と共に ScreenOS データベースに保存されている場合があります。また CA 証明書が CRL URL(LDAP または HTTP) を含んでおり、CA データベースに保存されている場合もあります。どちらの方法でも CRL が入手できない場合は、手動でセキュリティデバイスにて CRL URL を入力できます。その手順については 29 ページの「CRL 設定を構成する」を参照してください。

これらのファイル (証明書ファイルには通常 .cer 拡張子が付いており、CRL には通常 .crl 拡張子が付いています) を受け取ったら、25 ページの「証明書を手動で要求する」で説明する手順でセキュリティデバイスにロードします。

注 : E メールを使用して PKCS10 ファイルを発行して自分の証明書を取得しようとするのであれば、E メールをシステム管理者に送信できるように ScreenOS 設定を正しく構成する必要があります。プライマリおよびセカンダリの DNS サーバーを設定し、SMTP サーバーと E メールアドレス設定を指定する必要があります。

証明書を手動で要求する

証明書が要求されると、セキュリティデバイスは鍵ペアを作成します。公開鍵は要求書に組み込まれ、最後には CA から受け取るデジタル署名されたローカル証明書に組み込まれます。

次の例では、セキュリティ管理者がカリフォルニア州、サニーベール市にある Juniper Networks 社開発部の Michael Zhang 氏に対して認証要求を作成しています。この証明書は、IP アドレス 10.10.5.44 のセキュリティデバイスで使用される予定です。管理者はセキュリティデバイスに、その要求を E メールで *admin@juniper.net.* のセキュリティ管理者に送信するように指示します。するとセキュリティ管理者は、要求をコピーして CA の証明書登録サイトの証明書要求テキストフィールドに貼り付けます。登録プロセスが完了すると、CA は証明書を通常は E メールでセキュリティ管理者に返送します。

注： *domain-component* と呼ばれる特別証明書識別文字列は、CLI を使用した場合にのみ利用できます。デバイスは、VPN ゲートウェイに IPSec ログオンするための証明書にこの値を使用できます。たとえば、デバイスはこの値を グループ IKE ID として使用し、「DC = Engineering, DC = NewYork」を含んだ ASN1_DN タイプ IKE を受け入れます。

証明書要求を作成する前に、システムクロックを設定し、ホスト名とドメイン名をセキュリティデバイスに割り当てしたことを確認してください (セキュリティデバイスが NSRP クラスタの中にある場合、ホスト名をクラスタ名に置き換えてください。詳細については、**11**-28 ページの「NSRP クラスタの作成」を参照してください。

WebUI

1. **証明書の生成**
   Objects > Certificates > New: 次のように入力してから **Generate** をクリックします。

   Name: Michael Zhang
   Phone: 408-730-6000
   Unit/Department: Development
   Organization: Juniper Networks
   County/Locality: Sunnyvale
   State: CA
   Country: US
   E-mail: mzhang@juniper.net
   IP Address: 10.10.5.44
   Write to file: (**選択**)
   RSA: (**選択**)
   Create new key pair of *1024* length: (**選択**)

   セキュリティデバイスによって PKCS #10 ファイルが生成され、そのファイルを E メールでするか、ディスクに保存するか、SCEP (簡易認証送受信プロトコル) で自動登録するように求めるメッセージが表示されます。

   E-mail to オプションを選択し、**admin@juniper.net** と入力してから **OK** をクリックします。

注： CA の中には、証明書内の E メールアドレスに対応していないところもあります。E メールアドレスをローカル証明書要求に含めないと、セキュリティデバイスを動的ピアとして構成する際に E メール アドレスをローカル IKE ID として使用することができません。代わりに完全修飾ドメイン名を使用する (ローカル証明書に含まれていれば) か、ローカル ID フィールドを空欄にすることができます。デフォルトにより、セキュリティデバイスが*ホスト名*、*ドメイン名*を送信します。動的ピアのローカル ID を指定しない場合は、IP セキュリティトンネルの反対側のデバイスで peer ID フィールドに*ホスト名*、*ドメイン名*を入力します。

1024 の値は、鍵ペアのビット長を示しています。証明書を SSL に使用している場合は (**3**-5 ページの「セキュアソケットレイヤー」を参照)、かならずご使用の Web ブラウザもサポートするビット長を使用してください。

E メールアドレスを使用することで、SMTP サーバーの IP アドレスが構成されているものと見なされます。**set admin mail server-name** { *ip_addr* | *dom_name* }.

2. **証明書要求**
   セキュリティ管理者はそのファイルを開いて内容をコピーします。コピーする際は、テキスト前後の空白スペースは含めずにテキスト全体をコピーするように注意します。「-----BEGIN CERTIFICATE REQUEST-----」で始まり、「-----END CERTIFICATE REQUEST-----」で終わりになります。

   セキュリティ管理者は CA の Web サイトの証明書要求の指示に従い、要求されたら PKCS #10 ファイルを該当するフィールドにペーストします。

3. **証明書取得**
   セキュリティ管理者は CA から証明書を E メールで受け取ったら、あなたに転送してくれます。それをテキストファイルにコピーして、ワークステーションに保存するか (後で WebUI でセキュリティデバイスにロードする場合)、TFTP サーバーに保存 (後で CLI でロードする場合) します。

CLI

1. **証明書の生成**

```
set pki x509 dn country-name US
set pki x509 dn email mzhang@juniper.net
set pki x509 dn ip 10.10.5.44
set pki x509 dn local-name “Santa Clara”
set pki x509 dn name “Michael Zhang”
set pki x509 dn org-name “Juniper Networks”
set pki x509 dn org-unit-name Development
set pki x509 phone 408-730-6000
set pki x509 dn state-name CA
set pki x509 default send-to admin@juniper.net
exec pki rsa new-key 1024
```

注 : E メールアドレスを使用することで、SMTP サーバーの IP アドレスが構成されているものと見なされます。**set admin mail server-name** { *ip_addr* | *dom_name* }。

   証明書要求は E メールで admin@juniper.net に送信されます。

2. **証明書要求**
   セキュリティ管理者はそのファイルを開いて内容をコピーします。コピーする際は、テキスト前後の空白スペースは含めずにテキスト全体をコピーするように注意します。「-----BEGIN CERTIFICATE REQUEST-----」で始まり、「-----END CERTIFICATE REQUEST-----」で終わりになります。

   セキュリティ管理者は CA の Web サイトの証明書要求の指示に従い、要求されたら PKCS #10 ファイルを該当するフィールドにペーストします。

3. **証明書取得**
   セキュリティ管理者は CA から証明書を E メールで受け取ったら、あなたに転送してくれます。それをテキストファイルにコピーして、ワークステーションに保存するか (後で WebUI でセキュリティデバイスにロードする場合)、TFTP サーバーに保存 (後で CLI でロードする場合) します。

証明書と CRL をロードする

CA は次の 3 つのファイルを、セキュリティデバイスにロードできるように返信してくれます。

- CA の公開鍵を含む CA 証明書
- あなたのローカルマシン (あなたの公開鍵) を識別するローカル証明書
- CA が取り消したあらゆる証明書がリストされた CRL

WebUI の例では、ファイルは管理者ワークステーションのディレクトリ名 C:\certs\ns にダウンロードされました。CLI の例では IP アドレス 198.168.1.5 の TFTP サーバーの TFTP ルートディレクトリにダウンロードされました。

注 : Juniper Networks セキュリティデバイスは、仮想システムを含め、ScreenOS 2.5 以降で構成されており、異なる CA のローカル証明の複数ロードに対応しています。

この例では、auth.cer (CA 証明書) および local.cer (公開鍵) という名の 2 つの証明書ファイルと、distrust.crl という名の CRL ファイルをロードする方法を説明します。

WebUI

1. Objects > Certificates: **Load Cert** を選択し、**Browse** をクリックします。
2. C:\certs ディレクトリへ進み、**auth.cer** を選択し、**Open** をクリックします。

   ディレクトリパスとファイル名 (C:\certs\ns\auth.cer) が File Browse フィールドに表示されます。
3. **Load** をクリックします。

   auth.cer 証明書ファイルがロードされます。
4. Objects > Certificates: **Load Cert** を選択し、**Browse** をクリックします。
5. C:\certs ディレクトリへ進み、**local.cer** を選択し、**Open** をクリックします。

   ディレクトリパスとファイル名 (C:\certs\ns\local.cer) が File Browse フィールドに表示されます。
6. **Load** をクリックします。

   local.cer 証明書ファイルがロードされます。
7. Objects > Certificates: **Load CRL** を選択し、**Browse** をクリックします。
8. C:\certs ディレクトリへ進み、**distrust.crl** を選択し、**Open** をクリックします。
9. **Load** をクリックします。

   distrust.crl の CRL ファイルがロードされます。

CLI

```
exec pki x509 tftp 198.168.1.5 cert-name auth.cer
exec pki x509 tftp 198.168.1.5 cert-name local.cer
exec pki x509 tftp 198.168.1.5 crl-name distrust.crl
```

CRL 設定を構成する

フェーズ 1 ネゴシエーションでは、参加者は CRL リストを参照し、IKE 交換中に受け取った認証が有効であるか確認します。CRL が ScreenOS データベースにもロードされていない場合、セキュリティデバイスは 証明書の中で定義された LDAP または HTTP CRL の位置で認証取り消しリスト検索をしようとします。証明書内に URL アドレスが定義されていない場合、セキュリティデバイスは CA 証明書のためユーザーが定義したサーバーの URL を使用することになります。デバイスに CA 証明書がロードされていない（たとえば、IKE 交換の間に受信した証明書チェーンの中間 CA）場合、その CA について CRL サーバーの URL は解決できません。この場合、WebUI の Default Cert Validation Settings セクションで CRL サーバーの URL を指定できます（次のページを参照）。ここで入力した CRL サーバー URL は、CA 証明書がデバイスに存在しない場合だけ使用されます。事前に定義されたデフォルトの URL はありません。

注 : X509 証明書内の CRL 分布点拡張子 (.cdp) は、HTTP URL か LDAP URL のどちらかです。

ScreenOS 2.5 以降では、CRL のロード時の CRL デジタル署名のチェックを使用不可にできます。ただし CRL 証明書チェックを不可にすることにより、デバイスのセキュリティ機能が損なわれます。

この例では、最初に Entrust CA サーバーが CRL を毎日チェックするために LDAP サーバー 2.2.2.121 に接続して CRL ファイルを探すよう構成します。次に、デフォルトの証明書検証設定で会社の LDAP サーバー 10.1.1.200 を使用して、毎日 CRL がチェックされるように構成します。

注 : Entrust CA 証明書の IDX (インデックス) 番号は 1 です。セキュリティデバイスにロードされたすべての CA 証明書の IDX 番号のリストを表示するには、CLI コマンド **get pki x509 list ca-cert** を実行します。

WebUI

Objects > Certificates (Show: CA) > Server Settings (NetScreen): 以下を入力して、**OK** をクリックします。

```
X509 Cert_Path Validation Level: Full
CRL Settings:
    URL Address: dap:///CN=Entrust,CN=en2001,CN=PublicKeyServices,
  CN=Services,CN=Configuration,DC=EN2001,DC=com?CertificateRevocati
  onList?base?objectclass=CRLDistributionPoint
    LDAP Server: 2.2.2.121
    Refresh Frequency: Daily
```

Objects > Certificates > Default Cert Validation Settings: 次のように入力してから **OK** をクリックします。

```
X509 Certificate Path Validation Level: Full
Certificate Revocation Settings:
    Check Method: CRL
    URL Address:
  ldap:///CN=NetScreen,CN=safecert,CN=PublicKeyServices,
  CN=Services,CN=Configuration,DC=SAFECERT,DC=com?CertificateRevoc
  ationList?base?objectclass=CRLDistributionPoint
    LDAP Server: 10.1.1.200
```

CLI

```
set pki authority 1 cert-path full
set pki authority 1 cert-status crl url “ldap:///CN=Entrust,CN=en2001,
    CN=PublicKeyServices,CN=Services,CN=Configuration,DC=EN2000,DC=com?
    CertificateRevocationList?base?objectclass=CRLDistributionPoint”
set pki authority 1 cert-status crl server-name 2.2.2.121
set pki authority 1 cert-status crl refresh daily
set pki authority default cert-path full
set pki authority default cert-status crl url “ldap:///CN=NetScreen,
    CN=safecert,CN=PublicKeyServices,CN=Services,CN=Configuration,DC=SAFE
    CERT,
    DC=com?CertificateRevocationList?base?objectclass=CRLDistributionPoint”
set pki authority default cert-status crl server-name 10.1.1.200
set pki authority default cert-status crl refresh daily
save
```

ローカル証明を自動で取得する

セキュア VPN 接続の確立時にデジタル証明書を使用して自分の身元を認証するには、最初に以下を実行します。

- 個人証明書を受け取ろうとする CA (認証局) の証明書を取得して、セキュリティデバイスにロードします。
- すでにロードした CA 証明書をもらった CA からローカル証明 （個人証明書とも呼びます) を取得し、このローカル証明をセキュリティデバイスにロードします。上記作業は手動あるいは、SCEP (簡易認証送受信プロトコル) を利用して自動で実行することができます。

ローカル証明を手動で要求する方法は、証明書から別の証明書へ情報をコピーしなければならないため、時間のかかる作業となります。このような手順を回避するため、自動の方法を使うことができます。

SCEP を使用する前に、以下を行ってください。

- DNS を構成して使用可能にします。(**2**-219 ページの「ドメイン名システムサポート」を参照してください。)
- システムクロックを設定します。(**2**-257 ページの「システムクロック」を参照してください。)
- ホスト名とドメイン名をセキュリティデバイスに割り当てます。(セキュリティデバイスが NSRP クラスタの中にある場合、ホスト名をクラスタ名に置き換えてください。詳細については、**11**-28 ページの「NSRP クラスタの作成」を参照してください。

この例では、ローカル証明を要求する自動の方法を使用します。Verisign CA に対して SCEP を使用します。次の CA 設定を行ってください。

- 全証明書パス有効化
- RA CGI: http://ipsec.verisign.com/cgi-bin/pkiclient.exe

注 : CGI (共通ゲートウェイインターフェース) は、Web サーバーがユーザー要求をアプリケーションプログラムに渡し、戻ってきたデータを受け取る標準的な方法です。CGI は HTTP (ハイパーテキスト転送プロトコル) の一部です。RA が存在しない場合にも RA CGI パスを指定してください。RA が存在しない場合は、CA CGI に指定された値を使用します。

- CA CGI: http://ipsec.verisign.com/cgi-bin/pkiclient.exe
- CA 証明書の自動保全性確認
- SCEP サーバーを識別する CA ID (Verisign SCEP サーバーが juniper.net といったドメイン名や Verisign があなたの会社に設定したドメインを使用する場合)
- パスワード パスワード
- 30 分毎の自動の証明書ポーリング (デフォルトではポーリングなし)

RSA 鍵ペアを作成し、鍵長さを 1024 ビットに指定して SCEP オペレーションを開始し、上記の CA 設定で Verisign CA からローカル証明を要求します。

WebUI を使用するときは、CA 証明書を名前で照会します。CLI を使用するときは CA 証明書を IDX (インデックス) 番号で照会します。この例では、Verisign CA の IDX 番号は「1」です。CA 証明書の IDX 番号を確認するには、**get pki x509 list ca-cert** コマンドを使用します。各証明書の IDX 番号、ID 番号が画面に表示されます。IDX 番号を書きとめておき、CA 証明書参照時にコマンド内で使用します。

WebUI

1. **CA サーバー設定**
   Objects > Certificates > Show CA > Server Settings (Verisign の場合): 次のように入力してから **OK** をクリックします。

   X509 certificate path validation level: Full
   SCEP Settings:
   RA CGI: http://ipsec.verisign.com/cgi-bin/pkiclient.exe
   CA CGI: http://ipsec.verisign.com/cgi-bin/pkiclient.exe

   > Advanced: 以下の詳細設定を入力してから、**Return** をクリックして、CA Server Settings 構成ページに戻ります。

   Polling Interval: 30
   Certificate Authentication: Auto
   Certificate Renew: 14

2. **ローカル証明要求**
   Objects > Certificates > New: 次のように入力してから **Generate** をクリックします。

   Name: Michael Zhang
   Phone: 408-730-6000
   Unit/Department: Development
   Organization: Juniper Networks
   County/Locality: Sunnyvale

State: CA
Country: US
Email: mzhang@juniper.net
IP Address: 10.10.5.44
Key Pair Information
RSA: (**選択**)
Create new key pair of **1024** length.

注 : 1024 の値は、鍵ペアのビット長を示しています。証明書を SSL (セキュアソケットレイヤー) に使用している場合は、かならずご使用の Web ブラウザもサポートするビット長を使用してください。

---

get pki x509 pkcs CLI コマンドを発行してセキュリティデバイスに PKCS #10 ファイルを生成させてから、次のいずれかを行います。

- PKCS #10 証明書要求ファイルを E メールアドレスへ送信
- ディスクへ保存
- ファイルを SCEP (簡易認証送受信プロトコル)対応認証局へ送信することにより自動登録

3. 自動登録

Automatically enroll to オプションを選択して **Existing CA server settings** オプションを選択し、ドロップダウンリストで **Verisign** を選択します。

Verisign に連絡をとり、証明書の要求を伝えてください。証明書をダウンロードできるようになる前に、Verisign は証明書要求を認定する必要があります。

CLI

1. CA サーバー設定

```
set pki authority 1 cert-path full
set pki authority 1 scep ca-cgi “http://ipsec.verisign.com/cgi-bin
    /pkiclient.exe”
set pki authority 1 scep ra-cgi “http://ipsec.verisign.com/cgi-bin
    /pkiclient.exe”
set pki authority 1 scep polling-int 30
set pki authority 1 scep renew-start 14
```

注 : CGI (共通ゲートウェイインターフェース) は、Web サーバーがユーザー要求をアプリケーションプログラムに渡し、戻ってきたデータを受け取る標準的な方法です。CGI は HTTP (ハイパーテキスト転送プロトコル) の一部です。

RA が存在しない場合にも RA CGI パスを指定してください。RA が存在しない場合は、CA CGI に指定された値を使用します。

---

2. ローカル証明要求

```
set pki x509 dn country-name US
set pki x509 dn email mzhang@juniper.net
set pki x509 dn ip 10.10.5.44
set pki x509 dn local-name “Santa Clara”
set pki x509 dn name “Michael Zhang”
set pki x509 dn org-name “Juniper Networks”
```

```
set pki x509 dn org-unit-name Development
set pki x509 phone 408-730-6000
set pki x509 dn state-name CA
exec pki rsa new 1024
```

3. **自動登録**

```
exec pki x509 scep 1
```

CA に対する証明書要求が初回である場合、CA 証明書の指紋値を示すプロンプトが現れます。CA に連絡をとり、これが正しい CA 証明書であることを確認してください。

Verisign に連絡をとり、証明書の要求を伝えてください。証明書をダウンロードできるようになる前に、Verisign は証明書要求を認定する必要があります。

証明書の自動更新

セキュリティデバイスが取得した証明書を SCEP (簡易認証送受信プロトコル) を使って自動的に更新できるようにすることも可能です。この機能によってセキュリティデバイスの証明書を期限切れになる前に更新することを覚えておかなくても済むようになり、しかも有効な証明書を常時管理する上でも役に立ちます。

この機能は、デフォルトでは使用不可に設定されています。セキュリティデバイスが、証明書を期限切れになる前に更新する要求を自動的に送信するように構成することができます。セキュリティデバイスに証明書更新要求を送信させる時期を、有効期限までの日数と分で設定できます。証明書ごとに異なる時間を設定することで、セキュリティデバイスがすべての証明書を一度に更新しなくても済むようにできます。

この機能が働くためには、セキュリティデバイスが SCEP サーバーにアクセスできなければならず、また更新処理中に証明書がセキュリティデバイスに存在しなければなりません。さらに、この機能が働くために、証明書を発行する CA は以下が可能なことを確認してください。

- 証明書要求の自動承認に対応している。
- 同じ DN (ドメイン名) を返すことができる。言い換えると、CA は新しい証明書中のサブジェクト名と SubjectAltName 拡張子を変更できません。

自動 SCEP 証明書更新機能を、すべての SCEP 証明書に対して、または証明書毎に使用可能または使用不可にできます。

鍵ペアの生成

セキュリティデバイスは、あらかじめ生成された鍵をメモリーに保存しています。事前生成鍵の数は、デバイスモデルによって異なります。通常の動作時、セキュリティデバイスは証明書の更新に十分な数の鍵を確保するために、鍵を使用するたびに新しい鍵を生成します。通常、デバイスには新しい鍵を必要とする前にそれを生成する時間があるため、鍵を生成するプロセスによって目立った影響が現れることはありません。セキュリティデバイスが大量の証明書を一度に更新し、そのため鍵を高速度で使用するような場合は、事前生成の鍵が足りなくなり、新規の要求ごとに迅速に生成しなければなりません。この場合、鍵の生成がセキュリティデバイスのパフォーマンスに影響を及ぼすことがあり、特に高可用性 (HA) 環境ではセキュリティデバイスのパフォーマンスが数分間低下します。

セキュリティデバイスの事前生成の鍵ペア数は、モデルによって異なります。詳細については、Juniper Networks セキュリティ製品の仕様書を参照してください。

OCSP (オンライン証明書ステータスプロトコル)

セキュリティデバイスが証明書を使用する作業を行うとき、通常はその証明書の有効性を確認することが重要です。証明書は、期限切れや取り消しにより無効になっている場合があります。証明書のステータスをチェックするデフォルトの方法は、証明書の取り消しリスト (CRL) を使用することです。OCSP (オンライン証明書ステータスプロトコル) は、証明書のステータスをチェックするもう 1 つの方法です。OCSP によって、証明書に関する詳細情報を得ることができ、ステータスチェックをさらにタイムリーな方法で行えます。

セキュリティデバイスは OCSP を使用しているとき、*OCSP クライアント* (または *要求者*) と呼ばれます。このクライアントは検証要求を *OCSP レスポンダ (受信側)* と呼ぶサーバーデバイスに送信します。ScreenOS は、OCSP レスポンダとして RSA Keon と Verisign をサポートしています。クライアントの要求には、チェックする証明書の識別情報が含まれます。セキュリティデバイスが OCSP 処理を開始する前に、このデバイスが OCSP レスポンダの位置を認識するように構成しておいてください。

注 : これまでの広範な評価の中で Valicert OCSP レスポンダでのテストにも成功しています。

OCSP レスポンダは要求受領後、証明書の状況情報が入手可能であるかを確認して、セキュリティデバイスに現在の状況を返します。OCSP レスポンダの応答は、証明書の取消し状況、受信側の名前、そして応答の有効性間隔からなります。応答がエラーメッセージでない限り、受信側は受信側の秘密鍵を使用して応答に署名をします。セキュリティデバイスは受信側の署名の有効性を検証するために、この受信側の証明書を使用します。受信側の証明書は、OCSP 応答に埋め込まれているか、ローカル保存されて OCSP 構成内に指定されています。証明書がローカル保存されている場合は、次のコマンドを使用してローカル保存された証明書を指定してください。

set pki authority *id_num1* **cert-status ocsp cert-verify id** *id_num2*

id_num1 は検証している証明書を発行した CA 証明書を識別し、*id_num2* はローカル保存された証明書を識別し、NetScreen デバイスはこのローカル保存の証明書を使用して OCSP 応答の署名を検証します。

受信側の証明書が OCSP 応答に埋め込まれていなかったりローカル保存されていない場合、セキュリティデバイスは当該の証明書を発行した CA 証明書を使って署名を確認します。

CLI コマンドを使用して OCSP にセキュリティデバイスを構成することができます。CLI コマンドのほとんどは、ID 番号を使用して取り消し参照 URL を CA 証明書と関連付けます。この ID 番号を求めるには、次の CLI コマンドを使用します。

get pki x509 list ca-cert

注 : CA 証明書をリスト表示するとき、セキュリティデバイスは CA 証明書に ID 番号を動的に割り当てます。この番号は、保管した証明書に変更を加えると変わります。

証明書取り消しチェック方法を指定する

取り消しチェック方法 (CRL 、OCSP 、またはなし) をある特定の CA の証明書に指定するには、次の CLI 構文を使用します。

set pki authority *id_num* **cert-status revocation-check { CRL | OCSP | none }**

id_num は、この証明書の ID 番号です。

次の例では OCSP 取り消しチェックを指定しています。

set pki authority 3 cert-status revocation-check ocsp

ID 番号 3 は、CA の証明書を識別します。

ステータスチェック属性を表示する

ある特定の CA のステータスチェック属性を表示するには、次の CLI 構文を使用します。

get pki authority *id_num* **cert-status**

id_num は、CA が発行した証明書の ID 番号です。

証明書 7 を発行した CA のステータスチェック属性を表示するには :

get pki authority 7 cert-status

オンライン証明書ステータスプロトコルレスポンダ URL を指定する

ある特定の証明書の OCSP レスポンダの URL 文字列を指定するには、次の CLI 構文を使用します。

set pki authority *id_num* **cert-status ocsp url** *url_str*

インデックス 5 の証明書を持つ CA の OCSP レスポンダ (http:\\192.168.10.10) の URL 文字列を指定するには、次の CLI 構文を使用します。

set pki authority 5 cert-status ocsp url http:\\192.168.10.10

証明書 5 の CRL サーバーの URL (http:\\192.168.2.1) を削除するには :

unset pki authority 5 cert-status ocsp url http:\\192.168.2.1

ステータスチェック属性を削除する

ある特定の証明書を発行した CA のすべての証明書ステータスチェック属性を削除するには、次の構文を使用します。

unset pki authority *id_num* **cert-status**

証明書 1 に関連するすべての取り消し属性を削除するには :

unset pki authority 1 cert-status

自己署名証明書

自己署名証明書は、同一エントリによって署名され、発行される証明書、つまり、証明書の発行人とサブジェクトが同じ証明書のことです。例えば、CA (認証局) は、すべてのルート CA を自己署名と認証しています。

セキュリティデバイスは、起動時に自己署名を自動生成しますが、これは SSL (セキュアソケットレイヤー) 用にあらかじめ設定された証明書がない場合、つまり初めて起動したときに行われます。自動生成された自己署名証明書を作成するセキュリティデバイスだけが、その証明書を使用します。この証明書は、デバイスからエクスポートされることはありません。セキュリティデバイスが NSRP (NetScreen Redundancy Protocol) クラスタにあっても、クラスタ内の他のメンバの PKI オブジェクトを同期する場合は、他の種類の証明書に自動生成された自己署名証明書は含まれません (NSRP メンバは、手動で生成された自己署名証明書を交換します。自己署名証明書の手動生成については、38 ページの「自己署名証明書の手動作成」を参照してください)。

自動生成された自己署名証明書はエクスポートできませんが、そのサブジェクト名と指紋はコピーすることができます。これは、リモート管理者に配信され、そこで後からサブジェクト名と指紋を使って、SSL のネゴシエーション中に受信した自己署名証明書を確認できます。サブジェクト名と指紋の確認は、中間一致攻撃に備えるための大切な予防措置です。この攻撃は、第三者が SSL 接続試行を傍受し、自分の自己署名証明書に応答することによって、標的となるセキュリティデバイスになりすますものです (自己署名証明書の確認については、37 ページの「証明書の検証」を参照してください)。

セキュリティデバイスに SSL (セキュアソケットレイヤー) 接続する場合、自己署名証明書を使用することができます。WebUI からデバイスを管理する場合、SSL を利用すれば、認証と暗号化を行うことにより管理トラフィックを保護できます。また、セキュリティデバイスの設定によって、管理接続試行を HTTP 利用 (デフォルトポート番号 80) から SSL 利用 (デフォルトポート番号 443) に転送することもできます。

注 : HTTP から SSL への転送機構を含む SSL の詳細については、3-5 ページの「セキュアソケットレイヤー」を参照してください。

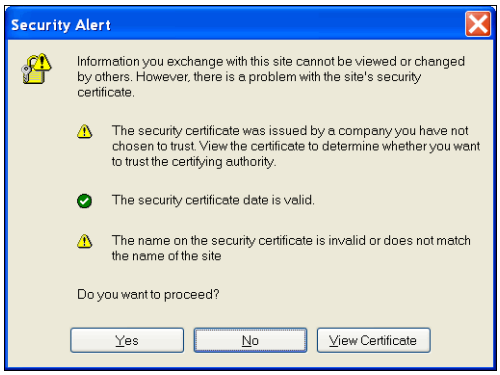
デフォルトでは、セキュリティデバイスは、SSL ネゴシエーションで使用するために、自動生成された自己署名証明書を利用しています。これは、デフォルトの SSL 証明書です。後から CA 署名証明書をインストールしたり、別の自己署名証明書を生成するよう設定する場合は、その他の SSL 用証明書の 1 つを利用します。自動生成された自己署名証明書を削除しても、別の SSL 用証明書に割り当てない場合は、デバイスの次回再起動時に別の自己署名証明書が自動生成されます。

注 : 別の自己署名証明書の作成方法については、38 ページの「自己署名証明書の手動作成」を参照してください。自動生成された自己署名証明書の削除方法については、43 ページの「自己署名証明書の削除」を参照してください。

証明書の検証

SSL のハンドシェイク中は、SSL クライアントに証明書を送信することによって、セキュリティデバイス自身を認証します。セキュリティデバイスが自己署名証明書を送信すると、CA が発行しなかったため、SSL クライアントは CA の署名のチェックで検証することはできません。そのような場合でも、セキュリティデバイス が SSL セッションの確立に使用する自己署名証明書を示すと、管理者のコンピュータ上のウェブブラウザは CA 保管庫にある CA 証明書で検証しようとします。そうした権限が見つからない場合は、図 16 のようなメッセージがブラウザ上に表示され、提供された証明書を許可するか拒否するかを管理者に問い合わせます。

図 16: 自己署名証明書のセキュリティ警報



初回起動後、初めてセキュリティデバイスに接続すると、システムクロックが正しくない場合があります。その結果、証明書の有効期間も間違っているおそれがあります。システムクロックを設定して、自己署名証明書を再生成しても、ウェブブラウザは認証 CA を見つけることができません。そのため、セキュリティデバイスが SSL 接続の自己署名証明書を使用するたびに、上記のメッセージを管理者に示さなければならないのです。

公平なサードパーティ CA の証明書検証を行わないと、SSL にログインする管理者は、受信した自己署名証明書が確かに接続しようとしているセキュリティデバイスからのものかどうかは分かりません (結局、証明書は、中間一致攻撃でセキュリティデバイスに見せかけようとしている侵入者の可能性があるのです)。管理者は、自己署名証明書のサブジェクト名と指紋から、受信した証明書を検証できます。サブジェクト名と指紋を管理者に発信すれば、セキュリティデバイスが後から証明書を発行するときに、管理者は自己署名証明書を検証できるのです。

自動生成された自己署名証明書のサブジェクト名と指紋を表示するには、次のコマンドを使用します。

```
device-> get pki x509 cert system
. . .
    CN=0043022002000186,CN=system generated,CN=self-signed,
. . .
finger print (md5) <e801eae4 56699fbc 324e38f2 4cfa5d47>
finger print (sha) <0113f5ec 6bd6d32b 4ef6ead9 f809eead 3a71435b>
```

注 : WebUI では、自動生成された自己署名証明書の詳細を表示することはできません。

サブジェクト名と指紋を確認したら、それをコピーして管理者に発信し (選択したセキュアな帯域外方式を使用)、その後管理者は、SSL を介してセキュリティデバイスに接続します。管理者の SSL クライアントが SSL ハンドシェイク中にセキュリティデバイスから証明書を受信すると、その中のサブジェクト名と指紋を、以前に帯域外で受信していた証明書と比較します。一致すれば、証明書が本物だと分かります。証明書を認証する信頼できる サードパーティの CA 権限がないため、比較対象のサブジェクト名と指紋がなければ、リモート管理者には証明書が本物かどうかが分かりません。

自己署名証明書の手動作成

セキュリティデバイスは、初回起動時に自己署名証明書を自動生成し、SSL の最初の接続をサポートします。しかし、セキュリティデバイスが自動生成するものとは別の自己署名証明書を生成する必要があります。自動生成された自己署名証明書を、管理者定義の自己署名証明書と交換するのは、以下のような場合が考えられます。

- 自動生成された自己署名証明書が、1024 ビットの固定鍵サイズを使用している場合。鍵のサイズを大きくするか小さくして、自分自身の自己署名鍵を生成する場合に、制御する必要があります。
- 自動生成した証明書とは別のサブジェクト名を使わなければなりません。
- 場合によっては、複数の自己署名証明書が必要となります。仮想システムに対応した セキュリティデバイスでは、ルートシステムとすべての仮想システムで自動生成された自己署名証明書を共有することができます。ただし、vsys 管理者は、自分自身の自己署名証明書を生成して、共有証明書の属性の代わりに、特定の証明書のサブジェクト名と指紋を管理者にチェックさせる方を優先します。

注 : 自動生成された自己署名証明書は、作成されたデバイスの外は通過しません。これとは違い、NSRP クラスタのセキュリティデバイスがクラスタ内の他のメンバと PKI オブジェクトを同期させている場合は、手動生成された自己署名証明書には他の証明書も含まれます。

自己署名証明書には、DN (識別名) フィールドやサブジェクト代替名、鍵サイズなどさまざまなコンポーネントを設定できますが、以下の CN (common name) の要素は常に DN の最後にきます。

"CN = *dev_serial_num*, CN = NetScreen self-signed"

自己署名証明書の当初の利用目的は、すばやく簡単にセキュリティデバイスへ SSL (セキュアソケットレイヤー) 接続することですが、それ以外の CA 署名証明書として利用することもできます。自己署名証明書には、以下の利用法があります。

- SSL (セキュアソケットレイヤー) でセキュリティデバイスへの管理トラフィックを保護する
- NSM (NetScreen-Security Manager) とセキュリティデバイス間のトラフィックを保護する
- VPN トンネルを確立した場合に IKE ピアを認証する

注 : ScreenOS の現在のリリースでは、SSL 用の自己署名証明書しかサポートされていません。

管理者定義の自己署名証明書を設定する

この例では、以下の SSL 用自己署名証明書のコンポーネントを定義します。

- 識別名 / サブジェクト名
  - 名前 : 4ssl
  - Organization: jnpr
  - FQDN: www.juniper.net
- 鍵タイプと長さ : RSA、1024 ビット

定義してから、証明書を生成し、確認してみます。次に、サブジェクト名と指紋 (「拇印」とも言います) をコピーして、SSL 経由でログインしている他の管理者に配布し、セキュリティデバイスを管理できるようにします。

管理者が SSL 経由でログインしようとすると、セキュリティデバイスはこの証明書を送信します。証明書を受信すると、それを開いて、以前受信した証明書のサブジェクト名と指紋について比較します。一致すれば、証明書が本物だと分かります。

WebUI

1. 証明書の属性を定義する

Objects > Certificates > New: 次のように入力してから Generate をクリックします。

Certificate Subject Information:
Name: 4ssl
Organization: jnpr
FQDN: www.juniper.net
Key Pair Information:
RSA: (**選択**)
Create new key pair of **1024** length.

2. 自己署名証明書を生成する

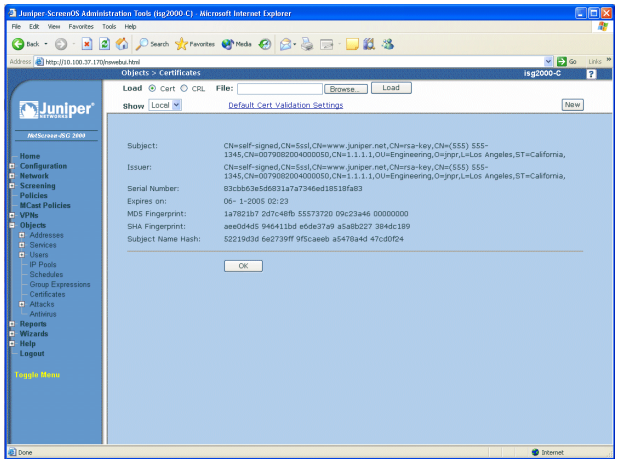
セキュリティデバイスが鍵生成を完了すると、証明書要求を構成します。
Generate Self-Signed Cert をクリックしてください。

3. 自己署名証明書を参照する

Objects > Certificates > Show Local: 作成した証明書の **Detail** をクリックします。

図 17 に示されているような証明書の詳細ページが表示されます。

図 17: 証明書の詳細



このページから、サブジェクト名と指紋をコピーして、セキュリティデバイスを管理するために SSL を使おうとしている他の管理者に発信します。SSL 接続が開始されると、受信した証明書が確かにセキュリティデバイスから来たものかどうかを確認します。

CLI

1. **証明書の属性を定義する**

```
set pki x509 dn name 4ssl
set pki x509 dn org-name jnpr
set pki x509 cert-fqdn www.juniper.net
save
```

2. **自己署名証明書を生成する**

Juniper Networks セキュリティデバイスが証明書要求で使用する公開鍵 / 秘密鍵ペアを生成するには、以下のコマンドを入力します。

```
exec pki rsa new-key 1024
```

鍵ペアが生成されると、次の証明書要求を構成します。

```
---BEGIN CERTIFICATE REQUEST---
MIIB0jCCATsCAQAwZTENMAsGA1UEChMESk5QUjEZMBcGA1UEAxMQMDA0MzAyMj
    Aw
MjAwMDE4NjEQMA4GA1UEAxMHcnNhLWtleTEYMBYGA1UEAxMPd3d3Lmp1bmlwZ
    XIu
bmV0MQ0wCwYDVQQDEwQ1c3NsMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQK
    BgQDP
aAteIkL4HxQmO1w1jv9NMmrWnzdVYnGrKrXnw2MaB3xEgouWrlymEkZetA2ouKeA
D24SL0h1YvJ7Sd9PvkhwHOnvP1zkOCWA84TgvxBzcAyeBnS1UpSwcC0admX0Da6
    T
80EUuGrmUWodddRFUc8o5d2VGTUOM7WgcFDZRSGQGwIDAQABoC0wKwYJKoZIh
    vcN
AQkOMR4wHDAaBgNVHREEEzARgg93d3cuanVuaXBlci5uZXQwDQYJKoZIhvcNAQEF
BQADgYEAgvDXI4H905y/2+k4omo9Y4XQrgq44Rj3jqXAYYMgQBd0Q8HoyL5NE3+i
QUkiYjMTWO2wIWzEr4u/tdAISEVTu03achZa3zIkUtn8sD/VYKhFlyPCBVvMiaHd
FzIHUgBuMrr+awowJDG6wARhR75w7pORXy7+aAmvIjew8YRre9s=
---END CERTIFICATE REQUEST---
```

鍵ペアの ID 番号を知るには、以下のコマンドを入力します。

```
get pki x509 list key-pair

Getting OTHER PKI OBJECT ...
IDX  ID num     X509 Certificate Subject Distinguish Name
=========================================================
0000 176095259
     CN=4ssl,CN=www.juniper.net,CN=rsa-key,CN=0043022002000186,
     O=jnpr,
=========================================================
```

自己署名証明書を生成するには、先ほどのコマンドの出力から分かった鍵ペアの ID 番号を参照して、以下のコマンドを入力してください。

```
exec pki x509 self-signed-cert key-pair 176095259
```

3. 自己署名証明書を参照する

作成した自己署名証明書を参照するには、以下のコマンドを入力します。

```
get pki x509 list local-cert

     Getting LOCAL CERT ...
     IDX  ID num     X509 Certificate Subject Distinguish Name
     =========================================================
     0000 176095261 LOCAL CERT friendly name <29>
     LOCAL CERT friendly name <29>
     CN=self-signed,CN=4ssl,CN=www.juniper.net,CN=rsa-key,CN=004302200200
          0186,
          O=jnpr,
     Expire on 10-19-2009 17:20, Issued By:
     CN=self-signed,CN=4ssl,CN=www.juniper.net,CN=rsa-key,CN=004302200200
          0186,
          O=jnpr,
     =========================================================
```

証明書のさらに詳しい情報を参照するには、証明書の ID 番号を使用して、以下のコマンドを入力します。

```
get pki x509 cert 176095261

     -0001 176095261 LOCAL CERT friendly name <29>
     CN=self-signed,CN=4ssl,CN=www.juniper.net,CN=rsa-key,CN=0043022002
          000186,
          O=jnpr,
     Expire on 10-19-2009 17:20, Issued By:
     CN=self-signed,CN=4ssl,CN=www.juniper.net,CN=rsa-key,CN=004302200200
          0186,
          O=jnpr,
     Serial Number: <9d1c03365a5caa172ace4f82bb5ec9da>
     subject alt name extension:
     email(1): (empty)
     fqdn(2): (www.juniper.net)
     ipaddr(7): (empty)
     no renew
     finger print (md5) <be9e0280 02bdd9d1 175caf23 6345198e>
     finger print (sha) <87e0eee0 c06f9bac 9098bd02 0e631c1b 26e37e0e>
     subject name hash: <d82be8ae 4e71a576 2e3f06fc a98319a3 5c8c6c27>
     use count: <1>
     flag <00000000>
```

この出力から、**subject name** と **fingerprint** をコピーして、セキュリティデバイスを管理するために SSL を使おうとしている他の管理者に発信します。SSL 接続が開始されると、受信した証明書が確かにセキュリティデバイスから来たものかどうかを確認します。

証明書の自動生成

セキュリティデバイスを初めて起動すると、自己署名証明書を自動生成します。この証明書の本来の目的は、セキュリティデバイスの初回起動時に、すばやく SSL をサポートすることにあります。この証明書を参照するには、以下の CLI コマンドを使用します。

```
get pki x509 cert system
    CN=0010062001000021,CN=system generated,CN=self-signed,
    Expire on 08- 3-2014 16:19, Issued By:
    CN=0010062001000021,CN=system generated,CN=self-signed,
    Serial Number: <c927f2044ee0cf8dc931cdb1fc363119>
    finger print (md5) <fd591375 83798574 88b3e698 62890b5d>
    finger print (sha) <40a1bda8 dcd628fe e9deaee1 92a2783c 817e26d9>
    subject name hash: <0324d38d 52f814fe 647aba3a 86eda7d4 a7834581>
```

デフォルトでは、セキュリティデバイスは、以下の条件が満たされると、起動処理中に自己署名証明書を自動生成します。

- デバイス上に、自動生成された自己署名証明書がない。
- SSL 用の証明書が割り当てられていない。

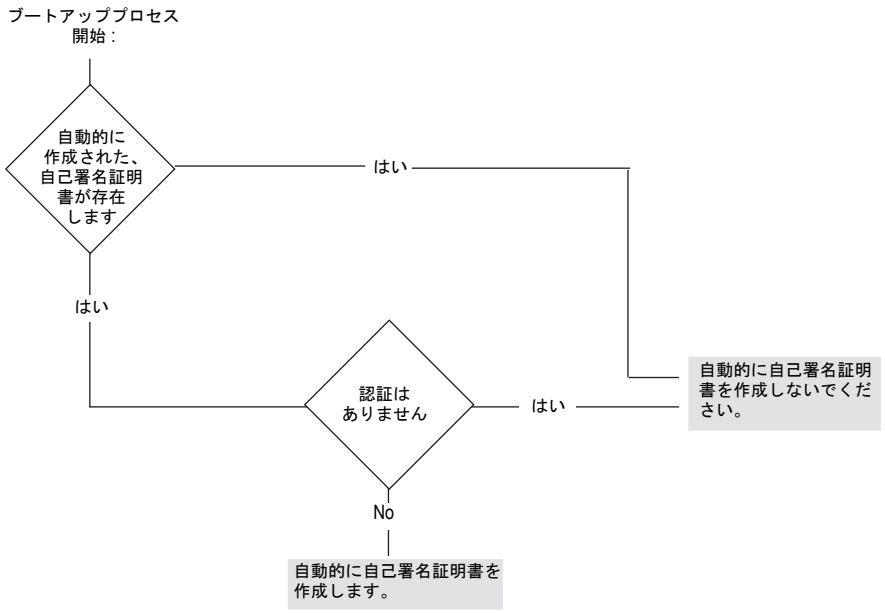
以下のコマンドを使用すると、証明書が SSL に設定済みかどうかを調べることができます。

```
get ssl
web SSL enable.
web SSL port number(443).
web SSL cert: Default - System Self-Signed Cert.
web SSL cipher(RC4_MD5).
```

上記のコマンド出力から、SSL が自動生成された (「System」) 自己署名証明書を使用しているかが分かります。

図 18 は、セキュリティデバイスの起動時に行う証明書生成の決定経路を表しています。

図 18: 証明書の自動生成用の決定経路



自動生成された自己署名証明書を削除する場合は、SSL に別の証明書を割り当ててから、デバイスをリセットしてください。セキュリティデバイスは、起動処理中に新しい証明書を再生成しません。次に SSL の設定を変更して、証明書を割り当てずにデバイスをリセットすると、セキュリティデバイスは、次回の起動処理中に新しい自己署名証明書を自動的に再作成します。

自己署名証明書の削除

他の証明書のタイプと同様に、自動生成されたものか手動生成されたものかに関係なく、自己署名証明書を削除することができます。自己署名証明書の代わりに、SSL 用に優先して使用する CA 署名証明書を取得する場合もあります。いずれの場合でも、自動生成された自己署名証明書を削除するには、以下の CLI コマンドを使用します。

```
delete pki object-id system
```

管理者設定の自己署名証明書を削除するには、以下のコマンドの *id_num* に削除する証明書の ID 番号を入力して、実行します。

```
delete pki object-id id_num
```

自動生成された自己署名証明書を削除して、後から新しい証明書を生成するには、以下を行います。

- SSL に他の証明書を割り当てない (以下のコマンドを使用します。**unset ssl cert**)。
- セキュリティデバイスをリセットする。

セキュリティデバイスは、自身に送信される HTTP トラフィック (デフォルトのポート番号 80) を SSL (デフォルトのポート番号 443) に転送できます。そのため、起動処理中に証明書が SSL で利用できるかどうかを確認するために、セキュリティデバイスは、自動生成された自己署名証明書があるか、または別の証明書が SSL に割り当てられているかを常にチェックしています。自動生成された自己署名証明書がなく、他の証明書も SSL に割り当てられていない場合は、セキュリティデバイスは自己署名証明書を自動生成します。

注 : 自動生成された自己署名証明書の削除は、CLI からのみ実行できます。

証明書の ID 番号を知るには、以下のコマンドを入力します。
get pki x509 list local-cert.

HTTP トラフィックから SSL への転送については、**3**-8 ページの「HTTP を SSL に転送する」を参照してください。

第 3 章

VPN (仮想プライベートネットワーク) のガイドライン

ScreenOS で VPN トンネルを構成する場合、さまざまな暗号のオプションが用意されています。簡単なトンネルを構成する場合でも選択を行う必要があります。本章の前半では基本的なサイトツーサイト VPN や基本的なダイヤルアップ VPN の選択肢を要約し、各オプションを選択するさまざまな理由を説明します。

章の後半では、ポリシーベースの VPN トンネルとルートベースの VPN トンネルの違いについて考察します。それからルートベースおよびポリシーベースのサイトツーサイト AutoKey IKE VPN トンネルのパケットフローについて調べ、パケットが通過するアウトバウンドおよびインバウンドの処理段階を理解します。本章では最後に、トンネルを構成するときに覚えておくと役立つ VPN 構成のヒントについて説明します。

本章のセクションは、以下のようになります。

- 46 ページの「暗号オプション」
  - 46 ページの「サイトツーサイトの暗号オプション」
  - 53 ページの「ダイヤルアップ VPN オプション」
- 59 ページの「ルートベーストンネルおよびポリシーベーストンネル」
- 61 ページの「パケットフロー : サイトツーサイト VPN」
- 66 ページの「トンネル構成のガイド」
- 68 ページの「ルートベース VPN (仮想プライベートネットワーク) のセキュリティ検討事項」
  - 69 ページの「Null ルート」
  - 70 ページの「ダイヤルアップまたはリース回線」
  - 71 ページの「リース回線または Null ルートへの VPN フェールオーバー」
  - 74 ページの「おとりトンネルインターフェース」
  - 74 ページの「トンネルインターフェースの仮想ルーター」
  - 75 ページの「別のトンネルへの再ルーティング」

暗号オプション

VPN の構成時には、使用する暗号について多くの決定を下さなければなりません。どの Diffie-Hellman グループを選択すべきか、どの暗号アルゴリズムを使用すればセキュリティとパフォーマンスの最適なバランスを保てるか、などの疑問が生じます。このセクションでは、基本的なサイトツーサイトの VPN トンネルと基本的なダイヤルアップ VPN トンネルの構成に必要なすべての暗号オプションについて説明し、使用するオプションの決定に役立つように各オプションの利点を説明します。

最初に、サイトツーサイト VPN トンネル (2 つのセキュリティデバイス間) かダイヤルアップ VPN トンネル (NetScreen リモート VPN クライアントからセキュリティデバイス) のどちらを構成するか決める必要があります。これはネットワークに関する決定ですが、2 タイプのトンネルの相違点は一部の暗号オプションに影響を与えます。このため、オプションは次の 2 つの図で説明されています。

- 「サイトツーサイトの暗号オプション」では、47 ページの図 19、「サイトツーサイト VPN トンネルの暗号オプション」について説明します。
- 「ダイヤルアップ VPN オプション」では、53 ページの図 20、「ダイヤルアップ VPN トンネルの暗号オプション」について説明します。

サイトツーサイトトンネルとダイヤルアップトンネルのどちらを構成するかを決定した後は、図 19 か図 20 をガイドとして参照できます。各図は、トンネルの構成時に選択すべき暗号の選択肢を示しています。図内に示されている各オプションを選択するために各図をたどってください。

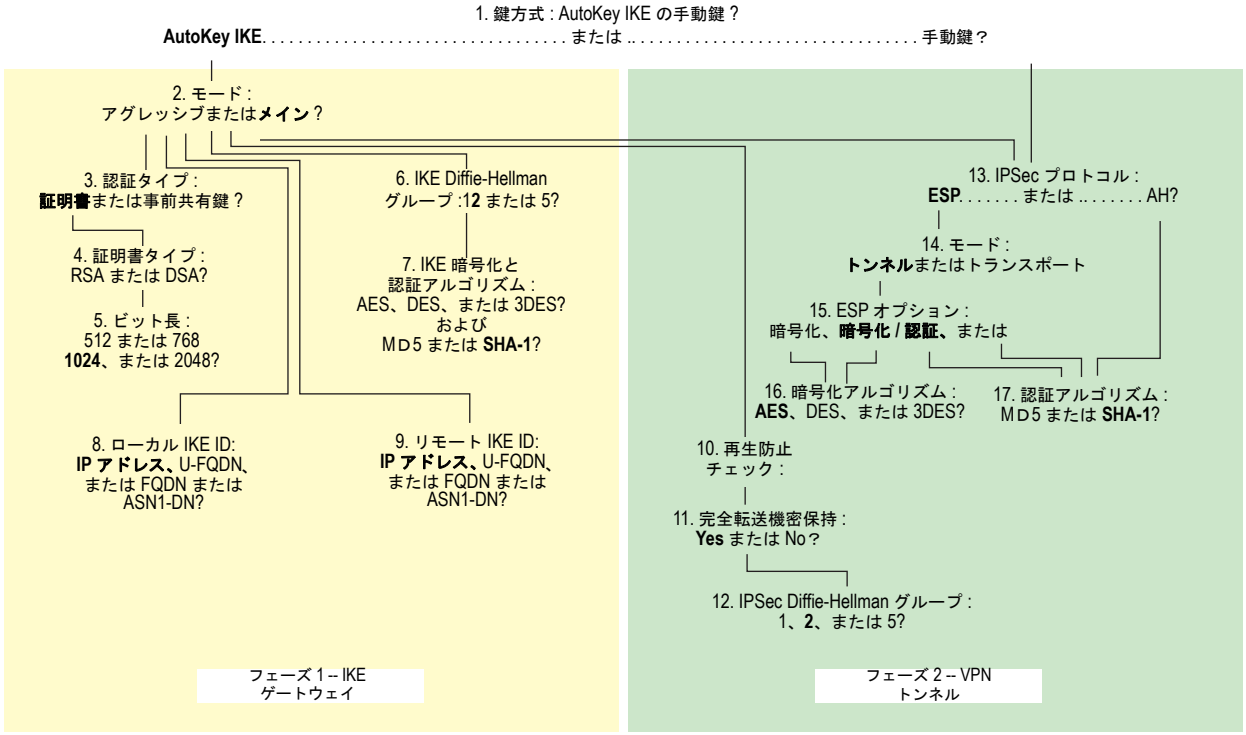
注 : 両方の種類のトンネルの構成例が第 4 章、「サイト間 VPN (仮想プライベートネットワーク)」と第 5 章「ダイヤルアップ仮想プライベート ネットワーク」で示されています。

サイトツーサイトの暗号オプション

基本的なサイトツーサイト VPN トンネルを構成しているときは、図 19 にある暗号オプションから選択する必要があります。各オプションの利点が後で説明されています。

注 : 47 ページの図 19 に推奨オプションが**太字**で示されています。各種の IPSec オプションの背景情報については、1 ページの「インターネットプロトコルセキュリティ」を参照してください。

図 19: サイトツーサイト VPN トンネルの暗号オプション



1. 鍵方式 : AutoKey IKE の手動鍵 ?

AutoKey IKE

- 推奨
- 自動的に鍵の更新を行い、鍵の新しさを保つため、セキュリティが向上します。

手動鍵

- IKE の問題のデバッグに役立ちます。
- トンネルの確立時に IKE ネゴシエーションの遅延がなくなります。

2. モード : アグレッシブまたはメイン ?

アグレッシブ

IPSec ピアのうち 1 つの IP アドレスが動的に割り当てられ、事前共有鍵が使用される場合に必要です。

メイン

- 推奨
- 識別保護を提供します。
- ダイヤルアップユーザーが静的 IP アドレスを使用している場合や、認証に証明書が使用されている場合に使用できます。

3. 認証タイプ : 事前共有鍵または証明書 ?

証明書

- 推奨
- 証明書を CA (認証局) で検証できるため、事前共有鍵よりもセキュリティが高くなります (詳細については、19 ページの「公開鍵暗号化」を参照してください) 。

事前共有鍵

PKI (公開鍵基盤) を必要としないため、簡単に使用でき素早くセットアップできます。

4. 証明書タイプ : RSA または DSA?

これはユーザーに証明書を与える CA に依存しています。片方の証明書のタイプが別の証明書のタイプより有利ということはありません。

5. ビット長 : 512、768、1024、または 2048?

512

処理のオーバーヘッドが最も少なくなります。

768

- 512 ビットよりもセキュリティが高くなります。
- 1024 ビットおよび 2048 ビットよりも処理のオーバーヘッドが少なくなります。

1024

- 推奨
- 512 ビットおよび 768 ビットよりもセキュリティが高くなります。
- 2048 ビットよりも処理のオーバーヘッドが少なくなります。

2048

最もセキュリティが高くなります。

6. IKE Diffie-Hellman グループ : 1、2 または 5?

Diffie-Hellman グループ 1

- Diffie-Hellman グループ 2 および 5 よりも処理のオーバーヘッドが少なくなります。
- Juniper Networks セキュリティハードウェアの処理が加速します。

Diffie-Hellman グループ 2

- 推奨
- Diffie-Hellman グループ 5 よりも処理のオーバーヘッドが少なくなります。
- Diffie-Hellman グループ 1 よりもセキュリティが高くなります。
- Juniper Networks セキュリティハードウェアの処理が加速します。

Diffie-Hellman グループ 5

最もセキュリティが高くなります。

7. IKE 暗号化と認証アルゴリズム : AES、DES、または 3DES および MD5 または SHA-1?

AES

- 推奨
- 鍵の長さが同じ場合、DES および 3DES よりも暗号が堅牢です。
- Juniper Networks セキュリティハードウェアの処理が加速します。
- FIPS (米国連邦情報処理規格) および Common Criteria EAL4 規格で承認されている暗号アルゴリズムです。

DES

- 3DES および AES よりも処理のオーバーヘッドが少なくなります。
- リモートピアが AES をサポートしない場合に便利です。

3DES

- DES よりも暗号のセキュリティが高くなります。
- Juniper Networks セキュリティハードウェアの処理が加速します。

MD5

SHA-1 よりも処理のオーバーヘッドが少なくなります。

SHA-1

- 推奨
- MD5 よりも暗号のセキュリティが高くなります。
- FIPS で認められている唯一の認証アルゴリズムです

8. ローカル IKE ID: IP アドレス (デフォルト)、U-FQDN、FQDN、または ASN1-DN?

IP アドレス

- 推奨
- ローカルセキュリティデバイスが静的 IP アドレスを使用している場合にのみ使用できます。
- 認証に事前共有鍵を使用しているときはデフォルトの IKE ID となります。
- IP アドレスが SubjectAltName フィールドに表示される場合は証明書と共に使用できます。

U-FQDN

ユーザー完全修飾ドメイン名 (U-FQDN - E メールアドレス): U-FQDN が SubjectAltName フィールドに表示される場合は事前共有鍵または証明書と共に使用できます。

FQDN

- 完全修飾ドメイン名 (FQDN): FQDN が SubjectAltName フィールドに表示される場合は事前共有鍵または証明書と共に使用できます。
- 動的 IP アドレスを持つ VPN ゲートウェイに役立ちます。
- 認証に RSA または DSA 証明書を使用しているときはデフォルトの IKE ID となります。

ASN1-DN

- 証明書とのみ使用できます。
- CA の発行する証明書が SubjectAltName フィールドをサポートしていない場合に便利です

9. リモート IKE ID: IP アドレス (デフォルト)、U-FQDN、FQDN、または ASN1-DN?

IP アドレス

- 推奨
- 認証に事前共有鍵を使用しており、ピアがセキュリティデバイスのときは、静的 IP アドレスのピアにリモート IKE ID を入力する必要がありません。
- 静的 IP アドレスを使用しているデバイスに使用できます。
- IP アドレスが SubjectAltName フィードに表示される場合は事前共有鍵または証明書と共に使用できます。

U-FQDN

ユーザー完全修飾ドメイン名 (U-FQDN - E メールアドレス): U-FQDN が SubjectAltName フィールドに表示される場合は事前共有鍵または証明書と共に使用できます。

FQDN

- 完全修飾ドメイン名 (FQDN): FQDN が SubjectAltName フィールドに表示される場合は事前共有鍵または証明書と共に使用できます。
- 動的 IP アドレスを持つ VPN ゲートウェイに役立ちます。
- 認証に証明書を使用しており、ピアがセキュリティデバイスのときは、リモート IKE ID を入力する必要がありません。

ASN1-DN

- 証明書とのみ使用できます。
- CA の発行する証明書が SubjectAltName フィールドをサポートしていない場合に便利です。

10. 再生防止チェック : No または Yes?

はい

- 推奨
- 受信者がパケットヘッダーのシーケンス番号をチェックできるようにし、犯罪者が代行受信した IPSec パケットを再送したときに Dos (サービス拒否) 攻撃が起きるのを防止します。

No

これを使用不可にすると、サードパーティのピアとの互換性の問題が解決することがあります。

11. 完全転送機密保持 : No または Yes?

はい

- 推奨
- 完全転送機密保持 (PFS): ピアが 2 回目の Diffie-Hellman の鍵交換を実行し、IPSec の暗号化 / 暗号解読に使用される鍵を作成するため、セキュリティが向上します。

いいえ

- トンネルを速くセットアップできます。
- IPSec ネゴシエーションのフェーズ 2 での処理が少なくなります。

12. IPSec Diffie-Hellman グループ : 1、2 または 5?

Diffie-Hellman グループ 1

- Diffie-Hellman グループ 2 および 5 よりも処理のオーバーヘッドが少なくなります。
- Juniper Networks セキュリティハードウェアの処理が加速します。

Diffie-Hellman グループ 2

- 推奨
- Diffie-Hellman グループ 5 よりも処理のオーバーヘッドが少なくなります。
- Diffie-Hellman グループ 1 よりもセキュリティが高くなります。
- Juniper Networks セキュリティハードウェアの処理が加速します。

Diffie-Hellman グループ 5

最もセキュリティが高くなります。

13. IPSec プロトコル : ESP または AH?

ESP

- 推奨
- セキュリティペイロードのカプセル化 (ESP): 機密性 (元の IP パケットの暗号化とカプセル化) と保全性 (認証) の両方を提供できます。
- 暗号化のみ、または認証のみを提供することもできます。

AH

認証ヘッダー (AH): IPSec ヘッダーおよび外部 IP ヘッダーを含む IP パケット全体の認証を行います。

14. モード : トンネルまたはトランスポート ?

Tunnel

- 推奨
- 元の IP ヘッダーを隠すことでプライバシを向上します。

トランスポート

L2TP-over-IPSec トンネルサポートで必要です

15. ESP オプション : 暗号化、暗号化 / 認証、または認証 ?

暗号化

- 暗号化 / 認証を使用するよりもパフォーマンスが速くなり、処理のオーバーヘッドが少なくなります。
- 機密性が必要で、認証が不要な場合に役立ちます。

暗号化 / 認証

- 推奨
- 機密性と認証が必要な場合に役立ちます。

Auth

認証が必要で、機密性が不要な場合に役立ちます。情報は機密ではないが、送信者であると言う人から本当に送られてきており、転送中にだれも内容を改ざんしていないことを確認することが重要な場合に使用できます。

16. 暗号化アルゴリズム : AES、DES、または 3DES?

AES

- 推奨
- 鍵の長さが同じ場合、DES および 3DES よりも暗号が堅牢です。
- Juniper Networks セキュリティハードウェアの処理が加速します。
- FIPS および Common Criteria EAL4 規格で承認されている暗号アルゴリズムです。

DES

- 3DES および AES よりも処理のオーバーヘッドが少なくなります。
- リモートピアが AES をサポートしない場合に便利です。

3DES

- DES よりも暗号のセキュリティが高くなります。
- Juniper Networks セキュリティハードウェアの処理が加速します。

17. 認証アルゴリズム : MD5 または SHA-1?

MD5

SHA-1 よりも処理のオーバーヘッドが少なくなります。

SHA-1

- 推奨
- MD5 よりも暗号のセキュリティが高くなります。

前のリストの推奨オプションを使用した場合、静的 IP アドレスを持つ 2 つのセキュリティデバイス間の汎用サイトツーサイト VPN の構成は、次の構成要素から成り立っています。

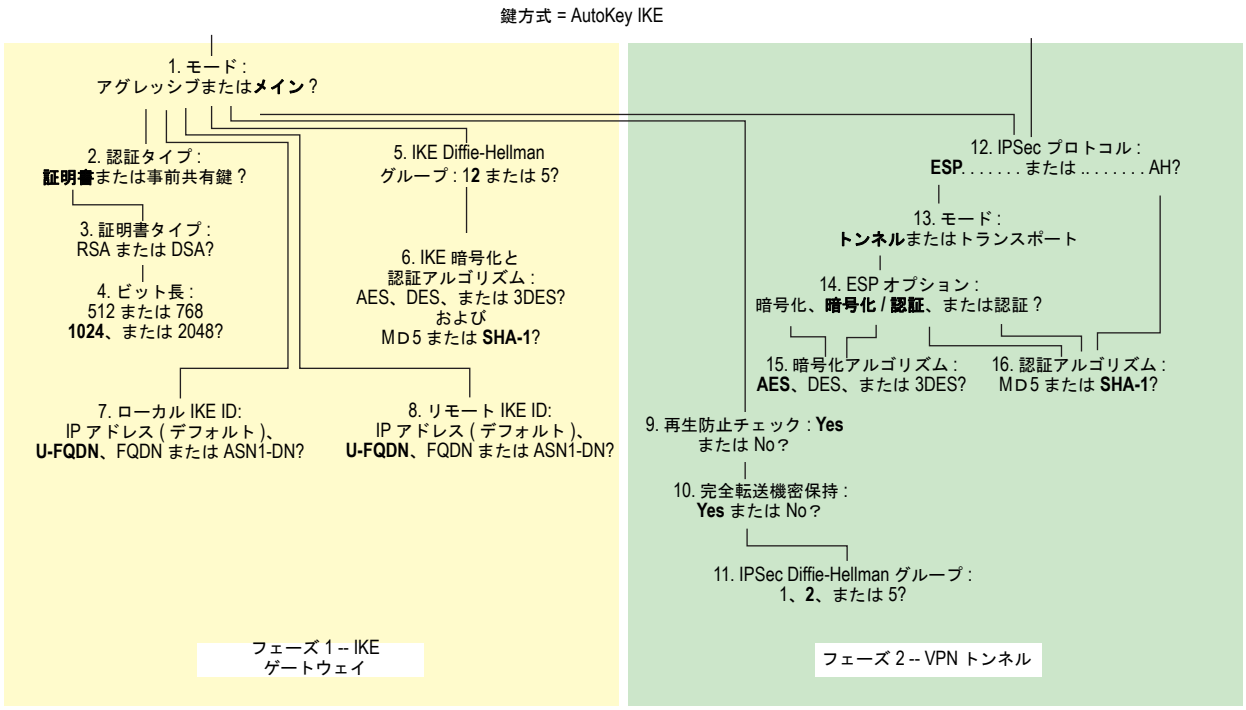
■ AutoKey IKE	■ 完全転送機密保持 (PFS) = yes
■ メインモード	■ フェーズ 2 Diffie-Hellman グループ 2
■ 1024 ビット証明書 (RSA または DSA)	■ セキュリティペイロードのカプセル化 (ESP)
■ フェーズ 1 Diffie-Hellman グループ 2	■ トンネルモード
■ 暗号化 = AES	■ 暗号化 / 認証
■ 認証 = SHA-1	■ 暗号化 = AES
■ IKE ID = IP アドレス (デフォルト)	■ 認証 = SHA-1
■ 再生防止保護 = yes	

ダイヤルアップVPN オプション

基本的なダイヤルアップ VPN トンネルを構成しているときは、図 20 にある暗号オプションから選択する必要があります。各オプションの利点が後で説明されています。

注 : 図 20 に推奨オプションが**太字**で示されています。各種の IPSec オプションの背景情報については、1 ページの「インターネットプロトコルセキュリティ」を参照してください。

図 20: ダイヤルアップ VPN トンネルの暗号オプション



1. モード : アグレッシブまたはメイン ?

アグレッシブ

- 推奨
- IPSec ピアのうち 1 つの IP アドレスが動的に割り当てられ、事前共有鍵が使用される場合に必要です。
- 認証用に証明書または事前共有鍵とともに使用できます。

メイン

識別保護を提供します。

2. 認証タイプ : 事前共有鍵または証明書 ?

証明書

- 推奨
- 証明書を CA (認証局) で検証できるため、事前共有鍵よりもセキュリティが高くなります (詳細については、19 ページの「公開鍵暗号化」を参照してください)。

事前共有鍵

PKI (公開鍵基盤) を必要としないため、簡単に使用でき素早くセットアップできます。

3. 証明書タイプ : RSA または DSA?

これはユーザーに証明書を与える CA に依存しています。片方の証明書のタイプが別の証明書のタイプより有利ということはありません。

4. ビット長 : 512、768、1024、または 2048?

512

処理のオーバーヘッドが最も少なくなります。

768

- 512 ビットよりもセキュリティが高くなります。
- 1024 ビットおよび 2048 ビットよりも処理のオーバーヘッドが少なくなります。

1024

- 推奨
- 512 ビットおよび 768 ビットよりもセキュリティが高くなります。
- 2048 ビットよりも処理のオーバーヘッドが少なくなります。

2048

最もセキュリティが高くなります。

5. IKE Diffie-Hellman グループ : 1、2 または 5?

Diffie-Hellman グループ 1

- Diffie-Hellman グループ 2 および 5 よりも処理のオーバーヘッドが少なくなります。
- Juniper Networks セキュリティハードウェアの処理が加速します。

Diffie-Hellman グループ 2

- 推奨
- Diffie-Hellman グループ 5 よりも処理のオーバーヘッドが少なくなります。
- Diffie-Hellman グループ 1 よりもセキュリティが高くなります。
- Juniper Networks セキュリティハードウェアの処理が加速します。

Diffie-Hellman グループ 5

最もセキュリティが高くなります。

6. IKE 暗号化と認証アルゴリズム : AES、DES、または 3DES および MD5 または SHA-1?

AES

- 推奨
- 鍵の長さが同じ場合、DES および 3DES よりも暗号が堅牢です。
- Juniper Networks セキュリティハードウェアの処理が加速します。
- FIPS および Common Criteria EAL4 規格で承認されている暗号アルゴリズムです

DES

- 3DES および AES よりも処理のオーバーヘッドが少なくなります。
- リモートピアが AES をサポートしない場合に便利です。

3DES

- DES よりも暗号のセキュリティが高くなります。
- Juniper Networks セキュリティハードウェアの処理が加速します。

MD5

SHA-1 よりも処理のオーバーヘッドが少なくなります。

SHA-1

- 推奨
- MD5 よりも暗号のセキュリティが高くなります。

7. ローカル IKE ID: IP アドレス (デフォルト)、U-FQDN、FQDN、または ASN1-DN?

IP アドレス (デフォルト)

- 静的 IP アドレスを使用しているデバイスに IKE ID を入力する必要がありません。
- 静的 IP アドレスを使用しているデバイスに使用できます。
- IP アドレスが SubjectAltName フィードに表示される場合は事前共有鍵または証明書と共に使用できます。

U-FQDN

- 推奨
- ユーザー完全修飾ドメイン名 (U-FQDN - E メールアドレス): U-FQDN が SubjectAltName フィールドに表示される場合は事前共有鍵または証明書と共に使用できます。

FQDN

- 完全修飾ドメイン名 (FQDN): FQDN が SubjectAltName フィールドに表示される場合は事前共有鍵または証明書と共に使用できます。
- 動的 IP アドレスを持つ VPN ゲートウェイに役立ちます。

ASN1-DN

- 証明書とのみ使用できます。
- CA の発行する証明書が SubjectAltName フィールドをサポートしていない場合に便利です。

8. リモート IKE ID: IP アドレス (デフォルト)、U-FQDN、FQDN、または ASN1-DN?

IP アドレス (デフォルト)

- 静的 IP アドレスを使用しているデバイスに IKE ID を入力する必要がありません。
- 静的 IP アドレスを使用しているデバイスに使用できます。
- IP アドレスが SubjectAltName フィードに表示される場合は事前共有鍵または証明書と共に使用できます。

U-FQDN

- 推奨
- ユーザー完全修飾ドメイン名 (U-FQDN - E メールアドレス): U-FQDN が SubjectAltName フィールドに表示される場合は事前共有鍵または証明書と共に使用できます。

FQDN

- 完全修飾ドメイン名 (FQDN): FQDN が SubjectAltName フィールドに表示される場合は事前共有鍵または証明書と共に使用できます。
- 動的 IP アドレスを持つ VPN ゲートウェイに役立ちます。

ASN1-DN

- 証明書とのみ使用できます。
- CA の発行する証明書が SubjectAltName フィールドをサポートしていない場合に便利です。

9. 再生防止チェック : No または Yes?

はい

- 推奨
- 受信者がパケットヘッダーのシーケンス番号をチェックできるようにし、犯罪者が代行受信した IPSec パケットを再送したときに Dos (サービス拒否) 攻撃が起きるのを防止します。

いいえ

これを使用不可にすると、サードパーティのピアとの互換性の問題が解決することがあります。

10. 完全転送機密保持 : No または Yes?

はい

- 推奨
- 完全転送機密保持 (PFS): ピアが 2 回目の Diffie-Hellman の鍵交換を実行し、IPSec の暗号化 / 暗号解読に使用される鍵を作成するため、セキュリティが向上します。

いいえ

- トンネルを速くセットアップできます。
- IPSec ネゴシエーションのフェーズ 2 での処理が少なくなります。

11. IPSec Diffie-Hellman グループ : 1、2 または 5?

Diffie-Hellman グループ 1

- Diffie-Hellman グループ 2 および 5 よりも処理のオーバーヘッドが少なくなります。
- Juniper Networks セキュリティハードウェアの処理が加速します。

Diffie-Hellman グループ 2

- 推奨
- Diffie-Hellman グループ 5 よりも処理のオーバーヘッドが少なくなります。
- Diffie-Hellman グループ 1 よりもセキュリティが高くなります。
- Juniper Networks セキュリティハードウェアの処理が加速します。

Diffie-Hellman グループ 5

最もセキュリティが高くなります。

12. IPSec プロトコル : ESP または AH?

ESP

- 推奨
- セキュリティペイロードのカプセル化 (ESP): 機密性 (元の IP パケットの暗号化とカプセル化) と保全性 (認証) の両方を提供できます。
- 暗号化のみ、または認証のみを提供することもできます。

AH
認証ヘッダー (AH): IPSec ヘッダーおよび外部 IP ヘッダーを含む IP パケット全体の認証を行います。

13. モード : トンネルまたはトランスポート ?

Tunnel
- 推奨
- 元の IP ヘッダーを隠すことでプライバシを向上します。

トランスポート
L2TP-over-IPSec トンネルサポートで必要です。

14. ESP オプション : 暗号化、暗号化 / 認証、または認証 ?

暗号化
- 暗号化 / 認証を使用するよりもパフォーマンスが速くなり、処理のオーバーヘッドが少なくなります。
- 機密性が必要で、認証が不要な場合に役立ちます。

暗号化 / 認証
- 推奨
- 機密性と認証が必要な場合に役立ちます。

認証
認証が必要で、機密性が不要な場合に役立ちます。情報は機密ではないが、送信者であると言う人から本当に送られてきており、転送中にだれも内容を改ざんしていないことを確認することが重要な場合に使用できます。

15. 暗号化アルゴリズム : AES、DES、または 3DES?

AES
- 推奨
- 鍵の長さが同じ場合、DES および 3DES よりも暗号が堅牢です
- Juniper Networks セキュリティハードウェアの処理が加速します。
- FIPS および Common Criteria EAL4 規格で承認されている暗号アルゴリズムです。

DES
- 3DES および AES よりも処理のオーバーヘッドが少なくなります。
- リモートピアが AES をサポートしない場合に便利です。

3DES
- DES よりも暗号のセキュリティが高くなります。
- Juniper Networks セキュリティハードウェアの処理が加速します。

16. 認証アルゴリズム : MD5 または SHA-1?

MD5

SHA-1 よりも処理のオーバーヘッドが少なくなります。

SHA-1

- 推奨
- MD5 よりも暗号のセキュリティが高くなります。

上記のリストの推奨オプションを使用した場合、静的 IP アドレスを持つ 2 つのセキュリティデバイス間の汎用ダイヤルアップ VPN の構成は、次の構成要素から成り立っています。

■ アグレッシブモード	■ 完全転送機密保持 (PFS) = yes
■ 1024 ビット証明書 (RSA または DSA)	■ フェーズ 2 Diffie-Hellman グループ 2
■ フェーズ 1 Diffie-Hellman グループ 2	■ セキュリティペイロードのカプセル化 (ESP)
■ 暗号化 = AES	■ トンネルモード
■ 認証 = SHA-1	■ 暗号化 / 認証
■ IKE ID = U-FQDN (E メールアドレス)	■ 暗号化 = AES
■ 再生防止保護 = yes	■ 認証 = SHA-1

ルートベーストンネルおよびポリシーベーストンネル

VPN をサポートするための セキュリティデバイスの構成は非常に柔軟です。ルートベースおよびポリシーベースの VPN トンネルを作成できます。また、暗号化や認証に使用する鍵を管理するため、各タイプのトンネルで手動鍵や AutoKey IKE を使用できます。

ポリシーベース VPN トンネルでは、トンネルはオブジェクト (またはビルディングブロック) として扱われ、ソース、宛先、サービス、およびアクションと共に VPN トラフィックを許可するポリシーを構成します。(VPN ポリシーアクションは実際には、*tunnel* ですが、特に記述がない場合には *permit* アクションとみなされます。) ポリシーベース VPN 構成では、ポリシーは VPN トンネルを名前で具体的に参照します。

ルートベース VPN では、ポリシーは VPN トンネルを具体的に参照しません。その代わりに、ポリシーは宛先アドレスを参照します。セキュリティデバイスが、宛先アドレスへ送信するためにトラフィックを経由させるインターフェースを見つけるためにルートルックアップを行う場合、特定の VPN トンネルがバインドされたトンネルインターフェースを経由するルートを見つけます。

注 : 通常、トンネルインターフェースは 1 つのトンネルにバインドされています。トンネルインターフェースを、複数のトンネルにバインドすることもできます。詳細については、256 ページの「1 つのトンネルインターフェースに対する複数のトンネル」を参照してください。

したがって、ポリシーベース VPN トンネルでは、トンネルをポリシーの構築要素として考えることができます。ルートベース VPN トンネルでは、トンネルはトラフィックを送信するための手段として、またポリシーはそのトラフィックの送信を許可または拒否する方法として考えることができます。

作成できるポリシーベース VPN トンネルの数は、デバイスがサポートするポリシーの数によって制限されます。作成するルートベース VPN トンネルの数は、デバイスがサポートするルートエントリの数またはトンネルインターフェースの数のいずれか低い方によって制限されます。

ルートベースの VPN トンネル構成は、VPN トラフィックに詳細な制限を設定しながらもトンネルリソースを節約したい場合に適しています。同じ VPN トンネルを参照するポリシーを多数作成できますが、各ポリシーは個別にリモートピアと関連付けられた IPSec SA (セキュリティアソシエーション) を作成します。各 SA は個別の VPN トンネルとみなされます。VPN に対するルートベースのアプローチでは、トラフィックの規制は送信手段と結びつけられていません。2 つのサイトの間にある単一の VPN トンネルを行き来するトラフィックを規制する何十ものポリシーを構成しても、1 つの IPSec SA だけが有効になります。また、ルートベース VPN 構成では、VPN トンネルを経由して到達した宛先を参照する、アクションが *deny* のポリシーを作成できます。これは、すでに説明したようにアクションが *permit* を意味する *tunnel* でなければならないポリシーベース VPN 構成の場合と異なります。

ルートベース VPN の他の利点は、VPN トンネルを経由して動的ルーティング情報を交換できる点にあります。VPN トンネルにバインドされたトンネルインターフェースで BGP (境界ゲートウェイプロトコル) などの動的ルーティングプロトコルのインスタンスを使用可能にできます。ローカルのルーティングインスタンスはトンネルを経由して、他方にバインドされたトンネルインターフェースで使用可能にされたネイバーとルーティング情報を交換します。

トンネルが動的ルーティングプロトコルを実行している大規模なネットワークに接続しておらず、トンネルを経由するトラフィックをフィルタするためにトンネルを節約したりいくつものポリシーを定義したりする必要がない場合、ポリシーベーストンネルが適しています。また、ダイヤルアップ VPN クライアントの先にはネットワークがないため、ポリシーベース VPN トンネルはダイヤルアップ VPN 構成に適しています。

とは言っても、ダイヤルアップクライアントが仮想内部 IP アドレスをサポートしている場合は (NetScreen-Remote はサポートしています)、ルートベース VPN 構成を使用する十分な理由があります。ルートベースダイヤルアップ VPN トンネルには次の利点があります。

- ポリシーの実施を要求するため、または要求しないためにトンネルインターフェースをどのゾーンにもバインドできます。
- ポリシーベース VPN 構成とは異なり、トラフィックが強制的にトンネルを経由するようにルートを定義できます。
- ルートベース VPN トンネルはハブアンドスポーク方式の構成に対するスポークの追加を簡素化します (313 ページの「ハブアンドスポーク方式 VPN の作成」を参照)。
- リモートクライアントのアドレスを 255.255.255.255/32 に構成することにより、ダイヤルアップ VPN クライアントから任意の IP アドレスを受け入れるようにプロキシ ID を調整できます。

- トンネルインターフェースで 1 つまたは複数の MIP (マップ IP) アドレスを定義できます。

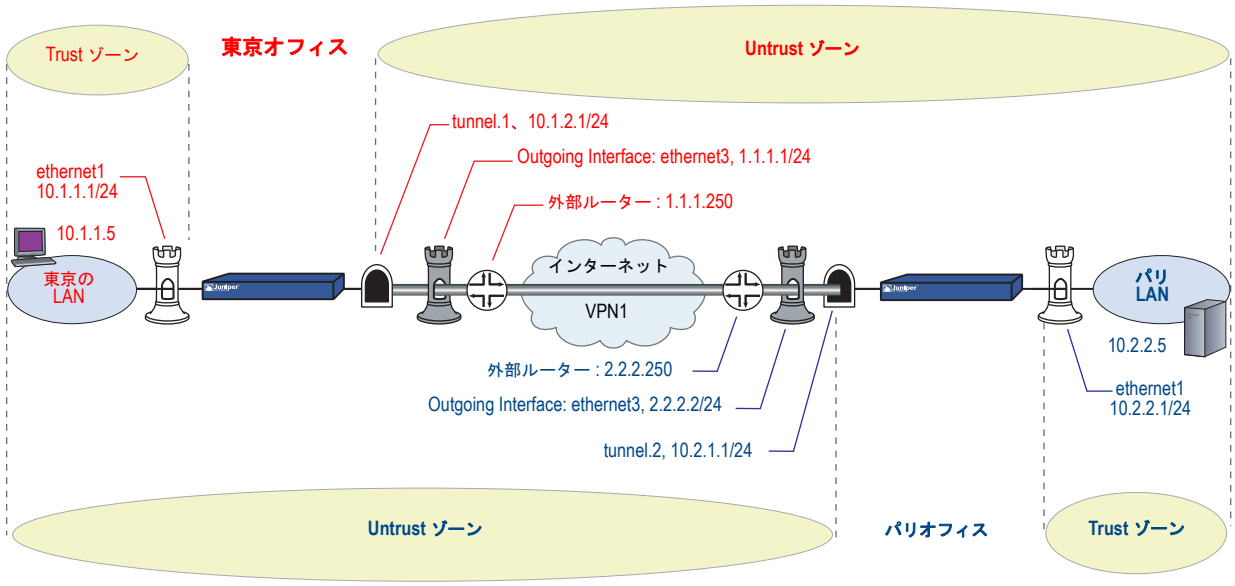
注 : ダイヤルアップクライアントのルートベース VPN 構成の例については、164 ページの「ルートベース ダイヤルアップ VPN、動的ピア」を参照してください。

パケットフロー : サイトツーサイト VPN

IPSec トンネルの作成に関係したコンポーネントの相互関連をよりよく理解するため、このセクションではトンネルを経由するパケットフローの処理について、セキュリティデバイスがアウトバウンド VPN トラフィックを送信する場合と、インバウンド VPN トラフィックを受信した場合の両方を説明します。ルートベース VPN の処理を説明した後に、ポリシーベース VPN のフローの場合の 2 つの相違点を説明した追記があります。

東京に本社を置くある会社は、パリの支社をちょうど開店したばかりで、IPSec トンネルを経由して 2 つのサイトを接続する必要があります。トンネルでは AutoKey IKE、ESP プロトコル、暗号化に AES、事前共有鍵を使用した認証に SHA-1 を使用し、再生防止チェックを使用可能にしています。セキュリティデバイスは各サイトを NAT モードで保護しており、全ゾーンが trust-vr ルーティングドメインにあります。アドレスは、61 ページの図 21 に表示されています。

図 21: サイト間 VPN トンネル



東京の LAN にある 10.1.1.5/32 から IPSec トンネルを経由してパリの LAN 10.2.2.5/32 へ送信されるパケットは、次のサブセクションで説明されているパスを通ります。

東京 (イニシエータ)

1. 10.1.1.5 にあるホストが宛先 10.2.2.5 のパケットを 10.1.1.1 へ送信します。10.1.1.1 は ethernet1 の IP アドレスで、ホストの TCP/IP 設定で構成されたデフォルトゲートウェイです。

2. Trust ゾーンにバインドされた ethernet1 にパケットが到着します。

3. Trust ゾーンの IP スプーフィング検出など、SCREEN オプションを使用可能にしている場合、セキュリティデバイスはこの時点で SCREEN モジュールをアクティブにします。SCREEN モジュールによるチェックの結果は、次の 3 つのうちいずれかになります。

   - SCREEN 機構が異常な動きを検出し、パケットを拒否する場合、NetScreen デバイスはパケットを破棄し、イベントログにその旨を記録します。
   - イベントを記録するがパケットを拒否はしない設定の場合 : ethernet1 用の SCREEN カウンターリストにイベントを記録し、次に進みます。
   - SCREEN 機構が異常な動きを検出しない場合、セキュリティデバイスはそのまま次の段階に進みます。

   Trust ゾーンに対してどの SCREEN オプションも有効にしていなかった場合は、セキュリティデバイスは何もせずに次に進みます。

4. セッションモジュールは、パケットを既存のセッションと一致させるためセッションルックアップを実行します。

   パケットが既存のセッションと一致しない場合は、先頭パケットに対し、以下のような処理を行います。

   逆に該当するセッションが見つかれば、既存のセッションエントリの情報を参照して、パケットを高速処理します。高速処理の場合、ルートルックアップとポリシールックアップは飛ばします。このセッションの先頭パケットを処理した段階で必要な情報は得られているので、省略しても構わないのです。

5. アドレスマッピングモジュールが、MIP (マップ IP) の設定で宛先 IP アドレス 10.2.2.5 が使われていないかどうかを確認します。10.2.2.5 が MIP で使われていなければ、次に進みます。(MIP、VIP、または NAT-dst [宛先アドレス変換] が関係するパケット処理の詳細について、**8**-29 ページの「NAT-Dst のパケットフロー」を参照してください)。

6. 宛先ゾーンを判断するには、ルートモジュールが 10.2.2.5 のルートルックアップを実行します (ルートモジュールは ingress インターフェースを使って、ルートルックアップにどの仮想ルーターを使うか判断します。)「vpn1」という名前の VPN トンネルにバインドされた tunnel.1 インターフェースを経由して 10.2.2.5 へトラフィックを導くルートエントリを見つけます。トンネルインターフェースは Untrust ゾーンにあります。ingress および egress インターフェースを判断することにより、セキュリティデバイスはソースおよび宛先ゾーンを判断しまた。この時点でポリシールックアップを実行できます。

7. ポリシーエンジンは、(対応する ingress および egress インターフェースで判断された) Trust ゾーン、Untrust ゾーンについて、条件に合致するポリシーを検索します。ソースアドレスとゾーン、宛先アドレスとゾーン、およびサービスを一致させるポリシーで指定されたアクションは許可されています。

8. IPSec モジュールは、リモートピアに関連付けられたアクティブなフェーズ 2 SA (セキュリティアソシエーション) が存在しているか確認します。フェーズ 2 SA チェックの結果は、次のいずれかになります。

   - IPSec モジュールがそのピアに関連付けられたアクティブなフェーズ 2 SA を発見した場合、手順 10. へ進みます。
   - IPSec モジュールがそのピアに関連付けられたアクティブなフェーズ 2 SA を発見しなかった場合、パケットをドロップし、IKE モジュールを起動します。

9. IKE モジュールは、リモートピアに関連付けられたアクティブなフェーズ 1 SA が存在しているか確認します。フェーズ 1 SA チェックの結果は、次のいずれかになります。

   - IKE モジュールがそのピアに関連付けられたアクティブなフェーズ 1 SA を発見した場合、この SA を使用してフェーズ 2 SA をネゴシエートします。
   - IKE モジュールがそのピアに関連付けられたアクティブなフェーズ 1 SA を発見しなかった場合、メインモードでフェーズ 1 のネゴシエーションを開始し、それからフェーズ 2 のネゴシエーションを行います。

10. IPSec モジュールはパケットに ESP ヘッダーを入れた後に外部 IP ヘッダーを入れます。ソース IP アドレスには出力インターフェースで指定されたアドレスを使用し、1.1.1.1 を外部ヘッダーに入れます。宛先 IP アドレスにはリモートゲートウェイで指定されたアドレスを使用し、2.2.2.2 を外部ヘッダーに入れます。続いて、ペイロードから元の IP ヘッダーにある次のヘッダーフィールドまでパケットを暗号化します。それから ESP トレーラから ESP ヘッダーまでパケットを認証します。

11. セキュリティデバイスは、暗号化と認証が行われた宛先 2.2.2.2 のパケットを、出力インターフェース（ethernet3）を経由して 1.1.1.250 の外部ルーターへ送信します。

パリ (受領者)

1. 2.2.2.2 にパケットが到着します。2.2.2.2 は Untrust ゾーンにバインドされたインターフェースである ethernet3 の IP アドレスです。

2. IPSec モジュールは外部パケットヘッダーに含まれた SPI、宛先 IP アドレス、および IPSec プロトコルを使用して、開始ピアと関連付けられたアクティブなフェーズ 2 SA、およびパケットの認証と解読を行う鍵がないか検索します。フェーズ 2 SA チェックの結果は、次のいずれかになります。

   - IPSec モジュールがそのピアに関連付けられたアクティブなフェーズ 2 SA を発見した場合、手順 4 へ進みます。
   - IPSec モジュールはピアに関連付けられたアクティブなフェーズ 2 SA を発見しなかったが、SPI ではなくソース IP アドレスを使用して非アクティブなフェーズ 2 SA を検索できた場合は、パケットをドロップしてイベントログにエントリを作成し、不正な SPI を受信したことを開始ピアに通知します。
   - IPSec モジュールがそのピアに関連付けられたアクティブなフェーズ 2 SA を発見しなかった場合、パケットをドロップし、IKE モジュールを起動します。

3. IKE モジュールは、リモートピアに関連付けられたアクティブなフェーズ 1 SA が存在しているか確認します。フェーズ 1 SA チェックの結果は、次のいずれかになります。

   - IKE モジュールがそのピアに関連付けられたアクティブなフェーズ 1 SA を発見した場合、この SA を使用してフェーズ 2 SA をネゴシエートします。
   - IKE モジュールがそのピアに関連付けられたアクティブなフェーズ 1 SA を発見しなかった場合、メインモードでフェーズ 1 のネゴシエーションを開始し、それからフェーズ 2 のネゴシエーションを行います。

4. IPSec モジュールが再生防止チェックを実行します。このチェックの結果は、次のいずれかになります。

   - すでに受信したシーケンス番号が検出され、パケットが再生防止チェックにパスしなかった場合、パケットをドロップします。
   - パケットが再生防止チェックをパスした場合は、次の段階に進みます。

5. IPSec モジュールがパケットの認証を試みます。認証チェックの結果は、次のいずれかになります。

   - パケットが認証チェックにパスしなかった場合、パケットをドロップします。
   - パケットが認証チェックをパスした場合は、次の段階に進みます。

6. IPSec モジュールはフェーズ 2 SA と鍵を使用してパケットを解読し、元のソースアドレス (10.1.1.5) と最終宛先 (10.2.2.5) を明らかにします。パケットは tunnel.1 にバインドされた vpn1 を経由して送信されたことが判明します。この時点から、セキュリティデバイスはパケットの ingress インターフェースが ethernet3 ではなく tunnel.1 であるかのように扱います。この時点で再生防止スライドウィンドウも調整します。

7. Untrust ゾーンに対して SCREEN オプションが有効になっていれば、セキュリティデバイスはこの時点で SCREEN モジュールをアクティブにします。SCREEN モジュールによるチェックの結果は、次の 3 つのうちいずれかになります。

   - SCREEN 機構が異常な動きを検出し、パケットを拒否する場合、NetScreen デバイスはパケットを破棄し、イベントログにその旨を記録します。
   - イベントを記録するがパケットを拒否はしない設定の場合 : ethernet3 用の SCREEN カウンターリストにイベントを記録し、次に進みます。
   - SCREEN 機構が異常な動きを検出しない場合、セキュリティデバイスはそのまま次の段階に進みます。

8. セッションモジュールは、パケットを既存のセッションと一致させるためセッションルックアップを実行します。それから先頭パケットの処理か高速処理のどちらかを実行します。

逆に該当するセッションが見つかれば、既存のセッションエントリの情報を参照して、パケットを高速処理します。高速処理の場合、最後の 2 つの手順 (パケットの暗号化と転送) に進みます。このセッションの先頭パケットを処理した段階で必要な情報は得られているので、省略しても構わないのです。

9. アドレスマッピングモジュールが、MIP (マップ IP) または仮想 IP (VIP) の設定で宛先 IP アドレス 10.2.2.5 が使われていないかどうかを確認します。10.2.2.5 が MIP や VIP で使われていなければ次に進みます。

10. ルートモジュールは最初に ingress インターフェースを使って、ルート検索に使用する仮想ルーターを判断します。この場合は trust-vr を使用します。それから trust-vr で 10.2.2.5 のルートルックアップを実行し、ethernet1 を経由してアクセスが行われたことを発見します。ingress インターフェース (tunnel.1) と egress インターフェース (ethernet1) を判断することにより、セキュリティデバイスはソースゾーンと宛先ゾーンを判断できます。tunnel.1 インターフェース は Untrust ゾーンにバインドされ、ethernet1 は Trust ゾーンにバインドされています。この時点でセキュリティデバイスはポリシールックアップを実行できます。

11. ポリシーエンジンが Untrust ゾーンから Trust ゾーンへのポリシーリストをチェックし、アクセスを許可するポリシーを見つけます。

12. セキュリティデバイスは、パケットを ethernet1 を経由して宛先の 10.2.2.5 に送信します。

追記 : ポリシーベース VPN

ポリシーベース VPN 構成のパケットフローは、ルートルックアップとポリシールックアップの 2 点で、ルートベース VPN 構成と異なります。

東京 (イニシエータ)

アウトバウンドのパケットフローのフェーズ 1 は、ルートルックアップとそれに続くポリシールックアップが行われるまで、ルートベース VPN 構成でもポリシーベース VPN 構成でも同じです。

- **ルートルックアップ :** 宛先ゾーンを判断するには、ルートモジュールが 10.2.2.5 のルートルックアップを実行します。特定のアドレスのエントリが見つからないため、ルートモジュールは Untrust ゾーンにバインドされている ethernet3 のルートを経由してパケットを送信します。ingress および egress インターフェースを判断することにより、セキュリティデバイスはソースおよび宛先ゾーンを判断しました。この時点でポリシールックアップを実行できます。

- **ポリシールックアップ :** ポリシーエンジンは Trust ゾーンと Untrust ゾーンの間のポリシールックアップを実行します。ルックアップはソースアドレスとゾーン、宛先アドレスとゾーン、およびサービスを一致させ、vpn1 という名前の VPN トンネルを参照するポリシーを見つけます。

セキュリティデバイスは、パケットを ethernet1 を経由して宛先の 10.2.2.5 に送信します。

パリ (受領者)
受領者側のインバウンドパケットフローの段階は、ルートベース VPN 構成もポリシーベース VPN 構成もほぼ同じです。ただし、トンネルがトンネルインターフェースではなくトンネルゾーンにバインドされている点が異なります。セキュリティデバイスはパケットが vpn1 を経由して来たことを認識します。vpn1 は Untrust-Tun トンネルゾーンにバインドされ、そのキャリアゾーンは Untrust ゾーンです。ルートベース VPN とは異なり、tunnel.1 ではなく ethernet3 が解読されたパケットの ingress インターフェースとして認識されます。

パケット解読の完了後、フローが変化します。この時点で、ルートルックアップとポリシールックアップが異なります。

- **ルートルックアップ :** ルートモジュールが 10.2.2.5 のルートルックアップを実行し、Trust ゾーンにバインドされた ethernet1 を経由してアクセスが行われたことを発見します。セキュリティデバイスは、Untrust ゾーンがソースゾーンであることを認識し (vpn1 が Untrust-Tun トンネルゾーンにバインドされており、そのキャリアゾーンが Untrust ゾーンのため)、egress インターフェースに基づいて宛先ゾーンを判断する (ethernet1 は Trust ゾーンにバインドされています) ことにより、vpn1 を参照する Untrust ゾーンから Trust ゾーンへのポリシーをチェックできます。

- **ポリシールックアップ :** ポリシーエンジンが Untrust ゾーンから Ｔｒｕｓｔ ゾーンへのポリシーリストをチェックし、10.2.2.5 へのアクセスを許可する、vpn1 という名前の VPN トンネルを参照するポリシーを見つけます。

その宛先に向けてパケットを転送します。

トンネル構成のガイド

このセクションでは、VPN トンネルを構成するためのガイドラインを説明します。IPSec VPN トンネルを構成する際には、以下の点を考慮に入れてください。

- ScreenOS では、フェーズ 1 ネゴシエーションの提案を 4 つまで、フェーズ 2 ネゴシエーションの提案も 4 つまでサポートしています。1 つのピアは、他のピアから提供されたフェーズ 1 提案と、フェーズ 2 提案を最低 1 つずつ受け入れるように構成する必要があります。フェーズ 1 と フェーズ 2 の IKE ネゴシエーションの詳細については、8 ページの「トンネルネゴシエーション」を参照してください。

- 認証に証明書を使用する場合、セキュリティデバイスに複数のローカル証明書がロードされているときは、各 VPN トンネル構成でどの証明書を使用するか指定する必要があります。証明書に関する詳細については、19 ページの「公開鍵暗号化」を参照してください。

- 基本的なポリシーベース VPN の場合 :

  - 定義済みのアドレス「Any」ではなく、ユーザー定義のアドレスをポリシーで使用します。

  - VPN の両端で構成されたポリシーで指定されているアドレスとサービスは一致していなければなりません。

  - 双方向性 VPN トラフィックには対称型ポリシーを使用します。

- 両方のピアのプロキシ ID は一致している必要があります。このことは、両方のピアのプロキシ ID で指定されたサービスは同じであり、一方のピアで指定されたローカル IP アドレスは他方のピアで指定されたリモート IP アドレスと同じであることを意味します。

注 : プロキシ ID は、ローカル IP アドレス、リモート IP アドレス、およびサービスの 3 つの部分から成る集合です。

- ルートベース VPN 構成のプロキシ ID はユーザーが構成できます。
- ポリシーベース VPN 構成では、ポリシーリストの中でその VPN トンネルを参照しているポリシーによって指定されたソースアドレス、宛先アドレス、およびサービスから、セキュリティデバイス (デフォルト) がプロキシ ID を導出します。ユーザーがポリシーベース VPN のプロキシ ID を定義して、導出されたプロキシ ID を置き換えることもできます。

プロキシ ID を必ず一致させる最も簡単な方法は、ローカルアドレスに 0.0.0.0/0、リモートアドレスに 0.0.0.0/0、サービスに「Any」を使用することです。プロキシ ID を使用してアクセス制御を行う代わりに、ポリシーを使用して VPN を行き来するトラフィックを制御します。ユーザーが構成可能なプロキシ ID を使用した VPN 構成の例については、77 ページの「サイト間 VPN (仮想プライベートネットワーク)」でルートベース VPN の例を参照してください。

注 : リモートアドレスがダイヤルアップ VPN クライアントの仮想内部アドレスの場合は、プロキシ ID のリモート IP アドレスとネットマスクに 255.255.255.255/32 を使用してください。

- ピアのプロキシ ID 設定が一致している限り、一方のピアがルートベース VPN を定義しており、他方のピアがポリシーベース VPN を定義していても問題ありません。ピア 1 がポリシーベース VPN 構成を使用しており、ピア 2 がルートベース VPN 構成を使用している場合、ピア 2 はピア 1 のポリシーから導出されたプロキシ ID と一致するプロキシ ID を定義する必要があります。ピア 1 が DIP プールを使用して NAT-src (ソースネットワークアドレス変換) を実行する場合、ピア 2 のプロキシ ID のリモートアドレスとしてその DIP プールのアドレスとネットマスクを使用します。たとえば、次のように設定できます。

DIP プールが次のアドレスの場合	プロキシ ID で次のアドレスを使用
1.1.1.8 - 1.1.1.8	1.1.1.8/32
1.1.1.20 - 1.1.1.50	1.1.1.20/26
1.1.1.100 - 1.1.1.200	1.1.1.100/25
1.1.1.0 - 1.1.1.255	1.1.1.0/24

NAT-src および NAT-dst とプロキシ ID を使用する場合の詳細については、137 ページの「アドレスがオーバーラップする VPN サイト」を参照してください。

注： ピア 1 でピア 2 のプロキシ ID と一致するプロキシ ID を定義することもできます。ピア 1 のユーザー定義プロキシ ID は、セキュリティデバイスがポリシーコンポーネントから導出するプロキシ ID に優先します。

- プロキシ ID は単一のサービスか全サービスをサポートするため、サービスグループを参照するポリシーベース VPN から導出されたプロキシ ID のサービスは「Any」とみなされます。

- 両方のピアが静的 IP アドレスを持っている場合、各ピアはその IP アドレスであるデフォルトの IKE ID を使用できます。ピアまたはダイヤルアップユーザーが動的に割り当てられた IP アドレスを持っている場合、そのピアまたはユーザーは他のタイプの IKE ID を使用する必要があります。動的ピアには FQDN が適しており、ダイヤルアップユーザーには U-FQDN (E メールアドレス) が適しています。事前共有鍵や証明書では FQDN と U-FQDN IKE ID の両タイプを使用できます (証明書の SubjectAltName フィールドに FQDN または U-FQDN が表示されている場合)。証明書を使用する場合、動的ピアやダイヤルアップユーザーは ASN1-DN の全部や一部を IKE ID として使用することもできます。

ルートベース VPN (仮想プライベートネットワーク) のセキュリティ検討事項

ルートの変更はポリシーベース VPN には影響を及ぼしませんが、ルートベース VPN に対しては別です。セキュリティデバイスは、静的ルートと動的ルーティングプロトコルを組み合わせたルートベース VPN トンネルを経由して、パケットを送信することができます。ルートを変更しない限り、セキュリティデバイスは常に、ルートベース VPN トンネルにバインドされたトンネルインターフェースを宛先とするパケットを暗号化して、転送します。

ただし、ルートベース VPN トンネル構成で VPN 監視を使用する場合、トンネルの状態はアップからダウンへと変化することがあります。この変更が起こると、そのトンネルにバインドされたインターフェースを参照するすべてのテーブルエントリは、非アクティブに変化します。そしてセキュリティデバイスは、本来暗号化されてそのトンネルインターフェースにバインドされたトンネルを介して送信される予定であったトラフィックに対してルートルックアップを行う際に、トンネルインターフェースを参照するルートを回避し、その次に長い距離にわたって一致するルートを検索します。検出されたルートが、デフォルトルートのこともあります。そしてセキュリティデバイスは、このルートを使用して、暗号化されていないトラフィック (つまり、*クリアテキスト*または*プレーンテキスト*) を、非トンネルインターフェースを介して公開 WAN に送信します。

元はクリアテキストで VPN トンネルを介して公開 WAN に送信する予定だったトラフィックを再ルーティングしないようにするには、そうしたトラフィックを別のトンネルに再ルーティングするか、リース回線に再ルーティングするか、または単純にドロップするように、以下のいずれかの対処法を使ってデバイスを設定します。

- 69 ページの「Null ルート」(トンネルインターフェースへのルートが非アクティブになった場合、トラフィックをドロップします)

- 70 ページの「ダイヤルアップまたはリース回線」(トンネルインターフェースへのルートが非アクティブになった場合、代わりのセキュアパスにトラフィックを再ルーティングします)

- 74 ページの「おとりトンネルインターフェース」(トンネルインターフェースへのルートが非アクティブになった場合、トラフィックをドロップします)
- 74 ページの「トンネルインターフェースの仮想ルーター」(トンネルインターフェースへのルートが非アクティブになった場合、トラフィックをドロップします)
- 75 ページの「別のトンネルへの再ルーティング」(トンネルインターフェースへのルートが非アクティブになった場合、代わりの VPN トンネルにトラフィックを再ルーティングします)

Null ルート

VPN トンネルの状態が「停止」に変わると、セキュリティデバイスはそのトンネルインターフェースを参照しているルートをすべて「非アクティブ」に変更します。トンネルインターフェースへのルートが使用不可となり、次の候補がデフォルトルートの場合 (例)、セキュリティデバイスは、元は VPN トンネルを介す予定だったトラフィックを転送するために、デフォルトルートを使用します。ルートが変更された場合に、公開 WAN にプレーンテキストでトラフィックを送信することを防ぐために、Null ルートを使用することができます。Null ルートはトンネルインターフェースを通るルートと同じ宛先アドレスをターゲットとしていますが、その代わりに、Null インターフェースへのトラフィックを示しています。Null インターフェースとは、送信されたトラフィックをドロップする論理インターフェースです。Null ルートには、トンネルインターフェースで使用するルートよりも高いメトリック値 (0 から離れた値) を指定して ANull ルートの優先順位が低くなるようにします。

注 : ScreenOS 5.1.0 より前のリリースでは、Null インターフェースはサポートされていません。ただし、おとりトンネルインターフェースを使用して、同様のことを実現できます。詳細については、74 ページの「おとりトンネルインターフェース」を参照してください。

例えば、tunnel.1 を経由してリモート LAN に向かう IP アドレス 10.2.2.0/24 のルートを作成すると、メトリックのデフォルト値 1 を自動的に受信します。

```
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
get route
…
Dest-Routes for <trust-vr> (4 エントリ )
```

	ID	IP-Prefix	インターフェース	ゲートウェイ	P	Pref	Mtr	Vsys
*	3	0.0.0.0/0	eth3	1.1.1.250	S	20	1	ルート
*	2	1.1.1.0/24	eth3	0.0.0.0	C	0	0	ルート
*	1	10.1.1.0/24	eth1	0.0.0.0	C	0	0	ルート
*	4	**10.2.2.0/24**	**tun.1**	0.0.0.0	S	20	**1**	ルート

上のルーティングテーブルで、アスタリスク (*) はルートがアクティブであることを、「S」は「静的ルート」を、「C」は「接続したルート」であることを表しています。

上のルーティングテーブルでは、セキュリティデバイスにはサブネット 10.2.2.0/24 にある任意のアドレスに向かうルートが 2 つあります。1 番目の選択肢は、そのアドレスと最も長く一致している 4 番のルートです。2　番目の選択肢は、デフォルトルート (0.0.0.0/0) です。

Null インターフェースを経由する 10.2.2.0/24 への別のルートを追加して、1 以上の値を割り当てると、そのルートはサブネット 10.2.2.0/24 にある任意のアドレスへの 2 番目のルーティングの選択肢となります。tunnel.1 を介した 10.2.2.0/24 へのルートが非アクティブとなると、セキュリティデバイスは Null インターフェースへのルートを使用します。セキュリティデバイスは、そのインターフェースに 10.2.2.0/24 のトラフィックを転送して、ドロップします。

```
set vrouter trust-vr route 10.2.2.0/24 interface null metric 10
get route
…
Dest-Routes for <trust-vr> (5 エントリ )
```

	ID	IP-Prefix	インターフェース	ゲートウェイ	P	Pref	Mtr	Vsys
*	3	0.0.0.0/0	eth3	1.1.1.250	S	20	1	ルート
*	2	1.1.1.0/24	eth3	0.0.0.0	C	0	0	ルート
*	1	10.1.1.0/24	eth1	0.0.0.0	C	0	0	ルート
	4	**10.2.2.0/24**	**tun.1**	0.0.0.0	S	20	**1**	ルート
*	5	**10.2.2.0/24**	**null**	0.0.0.0	S	20	**10**	ルート

上のルーティングテーブルでは、tunnel.1 を通る 10.2.2.0/24 へのルートが非アクティブになっています (1 番左の列にアスタリスクがないことで示されています)。そのため、セキュリティデバイスは、宛先アドレスと最も長く一致する次のルートを検索して、5 番のルートを見つけます (5 番の次の選択肢は、ID 3 のデフォルトルートです)。そして、セキュリティデバイスは、10.2.2.0/24 のトラフィックを Null インターフェースに転送し、それをドロップします。その結果、tunnel.1 を使用しているルートが非アクティブになると、セキュリティデバイスは 3 番のルートを使用せずに 10.2.2.0/24 のトラフィックをドロップして、1.1.1.250 におけるルーターへのクリアテキストとして ethernet3 を転送します。

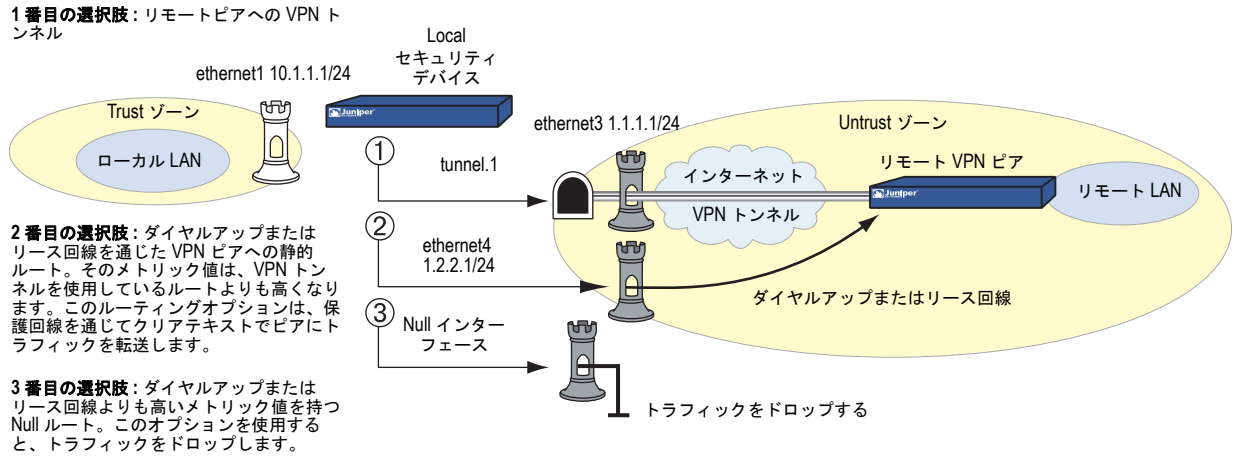
ダイヤルアップまたはリース回線

リモートピアへのトンネルが非アクティブになったときに、そのピアへのトラフィックをドロップしない場合は、ダイヤルアップまたはリース回線を流れるピアに、代わりのルートを追加することができます。この代替ルートは、VPN トンネルを通るルートにあるものと同じ宛先 IP アドレスを使用していますが、egress インターフェースは異なり、メトリック値も低くなっています。VPN トンネルを通るルートが非アクティブになると、セキュリティデバイスはダイヤルアップまたはリース回線を通ってリモートピアに向かうトラフィックを再ルーティングします。

次の選択肢となるルートとしてダイヤルアップまたはリース回線を使用している場合、1 番目と 2 番目の選択肢のルートが同時に非アクティブとなる可能性があります。そのような場合、セキュリティデバイスは 3 番目の選択肢を使用しますが、それがデフォルトルートかもしれません。そうした状況を考慮して、ダイ

ヤルアップまたはリース回線のルートを 2 番目の選択肢に、そして Null ルートを 3 番目の選択肢に設定してください (69 ページの「Null ルート」を参照)。図 22 は、ルーティングフェールオーバーを処理するこうしたオプションが一緒になってどのように動作するかを示しています。

図 22: VPN トラフィックのルーティングフェールオーバー代替ルート



リース回線または Null ルートへの VPN フェールオーバー

この例では、デバイス A の背後にある支社から、デバイス B の背後にある企業ネットワークまで、セキュア VPN 接続を通じてトラフィックを送信します。トンネルが失敗した場合は、リース回線を通じて企業オフィスまでトラフィックを送信します。VPN トンネルとリース回線が両方失敗した場合、デバイス A はトラフィックをクリアテキストでインターネットに送信するのではなく、ドロップします。

10.2.2.0/24 に向かうルートを デバイス A 上に 3 つ作成して、それぞれに異なるメトリック値を割り当てます。

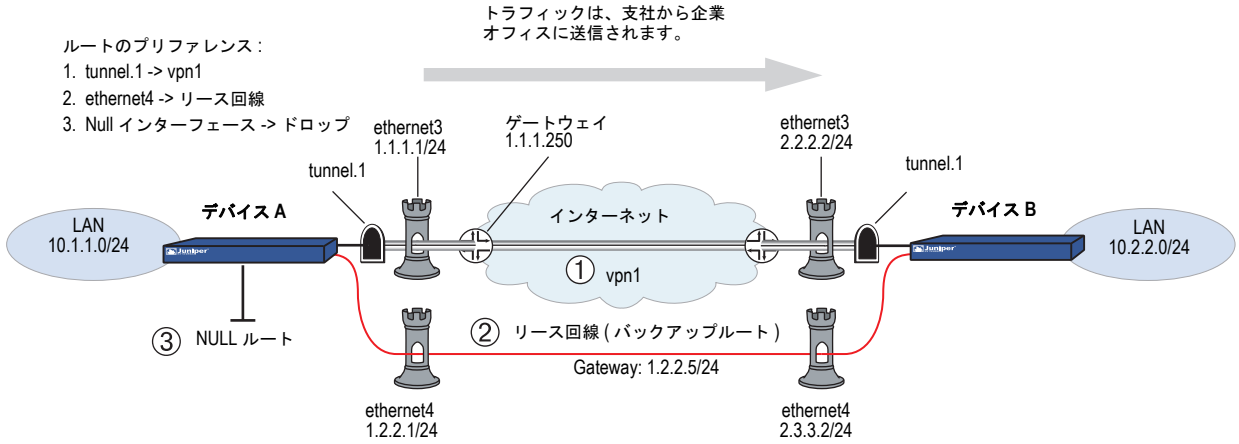
- **優先ルート** - vpn1 にバインドされた tunnel.1 を使用します (メトリック値 = 1)。
- **2 次ルート** - ethernet4 と 1.2.2.5 におけるゲートウェイを使用して、リース回線を使用します (メトリック値 = 2)。
- **3 次ルート** - Null インターフェースを使用してトラフィックをドロップします (メトリック値 = 10)。

優先ルートを作成すると、静的ルートにはデフォルトのメトリック値 (1) を使用します。メトリック値 2 は 2 次ルート、つまりリース回線を通るバックアップルートに割り当てます (72 ページの図 23 で示す部分)。そのメトリック値は、VPN トンネルを使用している優先ルートよりも低くなります。セキュリティデバイスは、VPN トンネルを通る優先ルートが失敗しない限り、2 次ルートを使用しません。

最後に、メトリック値 10 の NULL ルートを追加します。優先ルートが失敗し、次に 2 次ルートも失敗すると、セキュリティデバイスは全パケットをドロップします。すべてのセキュリティゾーンは、trust-vr ルーティングドメインに存在します。

注： この例では、デバイス A 上の 4 つのルート設定 (フェールオーバー 3 つ ＋ デフォルトルート) だけを示しています。

図 23: リース回線から Null ルートへと移行するルーティングフェールオーバー



WebUI (デバイス A)

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250
Metric: 1

Network > Routing > Routing Entries > trust-vr New: 以下を入力し **OK** をクリックします。

Network Address/Netmask: 10.2.2.0/24
Gateway: (選択)
Interface: tunnel.1
Gateway IP Address: 0.0.0.0
Metric: 1

Network > Routing > Routing Entries > trust-vr New: 以下を入力し **OK** をクリックします。

Network Address/Netmask: 10.2.2.0/24
Gateway: (選択)
Interface: ethernet4
Gateway IP Address: 1.2.2.5
Metric: 2

Network > Routing > Routing Entries > trust-vr New: 以下を入力し **OK** をクリックします。

Network Address/Netmask: 10.2.2.0/24
Gateway: (選択)
Interface: Null
Gateway IP Address: 0.0.0.0
Metric: 10

CLI (デバイス A)

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 10.2.2.0/24 interface ethernet4 gateway 1.2.2.5 metric
    2
set vrouter trust-vr route 10.2.2.0/24 interface null metric 10
save
```

新しいルートがあることは、**get route** コマンドを実行することにより確認できます。

```
device-C-> get route


IPv4 Dest-Routes for <untrust-vr> (0 entries)
---------------------------------------------------------------------------------
H: Host C: Connected S: Static A: Auto-Exported
I: Imported R: RIP P: Permanent D: Auto-Discovered
iB: IBGP eB: EBGP O: OSPF E1: OSPF external type 1
E2: OSPF external type 2


IPv4 Dest-Routes for <trust-vr> (7 entries)
---------------------------------------------------------------------------------
   ID          IP-Prefix      Interface         Gateway   P Pref    Mtr      Vsys
---------------------------------------------------------------------------------
*   8          0.0.0.0/0         eth1/1     10.100.37.1   S   20      1     Root
*   7         1.1.1.1/32         eth1/2         0.0.0.0   H    0      0     Root
*   3     192.168.1.1/32            mgt         0.0.0.0   H    0      0     Root
*   2     192.168.1.0/24            mgt         0.0.0.0   C    0      0     Root
*   4     10.100.37.0/24         eth1/1         0.0.0.0   C    0      0     Root
*   5   10.100.37.170/32         eth1/1         0.0.0.0   H    0      0     Root
*   6         1.1.1.0/24         eth1/2         0.0.0.0   C    0      0     Root
```

ID 5 のルートテーブルエントリは、tunnel へ向かう 10.2.2.0/24 のトラフィックを表し、VPN トンネルを経由します。トラフィックの優先ルートは、10.2.2.0 ネットワークに到着します。そのトンネルが失敗すると、2 番目の最良ルートは、1.2.2.5 にあるゲートウェイを経由するリース回線上の エントリ 6 となります。ルートエントリ 6 の接続に失敗すると、ルートエントリ 7 が次の最良ルートとなります。そして、セキュリティデバイスは、10.2.2.0/24 のトラフィックを Null インターフェースに誘導し、それをドロップします。

おとりトンネルインターフェース

VPN トンネルから Null インターフェースへのトラフィックがフェールオーバーする (そしてドロップする) 代わりに、機能しないトンネルインターフェースを使用して、同様のことを実現することができます。

注 : ScreenOS 5.1.0 より前のリリースでは、Null インターフェースはサポートされていません (69 ページの「Null ルート」を参照)。ただし、おとりトンネルインターフェースを使用して、同様のことを実現できます。

おとりトンネルインターフェースを設定するには、次の手順を実行します。

1. 第 2 トンネルインターフェースを作成し、それを VPN トンネルにバインドしないようにします。実際には、第 1 トンネルインターフェースと同じ仮想ルーティングドメイン内に存在するトンネルゾーンにバインドします。

注 : トンネルインターフェースがトンネルゾーンにバインドされていれば、その状態は常にアップとなります。

2. この第 2 トンネルインターフェースを使用して、同じ宛先への第 2 ルートを定義し、それに優先ルートよりも高いメトリック (0 から離れた値) を割り当てます。

   機能しているトンネルインターフェースの状態がアップからダウンに変化し、そのインターフェースを参照するルートテーブルエントリが非アクティブになる場合は、以降のすべてのルートルックアップは、機能していないトンネルインターフェースへのこの第 2 ルートを検出します。セキュリティデバイスはトラフィックを第 2 トンネルインターフェースに転送しますが、このインターフェースは VPN トンネルにバインドされていないために、デバイスはトラフィックをドロップします。

トンネルインターフェースの仮想ルーター

VPN トンネルを通るルートが非アクティブとなり、元はそのトンネルを通過してデフォルトルートに行くはずだったトラフィックがフェールオーバーすることを防ぐために、VPN トラフィック専用の特別な仮想ルーティングドメインを作成することができます。これを設定するには、次の手順を実行します。

1. トンネルインターフェースにポイントされたすべてのルートに対して使用する別の仮想ルーターを作成し、これにたとえば、「VR-VPN」のように名前をつけます。

2. セキュリティゾーンを作成し、これにたとえば、「VPN zone」という名前をつけて VR-VPN にバインドします。

3. すべてのトンネルインターフェースを VPN ゾーンにバインドし、さらに VPN トンネルを介してアクセスするリモートサイトのすべてのアドレスをこのゾーンに配置します。

4. その他のすべての仮想ルーター内に、暗号化しトンネルを介して送信するトラフィックの VR-VPN へ静的ルートを構成します。必要であれば、複合化したトラフィックの VR-VPN からその他の仮想ルーターへの静的ルートを定義します。このようなルートは、インバウンド VPN トラフィックがリモートサイトから起動される場合に、このトラフィックがトンネルを経由するのを許可するために必要となります。

   トンネルインターフェースの状態がアップからダウンへ変化しても、セキュリティデバイスは VR-VPN にトラフィックを転送しますが、このインターフェースの状態は非アクティブであり、他にマッチングするルートが存在しないため、セキュリティデバイスはトラフィックをドロップします。

別のトンネルへの再ルーティング

同じリモートピアへ向かう VPN トンネルを 2 つ以上設定することができます。あるトンネルが停止した場合、セキュリティデバイスは別の VPN トンネルを通るようトラフィックを再ルーティングできます。冗長 VPN トンネルの設定とその例については、以下を参照してください。

- **11-**51 ページの「アクティブトンネルからバックアップトンネルへのフェールオーバー」
- **11-**70 ページの「2 系統のアクティブなトンネルの構成」
- **11-**77 ページの「トンネルのフェールオーバーウェイトの構成」

第 4 章

サイト間 VPN (仮想プライベートネットワーク)

本章では、2 台の Juniper Networks セキュリティデバイス間でサイト間仮想プライベートネットワーク (VPN) を構成する方法について説明します。また、ルートベースおよびポリシーベース VPN トンネルを検証し、トンネルを設定するときに考慮する必要がある様々な要素、およびいくつかの例を提供します。

本章のセクションは、以下のようになります。

- 78 ページの「サイト間 VPN 構成」
  - 84 ページの「ルートベースのサイト間 VPN、AutoKey IKE」
  - 93 ページの「ポリシーベースのサイト間 VPN、AutoKey IKE」
  - 99 ページの「ルートベースのサイト間 VPN、動的ピア」
  - 107 ページの「ポリシーベースのサイト間 VPN、動的ピア」
  - 116 ページの「ルートベースのサイト間 VPN、手動鍵」
  - 122 ページの「ポリシーベースのサイト間 VPN、手動鍵」
- 127 ページの「FQDN を使用した動的 IKE ゲートウェイ」
  - 128 ページの「エイリアス」
  - 129 ページの「FQDN を使用した AutoKey IKE ピアを設定する」
- 137 ページの「アドレスがオーバーラップする VPN サイト」
- 148 ページの「透過モード VPN」

サイト間 VPN 構成

IPSec VPN トンネルは、2 つのゲートウェイの間に存在していて、それぞれのゲートウェイが IP アドレスを必要とします。両方のゲートウェイが固定 IP アドレスを持っているときは、次のタイプのトンネルを構成することができます。

- サイト間 VPN、AutoKey IKE トンネル (事前共有鍵あるいは証明書つき)
- サイト間 VPN、手動鍵トンネル

ゲートウェイの 1 つが固定アドレスを持ち、もう 1 つのゲートウェイが動的に割り当てられたアドレスを持っている場合には、次のタイプのトンネルを構成することができます。

- 動的ピアサイト間 VPN、AutoKey IKE トンネル (事前共有鍵あるいは証明書つき)

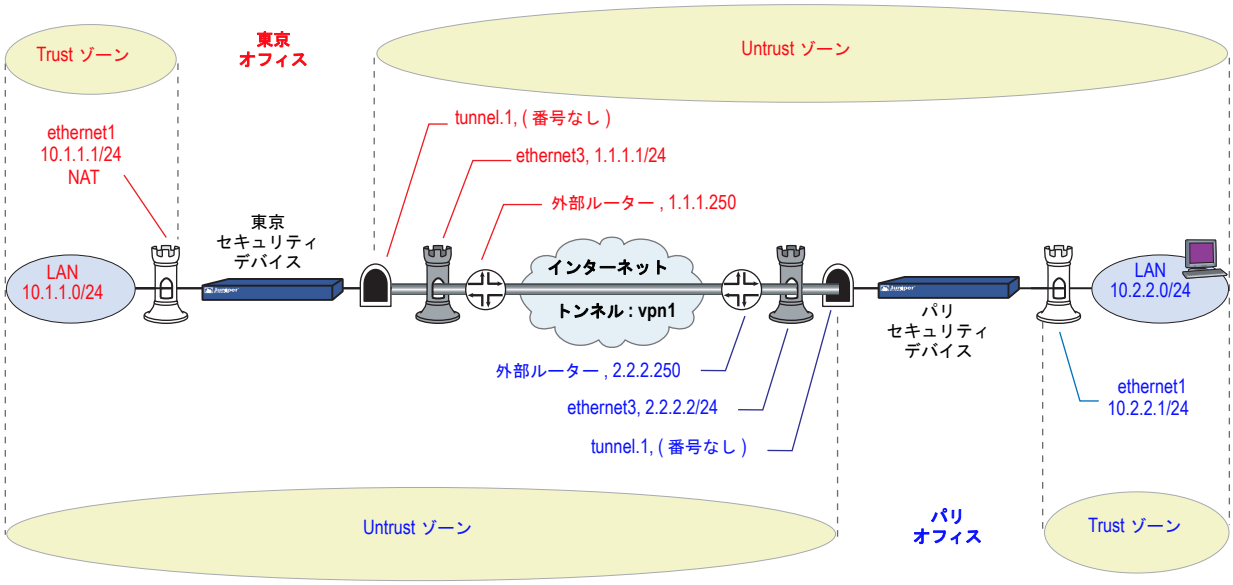
ここで使われているように、静的サイト間 VPN は、それぞれセキュリティデバイスがセキュアゲートウェイとして動作している 2 つのサイトをつなぐ IPSec トンネルを含みます。双方のデバイスで出力インターフェースとして使われる、物理的インターフェースあるいはサブインターフェースは、固定 IP アドレスを持ち、内部ホストも固定 IP アドレスを持っています。セキュリティデバイスが透過モードの場合は、VLAN1 アドレスを出力インターフェースの IP アドレスとして使います。静的サイト間 VPN では、リモートゲートウェイの IP アドレスが一定で到達可能であるため、トンネルのいずれの端のホストも VPN トンネル設定を起動することができます。

セキュリティデバイスの 1 つの出力インターフェースが、動的に割り当てられた IP アドレスを持っている場合には、デバイスは動的ピアと呼ばれ VPN の構成が異なります。動的ピアサイト間 VPN では、リモートゲートウェイのみがローカルゲートウェイから到達できる固定 IP アドレスを持っているため、動的ピアの背後にあるホストのみが VPN トンネル設定を起動することができます。ただし、いったん動的ピアと静的ピアの間にトンネルが設定されたら、どちらのゲートウェイの背後にあるホストでも、宛先ホストが固定 IP アドレスを持っていたら、VPN トラフィックを起動することができます。

注 : 使用可能な VPN オプションの基本的な内容については、1 ページの「インターネットプロトコルセキュリティ」を参照してください。各種のオプションを選択する際の手引きは、45 ページの「VPN (仮想プライベートネットワーク) のガイドライン」を参照してください。

サイト間 VPN トンネルを構成するには、トンネル構成をその他の設定、インターフェース、アドレス、ルート、およびポリシーのトンネル構成と調整する必要があります。このセクションの 3 つの VPN 構成例は、「東京のオフィスが IPSec VPN トンネルを介してパリのオフィスと安全に通信したい」ということに基づいて設定されています。

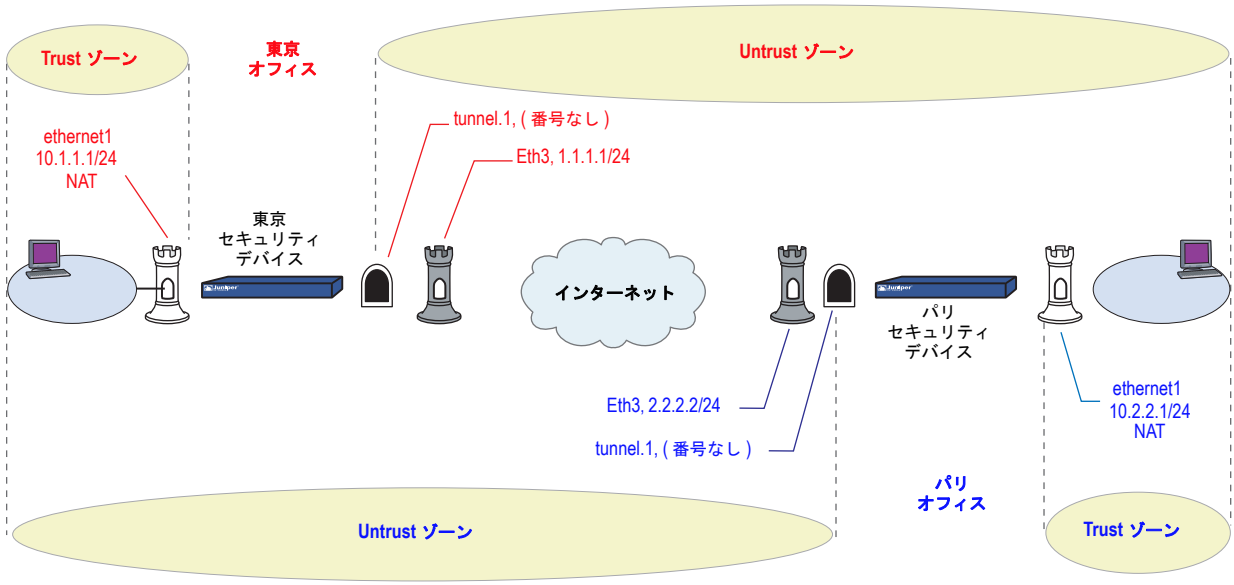
図 24: サイト間 VPN トンネルの構成



両方のオフィスの管理者は、以下の設定を構成します。

- インターフェース - セキュリティゾーンとトンネル
- アドレス
- VPN(次のいずれか)
  - AutoKey IKE
  - 動的ピア
  - 手動鍵
- ルート
- ポリシー

図 25: サイト間トンネルの構成 ー インターフェース



1. インターフェース - セキュリティゾーンとトンネル

東京オフィスの管理者は、図 25 の上半分に示されている設定を使用して、セキュリティゾーンおよびトンネルインターフェースを構成します。パリの管理者は、図の下半分に示されている設定を使用して、これらを構成します。

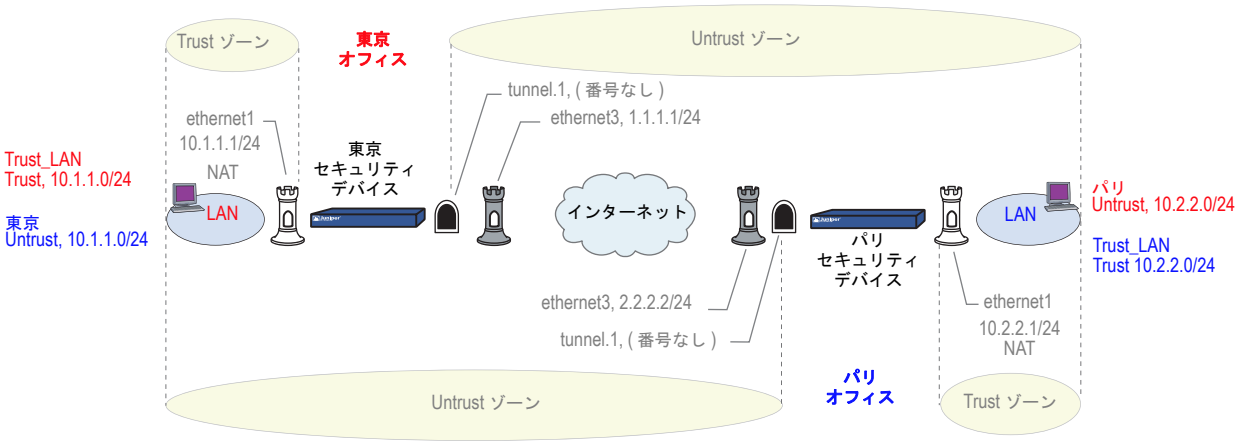
Ethernet3 は、VPN トラフィックの出力インターフェース、およびもう一方のトンネルから送信される VPN トラフィックのリモートゲートウェイになります。

Ethernet1 は、NAT モードなので、各管理者は、IP アドレスをすべての内部ホストに割り当てることができます。また、トラフィックが Trust ゾーンから Untrust ゾーンに送られるときに、セキュリティデバイスは、パケットヘッダーのソース IP アドレスを Untrust ゾーンインターフェースのアドレス、ethernet3 (東京の場合 1.1.1.1、パリの場合 2.2.2.2) に変換します。

ルートベース VPN について、各管理者は、トンネルインターフェース tunnel.1 を VPN トンネル vpn1 にバインドします。リモートオフィス LAN のアドレス空間へのルートを定義することで、セキュリティデバイスは、その LAN にバインドされているすべてのトラフィックを tunnel.1 インターフェースに送ります。このため、tunnel.1 がバインドされているトンネルを介します。

ポリシーベース NAT サービスは必要でないため、ルートベース VPN 構成では tunnel.1 に IP アドレス / ネットマスクを割り当てる必要がありません。また、ポリシーベース VPN 構成のトンネルインターフェースさえも必要ありません。

図 26: サイト間トンネルの構成 ー アドレス



2. アドレス

管理者は、今後インバウンドおよびアウトバウンドポリシーで使用するため、アドレスを定義します。東京オフィスの管理者は、図 26 の上半分に示されているアドレスを定義します。パリの管理者は、図の下半分に示されているアドレスを使用して、これらを構成します。

ポリシーベース VPN に対して、セキュリティデバイスは、ポリシーからプロキシ ID を定義します。VPN トンネルの両端でセキュリティデバイスにより使用されるプロキシ ID は、完全に一致する必要があるので、トンネルの一方の端で特定のアドレスを使用している場合、IP アドレスが 0.0.0.0/0 である定義済みアドレス「ANY」をトンネルのもう一方の端で使用することはできません。次に例を示します。

東京のプロキシ ID が次の場合

From: 0.0.0.0/0
To: 10.2.2.0/24
Service: ANY

パリのプロキシ ID が次の場合

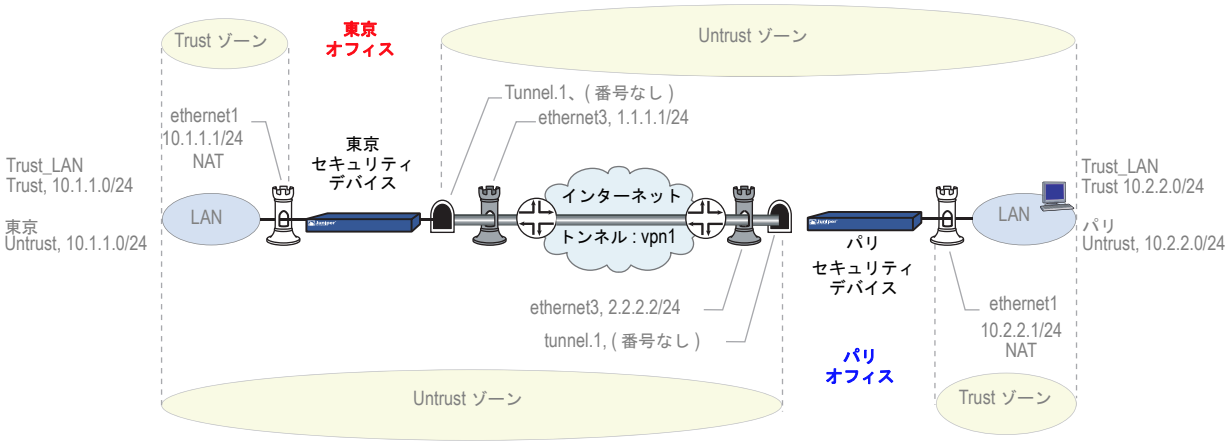
To: 10.1.1.0/24
From: 10.2.2.0/24
Service: ANY

この場合、プロキシ ID は 一致せず、IKE ネゴシエーションは失敗します。

注 : ScreenOS 5.0.0 からは、ポリシーベース VPN 構成で参照される VPN トンネルのプロキシ ID を定義することもできます。

ルートベース VPN の場合、「0.0.0.0/0,-0.0.0.0/0-any」を使用して、ローカル / リモートの IP アドレス、およびプロキシ ID のサービスタイプを定義できます。次に、ソースアドレス、宛先アドレス、およびサービスタイプによりポリシーを制限して、インバウンドおよびアウトバウンド VPN トラフィックを特定できます。

図 27: サイト間トンネルの構成 ― VPN トンネル



3. VPN

以下の 3 つの VPN のいずれかを構成できます。

- AutoKey IKE

  AutoKey IKE 方法は、事前共有鍵または証明書を使用して、ユーザーが定義した間隔 (鍵寿命と呼ばれます) で、暗号化パスワードおよび認証鍵を自動的にリフレッシュ、つまり変更します。通常、これらの鍵を頻繁に更新することで、セキュリティを強化できますが、鍵寿命が極端に短い場合、全体の性能が低下することがあります。

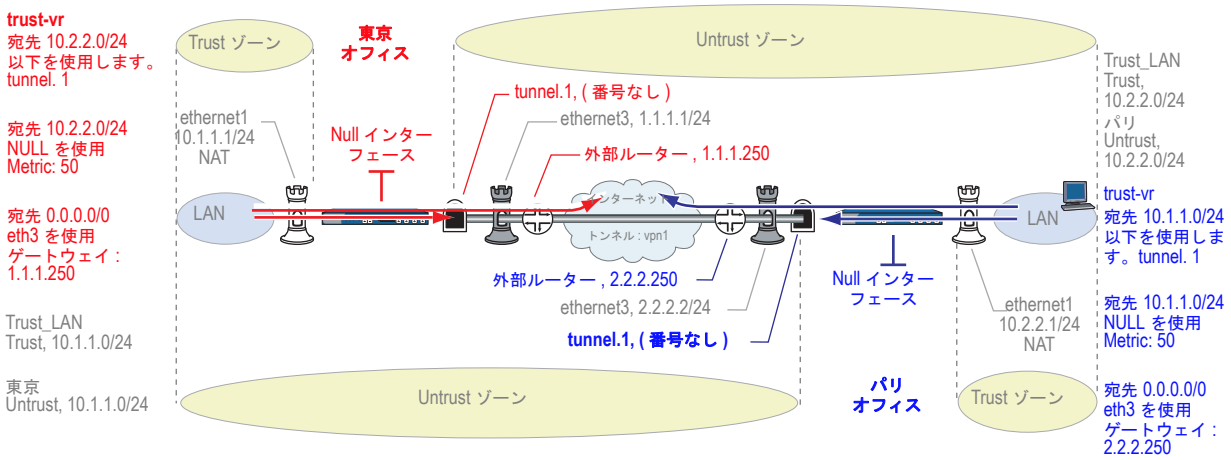
- 動的ピア

  動的ピアは、動的に割り当てられた IP アドレスを持つリモートゲートウェイです。リモートピアの IP アドレスは、IKE ネゴシエーションの開始ごとに異なることがあるので、ピアの後ろのホストは、VPN トラフィックを起動する必要があります。また、認証の事前共有鍵を使用する場合、ピアは、それ自体の識別のために、アグレッシブモードで Phase 1 の最初のメッセージをネゴシエートする間に IKE ID を送信する必要があります。

- 手動鍵

  手動鍵方法では、暗号化パスワードや認証鍵を手動で設定および更新する必要があります。この方法は、VPN トンネルの小さなセットで実行できるオプションです。

図 28: サイト間トンネルの構成 ー ルート



4. ルート

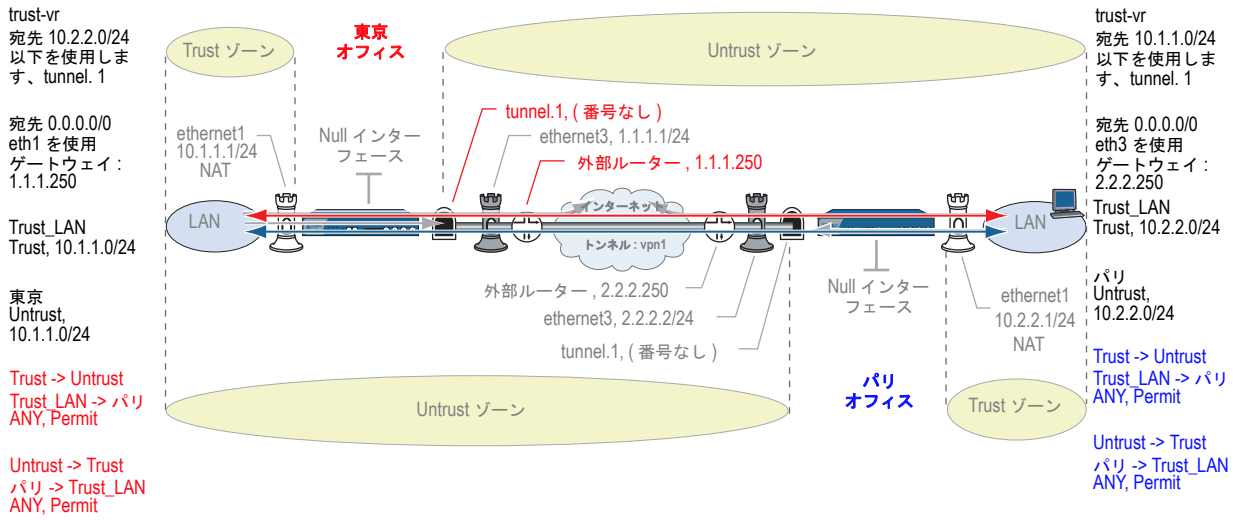
各サイトの管理者は、少なくとも以下のルートを構成する必要があります。

- tunnel.1 を使用するリモート LAN のアドレスに送られるトラフィックのルート
- ethernet3 を介してインターネットに送られ、次に、外部ルーター (東京オフィスの場合 1.1.1.250、パリオフィスの場合 2.2.2.250) に送られる外部 VPN トンネルトラフィックなどの、その他すべてのトラフィックのデフォルトルート。外部ルーターは、セキュリティデバイスが、ルーティングテーブルに特定のルートを持たないトラフィックを転送するデフォルトのゲートウェイです。

注 : 東京オフィスのセキュリティデバイスは、その外部 IP アドレスを ISP から動的に受信する場合 (つまり、パリオフィスから見たときに、東京オフィスのセキュリティデバイスがその動的ピアになる場合)、ISP は、東京オフィスのセキュリティデバイスにデフォルトのゲートウェイ IP アドレスを自動的に提供します。

- Null ルート。tunnel.1 の状態が「停止」に変わり、tunnel.1 を参照するすべてのルートが非アクティブになると、セキュリティデバイスは、ethernet3 から暗号化されずにリモート LAN に向かうデフォルトの転送トラフィックは使用しません。Null ルートは、宛先アドレスとしてリモート LAN を使用しますが、これは Null インターフェース、つまり送信されるトラフィックをドロップする論理インターフェースを指します。Null ルートには、tunnel.1 を利用するリモート LAN へのルートよりも高いメトリック値 (0 から離れた値) を指定して、tunnel.1 インターフェースを参照するルートよりも Null ルートの優先順位が低くなるようにします。

図 29: サイト間トンネルの構成 ― ポリシー



5. ポリシー

各サイトの管理者は、2 つのオフィス間でのトラフィックを許可する以下のポリシーを定義します。

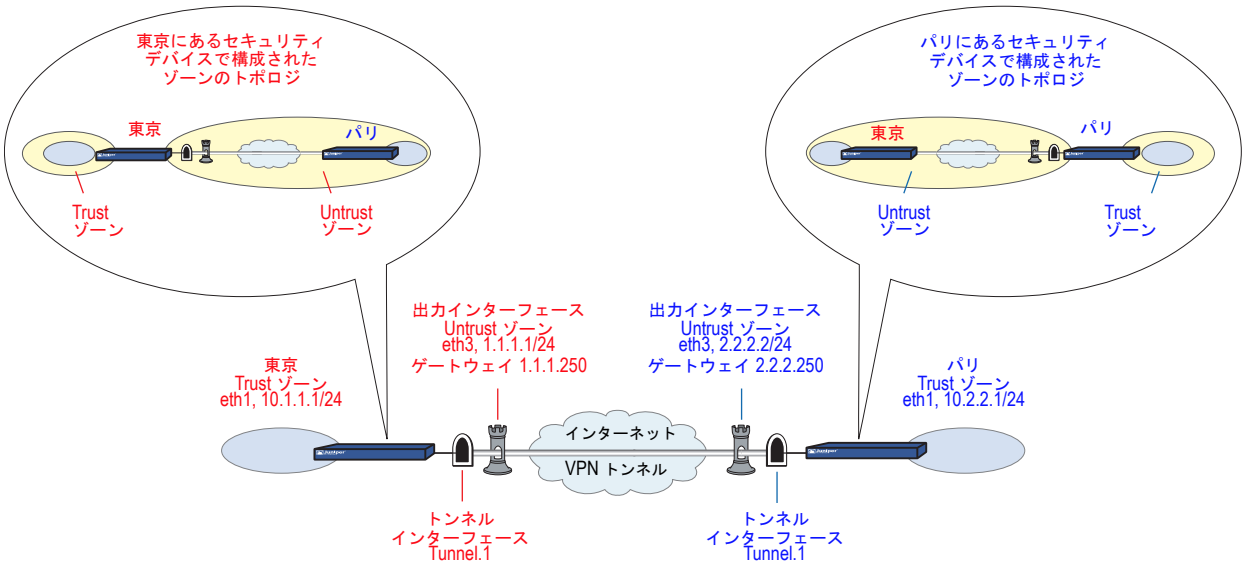
- Trust ゾーンの「Trust_LAN」から Untrust ゾーンの「パリ」または「東京」への任意のトラフィックを許可するポリシー
- Untrust ゾーンの「パリ」または「東京」から Trust ゾーンの「Trust_LAN」への任意のトラフィックを許可するポリシー

リモートサイトへの優先ルートは、VPN トンネル vpn1 にバインドされる、tunnel.1 を指定するので、ポリシーは、VPN トンネルを参照する必要はありません。

ルートベースのサイト間 VPN、AutoKey IKE

この例では、事前共有の秘密あるいは証明書のペア (それぞれトンネルの両端) を使用する AutoKey IKE トンネルが東京とパリのオフィスを安全な接続でつなぎます。フェーズ 1 と フェーズ 2 セキュリティレベルに対して、フェーズ 1 プロポーザル (事前共有鍵方法の場合の pre-g2-3des-sha、または証明書の場合の rsa-g2-3des-sha のいずれか) を指定し、フェーズ 2 のプロポーザルに対する定義済みの「Compatible」セットを選択します。すべてのゾーンは、trust-vr 内にあります。

図 30: ルートベースのサイト間 VPN、AutoKey IKE



事前共有鍵か証明書を使用してのルートベース AutoKey IKE トンネルの設定は、以下の手順に従ってください。

1. IP アドレスをセキュリティゾーンの物理的インターフェースとトンネルインターフェースにバインドさせます。

2. VPN トンネルを構成し、出力インターフェースを Untrust ゾーンに指定し、トンネルインターフェースにバインドしてから、プロキシ ID を構成します。

3. ローカルとリモート端点の IP アドレスを Trust および Untrust ゾーンのアドレス帳に入力します。

4. trust-vr の外部ルーターのデフォルトルート、トンネルインターフェースを介した宛先へのルート、宛先への Null ルートを入力します。Null ルートには高いメトリック値（0 よりかなり大きい値）を割り当てて、宛先へのルートの第 2 候補となるようにしてください。トンネル インターフェースの状態が「ダウン（停止）」に変わり、そのインターフェースを参照しているルートが非アクティブになると、セキュリティ デバイスは、暗号化されていないトラフィックを転送するデフォルト ルートではなく、送信されるトラフィックを基本的にすべてドロップする Null ルートを利用します。

5. VPN トラフィックのポリシーを各サイト間をパスするように設定します。

以下の例では、事前共有された鍵は h1p8A24nG5 です。双方の参加者が、すでに RSA 証明書を所有し、Entrust を CA (認証局) として使っていることが前提になっています（証明書の入手とロード方法については、24 ページの「証明書および CRL」を参照してください）。

WebUI (東京)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (選択)
Interface: ethernet3 (trust-vr)

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Trust_LAN
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Trust

Policy > Policy Elements > > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Paris_Office
IP Address/Domain Name:
IP/Netmask: (選択), 10.2.2.0/24
Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: To_Paris
Security Level: Custom
Remote Gateway Type:
Static IP Address: (選択), IP Address/Hostname: 2.2.2.2

事前共有鍵

Preshared Key: h1p8A24nG5
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Main (ID 保護)

(または)

証明書

Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): rsa-g2-3des-sha
Preferred certificate (optional)
Peer CA: Entrust
Peer Type: X509-SIG

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: Tokyo_Paris
Security Level: Compatible
Remote Gateway:
Predefined: (選択), To_Paris

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Security Level: Compatible
Bind to: Tunnel Interface, tunnel.1
Proxy-ID: (選択)
Local IP / Netmask: 10.1.1.0/24
Remote IP / Netmask: 10.2.2.0/24
Service: ANY

4. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.2.2.0/24
Gateway: (選択)
Interface: Tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.2.2.0/24
Gateway: (選択)
Interface: Null
Gateway IP Address: 0.0.0.0
Metric: 10

5. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Name: To_Paris
Source Address: Trust_LAN
Destination Address: Paris_Office
Service: ANY
Action: Permit
Position at Top: (選択)

Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

Name: From_Paris
Source Address: Paris_Office
Destination Address: Trust_LAN
Service: ANY
Action: Permit
Position at Top: (選択)

WebUI (パリ)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.2.2.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (選択)
Interface: ethernet3 (trust-vr)

2. アドレス

Policy > Policy Elements > > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Trust_LAN
IP Address/Domain Name:
IP/Netmask: (選択), 10.2.2.0/24
Zone: Trust

Policy > Policy Elements > > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Tokyo_Office
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: To_Tokyo
Security Level: Custom
Remote Gateway Type:
Static IP Address: (選択), IP Address/Hostname: 1.1.1.1

事前共有鍵

Preshared Key: h1p8A24nG5
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Main (ID 保護)

(または)

証明書

Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): rsa-g2-3des-sha
Preferred certificate (optional)
Peer CA: Entrust
Peer Type: X509-SIG

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

Name:Paris_Tokyo
Security Level: Compatible
Remote Gateway:
Predefined: (選択), To_Tokyo

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Security Level: Compatible
Bind to: Tunnel Interface, tunnel.1
Proxy-ID: (選択)
Local IP / Netmask: 10.2.2.0/24
Remote IP / Netmask: 10.1.1.0/24
Service: ANY

4. **ルート**

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 2.2.2.250

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
Gateway: (選択)
Interface: Tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
Gateway: (選択)
Interface: Null
Gateway IP Address: 0.0.0.0
Metric: 10

5. **ポリシー**

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Name: To_Tokyo
Source Address:
Address Book Entry: (選択), Trust_LAN
Destination Address:
Address Book Entry: (選択), Tokyo_Office
Service: ANY
Action: Permit
Position at Top: (選択)

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Name: From_Tokyo
Source Address:
Address Book Entry: (選択), Tokyo_Office
Destination Address:
Address Book Entry: (選択), Trust_LAN
Service: ANY
Action: Permit
Position at Top: (選択)

CLI (東京)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. アドレス

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust Paris_Office 10.2.2.0/24
```

3. VPN

事前共有鍵

```
set ike gateway To_Paris address 2.2.2.2 main outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn Tokyo_Paris gateway To_Paris sec-level compatible
set vpn Tokyo_Paris bind interface tunnel.1
set vpn Tokyo_Paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

(または)

認定書

```
set ike gateway To_Paris address 2.2.2.2 main outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway To_Paris cert peer-ca 1
set ike gateway To_Paris cert peer-cert-type x509-sig
set vpn Tokyo_Paris gateway To_Paris sec-level compatible
set vpn Tokyo_Paris bind interface tunnel.1
set vpn Tokyo_Paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

注 : 番号 1 は、CA ID 番号です。CA の ID 番号を調べるには、**get ike ca** コマンドを使用してください。

4. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 10.2.2.0/24 interface null metric 10
```

5. ポリシー

```
set policy top name “To Paris” from trust to untrust Trust_LAN Paris_Office any
    permit
set policy top name “From Paris” from untrust to trust Paris_Office Trust_LAN any
    permit
save
```

CLI (パリ)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. アドレス

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust Tokyo_Office 10.1.1.0/24
```

3. VPN

事前共有鍵

```
set ike gateway To_Tokyo address 1.1.1.1 main outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn Paris_Tokyo gateway To_Tokyo sec-level compatible
set vpn Paris_Tokyo bind interface tunnel.1
set vpn Paris_Tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

(または)

認定書

```
set ike gateway To_Tokyo address 1.1.1.1 main outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway To_Tokyo cert peer-ca 1
set ike gateway To_Tokyo cert peer-cert-type x509-sig
set vpn Paris_Tokyo gateway To_Tokyo sec-level compatible
set vpn Paris_Tokyo bind interface tunnel.1
set vpn Paris_Tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

4. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
set vrouter trust-vr route 10.1.1.0/24 interface null metric 10
```

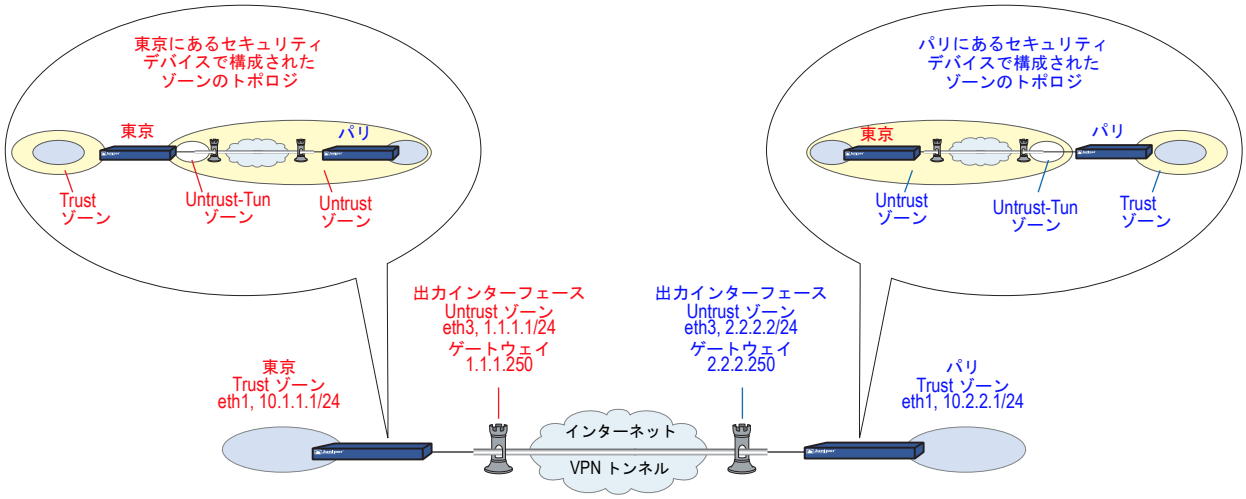
5. ポリシー

```
set policy top name “To Tokyo” from trust to untrust Trust_LAN Tokyo_Office any
    permit
set policy top name “From Tokyo” from untrust to trust Tokyo_Office Trust_LAN any
    permit
save
```

ポリシーベースのサイト間 VPN、AutoKey IKE

この例では、事前共有の秘密あるいは証明書のペア (それぞれトンネルの両端) を使用する AutoKey IKE トンネルが東京とパリのオフィスを安全な接続でつなぎます。フェーズ 1 と フェーズ 2 セキュリティレベルに対して、フェーズ 1 プロポーザル (事前共有鍵方法の場合の pre-g2-3des-sha、または証明書の場合の rsa-g2-3des-sha のいずれか) を指定し、フェーズ 2 のプロポーザルに対する定義済みの「Compatible」セットを選択します。すべてのゾーンは、trust-vr 内にあります。

図 31: ポリシーベースのサイト間 VPN、AutoKey IKE



事前共有の秘密あるいは証明書で、AutoKey IKE を使っての AutoKey IKE トンネルの設定は、以下のステップを含みます。

1. セキュリティゾーンインターフェース IP アドレスを定義します。
2. ローカルおよびリモート端点のアドレス帳項目を作成します。
3. リモートゲートウェイと鍵交換モードを定義して、事前共有秘密あるいは証明書を指定します。
4. Autokey IKE VPN を作成します。
5. 外部ルーターのデフォルトルートを設定します。
6. ポリシーを構成します。

以下の例では、事前共有された鍵は h1p8A24nG5 です。双方の参加者が、すでに RSA 証明書を所有し、Entrust を CA (認証局) として使っていることが前提になっています（証明書の入手とロード方法については、24 ページの「証明書および CRL」を参照してください)。

WebUI (東京)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Trust_LAN
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Paris_Office
IP Address/Domain Name:
IP/Netmask: (選択), 10.2.2.0/24
Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: To_Paris
Security Level: Custom
Remote Gateway Type:
Static IP Address: (選択), IP Address/Hostname: 2.2.2.2

事前共有鍵

Preshared Key: h1p8A24nG5
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **OK** をクリックして基本ゲートウェイ構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Main (ID 保護)

(または)

証明書

Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **OK** をクリックして基本ゲートウェイ構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): rsa-g2-3des-sha
Mode (Initiator): Main (ID 保護)
Preferred certificate (optional)
Peer CA: Entrust
Peer Type: X509-SIG

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: Tokyo_Paris
Security Level: Compatible
Remote Gateway: Predefined: (選択), To_Paris

4. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

5. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Name: To/From Paris
Source Address:
Address Book Entry: (選択), Trust_LAN
Destination Address:
Address Book Entry: (選択), Paris_Office
Service: ANY
Action: Tunnel
Tunnel VPN: Tokyo_Paris
Modify matching bidirectional VPN policy: (選択)
Position at Top: (選択)

WebUI (パリ)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.2.2.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 2.2.2.2/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Trust_LAN
IP Address/Domain Name:
IP/Netmask: (選択), 10.2.2.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Tokyo_Office
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: To_Tokyo
Security Level: Custom
Remote Gateway Type:
Static IP Address: (選択), IP Address/Hostname: 1.1.1.1

事前共有鍵

Preshared Key: h1p8A24nG5
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Main (ID 保護)

(または)

証明書

Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): rsa-g2-3des-sha
Mode (Initiator): Main (ID 保護)
Preferred certificate (optional)
Peer CA: Entrust
Peer Type: X509-SIG

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: Paris_Tokyo
Security Level: Compatible
Remote Gateway: Predefined: (選択), To_Tokyo

4. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 2.2.2.250

5. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Name: To/From Tokyo
Source Address:
Address Book Entry: (選択), Trust_LAN
Destination Address:
Address Book Entry: (選択), Tokyo_Office
Service: ANY
Action: Tunnel
Tunnel VPN: Paris_Tokyo
Modify matching bidirectional VPN policy: (選択)
Position at Top: (選択)

CLI (東京)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. アドレス

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust paris_office 10.2.2.0/24
```

3. VPN

事前共有鍵

```
set ike gateway to_paris address 2.2.2.2 main outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn tokyo_paris gateway to_paris sec-level compatible
```

(または)

証明書

```
set ike gateway to_paris address 2.2.2.2 main outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway to_paris cert peer-ca 1
set ike gateway to_paris cert peer-cert-type x509-sig
set vpn tokyo_paris gateway to_paris sec-level compatible
```

注： 番号 1 は、CA ID 番号です。CA の ID 番号を調べるには、**get ike ca** コマンドを使用してください。

4. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

5. ポリシー

```
set policy top name “To/From Paris” from trust to untrust Trust_LAN paris_office
    any tunnel vpn tokyo_paris
set policy top name “To/From Paris” from untrust to trust paris_office Trust_LAN
    any tunnel vpn tokyo_paris
save
```

CLI (パリ)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
```

2. アドレス

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust tokyo_office 10.1.1.0/24
```

3. VPN

事前共有鍵

```
set ike gateway to_tokyo address 1.1.1.1 main outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn paris_tokyo gateway to_tokyo sec-level compatible
```

(または)

証明書

```
set ike gateway to_tokyo address 1.1.1.1 main outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway to_tokyo cert peer-ca 1
set ike gateway to_tokyo cert peer-cert-type x509-sig
set vpn paris_tokyo gateway to_tokyo tunnel proposal nopfs-esp-3des-sha
```

4. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
```

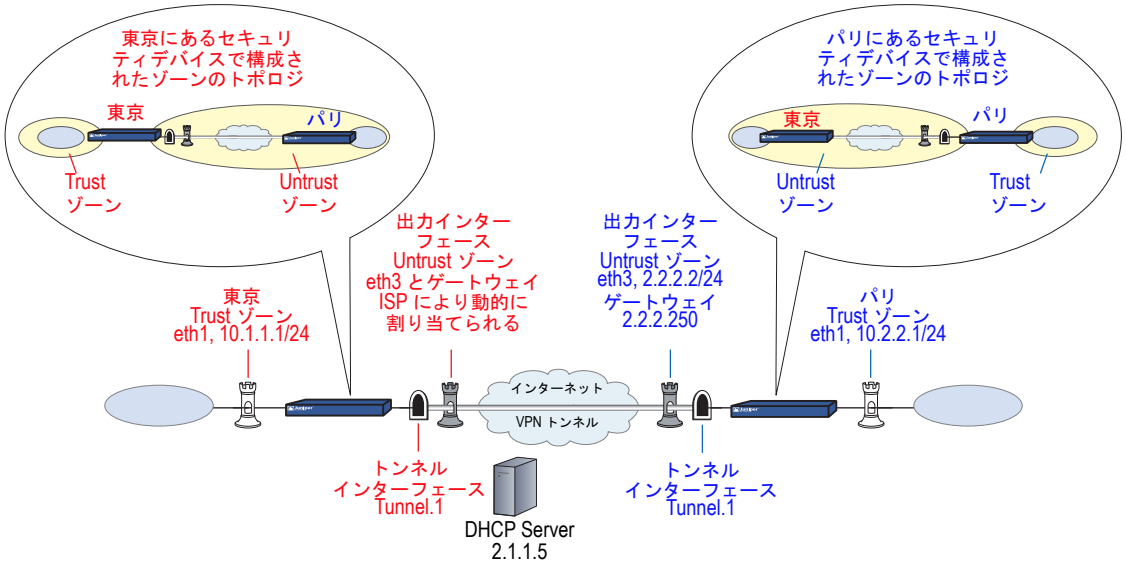
5. ポリシー

```
set policy top name “To/From Tokyo” from trust to untrust Trust_LAN tokyo_office
    any tunnel vpn paris_tokyo
set policy top name “To/From Tokyo” from untrust to trust tokyo_office Trust_LAN
    any tunnel vpn paris_tokyo
save
```

ルートベースのサイト間 VPN、動的ピア

この例では、事前共有鍵あるいは証明書のペア (それぞれトンネルの両端) を使用する AutoKey IKE VPN トンネルが東京とパリのオフィスを保護するセキュリティデバイス間を安全な接続でつなぎます。パリのセキュリティデバイスの Untrust ゾーンインターフェースは、静的 IP アドレスを持っています。東京オフィスにサービスしている ISP は、自身の Untrust ゾーンインターフェースの IP アドレスを DHCP を介して動的に割り当てます。パリのセキュリティデバイスだけに Untrust ゾーンの固定アドレスがあるので、VPN トラフィックは、東京オフィスのホストから発信される必要があります。トンネルが確立されたら、トンネルのトラフィックはいずれの端点からも発信することができます。すべてのセキュリティゾーンとトンネルゾーンは trust-vr にあります。

図 32: ルートベースのサイト間 VPN、動的ピア



事前共有鍵は h1p8A24nG5 です。双方の参加者がすでに Verisign の CA (認証局) からの RSA 証明書を持っていて、E メールアドレス *pmason@abc.com* がデバイス A のローカル証明書に記載されていることが前提になっています (証明書の入手とロードの方法に関しては、24 ページの「証明書および CRL」を参照してください)。フェーズ 1 とフェーズ 2 セキュリティレベルに対して、フェーズ 1 プロポーザル (事前共有鍵方法の場合の pre-g2-3des-sha、または証明書の場合の rsa-g2-3des-sha のいずれか) を指定し、フェーズ 2 のプロポーザルに対する定義済みの「Compatible」セットを選択します。

VPN トンネルの各終端にあるセキュリティデバイス上に、次の 3 つのルートを入力します。

- trust-vr の外部ルーターのデフォルトルート
- トンネル インターフェース経由の宛先までのルート
- 宛先までの Null ルート Null ルートには高いメトリック値（0 よりかなり大きい値）を割り当てて、宛先へのルートの第 2 候補となるようにしてください。トンネル インターフェースの状態が「ダウン（停止）」に変わり、そのインターフェースを参照しているルートが非アクティブになると、セキュリティ デバイスは、暗号化されていないトラフィックを転送するデフォルト

ルートではなく、送信されるトラフィックを基本的にすべてドロップする Null ルートを利用します。

最後に、ポリシーを設定して、2 つのサイト間の双方向トラフィックを許可します。

WebUI (東京)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 以下を入力して **Apply** をクリックします。

Zone Name: Untrust

次のように入力してから **OK** をクリックします。

Obtain IP using DHCP: (選択)

注 : WebUI から DHCP サーバーの IP アドレスを指定することはできませんが、CLI から指定できます。

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (選択)
Interface: ethernet3 (trust-vr)

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Trust_LAN
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Paris_Office
IP Address/Domain Name:
IP/Netmask: (選択), 10.2.2.0/24
Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: To_Paris
Security Level: Custom
Remote Gateway Type:
Static IP Address: (**選択**), IP Address/Hostname: 2.2.2.2

事前共有鍵

Preshared Key: h1p8A24nG5
Local ID: pmason@abc.com
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Aggressive

(または)

証明書

Local ID: pmason@abc.com
Outgoing Interface: ethernet3

注 : U-FQDN 「pmason@abc.com」証明書の SubjectAltName フィールドに必要です。

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): rsa-g2-3des-sha
Mode (Initiator): Aggressive
Preferred Certificate (optional):
Peer CA: Verisign
Peer Type: X509-SIG

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: Tokyo_Paris
Security Level: Compatible
Remote Gateway:
Predefined: (**選択**), To_Paris

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface: (**選択する**), tunnel.1
Proxy-ID: (**選択**)
Local IP / Netmask: 10.1.1.0/24
Remote IP / Netmask: 10.2.2.0/24
Service: ANY

4. **ルート**

   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選択)
   Interface: ethernet3
   Gateway IP Address: 0.0.0.0

注 : ISP は、DHCP を通じてゲートウェイ IP アドレスを動的に割り当てます。

   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 10.2.2.0/24
   Gateway: (選択)
   Interface: Tunnel.1
   Gateway IP Address: 0.0.0.0

   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 10.2.2.0/24
   Gateway: (選択)
   Interface: Null
   Gateway IP Address: 0.0.0.0
   Metric: 10

5. **ポリシー**

   Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Trust_LAN
   Destination Address:
   Address Book Entry: (選択), Paris_Office
   Service: ANY
   Action: Permit
   Position at Top: (選択)

   Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Paris_Office
   Destination Address:
   Address Book Entry: (選択), Trust_LAN
   Service: ANY
   Action: Permit
   Position at Top: (選択)

WebUI (パリ)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.2.2.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (選択)
Interface: ethernet3 (trust-vr)

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Trust_LAN
IP Address/Domain Name:
IP/Netmask: (選択), 10.2.2.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Tokyo_Office
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: To_Tokyo
Security Level: Custom
Remote Gateway Type:
Dynamic IP Address: (選択), Peer ID: pmason@abc.com

事前共有鍵

Preshared Key: h1p8A24nG5
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Aggressive

(または)

証明書

Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): rsa-g2-3des-sha
Mode (Initiator): Aggressive
Preferred Certificate (optional):
Peer CA: Verisign
Peer Type: X509-SIG

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: Paris_Tokyo
Security Level: Compatible
Remote Gateway:
Predefined: (**選択**), To_Tokyo

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface: (**選択する**), tunnel.1
Proxy-ID: (**選択**)
Local IP / Netmask: 10.2.2.0/24
Remote IP / Netmask: 10.1.1.0/24
Service: ANY

4. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: ethernet3
Gateway IP Address: (**選択**), 2.2.2.250

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
Gateway: (**選択**)
Interface: Tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
Gateway: (選択)
Interface: Null
Gateway IP Address: 0.0.0.0
Metric: 10

5. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Trust_LAN
Destination Address:
Address Book Entry: (選択), Tokyo_Office
Service: ANY
Action: Permit
Position at Top: (選択)

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Tokyo_Office
Destination Address:
Address Book Entry: (選択), Trust_LAN
Service: ANY
Action: Permit
Position at Top: (選択)

CLI (東京)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 dhcp client
set interface ethernet3 dhcp client settings server 1.1.1.5
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. アドレス

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust Paris_Office 10.2.2.0/24
```

3. VPN

事前共有鍵

```
set ike gateway To_Paris address 2.2.2.2 aggressive local-id pmason@abc.com
    outgoing-interface ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn Tokyo_Paris gateway To_Paris tunnel sec-level compatible
set vpn Tokyo_Paris bind interface tunnel.1
set vpn Tokyo_Paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

(または)

証明書

```
set ike gateway To_Paris address 2.2.2.2 aggressive local-id pmason@abc.com
    outgoing-interface ethernet3 proposal rsa-g2-3des-sha
set ike gateway To_Paris cert peer-ca 1
set ike gateway To_Paris cert peer-cert-type x509-sig
set vpn Tokyo_Paris gateway To_Paris tunnel sec-level compatible
set vpn Tokyo_Paris bind interface tunnel.1
set vpn Tokyo_Paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

注 : U-FQDN 「pmason@abc.com」証明書の SubjectAltName フィールドに必要です。

番号 1 は、CA ID 番号を示します。CA の ID 番号を調べるには、**get ike ca** コマンドを使用してください。

4. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 10.2.2.0/24 interface null metric 10
```

注 : ISP は、DHCP を通じて動的にゲートウェイ IP を提供するため、ここでは指定できません。

5. ポリシー

```
set policy top from trust to untrust Trust_LAN Paris_Office any permit
set policy top from untrust to trust Paris_Office Trust_LAN any permit
save
```

CLI (パリ)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. アドレス

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust Tokyo_Office 10.1.1.0/24
```

3. VPN

事前共有鍵

```
set ike gateway To_Tokyo dynamic pmason@abc.com aggressive outgoing-interface
    ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn Paris_Tokyo gateway To_Tokyo tunnel sec-level compatible
set vpn Paris_Tokyo bind interface tunnel.1
set vpn Paris_Tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

(または)

証明書

```
set ike gateway To_Tokyo dynamic pmason@abc.com aggressive outgoing-interface
    ethernet3 proposal rsa-g2-3des-sha
set ike gateway To_Tokyo cert peer-ca 1
set ike gateway To_Tokyo cert peer-cert-type x509-sig
set vpn Paris_Tokyo gateway To_Tokyo tunnel sec-level compatible
set vpn Paris_Tokyo bind interface tunnel.1
set vpn Paris_Tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

注 : 番号 1 は、CA ID 番号です。CA の ID 番号を調べるには、**get ike ca** コマンドを使用してください。

4. **ルート**

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
set vrouter trust-vr route 10.1.1.0/24 interface null metric 10
```

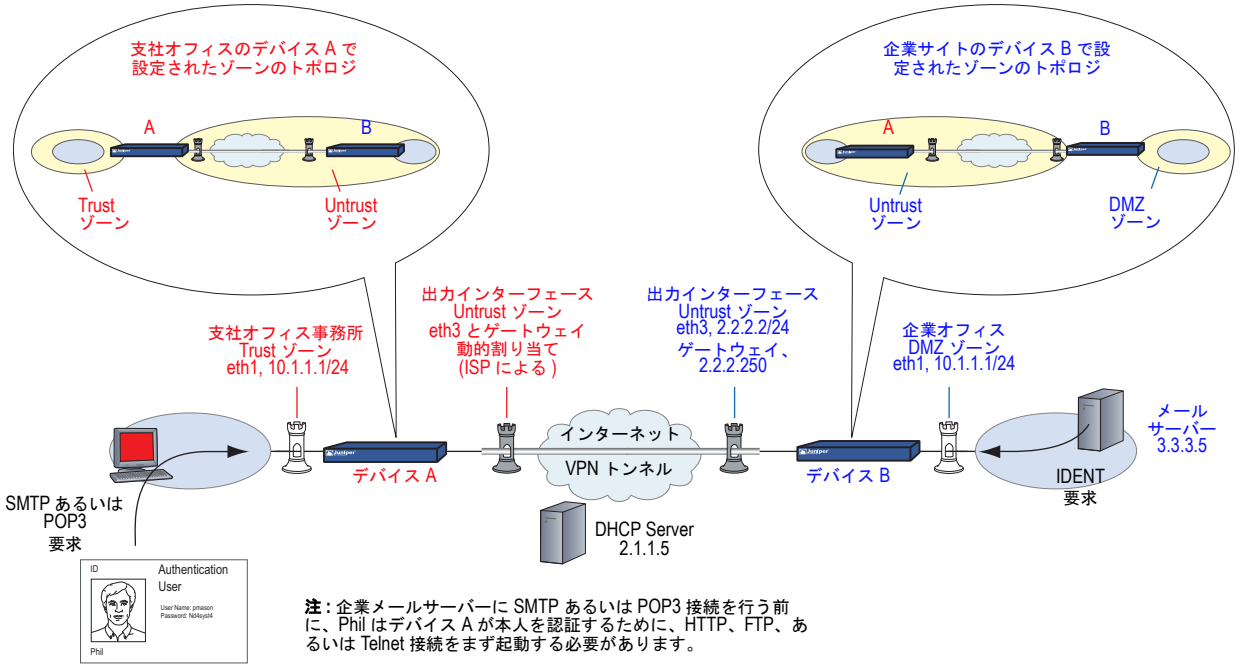
5. **ポリシー**

```
set policy top from trust to untrust Trust_LAN Tokyo_Office any permit
set policy top from untrust to trust Paris_Office Trust_LAN any permit
save
```

ポリシーベースのサイト間 VPN、動的ピア

この例では、VPN トンネルセキュリティはデバイス A の背後の Trust ゾーンのユーザーとデバイス B に保護された本社 DMZ ゾーンのメールサーバーをつなぎます。デバイス B の Untrust ゾーンインターフェースは、静的 IP アドレスを持っています。デバイス A にサービスしている ISP は、自身の Untrust ゾーンインターフェースの IP アドレスを DHCP を介して動的に割り当てます。デバイス B のみが自身の Untrust ゾーンに固定アドレスを持っているため、VPN トラフィックは、デバイス A の背後からホストを発信する必要があります。デバイス A がトンネルを確立したら、トンネルを通過するトラフィックはどちらの端点からも発信することができます。すべてのゾーンは、trust-vr ルーティングドメインにあります。

図 33: ポリシーベースのサイト間 VPN、動的ピア



この例では、ローカル認証ユーザーは、Phil (ログイン名 : pmason; パスワード : Nd4syst4) で、企業サイトのメールサーバーから E メールを取り出すことを希望しています。この場合、認証が 2 回行われます。まず、デバイス A は、送られたトラフィックをトンネルに通す前に認証します。次に、メールサーバープログラムが、IDENT 要求をトンネルを通じて送信することで認証します。

注 : 次に、メールサーバープログラムが、IDENT 要求をトンネルを通じて送信することで認証します。Phil は認証ユーザーなので、SMTP あるいは POP3 要求を発行する前に、まずデバイス A がファイアウォールユーザー / ログインプロンプトで認証を行えるように、HTTP、FTP、あるいは Telnet 接続を起動する必要があります。デバイス A が認証を済ませたら、VPN トンネルを経由して本社メールサーバーとコンタクトをとる許可を得られます。

メールサーバーは、デバイス A と B の管理者が顧客サービス (TCP、ポート 113) を追加して、トンネルを通って 10.10.10.0/24 サブネットに到達するトラフィックを許可するポリシーを設定する場合にのみ、トンネルを通じて IDENT 要求を送信することができます。

事前共有鍵は h1p8A24nG5 です。双方の参加者がすでに Verisign の CA (認証局) からの RSA 証明書を持っていて、E メールアドレス *pmason@abc.com* がデバイス A のローカル証明書に記載されていることが前提になっています (証明書の入手とロードの方法に関しては、24 ページの「証明書および CRL」を参照してください)。フェーズ 1 とフェーズ 2 セキュリティ レベルに対して、フェーズ 1 プロポーザル（事前共有鍵方法の場合は pre-g2-3des-sha、または証明書の場合は rsa-g2-3des-sha のいずれか）を指定し、フェーズ 2 のプロポーザルに対して定義済みの「Compatible」を選択します。

WebUI (デバイス A)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Obtain IP using DHCP: (選択)

注 : WebUI から DHCP サーバーの IP アドレスを指定することはできませんが、CLI から指定できます。

2. ユーザー

Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

User Name: pmason
Status: Enable
Authentication User: (選択)
User Password: Nd4syst4
Confirm Password: Nd4syst4

3. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Trusted_network
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Mail_Server
IP Address/Domain Name:
IP/Netmask: (選択), 3.3.3.5/32
Zone: Untrust

4. **Services**

   Policy > Policy Elements > Services > Custom > New: 次のように入力してから **OK** をクリックします。

   Service Name: Ident
   Service Timeout:
   Use protocol default: (選択)
   Transport Protocol: TCP (選択)
   Source Port: Low 0, High 65535
   Destination Port: Low 113, High 113

   Policy > Policy Elements > Services > Group > New: 次のように入力し、次のサービスを移動してから **OK** をクリックします。

   Group Name: Remote_Mail
   Group Members << Available Members:
   HTTP
   FTP
   Telnet
   Ident
   MAIL
   POP3

5. **VPN**

   VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

   Gateway Name: To_Mail
   Security Level: Custom
   Remote Gateway Type:
   Static IP Address: (選択), IP Address/Hostname: 2.2.2.2

事前共有鍵

Preshared Key: h1p8A24nG5
Local ID: pmason@abc.com
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Aggressive

(または)

証明書

Local ID: pmason@abc.com
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): rsa-g2-3des-sha
Mode (Initiator): Aggressive
Preferred Certificate (optional):
Peer CA: Verisign
Peer Type: X509-SIG

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

Name: branch_corp
Security Level: Compatible
Remote Gateway Tunnel: To_Mail

6. Route

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 0.0.0.0

注 : ISP は、DHCP を通じてゲートウェイ IP アドレスを動的に割り当てます。

---

7. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Trusted_network
Destination Address:
Address Book Entry: (選択), Mail_Server
Service: Remote_Mail
Action: Tunnel
VPN Tunnel: branch_corp
Modify matching bidirectional VPN policy: (選択)
Position at Top: (選択)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

Authentication: (選択)
Auth Server: Local
User: (選択), Local Auth User - pmason

WebUI (デバイス B)

1. インターフェース

Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

Zone Name: DMZ
Static IP: (ある場合は選択する)
IP Address/Netmask: 3.3.3.3/24

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 2.2.2.2/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Mail Server
IP Address/Domain Name:
IP/Netmask: (選択), 3.3.3.5/32
Zone: DMZ

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: branch office
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Untrust

3. Services

Policy > Policy Elements > Services > Custom > New: 次のように入力してから **OK** をクリックします。

Service Name: Ident
Service Timeout:
Use protocol default: (選択)
Transport Protocol: TCP (選択)
Source Port: Low 0, High 65535
Destination Port: Low 113, High 113

Policy > Policy Elements > Services > Groups > New: 次のように入力し、次のサービスを移動してから **OK** をクリックします。

Group Name: Remote_Mail
Group Members << Available Members:
Ident
MAIL
POP3

4. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: To_branch
Security Level: Custom
Remote Gateway Type:
Dynamic IP Address: (選択), Peer ID: pmason@abc.com

事前共有鍵

Preshared Key: h1p8A24nG5
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Aggressive

(または)

証明書

Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): rsa-g2-3des-sha
Mode (Initiator): Aggressive
Preferred Certificate (optional):
Peer CA: Verisign
Peer Type: X509-SIG

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: corp_branch
Security Level: Compatible
Remote Gateway:
Predefined: (選択), To_branch

5. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 2.2.2.250

6. ポリシー

Policies > (From: DMZ, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Mail_Server
Destination Address:
Address Book Entry: (選択), branch_office
Service: Remote_Mail
Action: Tunnel
VPN Tunnel: corp_branch
Modify matching bidirectional VPN policy: (選択)
Position at Top: (選択)

CLI (デバイス A)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 dhcp client
set interface ethernet3 dhcp client settings server 1.1.1.5
```

2. ユーザー

```
set user pmason password Nd4syst4
```

3. **アドレス**
   set address trust “trusted network” 10.1.1.0/24
   set address untrust “mail server” 3.3.3.5/32

4. **Services**
   set service ident protocol tcp src-port 0-65535 dst-port 113-113
   set group service remote_mail
   set group service remote_mail add http
   set group service remote_mail add ftp
   set group service remote_mail add telnet
   set group service remote_mail add ident
   set group service remote_mail add mail
   set group service remote_mail add pop3

5. **VPN**

事前共有鍵

```
set ike gateway to_mail address 2.2.2.2 aggressive local-id pmason@abc.com
    outgoing-interface ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn branch_corp gateway to_mail sec-level compatible
```

(または)

証明書

```
set ike gateway to_mail address 2.2.2.2 aggressive local-id pmason@abc.com
    outgoing-interface ethernet3 proposal rsa-g2-3des-sha
set ike gateway to_mail cert peer-ca 1
set ike gateway to_mail cert peer-cert-type x509-sig
set vpn branch_corp gateway to_mail sec-level compatible
```

注 : U-FQDN 「pmason@abc.com」証明書の SubjectAltName フィールドに必要です。

番号 1 は、CA ID 番号を示します。CA の ID 番号を調べるには、**get ike ca** コマンドを使用してください。

6. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3

注 : ISP は、DHCP を通じてゲートウェイ IP アドレスを動的に割り当てます。

7. **ポリシー**
   set policy top from trust to untrust “trusted network” “mail server” remote_mail
   tunnel vpn branch_corp auth server Local user pmason
   set policy top from untrust to trust “mail server” “trusted network” remote_mail
   tunnel vpn branch_corp
   save

CLI (デバイス B)

1. インターフェース

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 3.3.3.3/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
```

2. アドレス

```
set address dmz “mail server” 3.3.3.5/32
set address untrust "branch office" 10.1.1.0/24
```

3. Services

```
set service ident protocol tcp src-port 0-65535 dst-port 113-113
set group service remote_mail
set group service remote_mail add ident
set group service remote_mail add mail
set group service remote_mail add pop3
```

4. VPN

事前共有鍵

```
set ike gateway to_branch dynamic pmason@abc.com aggressive
    outgoing-interface ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn corp_branch gateway to_branch tunnel sec-level compatible
```

(または)

証明書

```
set ike gateway to_branch dynamic pmason@abc.com aggressive
    outgoing-interface ethernet3 proposal rsa-g2-3des-sha
set ike gateway to_branch cert peer-ca 1
set ike gateway to_branch cert peer-cert-type x509-sig
set vpn corp_branch gateway to_branch sec-level compatible
```

注 : 番号 1 は、CA ID 番号です。CA の ID 番号を調べるには、**get ike ca** コマンドを使用してください。

---

5. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
```

6. ポリシー

```
set policy top from dmz to untrust “mail server” "branch office" remote_mail
    tunnel vpn corp_branch
set policy top from untrust to dmz "branch office" “mail server” remote_mail
    tunnel vpn corp_branch
save
```

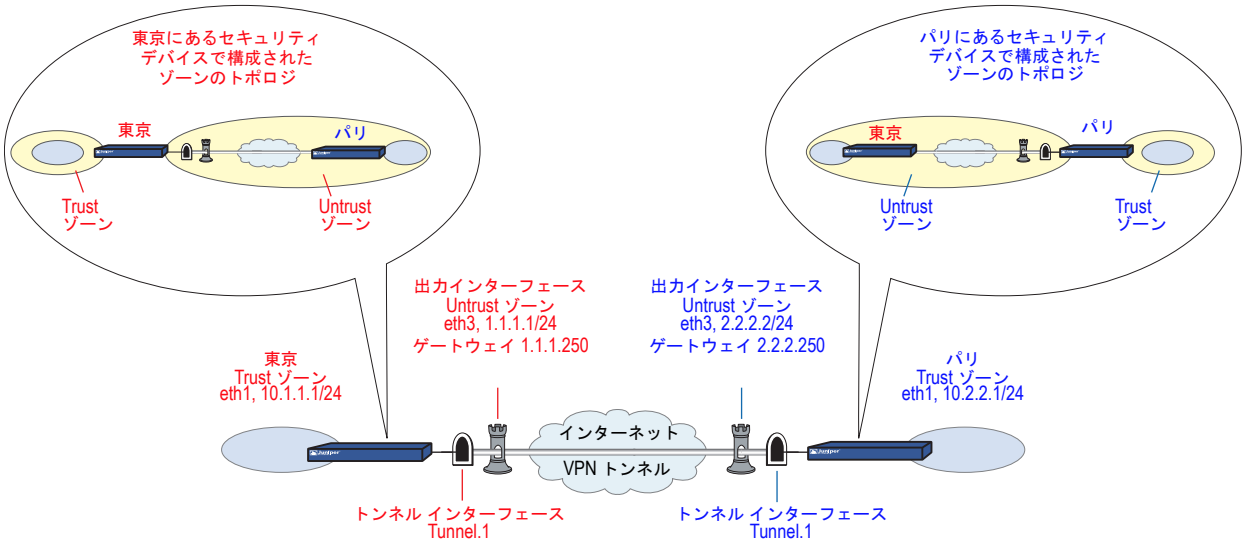
ルートベースのサイト間 VPN、手動鍵

この例では、手動鍵トンネルは、東京にあるオフィスとパリにあるオフィスを安全な通信でつなぎます。各サイトの Trust ゾーンは、NAT モードです。アドレスは次のとおりです。

- 東京 :
  - Trust ゾーンインターフェース (ethernet1): 10.1.1.1/24
  - Untrust ゾーンインターフェース (ethernet3): 1.1.1.1/24
- パリ :
  - Trust ゾーンインターフェース (ethernet1): 10.2.2.1/24
  - Untrust ゾーンインターフェース (ethernet3): 2.2.2.2/24

Trust、Untrust の各ゾーンは、trust-vr ルーティングドメインに属します。Untrust ゾーンインターフェース (ethernet3) は、VPN トンネルの出力インターフェースとして機能します。

図 34: ルートベースのサイト間 VPN、手動鍵



トンネルを設定するには、トンネルの両端のセキュリティデバイスの次の手順にしたがってください。

1. IP アドレスをセキュリティゾーンの物理的インターフェースとトンネルインターフェースにバインドさせます。
2. VPN トンネルを構成し、出力インターフェースを Untrust ゾーンに指定し、トンネルインターフェースにバインドします。
3. ローカルとリモート端点の IP アドレスを Trust および Untrust ゾーンのアドレス帳に入力します。

4. trust-vr の外部ルーターのデフォルトルート、トンネルインターフェースを介した宛先へのルート、宛先への Null ルートを入力します。Null ルートには高いメトリック値（0 よりかなり大きい値）を割り当てて、宛先へのルートの第 2 候補となるようにしてください。トンネル インターフェースの状態が「ダウン（停止)」に変わり、そのインターフェースを参照しているルートが非アクティブになると、セキュリティ デバイスは、暗号化されていないトラフィックを転送するデフォルト ルートではなく、送信されるトラフィックを基本的にすべてドロップする Null ルートを利用します。

5. VPN トラフィックのポリシーを各サイト間をパスするように設定します。

WebUI (東京)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (選択)
Interface: ethernet3 (trust-vr)

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Trust_LAN
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Paris_Office
IP Address/Domain Name:
IP/Netmask: (選択), 10.2.2.0/24
Zone: Untrust

3. **VPN**

VPNs > Manual Key > New: 次のように入力してから **OK** をクリックします。

VPN Tunnel Name: Tokyo_Paris
Gateway IP: 2.2.2.2
Security Index: 3020 (**ローカル**), 3030 (**リモート**)
Outgoing Interface: ethernet3
ESP-CBC: (**選択**)
Encryption Algorithm: 3DES-CBC
Generate Key by Password: asdlk24234
Authentication Algorithm: SHA-1
Generate Key by Password: PNas134a

> Advanced: 次の高度な設定を入力してから **Return** をクリックし、基本手動鍵トンネル構成ページに戻ります。

Bind to: Tunnel Interface, tunnel.1

4. **ルート**

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.2.2.0/24
Gateway: (**選択**)
Interface: Tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.2.2.0/24
Gateway: (**選択**)
Interface: Null
Gateway IP Address: 0.0.0.0
Metric: 10

5. **ポリシー**

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Name: To_Paris
Source Address:
Address Book Entry: (**選択**), Trust_LAN
Destination Address:
Address Book Entry: (**選択**), Paris_Office
Service: ANY
Action: Permit
Position at Top: (**選択**)

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Name: From_Paris
Source Address:
Address Book Entry: (選択), Paris_Office
Destination Address:
Address Book Entry: (選択), Trust_LAN
Service: ANY
Action: Permit
Position at Top: (選択)

WebUI (パリ)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.2.2.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (選択)
Interface: ethernet3 (trust-vr)

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Trust_LAN
IP Address/Domain Name:
IP/Netmask: (選択), 10.2.2.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Tokyo_Office
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Untrust

3. **VPN**

VPNs > Manual Key > New: 次のように入力してから **OK** をクリックします。

VPN Tunnel Name: Paris_Tokyo
Gateway IP: 1.1.1.1
Security Index: 3030 (**ローカル**), 3020 (**リモート**)
Outgoing Interface: ethernet3
ESP-CBC: (**選択**)
Encryption Algorithm: 3DES-CBC
Generate Key by Password: asdlk24234
Authentication Algorithm: SHA-1
Generate Key by Password: PNas134a

> Advanced: 次の高度な設定を入力してから **Return** をクリックし、基本手動鍵トンネル構成ページに戻ります。

Bind to: Tunnel Interface, tunnel.1

4. **ルート**

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: ethernet3
Gateway IP Address: 2.2.2.250

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
Gateway: (**選択**)
Interface: Tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
Gateway: (**選択**)
Interface: Null
Gateway IP Address: 0.0.0.0
Metric: 10

5. **ポリシー**

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Name: To_Tokyo
Source Address:
Address Book Entry: (**選択**), Trust_LAN
Destination Address:
Address Book Entry: (**選択**), Tokyo_Office
Service: ANY
Action: Permit
Position at Top: (**選択**)

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Name: From_Tokyo
Source Address:
Address Book Entry: (選択), Tokyo_Office
Destination Address:
Address Book Entry: (選択), Trust_LAN
Service: ANY
Action: Permit
Position at Top: (選択)

CLI (東京)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. アドレス

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust Paris_Office 10.2.2.0/24
```

3. VPN

```
set vpn Tokyo_Paris manual 3020 3030 gateway 2.2.2.2 outgoing-interface
    ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a
set vpn Tokyo_Paris bind interface tunnel.1
```

4. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 10.2.2.0/24 interface null metric 10
```

5. ポリシー

```
set policy top name "To Paris"To Parisî from trust to untrust Trust_LAN Paris_Office
    any permit
set policy top name "From Parisî from untrust to trust Paris_Office Trust_LAN any
    permit
save
```

CLI (パリ)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. アドレス

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust Tokyo_Office 10.1.1.0/24
```

3. **VPN**

```
set vpn Paris_Tokyo manual 3030 3020 gateway 1.1.1.1 outgoing-interface
    ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a
set vpn Paris_Tokyo bind interface tunnel.1
```

4. **ルート**

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
set vrouter trust-vr route 10.1.1.0/24 interface null metric 10
```

5. **ポリシー**

```
set policy top name "To Tokyo" from trust to untrust Trust_LAN Tokyo_Office any
    permit
set policy top name "From Tokyo" from untrust to trust Tokyo_Office Trust_LAN any
    permit
save
```

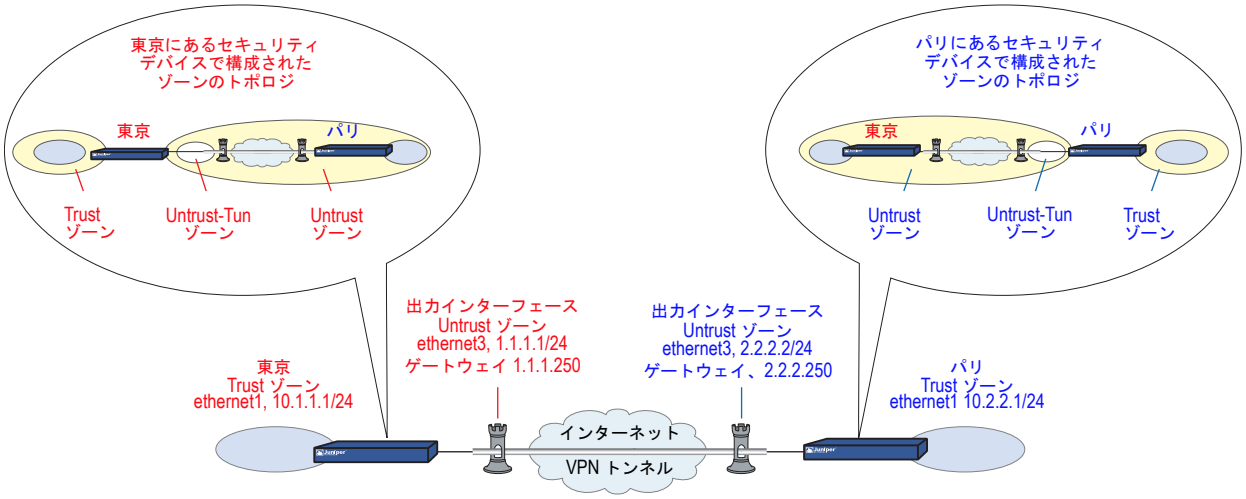
ポリシーベースのサイト間VPN、手動鍵

この例では、手動鍵トンネルは、東京にあるオフィスとパリにあるオフィスを 3DES 暗号と、SHA-1 認証の ESP を使って安全な通信でつなぎます。各サイトの Trust ゾーンは、NAT モードです。アドレスは次のとおりです。

- 東京 :
  - Trust インターフェース (ethernet1): 10.1.1.1/24
  - Untrust インターフェース (ethernet3): 1.1.1.1/24
- パリ :
  - Trust インターフェース (ethernet1): 10.2.2.1/24
  - Untrust インターフェース (ethernet3): 2.2.2.2/24

Trust および Untrust セキュリティゾーンと Untrust-Tun トンネルゾーンは、trust-vr ルーティングドメインにあります。Untrust ゾーンインターフェース (ethernet3) は、VPN トンネルの出力インターフェースとして機能します。

図 35: ポリシーベースのサイト間 VPN、手動鍵



トンネルを設定するには、トンネルの両端のセキュリティデバイスに、次の 5 つの手順を実行してください。

1. セキュリティゾーンにバインドされている物理インターフェースに IP アドレスを割り当てます。
2. VPN トンネルを設定して、その出力インターフェースを Untrust ゾーンに指定します。
3. ローカルとリモート端点の IP アドレスを Trust および Untrust アドレス帳に入力します。
4. 外部ルーターのデフォルトルートを入力します。
5. トンネルを両方向にできるように、VPN トラフィックのポリシーを設定します。

WebUI (東京)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: Trust_LAN
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 10.1.1.0/24
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: Paris_Office
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 10.2.2.0/24
   Zone: Untrust

3. **VPN**
   VPNs > Manual Key > New: 次のように入力してから **OK** をクリックします。

   VPN Tunnel Name: Tokyo_Paris
   Gateway IP: 2.2.2.2
   Security Index: 3020 (**ローカル**), 3030 (**リモート**)
   Outgoing Interface: ethernet3
   ESP-CBC: (**選択**)
   Encryption Algorithm: 3DES-CBC
   Generate Key by Password: asdlk24234
   Authentication Algorithm: SHA-1
   Generate Key by Password: PNas134a

   > Advanced: 次の高度な設定を入力してから **Return** をクリックし、基本手動鍵トンネル構成ページに戻ります。

   Bind to: Tunnel Zone, Untrust-Tun

4. **ルート**
   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (**選択**)
   Interface: ethernet3
   Gateway IP Address: 1.1.1.250

5. **ポリシー**
   Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Name: To/From Paris
   Source Address:
   Address Book Entry: (**選択**), Trust_LAN
   Destination Address:
   Address Book Entry: (**選択**), Paris_Office
   Service: ANY
   Action: Tunnel
   Tunnel VPN: Tokyo_Paris
   Modify matching bidirectional VPN policy: (**選択**)
   Position at Top: (**選択**)

WebUI (パリ)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.2.2.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。
Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 2.2.2.2/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Trust_LAN
IP Address/Domain Name:
IP/Netmask: (選択), 10.2.2.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Tokyo_Office
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Untrust

3. VPN

VPNs > Manual Key > New: 次のように入力してから **OK** をクリックします。

VPN Tunnel Name: Paris_Tokyo
Gateway IP: 1.1.1.1
Security Index (HEX Number): 3030 (ローカル), 3020 (リモート)
Outgoing Interface: ethernet3
ESP-CBC: (選択)
Encryption Algorithm: 3DES-CBC
Generate Key by Password: asdlk24234
Authentication Algorithm: SHA-1
Generate Key by Password: PNas134a

> Advanced: 次の高度な設定を入力してから **Return** をクリックし、基本手動鍵トンネル構成ページに戻ります。

Bind to: Tunnel Zone, Untrust-Tun

4. **ルート**
   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選択)
   Interface: ethernet3
   Gateway IP Address: 2.2.2.250

5. **ポリシー**
   Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Name: To/From Tokyo
   Source Address:
   Address Book Entry: (選択), Trust_LAN
   Destination Address:
   Address Book Entry: (選択), Tokyo_Office
   Service: ANY
   Action: Tunnel
   Tunnel VPN: Paris_Tokyo
   Modify matching bidirectional VPN policy: (選択)
   Position at Top: (選択)

CLI (東京)

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **アドレス**
   set address trust Trust_LAN 10.1.1.0/24
   set address untrust paris_office 10.2.2.0/24

3. **VPN**
   set vpn tokyo_paris manual 3020 3030 gateway 2.2.2.2 outgoing-interface ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a
   set vpn tokyo_paris bind zone untrust-tun

4. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

5. **ポリシー**
   set policy top name "To/From Paris" from trust to untrust Trust_LAN paris_office any tunnel vpn tokyo_paris
   set policy top name "To/From Paris" from untrust to trust paris_office Trust_LAN any tunnel vpn tokyo_paris
   save

CLI (パリ)

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.2.2.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 2.2.2.2/24

2. **アドレス**
   set address trust Trust_LAN 10.2.2.0/24
   set address untrust tokyo_office 10.1.1.0/24

3. **VPN**
   set vpn paris_tokyo manual 3030 3020 gateway 1.1.1.1 outgoing-interface ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a
   set vpn paris_tokyo bind zone untrust-tun

4. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250

5. **ポリシー**
   set policy top name "To/From Tokyo" from trust to untrust Trust_LAN tokyo_office any tunnel vpn paris_tokyo
   set policy top name "To/From Tokyo" from untrust to trust tokyo_office Trust_LAN any tunnel vpn paris_tokyo
   save

FQDN を使用した動的 IKE ゲートウェイ

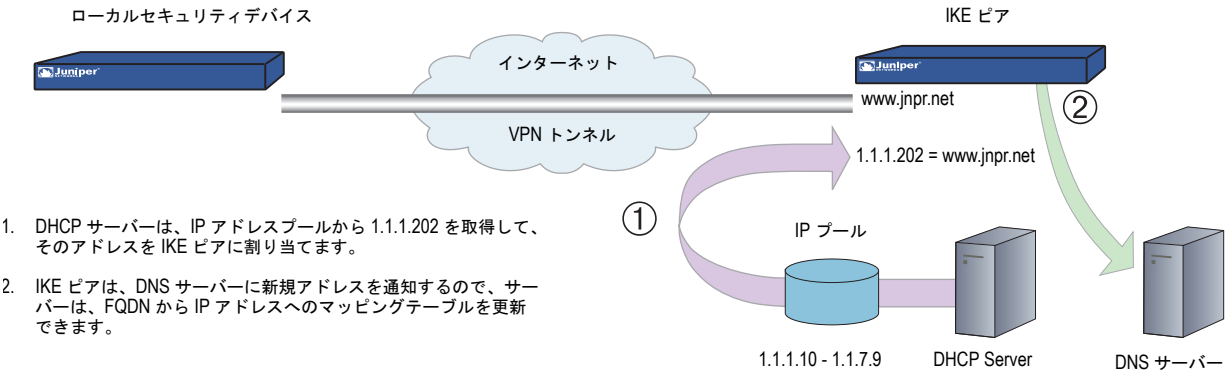
IP アドレスを動的に取得する IKE ピアでは、その完全修飾ドメイン名 (FQDN) をリモートゲートウェイのローカル構成に指定できます。たとえば、インターネットサービスプロトコル (ISP) は、DHCP を介して IP アドレスをそのカスタマに割り当てます。ISP は、大きなアドレスプールからアドレスを取得して、カスタマがオンラインになったときに割り当てます。IKE ピアには、一定の FQDN がありますが、予期せぬうちに変わる IP アドレスもあります。IKE ピアには、動的に割り当てられている IP アドレスに FQDN をマッピング (動的 DNS として知られるプロセス) するドメイン名システム (DNS) を保守するときに使用できる 3 つの方法があります。

- リモート IKE ピアがセキュリティデバイスの場合、管理者は、セキュリティデバイスが新しい IP アドレスを ISP から受信するたびにその FQDN から IP アドレスへのマッピングを更新するように、DNS サーバーに手動で通知できます。

- リモート IKE ピアが、動的 DNS ソフトウェアを実行しているその他の VPN 端末デバイスの場合、そのソフトウェアは、DNS サーバーにアドレスの変更を自動的に通知できます。そのため、サーバーは、FQDN から IP アドレスへのマッピングテーブルを更新できます。

- リモート IKE ピアが、セキュリティデバイスまたはその他の VPN 端末デバイスの場合、その後ろのホストは、アドレス変更の DNS サーバーを警告する、FQDN から IP アドレスへの自動更新プログラムを実行できます。

図 36: 動的 IP アドレスを使用する IKE ピア

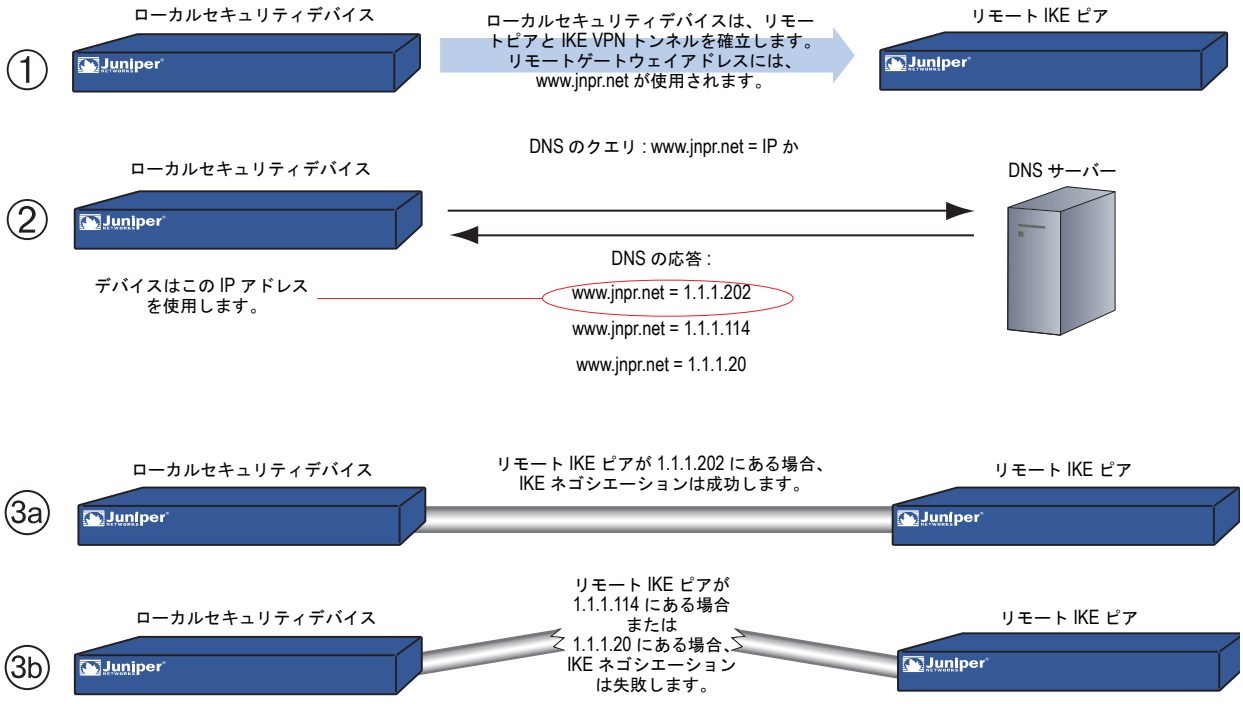


これで、リモート IKE ピアの現在の IP アドレスを理解しなくても、IP アドレスではなく FQDN を使用するピアに AutoKey IKE VPN トンネルを構成できます。

エイリアス

ローカルセキュリティデバイスが検索する DNS サーバーで必要な IP アドレスが 1 つだけの場合、リモート IKE ピアの FQDN にエイリアスを使用できます。DNS サーバーが複数の IP アドレスを返す場合、ローカルデバイスは、最初に受信したアドレスを使用します。DNS サーバーがアドレスを返す順序は確定できないため、ローカルセキュリティデバイスは、間違った IP アドレスを使用する可能性があり、この場合 IKE ネゴシエーションは失敗します。

図 37: IKE ネゴシエーションの成否につながる複数の DNS 応答

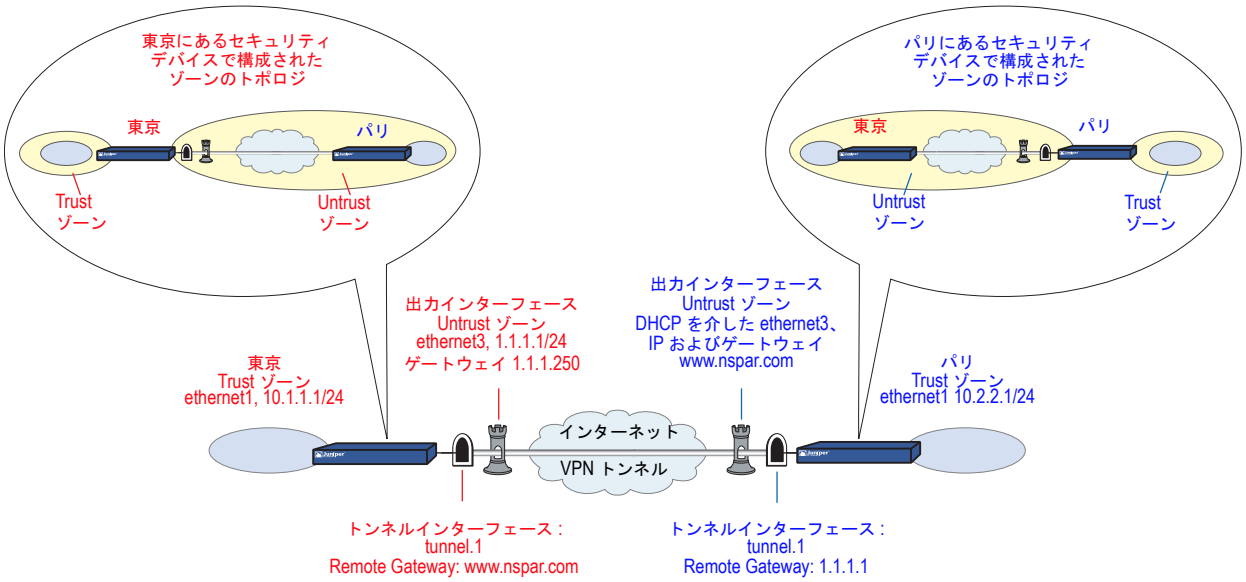


FQDN を使用した AutoKey IKE ピアを設定する

この例では、事前共有の秘密あるいは証明書のペア (それぞれトンネルの両端) を使用する AutoKey IKE VPN が 2 つのオフィス間を安全な接続でつなぎます。パリオフィスには、IP アドレスが動的に割り当てられているので、東京オフィスは、リモートピアの FQDN (www.nspar.com) を VPN トンネル構成のリモートゲートウェイのアドレスとして使用します。

図 38 に示される構成は、ルートベースの VPN トンネルのものです。フェーズ 1 と フェーズ 2 セキュリティレベルに対して、フェーズ 1 プロポーザル (事前共有鍵方法の場合の pre-g2-3des-sha、または証明書の場合の rsa-g2-3des-sha のいずれか) を指定し、フェーズ 2 のプロポーザルに対する定義済みの「Compatible」セットを選択します。すべてのゾーンは、trust-vr 内にあります。

図 38: FQDN を使用した AutoKey IKE ピア



事前共有鍵か証明書を使用してのルートベース AutoKey IKE トンネルの設定は、以下の手順に従ってください。

1. IP アドレスをセキュリティゾーンの物理的インターフェースとトンネルインターフェースにバインドさせます。
2. リモートゲートウェイと鍵交換モードを定義して、事前共有秘密あるいは証明書を指定します。
3. VPN トンネルを構成し、出力インターフェースを Untrust ゾーンに指定し、トンネルインターフェースにバインドしてから、プロキシ ID を構成します。
4. ローカルとリモート端点の IP アドレスを Trust および Untrust アドレス帳に入力します。

5. trust-vr の外部ルーターのデフォルトルート、トンネルインターフェースを介した宛先へのルート、宛先への Null ルートを入力します。Null ルートには高いメトリック値（0 よりかなり大きい値）を割り当てて、宛先へのルートの第 2 候補となるようにしてください。トンネル インターフェースの状態が「ダウン（停止）」に変わり、そのインターフェースを参照しているルートが非アクティブになると、セキュリティ デバイスは、暗号化されていないトラフィックを転送するデフォルト ルートではなく、送信されるトラフィックを基本的にすべてドロップする Null ルートを利用します。

6. トラフィックのポリシーを各サイト間をパスするように設定します。

以下の例では、事前共有された鍵は h1p8A24nG5 です。双方の参加者が、すでに RSA 証明書を所有し、Entrust を CA (認証局) として使っていることが前提になっています（証明書の入手とロード方法については、19 ページの「公開鍵暗号化」を参照してください）。

WebUI (東京)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (選択)
Interface: ethernet3 (trust-vr)

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Trust_LAN
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Paris_Office
IP Address/Domain Name:
IP/Netmask: (選択), 10.2.2.0/24
Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: To_Paris
Security Level: Custom
Remote Gateway Type:
Static IP Address: (選択), IP Address/Hostname: www.nspar.com

事前共有鍵

Preshared Key: h1p8A24nG5
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Main (ID 保護)

(または)

証明書

Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): rsa-g2-3des-sha
Preferred certificate (optional)
Peer CA: Entrust
Peer Type: X509-SIG

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: Tokyo_Paris
Security Level: Compatible
Remote Gateway:
Predefined: (選択), To_Paris

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Security Level: Compatible
Bind to: Tunnel Interface, tunnel.1
Proxy-ID: (選択)
Local IP / Netmask: 10.1.1.0/24
Remote IP / Netmask: 10.2.2.0/24
Service: ANY

4. **ルート**
   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (**選択**)
   Interface: ethernet3
   Gateway IP Address: 0.0.0.0

注 : ISP は、DHCP を通じてゲートウェイ IP アドレスを動的に割り当てます。

   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 10.2.2.0/24
   Gateway: (**選択**)
   Interface: Tunnel.1
   Gateway IP Address: 0.0.0.0

   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 10.2.2.0/24
   Gateway: (**選択**)
   Interface: Null
   Gateway IP Address: 0.0.0.0
   Metric: 10

5. **ポリシー**
   Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Name: To_Paris
   Source Address: Trust_LAN
   Destination Address: Paris_Office
   Service: ANY
   Action: Permit
   Position at Top: (**選択**)

   Policies > Policy (From: Untrust, To: Trust) > New Policy: 次のように入力してから **OK** をクリックします。

   Name: From_Paris
   Source Address: Paris_Office
   Destination Address: Trust_LAN
   Service: ANY
   Action: Permit
   Position at Top: (**選択**)

WebUI (パリ)

1. ホストネームとドメインネーム

Network > DNS: 以下を入力して **Apply** をクリックします。

Host Name: www
Domain Name: nspar.com

2. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.2.2.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Obtain IP using DHCP: (選択)

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (選択)
Interface: ethernet3 (trust-vr)

3. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Trust_LAN
IP Address/Domain Name:
IP/Netmask: (選択), 10.2.2.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Tokyo_Office
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Untrust

4. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: To_Tokyo
Security Level: Custom
Remote Gateway Type:
Static IP Address: (選択), IP Address/Hostname: 1.1.1.1

事前共有鍵

Preshared Key: h1p8A24nG5
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Main (ID 保護)

(または)

証明書

Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): rsa-g2-3des-sha
Preferred certificate (optional)
Peer CA: Entrust
Peer Type: X509-SIG

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

Name: Paris_Tokyo
Security Level: Custom
Remote Gateway:
Predefined: (選択), To_Tokyo

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Security Level: Compatible
Bind to: Tunnel Interface, tunnel.1
Proxy-ID: (選択)
Local IP / Netmask: 10.2.2.0/24
Remote IP / Netmask: 10.1.1.0/24
Service: ANY

5. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 2.2.2.250

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
Gateway: (選択)
Interface: Tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
Gateway: (選択)
Interface: Null
Gateway IP Address: 0.0.0.0
Metric: 10

6. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Name: To_Tokyo
Source Address: Trust_LAN
Destination Address: Tokyo_Office
Service: ANY
Action: Permit
Position at Top: (選択)

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Name: From_Tokyo
Source Address: Tokyo_Office
Destination Address: Trust_LAN
Service: ANY
Action: Permit
Position at Top: (選択)

CLI (東京)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. アドレス

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust paris_office 10.2.2.0/24
```

3. VPN

事前共有鍵

```
set ike gateway to_paris address www.nspar.com main outgoing-interface
    ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn tokyo_paris gateway to_paris sec-level compatible
set vpn tokyo_paris bind interface tunnel.1
set vpn tokyo_paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

(または)

認定書

```
set ike gateway to_paris address www.nspar.com main outgoing-interface
    ethernet3 proposal rsa-g2-3des-sha
set ike gateway to_paris cert peer-ca 1
set ike gateway to_paris cert peer-cert-type x509-sig
set vpn tokyo_paris gateway to_paris sec-level compatible
set vpn tokyo_paris bind interface tunnel.1
set vpn tokyo_paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

注： 番号 1 は、CA ID 番号です。CA の ID 番号を調べるには、**get ike ca** コマンドを使用してください。

4. **ルート**

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 10.2.2.0/24 interface null metric 10
```

5. **ポリシー**

```
set policy top name "To Paris" from trust to untrust Trust_LAN paris_office any
    permit
set policy top name "From Paris" from untrust to trust paris_office Trust_LAN any
    permit
save
```

CLI (パリ)

1. **ホストネームとドメインネーム**

```
set hostname www
set domain nspar.com
```

2. **インターフェース**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip dhcp-client enable
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

3. **アドレス**

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust tokyo_office 10.1.1.0/24
```

4. **VPN**

事前共有鍵

```
set ike gateway to_tokyo address 1.1.1.1 main outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn paris_tokyo gateway to_tokyo sec-level compatible
set vpn paris_tokyo bind interface tunnel.1
set vpn paris_tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

(または)

認定書

```
set ike gateway to_tokyo address 1.1.1.1 main outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway to_tokyo cert peer-ca 1
set ike gateway to_tokyo cert peer-cert-type x509-sig
set vpn paris_tokyo gateway to_tokyo sec-level compatible
set vpn paris_tokyo bind interface tunnel.1
set vpn paris_tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

5. **ルート**

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
set vrouter trust-vr route 10.1.1.0/24 interface null metric 10
```

6. **ポリシー**

```
set policy top name "To Tokyo" from trust to untrust Trust_LAN tokyo_office any
    permit
set policy top name "From Tokyo" from untrust to trust tokyo_office Trust_LAN any
    permit
save
```

アドレスがオーバーラップする VPN サイト

プライベート IP アドレスの範囲は比較的小さいため、2 つの VPN ピアの保護ネットワークのアドレスがオーバーラップすることがあります。双方向の VPN トラフィックが、アドレスがオーバーラップしている両端間で受け渡しされる場合、トンネルの両端にあるセキュリティデバイスは、ソースおよび宛先ネットワークアドレス変換 (NAT-src および NAT-dst) をデバイス間で受け渡しされる VPN トラフィックに適用する必要があります。

注 : ここでいう「アドレス空間の重複」とは、2 つのネットワークで、IP アドレス範囲の一部または全部が一致してしまっている、という状況のことです。

NAT-src については、トンネルの両端のインターフェースは、各サブネットに動的 IP (DIP) プールがある一意のサブネットに IP アドレスを持つ必要があります。アウトバウンド VPN トラフィックを規制するポリシーは、DIP プールアドレスを使用する NAT-src を適用して、元のソースアドレスを中立的なアドレス空間のアドレスに変換できます。

注 : DIP プールのアドレスのレンジは、トンネルインターフェースと同じサブネットになければなりませんが、プールはそのサブネットにあるインターフェース IP アドレスや MIP あるいは VIP アドレスを含むことはできません。セキュリティゾーンインターフェースでは、インターフェース IP アドレスとは異なるサブネットの拡張 IP アドレスと付属する DIP プールも定義することができます。詳細については、**2**-146 ページの「異なるサブネットでの DIP の使用」を参照してください。

インバウンド VPN トラフィックに NAT-dst を提供する場合、次の 2 つのオプションがあります。

- ポリシーベースの NAT-dst: ポリシーは、NAT-dst を適用して、インバウンド VPN トラフィックをトンネルインターフェースと同じサブネットにある (ただし、アウトバウンド VPN トラフィックに使用されるローカル DIP とは同じ範囲にない) アドレス、またはセキュリティデバイスがそのルートテーブルにエントリを持つ別のサブネットのアドレスに変換できます (NAT-dst 構成時のルーティングについては、**8**-32 ページの「NAT-Dst のルーティング」を参照してください)。

- MIP (マップ IP): ポリシーは、宛先アドレスとして MIP を参照できます。MIP は、トンネルインターフェースと同じサブネットにある (ただし、アウトバウンド VPN トラフィックに使用されるローカル DIP とは同じ範囲にない) アドレスを使用します （MIP の詳細については、**8**-61 ページの「マップ IP アドレス」を参照してください。）

アドレスがオーバーラップしているサイト間の VPN トラフィックは、両方向でのアドレス変換が必要です。アウトバウンドトラフィックのソースアドレスは、インバウンドトラフィックの宛先アドレスとは同じにすることができない (つまり、NAT-dst アドレスまたは MIP は DIP プールに入れることができない) ので、インバウンドおよびアウトバウンドポリシーで参照されるアドレスは対照的にはなりません。

セキュリティデバイスで、同じトンネルを介する両方向の VPN トラフィックに対してソースおよび宛先アドレス変換を実行する場合、次のいずれかを行います。

- ポリシーベース VPN 構成のプロキシ ID を定義します。特にポリシーの VPN トンネルを参照する場合、セキュリティデバイスは、そのトンネルのポリシーのコンポーネントからプロキシ ID を取得します。セキュリティデバイスは、ポリシーが最初に作成されるとき、およびデバイスがその後、再起動されるたびに、プロキシ ID を取得します。ただし、ポリシーで参照される VPN トンネルのプロキシ ID を手動で定義する場合、セキュリティデバイスは、ポリシーから取得されるプロキシ ID ではなく、ユーザー定義プロキシ ID を適用します。

注 : プロキシ ID は、ローカルアドレス、リモートアドレス、およびサービスの指定集合とトラフィックが一致するときに、そのトラフィックがトンネルを通過することを許可する IKE ピア間の同意のようなものです。

- ルートベースの VPN トンネル構成を使用します。ただし、この構成では、ユーザー定義プロキシ ID が必要です。これは、ルートベースの VPN 構成では、ポリシーの VPN トンネルは特に参照しないからです。その代わり、ポリシーは、特定の宛先へのアクセスを制限 (許可または拒否) します。その宛先へのルートは、VPN トンネルにバインドされるトンネルインターフェースをポイントします。VPN トンネルは、ソースアドレス、宛先アドレスおよびサービスからのプロキシ ID を取得できるポリシーと直接関連付けられていないので、そのプロキシ ID は手動で定義しなければなりません。（ルートベースの VPN 構成でも、1 つの VPN トンネル、すなわち 1 つのフェーズ 2 SA を利用する、複数のポリシーを作成できることに注意してください。）

アドレス空間がオーバーラップしている 2 つのサイト間の VPN トンネルを示す図 39 のアドレスについて考えます。

図 39: ピアサイトで重複するアドレス

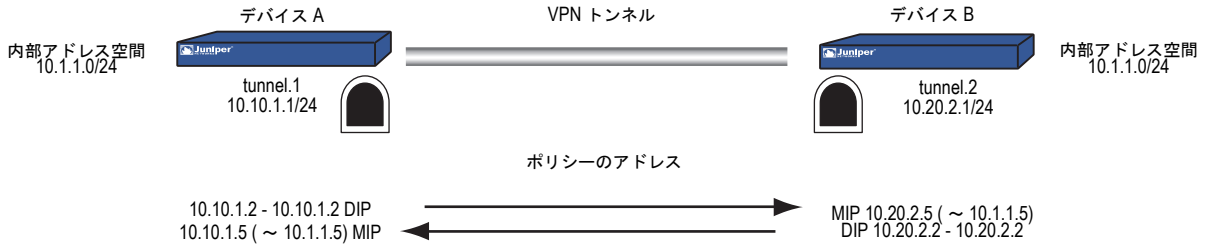


図 39 で示したセキュリティデバイスが、ポリシーベースの VPN 構成でするように、ポリシーからプロキシ ID を取得する場合、インバウンドおよびアウトバウンドポリシーは、以下のポリシー ID を生成します。

デバイス A				**デバイス B**			
	Local	リモート	Service		Local	リモート	Service
アウトバウンド	10.10.1.2/32	10.20.2.5/32	Any	インバウンド	10.20.2.5/32	10.10.1.2/32	Any
インバウンド	10.10.1.5/32	10.20.2.2/32	Any	アウトバウンド	10.20.2.2/32	10.10.1.5/32	Any

表に示されているように、プロキシ ID は、アウトバウンド VPN トラフィック、およびインバウンド用の 2 種類あります。1 つはアウトバウンド VPN トラフィック用、もう 1 つはインバウンド用です。デバイス A が、まず、10.10.1.2/32 から 10.20.2.5/32 にトラフィックを送信すると、2 つのピアは、IKE ネゴシエーションを実行して、フェーズ 1 およびフェーズ 2 のセキュリティアソシエーション (SA) を生成します。フェーズ 2 の SA は、デバイス A のアウトバウンドプロキシ ID、およびデバイス B のインバウンドプロキシ ID になります。

デバイス B がトラフィックをデバイス A に送信する場合、10.20.2.2/32 から 10.10.1.5/32 へのトラフィックのポリシールックアップは、このようなプロキシ ID のアクティブフェーズ 2 SA がないことを示します。したがって、2 つのピアは、既存のフェーズ 1 SA (寿命が切れていないことが前提です) を使用して、別のフェーズ 2 SA をネゴシエートします。結果のプロキシ ID は、デバイス A のインバウンドプロキシ ID、およびデバイス B のアウトバウンドプロキシ ID として上記に示されています。アドレスが非対称で、異なるプロキシ ID が必要なため、フェーズ 2 SA は 2 つあります。

つまり、VPN トンネルは 2 つあります。双方向 VPN トラフィックのトンネルを 1 つだけ作成するには、トンネルの両端で変換されるソースおよび宛先アドレスが範囲に含まれるアドレスを使用して、以下のプロキシ ID を定義します。

デバイス A			**デバイス B**		
Local	リモート	Service	Local	リモート	Service
10.10.1.0/24	10.20.2.0/24	Any	10.20.2.0/24	10.10.1.0/24	Any
		または			
0.0.0.0/0	0.0.0.0/0	Any	0.0.0.0/0	0.0.0.0/0	Any

上記のプロキシ ID は、2 つのサイト間にあるインバウンドおよびアウトバウンドの両方の VPN トラフィックのアドレスを含みます。アドレス 10.10.1.0/24 は、DIP プール 10.10.1.2 - 10.10.1.2、および MIP 10.10.1.5 の両方を含みます。同様に、アドレス 10.20.2.0/24 は、DIP プール 10.20.2.2 - 10.20.2.2、および MIP 10.20.2.5 の両方を含みます。上記のプロキシ ID は対称的です。つまり、デバイス A のローカルアドレスは、デバイス B のリモートアドレスであり、またその逆のことも言えます。デバイス A は、トラフィックをデバイス B に送信し、フェーズ 2 SA およびプロキシ ID は、デバイス B からデバイス A に送信されるトラフィックにも適用されます。そのため、2 つのサイト間の双方向トラフィックには、1 つのフェーズ 2 SA、つまり 1 つの VPN トンネルだけが必要です。

注： アドレス 0.0.0.0/0 は、すべての IP アドレスを含むので、DIP プールおよび MIP のアドレスも含まれます。

同じデバイスに構成されている NAT-src と NAT-dst のアドレスがそれぞれ異なるサブネットにあるときに、アドレス空間がオーバーラップしているサイト間の双方向トラフィックに対して VPN トンネルを 1 つだけ作成するには、そのトンネルのプロキシ ID を (ローカル IP) 0.0.0.0/0 - (リモート IP) 0.0.0.0/0 - *service type* にする必要があります。プロキシ ID のアドレスをより制限する場合、NAT-src および NAT-dst のアドレスは、同じサブネットになければなりません。

この例では、本社サイトの「デバイス A」と支社の「デバイス B」間に VPN トンネルを構成します。VPN の両端のアドレス空間はオーバーラップしていて、どちらも、10.1.1.0/24 サブネットのアドレスを使用します。この競合を解決するには、NAT-src を使用して、アウトバウンド VPN トラフィックのソースアドレスを変換し、NAT-dst を使用して、インバウンド VPN トラフィックの宛先アドレスを変換します。ポリシーでは、企業 LAN のすべてのアドレスから支社の FTP サーバーへのアクセスを許可し、支社のすべてのアドレスから企業サイトへの FTP サーバーへのアクセスを許可しています。

注： ソースおよび宛先のネットワークアドレス変換 (NAT-src および NAT-dst) についての詳細は、*第 8 部: アドレス変換*を参照してください。

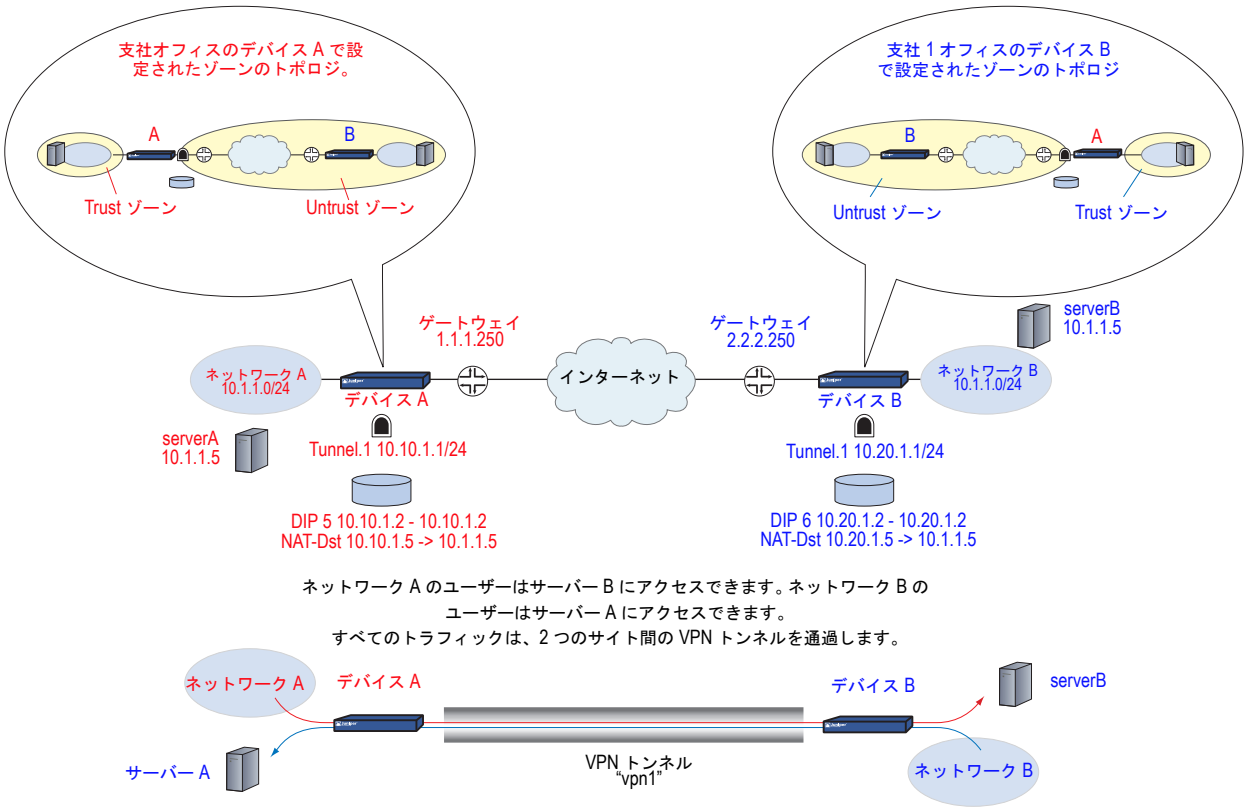
トンネルの両端での VPN トンネル構成には、以下のパラメータを使用します。すなわち、AutoKey IKE、事前共有鍵 (「netscreen1」) を設定し、セキュリティレベルは、フェーズ 1、フェーズ 2 のプロポーザルとも、「Compatible」としてあらかじめ定義しておいたレベルとします (これらのプロポーザルに関する詳細については、8 ページの「トンネルネゴシエーション」を参照してください)。

本社のデバイス A の出力インターフェースは、IP アドレスが 1.1.1.1/24 で Untrust ゾーンにバインドされる ethernet3 です。支社のデバイス B は、このアドレスをリモート IKE ゲートウェイとして使用します。

支社のデバイス B の出力インターフェースは、IP アドレスが 2.2.2.2/24 で Untrust ゾーンにバインドされる ethernet3 です。本社のデバイス A は、このアドレスをリモート IKE ゲートウェイとして使用します。

両方のセキュリティデバイスの Trust ゾーンインターフェースは、ethernet1 で、IP アドレスは 10.1.1.1/24 です。両方のセキュリティデバイスのすべてのゾーンは、trust-vr ルーティングドメイン内にあります。

図 40: NAT-Src と NAT-Dst のトンネルインターフェース



WebUI (デバイス A)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): Untrust (trust-vr)
Fixed IP: (選択)
IP Address/Netmask: 10.10.1.1/24

2. DIP

Network > Interfaces > Edit (tunnel.1) > DIP > New: 次のように入力してから **OK** をクリックします。

ID: 5
IP Address Range: (選択), 10.10.1.2 ～ 10.10.1.2
Port Translation: (選択)
In the same subnet as the interface IP or its secondary IPs: (選択)

3. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: corp
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: virtualA
IP Address/Domain Name:
IP/Netmask: (選択), 10.10.1.5/32
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: branch1
IP Address/Domain Name:
IP/Netmask: (選択), 10.20.1.2/32
Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: serverB
IP Address/Domain Name:
IP/Netmask: (選択), 10.20.1.5/32
Zone: Untrust

4. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: branch1
Type: Static IP: (選択), Address/Hostname: 2.2.2.2
Preshared Key: netscreen1
Security Level: Compatible
Outgoing Interface: ethernet3

注 : ここでは出力インターフェースに、トンネルインターフェースの先にあるゾーンを指定していますが、必ずしもそうでなくても構いません。

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface, tunnel.1
Proxy-ID: (選択)
Local IP/Netmask: 10.10.1.0/24
Remote IP/Netmask: 10.20.1.0/24
Service: ANY

5. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.20.1.0/24
Gateway: (選択)
Interface: Tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.20.1.0/24
Gateway: (選択)
Interface: Null
Gateway IP Address: 0.0.0.0
Metric: 10

6. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), corp
Destination Address:
Address Book Entry: (選択), serverB
Service: FTP
Action: Permit
Position at Top: (選択)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

NAT:
Source Translation: (選択)
DIP On: 5 (10.10.1.2-10.10.1.2)/X-late

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), branch1
Destination Address:
Address Book Entry: (選択), virtualA
Service: FTP
Action: Permit
Position at Top: (選択)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

NAT:
Destination Translation: (選択)
Translate to IP: (選択), 10.1.1.5
Map to Port:（オフ）

WebUI (デバイス B)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): Untrust (trust-vr)
Fixed IP: (選択)
IP Address/Netmask: 10.20.1.1/24

2. DIP

Network > Interfaces > Edit (tunnel.1) > DIP > New: 次のように入力してから **OK** をクリックします。

ID: 6
IP Address Range: (選択), 10.20.1.2 ～ 10.20.1.2
Port Translation: (選択)
In the same subnet as the interface IP or its secondary IPs: (選択)

3. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: branch1
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: virtualB
IP Address/Domain Name:
IP/Netmask: (選択), 10.20.1.5/32
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: corp
IP Address/Domain Name:
IP/Netmask: (選択), 10.10.1.2/32
Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: serverA
IP Address/Domain Name:
IP/Netmask: (選択), 10.10.1.5/32
Zone: Untrust

4. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: corp
Type: Static IP: (選択), Address/Hostname: 1.1.1.1
Preshared Key: netscreen1
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface, tunnel.1
Proxy-ID: (選択)
Local IP / Netmask: 10.20.1.0/24
Remote IP / Netmask: 10.10.1.0/24
Service: ANY

注 : ここでは出力インターフェースに、トンネルインターフェースの先にあるゾーンを指定していますが、必ずしもそうでなくても構いません。

5. **ルート**

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: ethernet3
Gateway IP Address: 2.2.2.250

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.10.1.0/24
Gateway: (**選択**)
Interface: Tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.10.1.0/24
Gateway: (**選択**)
Interface: Null
Gateway IP Address: 0.0.0.0
Metric: 10

6. **ポリシー**

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), corp
Destination Address:
Address Book Entry: (**選択**), serverA
Service: FTP
Action: Permit
Position at Top: (**選択**)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

NAT:
Source Translation: (**選択**)
DIP on: 6 (10.20.1.2-10.20.1.2)/X-late

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), corp
Destination Address:
Address Book Entry: (**選択**), virtualB
Service: FTP
Action: Permit
Position at Top: (**選択**)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

NAT:
Destination Translation: (選択)
Translate to IP: 10.1.1.5
Map to Port:（オフ）

CLI (デバイス A)

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24
   set interface tunnel.1 zone untrust
   set interface tunnel.1 ip 10.10.1.1/24
2. **DIP**
   set interface tunnel.1 dip 5 10.10.1.2 10.10.1.2
3. **アドレス**
   set address trust corp 10.1.1.0/24
   set address trust virtualA 10.10.1.5/32
   set address untrust branch1 10.20.1.2/32
   set address untrust serverB 10.20.1.5/32
4. **VPN**
   set ike gateway branch1 address 2.2.2.2 outgoing-interface ethernet3 preshare netscreen1 sec-level compatible
   set vpn vpn1 gateway branch1 sec-level compatible
   set vpn vpn1 bind interface tunnel.1
   set vpn vpn1 proxy-id local-ip 10.10.1.0/24 remote-ip 10.20.1.0/24 any

---

注 : ここでは出力インターフェースに、トンネルインターフェースの先にあるゾーンを指定していますが、必ずしもそうでなくても構いません。

---

5. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
   set vrouter trust-vr route 10.20.1.0/24 interface tunnel.1
   set vrouter trust-vr route 10.20.1.0/24 interface null metric 10
6. **ポリシー**
   set policy top from trust to untrust corp serverB ftp nat src dip-id 5 permit
   set policy top from untrust to trust branch1 virtualA ftp nat dst ip 10.1.1.5 permit
   save

CLI (デバイス B)

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 2.2.2.2/24
   set interface tunnel.1 zone untrust
   set interface tunnel.1 ip 10.20.1.1/24

2. **DIP**
   set interface tunnel.1 dip 6 10.20.1.2 10.20.1.2
3. **アドレス**
   set address trust branch1 10.1.1.0/24
   set address trust virtualB 10.20.1.5/32
   set address untrust corp 10.10.1.2/32
   set address untrust serverA 10.10.1.5/32
4. **VPN**
   set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3 preshare netscreen1 sec-level compatible
   set vpn vpn1 gateway corp sec-level compatible
   set vpn vpn1 bind interface tunnel.1
   set vpn vpn1 proxy-id local-ip 10.20.1.0/24 remote-ip 10.10.1.0/24 any

注 : ここでは出力インターフェースに、トンネルインターフェースの先にあるゾーンを指定していますが、必ずしもそうでなくても構いません。

5. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
   set vrouter trust-vr route 10.10.1.0/24 interface tunnel.1
   set vrouter trust-vr route 10.10.1.0/24 interface null metric 10
6. **ポリシー**
   set policy top from trust to untrust branch1 serverA ftp nat src dip-id 6 permit
   set policy top from untrust to trust corp virtualB ftp nat dst ip 10.1.1.5 permit
   save

透過モード VPN

セキュリティデバイスインターフェースが透過モードの場合 (つまり、IP アドレスがなく、OSI モデルのレイヤ 2 で機能している場合)、VLAN1 IP アドレスを VPN 終端点として使用できます。インターフェースがルートまたは NAT モードのとき (つまり、IP アドレスがあり、レイヤ 3 で機能しているとき) に使用されている場合、出力インターフェースの代わりに、VPN トンネルは出力ゾーンを参照します。デフォルトでは、トンネルは、出力ゾーンとして V1-Untrust ゾーンを使用します。同じ出力ゾーンに複数のインターフェースがバインドされている場合、VPN トンネルは、このいずれかを使用できます。

注 : OSI モデルは、ネットワークプロトコルアーキテクチャのネットワーキング業界標準モデルです。OSI モデルは、いくつかのレイヤで構成されていて、レイヤ 2 はデータリンクレイヤで、レイヤ 3 はネットワークレイヤです。

現在のリリースでは、インターフェースが透過モードにあるセキュリティデバイスは、ポリシーベース VPN だけをサポートします。透過モードについての詳細は、**2**-82 ページの「透過モード」を参照してください。

両方のセキュリティデバイスのインターフェースが透過モードである必要はありません。トンネルのいずれかの終端にあるデバイスのインターフェースを透過モードにし、もう一方のデバイスをルートまたは NAT モードにできます。

この例では、インターフェースが透過モードで機能している 2 つのセキュリティデバイス間で、ポリシーベース AutoKey IKE VPN トンネルを設定します。

注 : 両方のセキュリティデバイスのインターフェースが透過モードである必要はありません。トンネルのいずれかの終端にあるデバイスのインターフェースを透過モードにし、もう一方のデバイスをルートまたは NAT モードにできます。

トンネルの両端にあるセキュリティデバイスの構成における重要な要素は以下のとおりです。

コンポーネント	デバイス A	デバイス B
V1-Trust ゾーン	インターフェース : ethernet1、0.0.0.0/0 (ローカル管理者に管理を許可する)	インターフェース : ethernet1、0.0.0.0/0 (ローカル管理者に管理を許可する)
V1-Untrust ゾーン	インターフェース : ethernet3、0.0.0.0/0	インターフェース : ethernet3、0.0.0.0/0
VLAN1 インターフェース	IP Address: 1.1.1.1/24 Manage IP: 1.1.1.2[1]	IP Address: 2.2.2.2/24 Manage IP: 2.2.2.3
アドレス	local_lan: V1-Trust の 1.1.1.0/24 peer_lan: V1-Untrust の 2.2.2.0/24	local_lan: V1-Trust の 2.2.2.0/24 peer_lan: V1-Untrust の 1.1.1.0/24
IKE ゲートウェイ	gw1、2.2.2.2、事前共有鍵 h1p8A24nG5、 security: compatible	gw1, 1.1.1.1, preshared key h1p8A24nG5, セキュリティ : compatible
VPN トンネル	セキュリティ : compatible	セキュリティ : compatible
ポリシー	local_lan -> peer_lan, すべてのサービス、 vpn1 peer_lan -> local_lan、任意のサービス、 vpn1	local_lan -> peer_lan, すべてのサービス、 vpn1 peer_lan -> local_lan、任意のサービス、 vpn1
外部ルーター	IP Address: 1.1.1.250	IP Address: 2.2.2.250
ルート	0.0.0.0/0、ゲートウェイ 2.2.2.250 の インターフェースを使用	0.0.0.0/0、ゲートウェイ 2.2.2.250 の インターフェースを使用

1.管理 IP アドレスを使用して管理トラフィックを受け取り、VLAN1 アドレスを使用して VPN トラフィックを終了させることにより、管理トラフィックと VPN トラフィックを区別できます。

インターフェースが透過モードにあるセキュリティデバイスでポリシーベース AutoKey IKE トンネルを構成するには、次の手順を行います。

1. 物理インターフェースから IP アドレスを削除し、これらをレイヤ 2 セキュリティゾーンにバインドします。
2. VLAN1 インターフェースの IP アドレスおよび管理 IP アドレスを割り当てます。
3. ローカルとリモート端点の IP アドレスを V1-Trust および V1-Untrust ゾーンのアドレス帳に入力します。
4. VPN トンネルを構成して、その出力インターフェースを V1-Untrust ゾーンに指定します。
5. trust-vr の外部ルーターのデフォルトルートを入力します。
6. VPN トラフィックのポリシーを各サイト間をパスするように設定します。

WebUI (デバイス A)

1. インターフェース

注 : VLAN1 IP アドレスを異なるサブネットに移動すると、セキュリティデバイスにより、前の VLAN1 インターフェースに関連する任意のルートが削除されます。セキュリティデバイスを WebUI を使用して構成する場合、ワークステーションは、まず VLAN1 アドレスにアクセスしてから、新しいアドレスと同じサブネット内に入る必要があります。VLAN1 アドレスを変更したら、ワークステーションの IP アドレスが新しい VLAN1 アドレスと同じサブネット内に入るように、この IP アドレスを変更する必要があります。また、場合によっては、セキュリティデバイスに物理的に隣接するようにワークステーションを再配置する必要があります。

Network > Interfaces > Edit (VLAN1 インターフェース): 次のように入力してから **OK** をクリックします。

IP Address/Netmask: 1.1.1.1/24
Manage IP: 1.1.1.2
Management Services: WebUI, Telnet, Ping

注 : V1-Trust ゾーンのローカル管理者が、VLAN1 管理 IP アドレスにアクセスできるように、V1-Trust ゾーンおよび VLAN1 インターフェースの両方で WebUI、Telnet、Ping の管理オプションを使用可能にします。WebUI を介した管理が、VLAN1 および V1-Trust ゾーンインターフェースで使用できない場合は、WebUI からセキュリティデバイスにアクセスしてこれらの設定をすることはできません。この場合、まず、コンソール接続を介してこれらのインターフェースで WebUI 管理を設定する必要があります。

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Management Services: WebUI, Telnet
Other Services: Ping

次のように選択してから **OK** をクリックします。

Zone Name: V1-Trust
IP Address/Netmask: 0.0.0.0/0

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: V1-Untrust
IP Address/Netmask: 0.0.0.0/0

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: local_lan
IP Address/Domain Name:
IP/Netmask: (**選択**), 1.1.1.0/24
Zone: V1-Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Peer_lan
IP Address/Domain Name:
IP/Netmask: (選択), 2.2.2.0/24
Zone: V1-Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: gw1
Security Level: Compatible
Remote Gateway Type:
Static IP Address: (選択), IP Address/Hostname: 2.2.2.2
Preshared Key: h1p8A24nG5
Outgoing Zone: V1-Untrust

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway:
Predefined: (選択), gw1

4. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: VLAN1 (VLAN)
Gateway IP Address: 1.1.1.250

5. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), local_lan
Destination Address:
Address Book Entry: (選択), peer_lan
Service: ANY
Action: Tunnel
Tunnel VPN: vpn1
Modify matching bidirectional VPN policy: (選択)
Position at Top: (選択)

WebUI (デバイス B)

1. インターフェース

注 : VLAN1 IP アドレスを異なるサブネットに移動すると、セキュリティデバイスにより、前の VLAN1 インターフェースに関連する任意のルートが削除されます。セキュリティデバイスを WebUI を使用して構成する場合、ワークステーションは、まず VLAN1 アドレスにアクセスしてから、新しいアドレスと同じサブネット内に入る必要があります。VLAN1 アドレスを変更したら、ワークステーションの IP アドレスが新しい VLAN1 アドレスと同じサブネット内に入るように、この IP アドレスを変更する必要があります。また、場合によっては、セキュリティデバイスに物理的に隣接するようにワークステーションを再配置する必要があります。

Network > Interfaces > Edit (VLAN1 インターフェース): 次のように入力してから **OK** をクリックします。

IP Address/Netmask: 2.2.2.2/24
Manage IP: 2.2.2.3
Management Services: WebUI, Telnet, Ping

注 : WebUI を介した管理が、VLAN1 および V1-Trust ゾーンインターフェースで使用できない場合は、WebUI からセキュリティデバイスにアクセスしてこれらの設定をすることはできません。この場合、まず、コンソール接続を介してこれらのインターフェースで WebUI 管理を設定する必要があります。

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Management Services: WebUI, Telnet
Other Services: Ping

次のように選択してから **OK** をクリックします。

Zone Name: V1-Trust
IP Address/Netmask: 0.0.0.0/0

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: V1-Untrust
IP Address/Netmask: 0.0.0.0/0

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: local_lan
IP Address/Domain Name:
IP/Netmask: (**選択**), 2.2.2.0/24
Zone: V1-Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: peer_lan
IP Address/Domain Name:
IP/Netmask: (選択), 1.1.1.0/24
Zone: V1-Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: gw1
Security Level: Compatible
Remote Gateway Type:
Static IP Address: (選択), IP Address/Hostname: 1.1.1.1
Preshared Key: h1p8A24nG5
Outgoing Zone: V1-Untrust

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway:
Predefined: (選択), gw1

4. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: VLAN1 (VLAN)
Gateway IP Address: 2.2.2.250

5. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), local_lan
Destination Address:
Address Book Entry: (選択), peer_lan
Service: ANY
Action: Tunnel
Tunnel VPN: vpn1
Modify matching bidirectional VPN policy: (選択)
Position at Top: (選択)

CLI (デバイス A)

1. インターフェースとゾーン

```
unset interface ethernet1 ip
unset interface ethernet1 zone
set interface ethernet1 zone v1-trust
set zone v1-trust manage web
set zone v1-trust manage telnet
set zone v1-trust manage ping
unset interface ethernet3 ip
unset interface ethernet3 zone
set interface ethernet3 zone v1-untrust
set interface vlan1 ip 1.1.1.1/24
set interface vlan1 manage-ip 1.1.1.2
set interface vlan1 manage web
set interface vlan1 manage telnet
set interface vlan1 manage ping
```

注 : V1-Trust ゾーンのローカル管理者が、VLAN1 管理 IP アドレスにアクセスできるように、V1-Trust ゾーンおよび VLAN1 インターフェースの両方で WebUI、Telnet、Ping の管理オプションを使用可能にします。

2. アドレス

```
set address v1-trust local_lan 1.1.1.0/24
set address v1-untrust peer_lan 2.2.2.0/24
```

3. VPN

```
set ike gateway gw1 address 2.2.2.2 main outgoing-interface v1-untrust preshare
    h1p8A24nG5 sec-level compatible
set vpn vpn1 gateway gw1 sec-level compatible
```

4. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway 1.1.1.250
```

5. ポリシー

```
set policy top from v1-trust to v1-untrust local_lan peer_lan any tunnel vpn vpn1
set policy top from v1-untrust to v1-trust peer_lan local_lan any tunnel vpn vpn1
save
```

CLI (デバイス B)

1. インターフェースとゾーン

```
unset interface ethernet1 ip
unset interface ethernet1 zone
set interface ethernet1 zone v1-trust
set zone v1-trust manage
unset interface ethernet3 ip
unset interface ethernet3 zone
set interface ethernet3 zone v1-untrust
set interface vlan1 ip 2.2.2.2/24
set interface vlan1 manage-ip 2.2.2.3
set interface vlan1 manage
```

2. アドレス

```
set address v1-trust local_lan 2.2.2.0/24
set address v1-untrust peer_lan 1.1.1.0/24
```

3. **VPN**
   set ike gateway gw1 address 1.1.1.1 main outgoing-interface v1-untrust preshare h1p8A24nG5 sec-level compatible
   set vpn vpn1 gateway gw1 sec-level compatible

4. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway 2.2.2.250

5. **ポリシー**
   set policy top from v1-trust to v1-untrust local_lan peer_lan any tunnel vpn vpn1
   set policy top from v1-untrust to v1-trust peer_lan local_lan any tunnel vpn vpn1
   save

第 5 章

ダイヤルアップ仮想プライベートネットワーク

Juniper Networks セキュリティ デバイスは、ダイヤルアップ VPN（仮想プライベート ネットワーク）接続をサポートできます。静的 IP アドレスを持つネットワーク デバイスを構成し、NetScreen-Remote クライアント、または動的 IP アドレスを持つ他のセキュリティ デバイスを使用して IPSec トンネルのセキュリティを確保できます。

本章のセクションは、以下のようになります。

- 158 ページの「ダイヤルアップ」
  - 159 ページの「ポリシーベース ダイヤルアップ VPN、AutoKey IKE」
  - 164 ページの「ルートベース ダイヤルアップ VPN、動的ピア」
  - 171 ページの「ポリシーベース ダイヤルアップ VPN、動的ピア」
  - 177 ページの「ダイヤルアップ VPN ユーザー用の双方向性ポリシー」
- 182 ページの「グループ IKE ID」
  - 182 ページの「証明書付きグループ IKE ID」
  - 184 ページの「ワイルドカードおよびコンテナ ASN1-DN IKE ID タイプ」
  - 187 ページの「グループ IKE ID（証明書）の作成」
  - 191 ページの「事前共有鍵を使用するグループ IKE ID の設定」
- 197 ページの「共有 IKE ID」

ダイヤルアップ

ユーザー単位で VPN ダイヤルアップのトンネルを構成するか、または 1 つのトンネル構成のみを必要とする VPN ダイアルアップグループにユーザーを組み込むことができます。また、グループ IKE ID ユーザーを作成することで、IKE ID が複数のダイヤルアップ IKE ユーザーの IKE ID の一部となる 1 人のユーザーを定義することもできます。グループ IKE ID ユーザーを作成して 1 人のユーザーを定義し、そのユーザーの IKE ID がダイヤルアップ IKE ユーザーの IKE ID の一部として使用されるようにすることもできます。

注： IKE ユーザーグループに関する詳細は、**9**-63 ページの「IKE ユーザーとユーザーグループ」を参照してください。Group IKE ID 機能に関する詳細については、182 ページの「グループ IKE ID」を参照してください。

ダイアルアップクライアントが NetScreen-Remote と同様に、仮想内部 IP アドレスをサポートする場合は、動的ピアダイアルアップ VPN、AutoKey IKE トンネル (事前共有鍵または認証を使用) を作成することもできます。静的 IP アドレスを持つ Juniper Networks セキュリティ ゲートウェイを構成し、NetScreen-Remote クライアント、または動的 IP アドレスを持つ他のセキュリティ デバイスを使用して IPSec トンネルのセキュリティを確保することもできます。

注： 使用可能な VPN オプションの基本的な内容については、1 ページの「インターネットプロトコルセキュリティ」を参照してください。各種のオプションを選択する際の手引きは、45 ページの「VPN (仮想プライベートネットワーク) のガイドライン」を参照してください。

ポリシーベース VPN トンネルを VPN ダイアルアップユーザー用に構成することができます。ダイヤルアップ動的ピアクライアントには、ポリシーベースまたはルーティングベースの VPN のいずれかを構成することができます。ダイヤルアップ動的ピアクライアントは、NetScreen-Remote と同様に、仮想内部 IP アドレスをサポートできるため、指定したトンネルインターフェースを介して仮想内部アドレスに向かうルーティングテーブルエントリを構成できます。そうすることによって、セキュリティ デバイスとそのピアをつなぐルートベース VPN トンネルを構成することができます。

注： ダイヤルアップ動的ピアクライアントとは、仮想内部 IP アドレスをサポートするダイアルアップクライアントです。

ダイヤルアップ動的ピアはサイト間動的ピアとほぼ同じものですが、ダイヤルアップ クライアントの内部 IP アドレスが仮想アドレスであるという点が異なります。

ポリシーベース ダイヤルアップVPN、AutoKey IKE

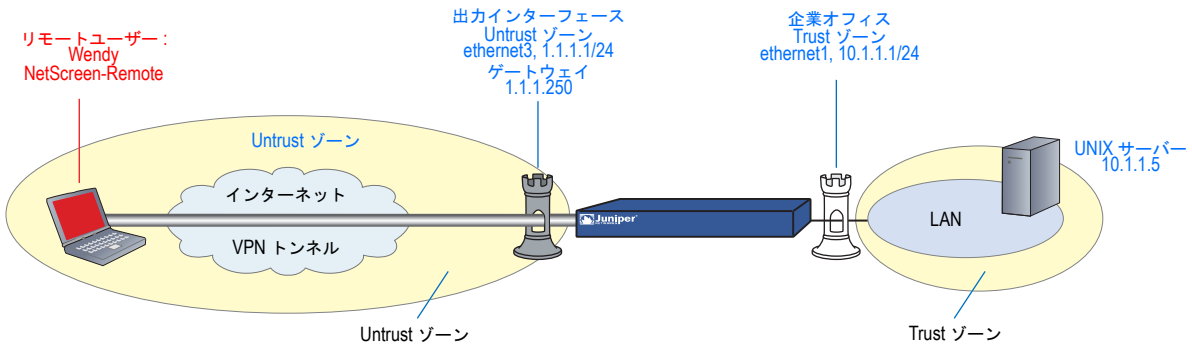
この例では、事前共有鍵または証明書のペア（各トンネル端に 1 つ）のどちらかを使用する AutoKey IKE トンネルを利用して、IKE ユーザーの Wendy と UNIX サーバーとの間でセキュア通信チャネルを実現します。この場合もトンネルは、3DES 暗号化パスワードおよび SHA-1 認証で ESP を使用します。

注 : 事前共有鍵は h1p8A24nG5 です。両方の参加者がすでに証明書を持っていると仮定します。証明書に関する詳細については、24 ページの「証明書および CRL」を参照してください。

事前共有鍵または証明書で AutoKey IKE を使用する AutoKey IKE トンネルをセットアップするには、企業サイトで次の構成が必要となります。

1. ともに trust-vr ルーティングドメインに存在する Trust ゾーンおよび Untrust ゾーンのインターフェースを構成する。
2. Trust ゾーンアドレス帳に UNIX サーバーのアドレスを入力する。
3. Wendy を IKE ユーザーとして定義する。
4. リモートゲートウェイおよび AutoKey IKE VPN を構成する。
5. デフォルトルートを設定する。
6. Untrust ゾーンから Trust ゾーンへの、ダイアルアップユーザーから UNIX へのアクセスを許可するポリシーを作成する。

図 41: ポリシーベース ダイヤルアップ VPN、AutoKey IKE



事前共有鍵は h1p8A24nG5 です。この例では、両方の参加者がすでに Verisign により発行された RSA 証明書を所有しており、NetScreen-Remote のローカル証明書に U-FQDN wparker@email.com *が含まれることを前提としています*（証明書の入手とロード方法については、24 ページの「証明書および CRL」を参照してください）。フェーズ 1 および 2 セキュリティ レベルに対して、フェーズ 1 プロポーザル（事前共有鍵方法の場合は pre-g2-3des-sha、または証明書の場合は rsa-g2-3des-sha のいずれか）を指定し、フェーズ 2 のプロポーザルに対して定義済みの「Compatible」を選択します。

WebUI

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24
次のように選択してから **OK** をクリックします。
Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: UNIX
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.5/32
Zone: Trust

3. ユーザー

Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

User Name: Wendy
Status: Enable (選択)
IKE User: (選択)
Simple Identity: (選択)
IKE Identity: wparker@email.com

4. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: Wendy_NSR
Security Level: Custom
Remote Gateway Type:
Dialup User: (選択), User: Wendy

証明書

Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): rsa-g2-3des-sha
Mode (Initiator): Aggressive
Preferred Certificate (optional):
Peer CA: Verisign
Peer Type: X509-SIG

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: Wendy_UNIX
Security Level: Compatible
Remote Gateway:
Predefined: (**選択**), Wendy_NSR

(または)

事前共有鍵



注意 : アグレッシブ モードは安全ではありません。ダイヤルアップ VPN ユーザーの場合、プロトコルの制限上、メイン モードと PSK（事前共有鍵）の組み合わせは使用できません。また、アグレッシブ モードは、本質的にセキュリティの問題があるためお勧めできません。したがって、PKI 証明書を持ったメイン モードのダイヤルアップ VPN ユーザーを構成することを強くお勧めします。

Preshared Key: h1p8A24nG5
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Aggressive

5. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

6. Policy

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Dial-Up VPN
Destination Address:
Address Book Entry: (**選択**), UNIX
Service: ANY
Action: Tunnel
Tunnel VPN: Wendy_UNIX
Modify matching bidirectional VPN policy: (**オフ**)
Position at Top: (**選択**)

CLI

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. アドレス

```
set address trust unix 10.1.1.5/32
```

3. ユーザー

```
set user wendy ike-id u-fqdn wparker@email.com
```

4. VPN

証明書

```
set ike gateway wendy_nsr dialup wendy aggressive outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway wendy_nsr cert peer-ca 1
set ike gateway wendy_nsr cert peer-cert-type x509-sig
set vpn wendy_unix gateway wendy_nsr sec-level compatible
```

注 : 番号 1 は、CA ID 番号です。CA の ID 番号を調べるには、**get pki x509 list ca-cert** コマンドを使用してください。

(または)

事前共有鍵



注意 : アグレッシブ モードは安全ではありません。ダイヤルアップ VPN ユーザーの場合、プロトコルの制限上、メイン モードと PSK（事前共有鍵）の組み合わせは使用できません。また、アグレッシブ モードは、本質的にセキュリティの問題があるためお勧めできません。したがって、PKI 証明書を持ったメイン モードのダイヤルアップ VPN ユーザーを構成することを強くお勧めします。

```
set ike gateway wendy_nsr dialup wendy aggressive outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn wendy_unix gateway wendy_nsr sec-level compatible
```

5. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

6. Policy

```
set policy top from untrust to trust “Dial-Up VPN” unix any tunnel vpn wendy_unix
save
```

NetScreen-Remote セキュリティポリシーエディタ

1. **Options > Secure > Specified Connections** をクリックします。
2. **Add a new connection** をクリックし、表示された新しい接続アイコンの横に **UNIX** と入力します。

3. 接続オプションを次のように構成します。

   Connection Security: Secure
   Remote Party Identity and Addressing:
   ID Type: IP Address, 10.1.1.5
   Protocol: All
   Connect using Secure Gateway Tunnel: (**選択**)
   ID Type: IP Address, 1.1.1.1

4. UNIX アイコンの左にある 「+」シンボルをクリックして接続ポリシーを拡張します。

5. **My Identity** をクリックします。次のいずれかを行ってください。

   Pre-shared Key > Enter Key をクリックします。**h1p8A24nG5** と入力してから **OK** をクリックします。

   ID Type: (**E-mail Address** を選択し)、**wparker@email.com** を入力します。

   (または)

   Select Certificate ドロップダウンリストから証明書を選択します。

   ID Type: (**E-mail Address** を選択します)

注 : 証明書の E メール アドレスは、自動的に識別フィールドに表示されます。

---

6. **Security Policy** アイコンをクリックして、**Aggressive Mode** を選択し、**Enable Perfect Forward Secrecy (PFS)** をオフにします。

7. Security Policy アイコンの左にある + シンボルをクリックしてから、Authentication (Phase 1) と Key Exchange (Phase 2) の左にある + シンボルをクリックし、ポリシーをさらに拡張します。

8. **Authentication (Phase 1) > Proposal 1** をクリックします。次の認証方法およびアルゴリズムを選択します。

   Authentication Method: Pre-Shared Key

   (または)

   Authentication Method: RSA Signatures
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Key Group: Diffie-Hellman Group 2

9. **Key Exchange (Phase 2) > Proposal 1** をクリックします。次の IPSec プロトコルを選択します。

   Encapsulation Protocol (ESP): (**選択**)
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Encapsulation: Tunnel

10. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: Triple DES
    Hash Alg: MD5
    Encapsulation: Tunnel

11. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel

12. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: DES
    Hash Alg: MD5
    Encapsulation: Tunnel

13. **File > Save Changes** をクリックします。

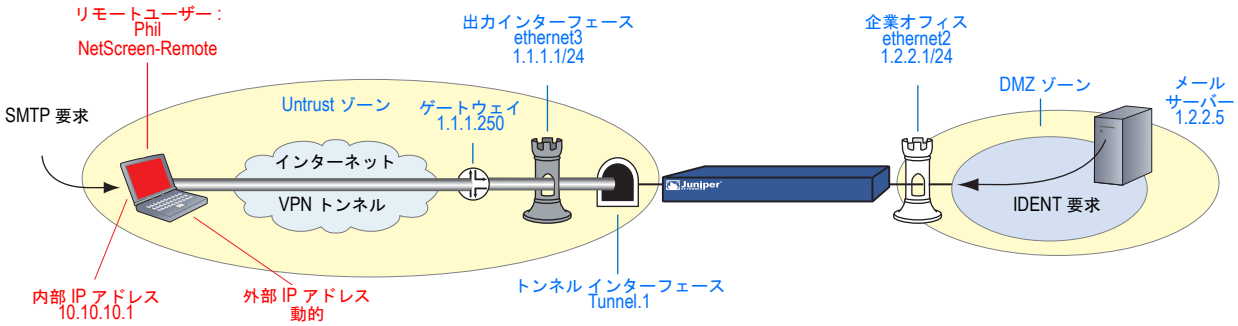
ルートベース ダイヤルアップVPN、動的ピア

この例では、VPN トンネルは、NetScreen-Remote の背後のユーザーを DMZ ゾーンのメール サーバーを保護するセキュリティ デバイスの Untrust ゾーン インターフェースに安全に接続します。Untrust ゾーンインターフェースは、静的 IP アドレスを持ちます。NetScreen-Remote クライアントは、動的に割り当てられた外部 IP アドレスと静的 (仮想) 内部 IP アドレスを持ちます。セキュリティ デバイスの管理者がピアの内部 IP アドレスを知っていなければならない理由として、次の 2 つがあります。

- ポリシーで使用する。
- 該当する VPN トンネルにバインドされたトンネルインターフェースにアドレスを結びつけるルートを作成する。

NetScreen-Remote クライアントがトンネルを確立すると、トンネルを介したトラフィックはいずれの端点からも発信することができます。セキュリティ デバイス上のすべてのゾーンは、trust-vr ルーティング ドメインに存在します。

図 42: ルートベース ダイヤルアップ VPN、動的ピア



この例では、Phil は企業サイトのメール サーバーから自分の E メールを取得しようとしています。E メールを取得しようとすると、Phil はメールサーバープログラムに認証され、トンネルを介して Phil に IDENT 要求が送られます。

注 : メール サーバーは、セキュリティ管理者がそれに対する顧客サービス（TCP、ポート 113）を追加し、トンネルを介して 10.10.10.1 に到達するトラフィックを許可する出力ポリシーを設定した場合にのみ、トンネルを介して IDENT 要求を送信できます。

事前共有鍵は h1p8A24nG5 です。ここでは、両方の参加者が Verisign により発行された RSA 証明書をすでに取得しており、NetScreen-Remote のローカル証明書に U-FQDN *pm@juniper.net が含まれていることを前提としています*（証明書の入手とロード方法については、24 ページの「証明書および CRL」を参照してください）。フェーズ 1 とフェーズ 2 セキュリティ レベルに対して、フェーズ 1 プロポーザル（事前共有鍵方法の場合は pre-g2-3des-sha、または証明書の場合は rsa-g2-3des-sha のいずれか）を指定し、フェーズ 2 のプロポーザルに対して定義済みの「Compatible」を選択します。

セキュリティ デバイスで、次の 3 つのルートを入力します。

- trust-vr の外部ルーターのデフォルトルート
- トンネル インターフェース経由の宛先までのルート
- 宛先までの Null ルート Null ルートには高いメトリック値（0 よりかなり大きい値）を割り当てて、宛先へのルートの第 2 候補となるようにしてください。トンネル インターフェースの状態が「ダウン（停止）」に変わり、そのインターフェースを参照しているルートが非アクティブになると、セキュリティ デバイスは、暗号化されていないトラフィックを転送するデフォルトルートではなく、送信されるトラフィックを基本的にすべてドロップする Null ルートを利用します。

最後に、Phil とメールサーバー間の双方向のトラフィックフローを許可するポリシーを作成します。

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

   Zone Name: DMZ
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.2.2.1/24

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

   Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

   Tunnel Interface Name: Tunnel.1
   Zone (VR): Untrust (trust-vr)
   Unnumbered: (選択)
   Interface: ethernet3 (trust-vr)

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: Mail Server
   IP Address/Domain Name:
   IP/Netmask: (選択), 1.2.2.5/32
   Zone: DMZ

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: Phil
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.10.10.1/32
   Zone: Untrust

3. **Services**
   Policy > Policy Elements > Services > Custom > New: 次のように入力してから **OK** をクリックします。

   Service Name: Ident
   Service Timeout:
   Use protocol default: (選択)
   Transport Protocol: TCP (選択)
   Source Port: Low 1, High 65535
   Destination Port: Low 113, High 113

Policy > Policy Elements > Services > Group > New: 次のように入力し、次のサービスを移動してから **OK** をクリックします。

Group Name: Remote_Mail
Group Members << Available Members:
Ident
MAIL
POP3

4. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: To_Phil
Security Level: Custom
Remote Gateway Type:
Dynamic IP Address: (**選択**), Peer ID: pm@juniper.net

事前共有鍵

Preshared Key: h1p8A24nG5
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Aggressive

(または)

証明書

Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): rsa-g2-3des-sha
Mode (Initiator): Aggressive
Preferred Certificate (optional):
Peer CA: Verisign
Peer Type: X509-SIG

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: corp_Phil
Security Level: Compatible
Remote Gateway:
Predefined: (**選択**), To_Phil

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface: (**選択する**), tunnel.1
Proxy-ID: (**選択**)
Local IP/Netmask: 1.2.2.5/32
Remote IP/Netmask: 10.10.10.1/32
Service: ANY

5. **ルート**

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.10.10.1/32
Gateway: (選択)
Interface: Tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.10.10.1/32
Gateway: (選択)
Interface: Null
Gateway IP Address: 0.0.0.0
Metric: 10

6. **ポリシー**

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Phil
Destination Address:
Address Book Entry: (選択), Mail Server
Service: Remote_Mail
Action: Permit
Position at Top: (選択)

Policies > (From: DMZ, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Mail Server
Destination Address:
Address Book Entry: (選択), Phil
Service: Remote_Mail
Action: Permit
Position at Top: (選択)

CLI

1. インターフェース

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 1.2.2.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. アドレス

```
set address dmz “mail server” 1.2.2.5/32
set address untrust phil 10.10.10.1/32
```

3. Services

```
set service ident protocol tcp src-port 1-65535 dst-port 113-113
set group service remote_mail
set group service remote_mail add ident
set group service remote_mail add mail
set group service remote_mail add pop3
```

4. VPN

事前共有鍵

```
set ike gateway to_phil dynamic pm@juniper.net aggressive outgoing-interface
    ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn corp_phil gateway to_phil sec-level compatible
set vpn corp_phil bind interface tunnel.1
set vpn corp_phil proxy-id local-ip 1.2.2.5/32 remote-ip 10.10.10.1/32 any
```

(または)

証明書

```
set ike gateway to_phil dynamic pm@juniper.net aggressive outgoing-interface
    ethernet3 proposal rsa-g2-3des-sha
set ike gateway to_phil cert peer-ca 1
set ike gateway to_phil cert peer-cert-type x509-sig
set vpn corp_phil gateway to_phil sec-level compatible
set vpn corp_phil bind interface tunnel.1
set vpn corp_phil proxy-id local-ip 1.2.2.5/32 remote-ip 10.10.10.1/32 any
```

注 : 番号 1 は、CA ID 番号です。CA の ID 番号を調べるには、**get pki x509 list ca-cert** コマンドを使用してください。

5. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.10.10.1/32 interface tunnel.1
set vrouter trust-vr route 10.10.10.1/32 interface null metric 10
```

6. ポリシー

```
set policy top from dmz to untrust “mail server” phil remote_mail permit
set policy top from untrust to dmz phil “mail server” remote_mail permit
save
```

NetScreen-Remote

1. **Options > Global Policy Settings** をクリックし、**Allow to Specify Internal Network Address** チェックボックスを選択します。

2. **Options > Secure > Specified Connections** を選択します。

3. **Add a new connection** ボタンをクリックし、表示された新しい接続アイコンの横に **Mail** と入力します。

4. 接続オプションを次のように構成します。

   Connection Security: Secure
   Remote Party Identity and Addressing:
   ID Type: IP Address, 1.2.2.5
   Protocol: All
   Connect using Secure Gateway Tunnel: (**選択**)
   ID Type: IP Address, 1.1.1.1

5. UNIX アイコンの左にある 「+」シンボルをクリックして接続ポリシーを拡張します。

6. **Security Policy** アイコンをクリックして、**Aggressive Mode** を選択し、**Enable Perfect Forward Secrecy (PFS)** をオフにします。

7. **My Identity** をクリックし、次のいずれかを行います。

   Pre-shared Key > Enter Key をクリックします。**h1p8A24nG5** と入力してから **OK** をクリックします。

   ID Type: E-mail Address; pm@juniper.net
   Internal Network IP Address: 10.10.10.1

   (または)

   Select Certificate ドロップダウン リストから、E メール アドレス「pm@juniper.net」を含む証明書を選択します。

   ID Type: E-mail Address; pm@juniper.net
   Internal Network IP Address: 10.10.10.1

8. Security Policy アイコンの左にある + シンボルをクリックしてから、Authentication (Phase 1) と Key Exchange (Phase 2) の左にある + シンボルをクリックし、ポリシーをさらに拡張します。

9. **Authentication (Phase 1) > Proposal 1** をクリックします。次の認証方法およびアルゴリズムを選択します。

   Authentication Method: Pre-Shared Key

   (または)

   Authentication Method: RSA Signatures
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Key Group: Diffie-Hellman Group 2

10. **Key Exchange (Phase 2) > Proposal 1** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: Triple DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel

11. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: Triple DES
    Hash Alg: MD5
    Encapsulation: Tunnel

12. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel

13. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

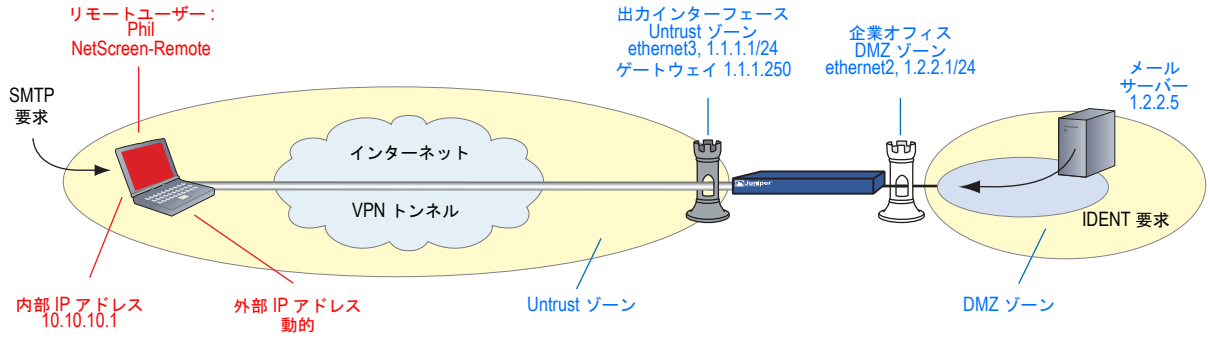
    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: DES
    Hash Alg: MD5
    Encapsulation: Tunnel

14. **File > Save Changes** をクリックします。

ポリシーベース ダイヤルアップVPN、動的ピア

この例では、VPN トンネルは、NetScreen-Remote の背後のユーザーを DMZ ゾーンのメール サーバーを保護するセキュリティ デバイスの Untrust ゾーン インターフェースに安全に接続します。Untrust ゾーンインターフェースは、静的 IP アドレスを持ちます。NetScreen-Remote クライアントは、動的に割り当てられた外部 IP アドレスと静的 (仮想) 内部 IP アドレスを持ちます。セキュリティ デバイスの管理者は、そのソースからのトラフィックにトンネルを通過させるポリシーで使用する Untrust アドレス帳に追加するために、クライアントの内部 IP アドレスを取得する必要があります。NetScreen-Remote クライアントがトンネルを確立すると、トンネルを介するトラフィックはいずれの端点からも発信することができます。

図 43: ポリシーベース ダイヤルアップ VPN、動的ピア



この例では、Phil は企業サイトのメール サーバーから自分の E メールを取得しようとしています。E メールを取得しようとすると、Phil はメールサーバープログラムに認証され、トンネルを介して Phil に IDENT 要求が送られます。

注 : メール サーバーは、セキュリティ管理者がそれに対する顧客サービス（TCP、ポート 113）を追加し、トンネルを介して 10.10.10.1 に到達するトラフィックを許可する出力ポリシーを設定した場合にのみ、トンネルを介して IDENT 要求を送信できます。

事前共有鍵は h1p8A24nG5 です。この例では、両方の参加者が Verisign により発行された RSA 証明書をすでに取得しており、NetScreen-Remote のローカル証明書に U-FQDN *pm@juniper.net* が含まれていることを前提としています (証明書の入手とロード方法に関しては、24 ページの「証明書および CRL」を参照してください。フェーズ 1 とフェーズ 2 セキュリティ レベルに対して、フェーズ 1 プロポーザル（事前共有鍵方法の場合は pre-g2-3des-sha、または証明書の場合は rsa-g2-3des-sha のいずれか）を指定し、フェーズ 2 のプロポーザルに対して定義済みの「Compatible」を選択します。

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

   Zone Name: DMZ
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.2.2.1/24

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Mail Server
IP Address/Domain Name:
IP/Netmask: (選択), 1.2.2.5/32
Zone: DMZ

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Phil
IP Address/Domain Name:
IP/Netmask: (選択), 10.10.10.1/32
Zone: Untrust

3. Services

Policy > Policy Elements > Services > Custom > New: 次のように入力してから **OK** をクリックします。

Service Name: Ident
Service Timeout:
Use protocol default: (選択)
Transport Protocol: TCP (選択)
Source Port: Low 1, High 65535
Destination Port: Low 113, High 113

Policy > Policy Elements > Services > Group > New: 次のように入力し、次のサービスを移動してから **OK** をクリックします。

Group Name: Remote_Mail
Group Members << Available Members:
Ident
MAIL
POP3

4. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: To_Phil
Security Level: Custom
Remote Gateway Type:
Dynamic IP Address: (選択), Peer ID: pm@juniper.net

事前共有鍵

Preshared Key: h1p8A24nG5
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Aggressive

(または)

証明書

Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): rsa-g2-3des-sha
Mode (Initiator): Aggressive
Preferred Certificate (optional):
Peer CA: Verisign
Peer Type: X509-SIG

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: corp_Phil
Security Level: Compatible
Remote Gateway:
Predefined: (**選択**), To_Phil

5. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

6. ポリシー

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Phil
Destination Address:
Address Book Entry: (**選択**), Mail Server
Service: Remote_Mail
Action: Tunnel
VPN Tunnel: corp_Phil
Modify matching bidirectional VPN policy: (**選択**)
Position at Top: (**選択**)

CLI

1. インターフェース

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 1.2.2.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. アドレス

```
set address dmz “mail server” 1.2.2.5/32
set address untrust phil 10.10.10.1/32
```

3. **Services**

```
set service ident protocol tcp src-port 1-65535 dst-port 113-113
set group service remote_mail
set group service remote_mail add ident
set group service remote_mail add mail
set group service remote_mail add pop3
```

4. **VPN**

事前共有鍵

```
set ike gateway to_phil dynamic pm@juniper.net aggressive outgoing-interface
    ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn corp_phil gateway to_phil sec-level compatible
```

(または)

証明書

```
set ike gateway to_phil dynamic pm@juniper.net aggressive outgoing-interface
    ethernet3 proposal rsa-g2-3des-sha
set ike gateway to_phil cert peer-ca 1
set ike gateway to_phil cert peer-cert-type x509-sig
set vpn corp_phil gateway to_phil sec-level compatible
```

注 : 番号 1 は、CA ID 番号です。CA の ID 番号を調べるには、**get pki x509 list ca-cert** コマンドを使用してください。

---

5. **ルート**

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

6. **ポリシー**

```
set policy top from untrust to dmz phil “mail server” remote_mail tunnel vpn
    corp_phil
set policy top from dmz to untrust "mail server" phil remote_mail tunnel vpn
    corp_phil
save
```

NetScreen-Remote

1. **Options > Global Policy Settings** をクリックし、**Allow to Specify Internal Network Address** を選択します。

2. **Options > Secure > Specified Connections** を選択します。

3. **Add a new connection** をクリックし、表示された新しい接続アイコンの横に **Mail** と入力してください。

4. 接続オプションを次のように構成します。

```
Connection Security: Secure
Remote Party Identity and Addressing:
    ID Type: IP Address, 1.2.2.5
    Protocol: All
    Connect using Secure Gateway Tunnel: ( 選択 )
    ID Type: IP Address, 1.1.1.1
```

5. UNIX アイコンの左にある 「+」シンボルをクリックして接続ポリシーを拡張します。

6. **Security Policy** アイコンをクリックして、**Aggressive Mode** を選択し、**Enable Perfect Forward Secrecy (PFS)** をオフにします。

7. **My Identity** をクリックし、次のいずれかを行います。

   Pre-shared Key > Enter Key をクリックします。**h1p8A24nG5** と入力してから **OK** をクリックします。

   Internal Network IP Address: 10.10.10.1
   ID Type: E-mail Address; pm@juniper.net

   (または)

   Select Certificate ドロップダウン リストから、E メール アドレス「pmason@email.com」を含む証明書を選択します。

   Internal Network IP Address: 10.10.10.1
   ID Type: E-mail Address; pm@juniper.net

8. Security Policy アイコンの左にある + シンボルをクリックしてから、Authentication (Phase 1) と Key Exchange (Phase 2) の左にある + シンボルをクリックし、ポリシーをさらに拡張します。

9. **Authentication (Phase 1) > Proposal 1** をクリックします。次の認証方法およびアルゴリズムを選択します。

   Authentication Method: Pre-Shared Key

   (または)

   Authentication Method: RSA Signatures
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Key Group: Diffie-Hellman Group 2

10. **Key Exchange (Phase 2) > Proposal 1** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: Triple DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel

11. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: Triple DES
    Hash Alg: MD5
    Encapsulation: Tunnel

12. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel

13. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: DES
    Hash Alg: MD5
    Encapsulation: Tunnel

14. **File > Save Changes** をクリックします。

ダイヤルアップVPN ユーザー用の双方向性ポリシー

ダイヤルアップ VPN 用に双方向性のポリシーを作成できます。この構成によって、動的ピア VPN 構成と類似した機能の利用が可能になります。ただし、動的ピア VPN 構成では、セキュリティ デバイス管理者は、出力ポリシーを構成する際に宛先アドレスとして使用できるように、ダイヤルアップ ユーザーの内部 IP アドレス空間を取得する必要があります（171 ページの「ポリシーベース ダイヤルアップ VPN、動的ピア」を参照してください）。ダイヤルアップ VPN ユーザー構成では、LAN サイトの管理者はダイアルアップユーザーの内部アドレス空間を知る必要はありません。LAN を保護するセキュリティ デバイスは、受信ポリシーのソース アドレスおよび出力ポリシーの宛先として、定義済みのアドレス「Dial-Up VPN」を使用します。

ダイヤルアップ VPN トンネルの双方向性ポリシーを作成する機能を利用することによって、接続が確立された後に、VPN 接続の LAN 端点からトラフィックを生成することが可能になります (リモート端は最初にトンネル作成を開始する必要があります)。ダイアルアップピア VPN トンネルとは異なり、この機能を利用するには、受信および出力ポリシーのサービスが同一であることが必要となることに注意してください。

注 : ScreenOS では、ダイヤルアップ VPN 構成を参照する双方向性ポリシーでのサービス グループおよびアドレス グループはサポートされていません。

同時に接続する 2 人以上のダイヤルアップ VPN ユーザーの内部アドレス空間は、オーバーラップすることがあります。たとえば、ダイヤルアップ ユーザーの A および B がどちらも、内部アドレス空間 10.2.2.0/24 を持つ場合があります。このような場合、セキュリティ デバイスは、ポリシー リストで検出した 1 番目のポリシーで参照される VPN を介して、ユーザー A および B の両者にすべてのアウトバウンド VPN トラフィックを送信します。たとえば、VPN を参照するユーザー A へのアウトバウンド ポリシーがポリシー リストの 1 番目に現れると、セキュリティ デバイスはユーザー A および B のためのすべてのアウトバウンド VPN トラフィックをユーザー A に送信します。

同様に、他のポリシーが VPN トンネルを参照するかしないかにかかわらず、ダイアルアップユーザーの内部アドレスが他の何らかのポリシー内のアドレスと偶然に重複することも考えられます。アドレスが重複する場合は、セキュリティ デバイスは、ソース アドレス、宛先アドレス、ソース ポート番号、宛先ポート番号、サービスの基本的なトラフィック属性が一致する 1 番目のポリシーを適用します。動的に生成されたアドレスを持つ双方向性ダイヤルアップ VPN ポリシーが、他のポリシーを静的アドレスで入れ替えることを避けるために、双方向性ダイヤルアップ VPN ポリシーをポリシーリストの低い位置に配置するようすお勧めします。

この例では、I*jf@ns.com* を持つ IKE ユーザー *dialup-j* 用の、*VPN_dial* という名前のダイアルアップ AutoKey IKE VPN トンネルに対する双方方向性ポリシーを構成します。フェーズ 1 ネゴシエーションに対し、事前共有鍵 *Jf11d7uU* でプロポーザル *pre-g2-3des-sha* を使用します。フェーズ 2 ネゴシエーションに対してプロポーザルの定義済みの「Compatible」を選択します。

IKE ユーザーは、Trust ゾーンの企業サーバーに到達するために、Untrust ゾーンからセキュリティ デバイスへの VPN 接続を開始します。IKE ユーザーが VPN 接続を確立すると、どちらのトンネル端からでもトラフィックを開始できます。

Trust ゾーンインターフェースは ethernet1 で、IP アドレス 10.1.1.1/24 を持ち、NAT モードで動作します。Untrust ゾーンインターフェースは ethernet3 で、IP アドレスは 1.1.1.1/24 です。デフォルトルートは、1.1.1.250 の外部ルーターを指します。

WebUI

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

2. オブジェクト

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Trust_net
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Trust

Policy > Policy Elements > Users > Local > New: 次のように入力してから **OK** をクリックします。

User Name: dialup-j
Status: Enable
IKE User: (選択)
Simple Identity: (選択); jf@ns.com

3. **VPN**

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: dialup1
Security Level: Custom
Remote Gateway Type:
Dialup User: (選択); dialup-j
Preshared Key: Jf11d7uU

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Aggressive

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: VPN_dial
Security Level: Compatible
Remote Gateway:
Create a Simple Gateway: (選択)
Gateway Name: dialup1
Type:
Dialup User: (選択); dialup-j
Preshared Key: Jf11d7uU
Security Level: Compatible
Outgoing Interface: ethernet3

4. **ルート**

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet1
Gateway IP Address: 1.1.1.250

5. **ポリシー**

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Dial-Up VPN
Destination Address:
Address Book Entry: (選択), trust_net
Service: ANY
Action: Tunnel
VPN Tunnel: VPN_dial
Modify matching bidirectional VPN policy: (選択)

CLI

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. オブジェクト

```
set address trust trust_net 10.1.1.0/24
set user dialup-j ike-id u-fqdn jf@ns.com
```

3. VPN

```
set ike gateway dialup1 dialup dialup-j aggressive outgoing-interface ethernet3
    preshare Jf11d7uU proposal pre-g2-3des-sha
set vpn VPN_dial gateway dialup1 sec-level compatible
```

4. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

5. ポリシー

```
set policy from untrust to trust “Dial-Up VPN” trust_net any tunnel vpn VPN_dial
set policy from trust to untrust trust_net “Dial-Up VPN” any tunnel vpn VPN_dial
save
```

NetScreen-Remote セキュリティポリシーエディタ

1. **Options > Secure > Specified Connections** をクリックします。
2. **Add a new connection** をクリックし、表示された新しい接続アイコンの横に **Corp** と入力します。
3. 接続オプションを次のように構成します。

   Connection Security: Secure
   Remote Party Identity and Addressing
   ID Type: IP Subnet
   Subnet: 10.1.1.0
   Mask: 255.255.255.0
   Protocol: All
   Connect using Secure Gateway Tunnel: (**選択**)
   ID Type: IP Address, 1.1.1.1

4. UNIX アイコンの左にある 「+」シンボルをクリックして接続ポリシーを拡張します。
5. **My Identity** をクリックします。次のいずれかを行ってください。

   Pre-shared Key > Enter Key をクリックします。**Jf11d7uU** と入力してから **OK** をクリックします。

   ID Type: (**E-mail Address** を選択し)、**jf@ns.com** を入力します。

6. **Security Policy** アイコンをクリックして、**Aggressive Mode** を選択し、**Enable Perfect Forward Secrecy (PFS)** をオフにします。

7. Security Policy アイコンの左にある + シンボルをクリックしてから、Authentication (Phase 1) と Key Exchange (Phase 2) の左にある + シンボルをクリックし、ポリシーをさらに拡張します。

8. **Authentication (Phase 1) > Proposal 1** をクリックします。次の認証方法およびアルゴリズムを選択します。

   Authentication Method: Pre-Shared Key

   (または)

   Authentication Method: RSA Signatures
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Key Group: Diffie-Hellman グループ 2

9. **Key Exchange (Phase 2) > Proposal 1** をクリックします。次の IPSec プロトコルを選択します。

   Encapsulation Protocol (ESP): (選択)
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Encapsulation: Tunnel

10. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (選択)
    Encrypt Alg: Triple DES
    Hash Alg: MD5
    Encapsulation: Tunnel

11. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (選択)
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel

12. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (選択)
    Encrypt Alg: DES
    Hash Alg: MD5
    Encapsulation: Tunnel

13. **File > Save Changes** をクリックします。

グループ IKE ID

企業によっては、多数のダイヤルアップ VPN ユーザーが存在することもあります。たとえば、営業部には数百人のユーザーが存在し、その多数がオフサイト時にセキュアダイアルアップ通信を必要とすることが考えられます。そのように多数のユーザーがいる場合、各自に対して個別にユーザー定義、ダイヤルアップ VPN 構成、およびポリシーを作成するのは実用的ではありません。

この問題を回避するために、グループ IKE ID 方式は、1 つのユーザー定義を複数のユーザーに対して使用できるようにします。グループ IKE ID ユーザー定義は、dn（識別名）に値を指定された証明書を持つすべてのユーザー、または IKE ID 全体およびその VPN クライアントの事前共有鍵が、セキュリティ デバイスの部分 IKE ID および事前共有鍵と一致するすべてのユーザーに適用されます。

注： ダイヤルアップ IKE ユーザーがセキュリティ デバイスに接続すると、セキュリティ デバイスは、ユーザーがグループ IKE ID ユーザー グループに属さない場合に備えて、まず IKE ID 全体でピア ゲートウェイ レコードを検索します。IKE ID 全体の検索でマッチングエントリが見つからなかった場合には、セキュリティ デバイスは受信埋め込み IKE ID と構成されたグループ IKE ID ユーザーとの間で IKE ID の部分一致をチェックします。

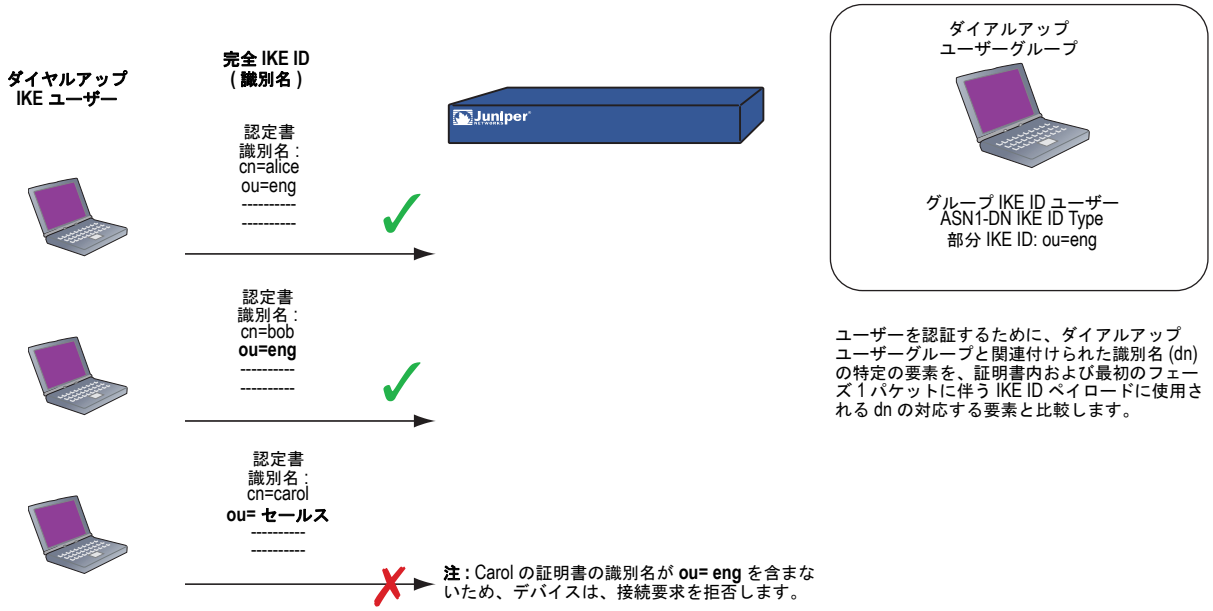
---

1 人のグループ IKE ID ユーザーを IKE ダイヤルアップ VPN ユーザー グループに追加し、そのグループがサポートする同時接続の最大数を指定します。同時セッションの最大数は、フェーズ 1 SA の最大数、またはプラットフォーム上で許可される VPN トンネルの最大数を超えることはできません。

証明書付きグループ IKE ID

証明書付きグループ IKE ID は、ユーザープロファイルを各ユーザー毎に個別に定義せずに、ダイアルアップ IKE ユーザーのグループに対して IKE 認証を実行する技法です。代わりに、セキュリティ デバイスは、部分 IKE ID を含む単一のグループ IKE ID ユーザー プロファイルを使用します。ダイヤルアップ IKE ユーザーは、自身の VPN クライアントでの VPN 構成が識別名要素を含む証明書を指定しており、その識別名要素がセキュリティ デバイス上のグループ IKE ID ユーザー プロファイル内の部分 IKE ID 定義として構成されたものと一致する場合に、正常にセキュリティ デバイスへの VPN トンネルを作成できます。

図 44: 証明書付きグループ IKE ID



次のように、証明書付きグループ IKE ID を設定できます。

セキュリティデバイス上 :

1. 一部 IKE 識別 (*ou = sales,o = netscreen* など) を持つ新しいグループ IKE ID ユーザーを作成し、何人のダイアルアップユーザーが IKE ID プロファイルを証してログオンできるかを指定します。

2. 新しい IKE ID ユーザーをダイアルアップユーザーグループに割り当てて、グループに名前を付けます。

注 : IKE ユーザーグループには、IKE ID ユーザーを 1 名のみ加えることができます。

---

3. ダイヤルアップ AutoKey IKE VPN 構成では、ダイヤルアップ ユーザー グループの名前を指定し、さらにフェーズ 1 ネゴシエーションがアグレッシブモードで行われること、そして認証に証明書（ダイヤルアップ VPN クライアントにロードされた証明書のタイプに応じて RSA または DSA）を使用することを指定します。

4. 指定されたダイヤルアップ VPN を介したインバウンドトラフィックを許可するポリシーを作成します。

VPN クライアント上 :

1. セキュリティ デバイス上の部分 IKE ID として定義された情報と同じもの情報を含む識別名を持つ証明書を入手してロードします。

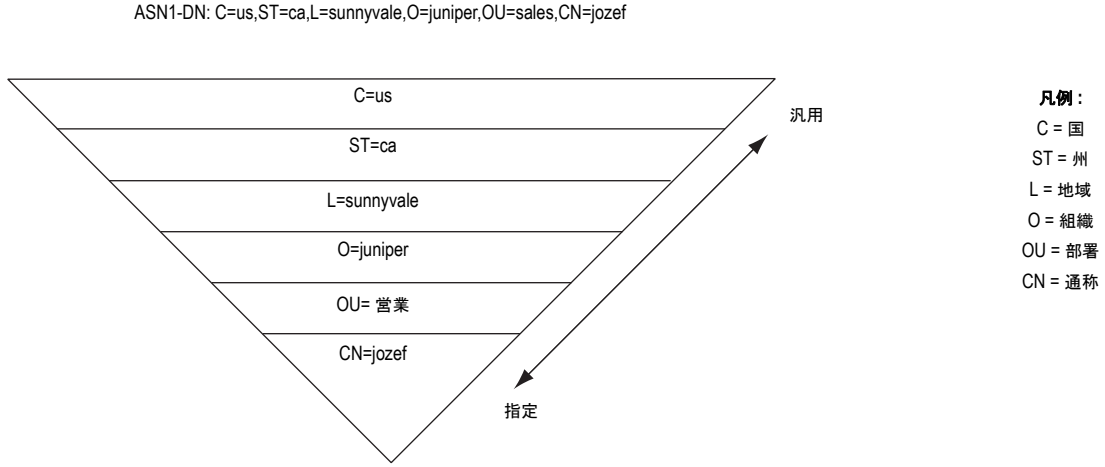
2. フェーズ 1 ネゴシエーションのアグレッシブ モードを使用して、セキュリティ デバイスへの VPN トンネルを構成し、ロード済みの証明書を指定し、ローカル IKE ID タイプに *Distinguished Name* を選択します。

以後、グループ IKE ID ユーザー プロファイルに定義された部分 IKE ID と適合する識別名要素を含む証明書を持つ各ダイヤルアップ IKE ユーザーは、セキュリティ デバイスへの VPN トンネルを正常に構築できます。たとえば、グループ IKE ID ユーザーが IKE ID *OU = sales, O = netscreen* を持つ場合、セキュリティ デバイスは、識別名にそれらの要素を含む証明書を持つ任意のユーザーからのフェーズ 1 ネゴシエーションを承認します。セキュリティ デバイスに接続できるダイヤルアップ IKE ユーザーの最大数は、グループ IKE ID ユーザー プロファイルに指定した同時セッションの最大数によって異なります。

ワイルドカードおよびコンテナ ASN1-DN IKE ID タイプ

グループ IKE ユーザー用に IKE ID を定義するときは、識別構成の IKE ID タイプとして、抽象構文記法バージョン 1、識別名 (ASN1-DN) を使用する必要があります。この記法は値からなる文字列で、多くの場合、汎用的なものから特定的なものへ順番に並べられていますが、そうでないこともあります。図 45 の例を参照してください。

図 45: ASN1 識別名



グループ IKE ID ユーザーを構成するときは、ピアの ASN1-DN ID を 次の 2 つのタイプのいずれかとして指定する必要があります。

- **ワイルドカード :** ScreenOS は、ダイヤルアップ IKE ユーザーの ASN1-DN 識別フィールドの値が、グループ IKE ユーザーの ASN1-DN 識別フィールドの値に適合する場合は、ダイヤルアップ IKE ユーザーの ID を認証します。ワイルドカード ID タイプは、識別フィールド 1 つあたりに 1 つのみの値をサポートします（たとえば、”ou = engE または “ou = swE はサポートしますが、“ou = eng,ou = sw” はサポートしません) B2 つの ASN1-DN 文字列の識別フィールドは、順序不同です。

- **コンテナ :** ScreenOS は、ダイヤルアップ IKE ユーザーの ASN1-DN 識別フィールドの値が、グループ IKE ユーザーの ASN1-DN 識別フィールドの値に厳密に適合する場合に、ダイヤルアップ IKE ユーザーの ID を認証します。コンテナ ID タイプは、各識別フィールドに対して複数のエントリをサポートします (たとえば、“ou = eng,ou = sw,ou = screenos”) をサポートします)。2 つの ASN1-DN 文字列の識別フィールドの値の順序は、一致する必要があります。

リモート IKE ユーザーに対して ASN1-DN ID を構成する場合は、「wildcard」または「container」のいずれかとしてタイプを指定し、ピアの証明書で受信を希望する ASN1-DN ID(たとえば、”c = us,st = ca,cn = kgreen”) を定義します。ローカル IKE ID に対して ASN1-DN ID を構成する場合は、キーワード [DistinguishedName] を使用します。大括弧を付けて、スペルに間違いがないように入力します。

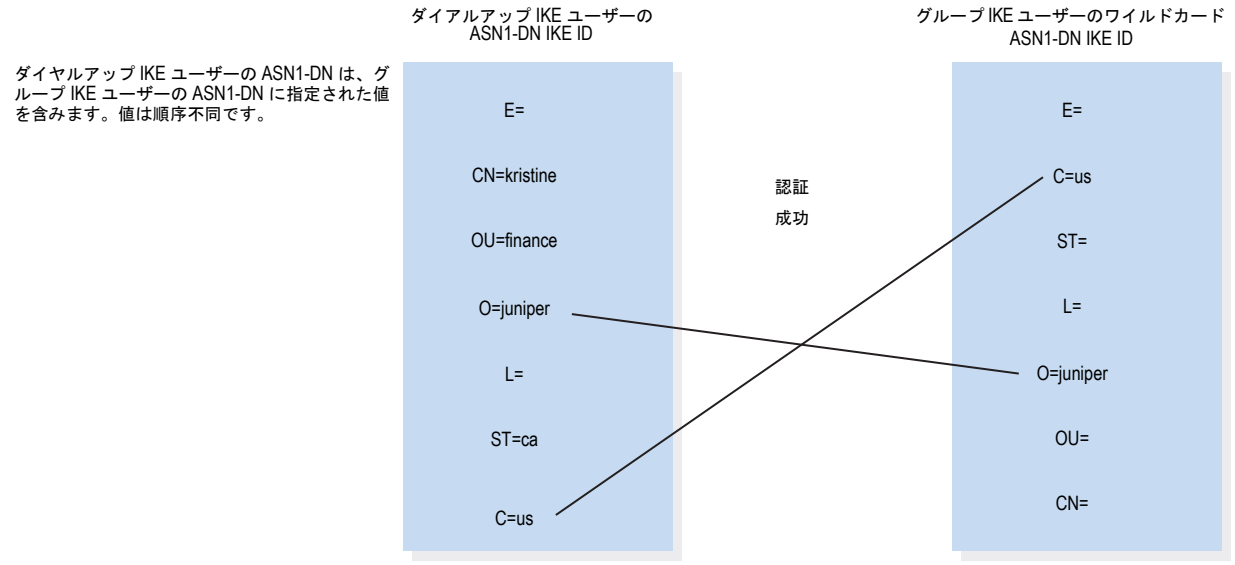
ワイルドカード ASN1-DN IKE ID

ワイルドカード ASN1-DN を利用する場合は、リモートピアの識別名 IKE ID がグループ IKE ユーザーの一部 ASN1-DN IKE ID と適合することが必要です。ASN1-DN 文字列のこれらの値は、順序不同です。たとえば、ダイアルアップ IKE ユーザーの ID およびグループ IKE ユーザーの ID が次のような場合を考えます。

- ダイヤルアップ IKE ユーザーの完全 ASN1-DN IKE ID:
  CN = kristine,OU = finance,**O = juniper**,ST = ca,**C = us**
- グループ IKE ユーザーの一部 ASN1-DN IKE ID: **C = us**,**O = juniper**

2 つの ID の値の順序が異なりますが、ワイルドカード ASN1-DN IKE ID は 2 つの IKE ID に正常に適合します。

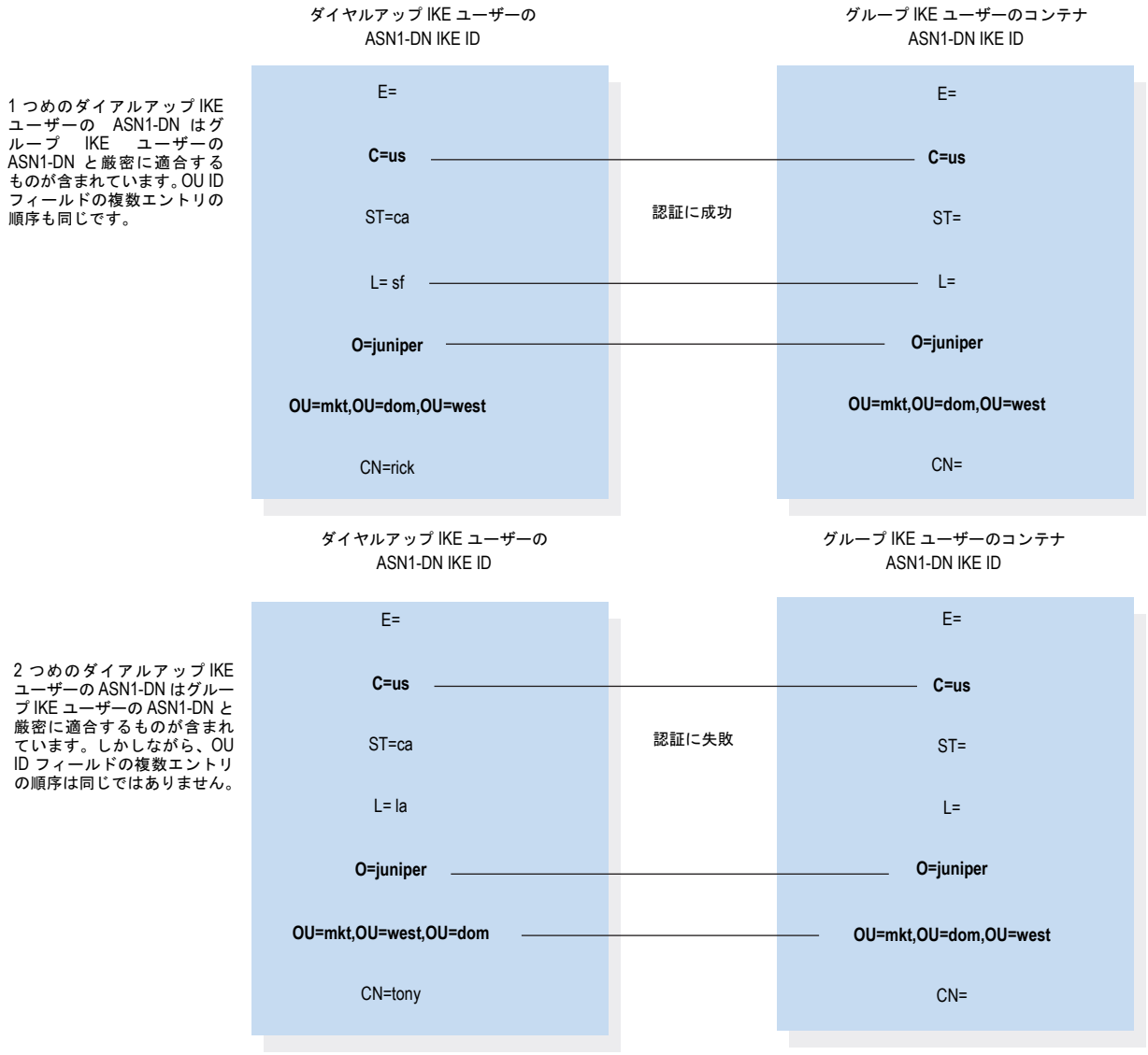
図 46: 正常なワイルドカード ASN1-DN 認証



コンテナ ASN1-DN IKE ID

コンテナ ASN1-DN ID によって、グループ IKE ユーザーの ID は各識別フィールドで複数のエントリを持つことができます。ScreenOS では、グループ IKE ユーザーの ID に厳密に適合する値がダイヤルアップ ユーザーの ID に含まれていれば、ダイヤルアップ IKE ユーザーは認証を受けることができます。ワイルドカード タイプとは異なり、ASN1-DN フィールドの順序は、ダイヤルアップ IKE ユーザーおよびグループ IKE ユーザーの両方の ID と一致する必要があり、これらのフィールド内の複数の値の順序も一致している必要があります。

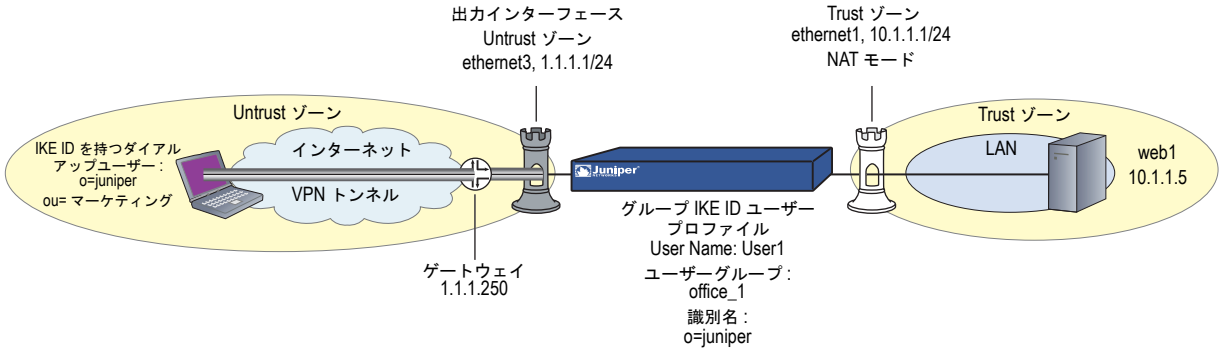
図 47: コンテナ ASN1-DN ID を使用した認証の成功と失敗



グループ IKE ID（証明書）の作成

この例では、*User1* という名前の新しいグループ IKE ID ユーザー定義を作成します。*O = netscreen* および *OU = marketing* を含む RSA 証明書を持つ VPN クライアントから、同時に最大 10 個のフェーズ 1 ネゴシエーションを承認するように構成します。CA (認証局) は Verisign です。ダイアルアップ IKE ユーザーグループには、*office_1* という名前をつけます。

図 48: グループ IKE ID



ダイヤルアップ IKE ユーザーは、自身の IKE ID として識別名を送信します。このグループのダイヤルアップ IKE ユーザーの識別名 (dn) は、次の連結文字列で表されると考えられます。

C=us,ST=ca,L=sunnyvale,**O=netscreen**,**OU=marketing**,CN=carrie nowocin,CN=a2010002,CN=ns500, CN=4085557800,CN=rsa-key,CN=10.10.5.44

ピアの証明書に *O = netscreen* および *OU = marketing* という値が現れ、ユーザーが識別名を IKE ID タイプとして使用しているため、セキュリティ デバイスはユーザーを認証します。

フェーズ 1 とフェーズ 2 のセキュリティ レベルに対しては、フェーズ 1 プロポーザル、つまり証明書に rsa-g2-3des-sha を指定し、フェーズ 2 のプロポーザルの定義済み「Compatible」セットを選択します。

ダイヤルアップ VPN、および HTTP トラフィックが VPN トンネルを介して Web サーバー *Web1* に到達するのを許可するポリシーを構成します。さらに、リモート VPN クライアント (NetScreen-Remote を使用) の構成が含まれます。

WebUI

1. **インターフェース**

   Network > Interfaces > Edit (ethernet1): 次のように入力してから **OK** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように選択してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: web1
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.5/32
   Zone: Trust

3. **ユーザー**
   Policy > Policy Elements > Users > Local > New: 次のように入力してから **OK** をクリックします。

   User Name: User1
   Status: (選択)
   IKE User: (選択)
   Number of Multiple Logins with same ID: 10
   Use Distinguished Name For ID: (選択)
   OU: marketing
   Organization: juniper

   Objects > User Groups > Local > New: Group Name フィールドに **office_1** と入力し、次の手順を行ってから **OK** をクリックします。

   User1 を選択し、**<<** ボタンを使用して Available Members 列から Group Members 列にこのユーザーを移動します。

4. **VPN**
   VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

   Gateway Name: Corp_GW
   Security Level: Custom
   Remote Gateway Type: Dialup User Group: (選択), Group: office_1
   Outgoing Interface: ethernet3

   > Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

   Security Level: Custom
   Phase 1 Proposal (Custom Security Level): rsa-g2-3des-sha
   Mode (Initiator): Aggressive
   Preferred Certificate (optional):
   Peer CA: Verisign
   Peer Type: X509-SIG

   VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

   VPN Name: corp_VPN
   Security Level: Compatible
   Remote Gateway: Predefined: (選択), Corp_GW

5. **ルート**
   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (**選択**)
   Interface: ethernet3
   Gateway IP Address: 1.1.1.250

6. **ポリシー**
   Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), Dial-Up VPN
   Destination Address:
   Address Book Entry: (**選択**), web1
   Service: HTTP
   Action: Tunnel
   Tunnel VPN:Corp_VPN
   Modify matching bidirectional VPN policy: (**オフ**)
   Position at Top: (**選択**)

CLI

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **アドレス**
   set address trust web1 10.1.1.5/32

3. **ユーザー**
   set user User1 ike-id asn1-dn wildcard o=juniper,ou=marketing share-limit 10
   set user-group office_1 user User1

4. **VPN**
   set ike gateway Corp_GW dialup office_1 aggressive outgoing-interface ethernet3 proposal rsa-g2-3des-sha
   set ike gateway Corp_GW cert peer-ca 1
   set ike gateway Corp_GW cert peer-cert-type x509-sig
   set vpn Corp_VPN gateway Corp_GW sec-level compatible

注 : 番号 1 は、CA ID 番号です。CA の ID 番号を調べるには、**get pki x509 list ca-cert** コマンドを使用してください。

5. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

6. **ポリシー**
   set policy top from untrust to trust “Dial-Up VPN” web1 http tunnel vpn Corp_VPN save

NetScreen-Remote セキュリティポリシーエディタ

1. **Options > Secure > Specified Connections** をクリックします。

2. **Add a new connection** をクリックし、表示された新しい接続アイコンの横に **web1** と入力してください。

3. 接続オプションを次のように構成します。

   Connection Security: Secure
   Remote Party Identity and Addressing
   ID Type: IP Address, 10.1.1.5
   Protocol: **All をハイライト表示させ、HTTP を入力し、Tab キーを押して 80 を入力します。**
   Connect using Secure Gateway Tunnel: (**選択**)
   ID Type: IP Address, 1.1.1.1

4. web1 アイコンの左にある 「+」シンボルをクリックして接続ポリシーを拡張します。

5. **My Identity** をクリックします。識別名に *o = netscreen,ou = marketing* を要素として持つ証明書を Select Certificate ドロップダウン リストから選択します。

   ID Type: **ドロップダウンリストから Distinguished Name を選択します。**

注 : この例では、NetScreen-Remote 適切な証明書がクライアントにロード済みであると想定しています。NetScreen-Remote への証明書のロード方法に関する詳細については、NetScreen-Remote の説明書を参照してください。

---

6. **Security Policy** アイコンをクリックして、**Aggressive Mode** を選択し、**Enable Perfect Forward Secrecy (PFS)** をオフにします。

7. Security Policy アイコンの左にある + シンボルをクリックしてから、Authentication (Phase 1) と Key Exchange (Phase 2) の左にある + シンボルをクリックし、ポリシーをさらに拡張します。

8. **Authentication (Phase 1) > Proposal 1** をクリックします。次の暗号化およびデータ保全性アルゴリズムを選択します。

   Authentication Method: RSA Signatures
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Key Group: Diffie-Hellman Group 2

9. **Key Exchange (Phase 2) > Proposal 1** をクリックします。次の IPSec プロトコルを選択します。

   Encapsulation Protocol (ESP): (**選択**)
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Encapsulation: Tunnel

10. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: Triple DES
    Hash Alg: MD5
    Encapsulation: Tunnel

11. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel

12. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

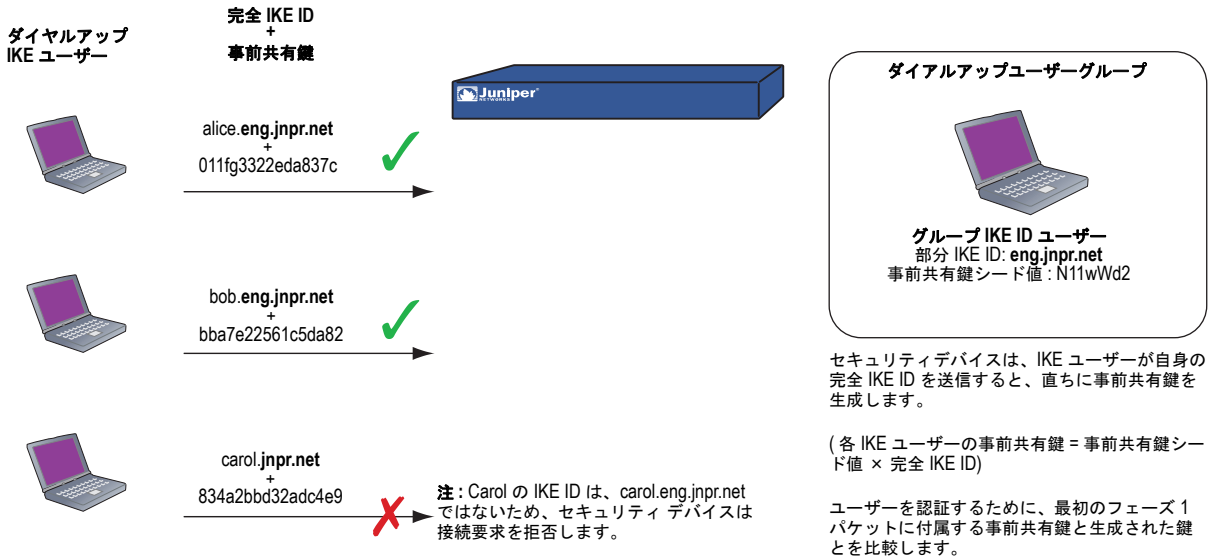
    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: DES
    Hash Alg: MD5
    Encapsulation: Tunnel

13. **File > Save Changes** をクリックします。

事前共有鍵を使用するグループ IKE ID の設定

事前共有鍵を使用するグループ IKE ID は、ユーザー プロファイルを各ユーザーに個別に定義することなく、ダイヤルアップ IKE ユーザーのグループに対する IKE 認証を実行する技法です。その代わりに、セキュリティ デバイスは、部分 IKE ID を含む単一のグループ IKE ID ユーザー プロファイルを使用します。VPN クライアント上で VPN 構成が正しい事前共有鍵を持ち、ユーザーの完全 IKE ID の最も右側の部分がグループ IKE ID ユーザー プロファイルの部分 IKE ID と適合する場合、ダイヤルアップ IKE ユーザーは正常にセキュリティ デバイスへの VPN トンネルを構築できます。

図 49: 事前共有鍵をもつグループ IKE ID



事前共有鍵機能でグループ IKE ID に使用する IKE ID タイプは、E メール アドレスまたは FQDN（完全修飾ドメイン名）のいずれかになります。

次のようにして、事前共有鍵を持つグループ IKE ID を設定できます。

セキュリティデバイス上 :

1. 部分 IKE ID で新しいグループ IKE ID ユーザーを作成し（たとえば、**juniper.net**）、何名のダイヤルアップ ユーザーがグループ IKE ID プロファイルを使用してログオンできるかを指定します。

2. 新しいグループ IKE ID ユーザーをダイアルアップユーザーグループに割り当てます。

3. ダイヤルアップ AutoKey IKE VPN 構成では、リモートゲートウェイに名前を付け (**road1** など)、ダイアルアップユーザーグループを指定して事前共有鍵シード値を入力します。

4. 次の CLI コマンドを使用し、事前共有鍵シード値と完全ユーザー IKE ID（例 **lisa@juniper.net**）を使用する各ダイヤルアップ ユーザーの事前共有鍵を作成します。

   exec ike preshare-gen *name_str usr_name_str*
   （例）**exec ike preshare-gen road1 lisa@juniper.net**

5. リモート VPN クライアントを構成する際に使用するために、事前共有鍵を記録します。

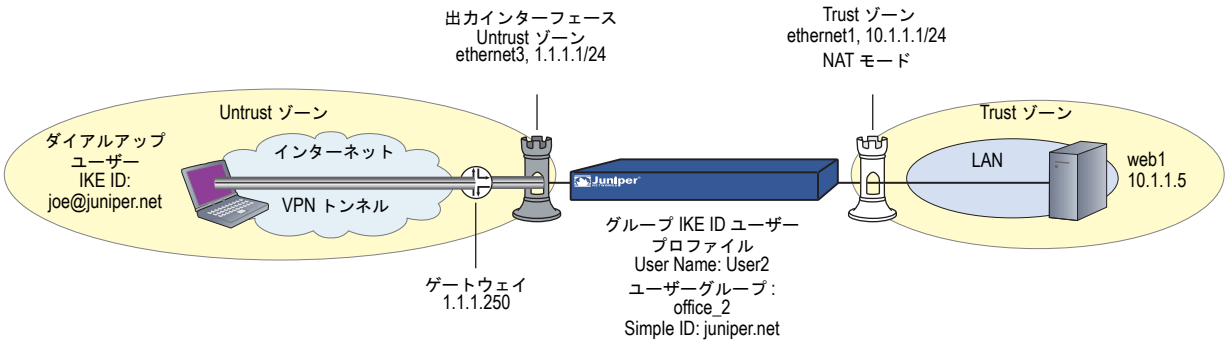
VPN クライアント上 :

フェーズ 1 ネゴシエーションのアグレッシブ モードを使用してセキュリティ デバイスへの VPN トンネルを構成し、セキュリティ デバイスであらかじめ作成した事前共有鍵を入力します。

それ以降、セキュリティ デバイスは、部分グループ IKE ID ユーザー プロファイルに適合するセクションを含む完全 IKE ID を持つ各ユーザーを正常に認証することができます。たとえば、グループ IKE ID ユーザーが IKE ID **juniper.net** を持つ場合、自身の IKE ID にそのドメイン名を持つ任意のユーザーは、セキュリティ デバイスでフェーズ 1 IKE ネゴシエーションをアグレッシブ モードで開始できます。例えば、次のように表示されます。**alice@juniper.net**、**bob@juniper.net**、および **carol@juniper.net**。そのようなユーザーが何人ログオンできるかは、グループ IKE ID ユーザープロファイルに指定された同時セッションの最大数によります。

この例では、*User2* という名前の新しいグループ IKE ID ユーザーを作成します。文字列 *juniper.net* で終わる IKE ID を含む事前共有鍵を持つ VPN クライアントからのフェーズ 1 ネゴシエーションを 10 個まで承認するように構成します。事前共有鍵のシード値は、*jk930k* です。ダイアルアップ IKE ユーザーグループには、*office_2* という名前を付けます。

図 50: グループ IKE ID (事前共有鍵)



フェーズ 1 とフェーズ 2 の両方のネゴシエーションに対して、「Compatible」として事前に定義されたセキュリティ レベルを選択します。すべてのセキュリティゾーンは、trust-vr ルーティングドメインに存在します。

WebUI

1. **インターフェース**

   Network > Interfaces > Edit (ethernet1): 次のように入力してから **OK** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように選択してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: web1
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 10.1.1.5/32
   Zone: Trust

3. **ユーザー**
   Policy > Policy Elements > Users > Local > New: 次のように入力してから **OK** をクリックします。

   User Name: User2
   Status: Enable
   IKE User: (**選択**)
   Number of Multiple Logins with same ID: 10
   Simple Identity: (**選択**)
   IKE Identity: juniper.net

   Policy > Policy Elements > User Groups > Local > New: Group Name フィールドに **office_2** と入力し、次の手順を行ってから **OK** をクリックします。

   User2 を選択し、**<<** ボタンを使用してこのユーザーを Available Members 列から Group Members 列に移動します。

4. **VPN**

注 : WebUI では事前共有鍵の値のみ入力が可能で、セキュリティ デバイスが事前共有鍵を取得するシード値は入力できません。事前共有鍵シード値を入力するには、IKE ゲートウェイを構成する際に CLI を使用する必要があります。

   VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

   VPN Name: corp_VPN
   Security Level: Compatible
   Remote Gateway: Predefined: (**選択**), Corp_GW

5. **ルート**
   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (**選択**)
   Interface: ethernet3
   Gateway IP Address: 1.1.1.250

6. **ポリシー**
   Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), Dial-Up VPN
   Destination Address:
   Address Book Entry: (**選択**), web1
   Service: HTTP
   Action: Tunnel

Tunnel VPN: Corp_VPN
Modify matching bidirectional VPN policy: (オフ)
Position at Top: (選択)

CLI

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **アドレス**
   set address trust web1 10.1.1.5/32

3. **ユーザー**
   set user User2 ike-id u-fqdn netscreen.com share-limit 10
   set user-group office_2 user User2

4. **VPN**
   set ike gateway Corp_GW dialup office_2 aggressive seed-preshare jk930k sec-level compatible
   set vpn Corp_VPN gateway Corp_GW sec-level compatible

5. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

6. **ポリシー**
   set policy top from untrust to trust “Dial-Up VPN” web1 http tunnel vpn Corp_VPN save

事前共有鍵の入手

事前共有鍵の取得は、次の CLI コマンドを使用することによってのみ可能です。

exec ike preshare-gen *name_str usr_name_str*

事前共有鍵シード値 *jk930k* に基づいた事前共有鍵（*Corp_GW* という名前のリモート ゲートウェイの構成に指定される）および個人ユーザー *heidi@juniper.net* の完全 ID は、*11ccce1d396f8f29ffa93d11257f691af96916f2* となります。

NetScreen-Remote セキュリティポリシーエディタ

1. **Options > Secure > Specified Connections** をクリックします。

2. **Add a new connection** をクリックし、表示された新しい接続アイコンの横に **web1** と入力してください。

3. 接続オプションを次のように構成します。

   Connection Security: Secure
   Remote Party Identity and Addressing
   ID Type: IP Address, 10.1.1.5
   Protocol: **All** をハイライト表示させ、**HTTP** を入力し、**Tab** キーを押して **80** を入力します。
   Connect using Secure Gateway Tunnel: (選択)
   ID Type: IP Address, 1.1.1.1

4. web1 アイコンの左にある 「+」シンボルをクリックして接続ポリシーを拡張します。

5. **Security Policy** アイコンをクリックして、**Aggressive Mode** を選択し、**Enable Perfect Forward Secrecy (PFS)** をオフにします。

6. **My Identity** をクリックします。**Pre-shared Key > Enter Key** をクリックします。**11ccce1d396f8f29ffa93d11257f691af96916f2** と入力してから、**OK** をクリックします。

   ID Type: (**E-mail Address** を選択し)、**heidi@juniper.net** と入力します。

7. Security Policy アイコンの左にある + シンボルをクリックしてから、Authentication (Phase 1) と Key Exchange (Phase 2) の左にある + シンボルをクリックし、ポリシーをさらに拡張します。

8. **Authentication (Phase 1) > Proposal 1** をクリックします。次の暗号化およびデータ保全性アルゴリズムを選択します。

   Authentication Method: Pre-Shared Key
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Key Group: Diffie-Hellman Group 2

9. **Authentication (Phase 1) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

   Authentication Method: Pre-Shared Key
   Encrypt Alg: Triple DES
   Hash Alg: MD5
   Key Group: Diffie-Hellman Group 2

10. **Authentication (Phase 1) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Authentication Method: Pre-Shared Key
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Key Group: Diffie-Hellman Group 2

11. **Authentication (Phase 1) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Authentication Method: Pre-Shared Key
    Encrypt Alg: DES
    Hash Alg: MD5
    Key Group: Diffie-Hellman Group 2

12. **Key Exchange (Phase 2) > Proposal 1** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: Triple DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel

13. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: Triple DES
    Hash Alg: MD5
    Encapsulation: Tunnel

14. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel

15. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: DES
    Hash Alg: MD5
    Encapsulation: Tunnel

16. **File > Save Changes** をクリックします。

共有 IKE ID

共有 IKE ID 機能は、多数のダイアルアップユーザーの配備を容易にします。セキュリティ デバイスは、この機能とともに、単一のグループ IKE ID および事前共有鍵を使用して、複数のダイヤルアップ VPN ユーザーを認証します。このようにして、共通の VPN 構成を介して大規模なリモートユーザーグループに対する IPSec 保護を提供します。

この機能は、事前共有鍵機能を用いたグループ IKE ID と似ていますが、次のような違いがあります。

- グループ IKE ID 機能を使用すると、IKE ID には E メール アドレスまたは FQDN（完全修飾ドメイン名）を利用できます。この機能を利用するためには、IKE ID は E メール アドレスであることが必要です。
- 各ユーザーの事前共有鍵を生成するのに事前共有鍵シード値および完全ユーザー IKE ID を使用する代わりに、グループのすべてのユーザーに対して単一の共有鍵を指定します。
- XAuth を使用して個人ユーザーを認証する必要があります。

セキュリティ デバイス上で共有 IKE ID および事前共有鍵をセットアップするには、次のように行います。

1. 新しいグループ IKE ID ユーザーを作成し、何人のダイアルアップユーザーがグループ IKE ID を使用してログオンできるかを指定します。この機能を利用するためには、E メール アドレスを IKE ID として使用します。
2. 新しいグループ IKE ID をダイアルアップユーザーグループに割り当てます。

3. ダイアルアップ -LAN 間 AutoKey IKE VPN 構成で共有 IKE ID ゲートウェイを作成します。

4. XAuth ユーザーを定義し、リモート IKE ゲートウェイ上で XAuth を使用可能にします。

VPN クライアント上 :

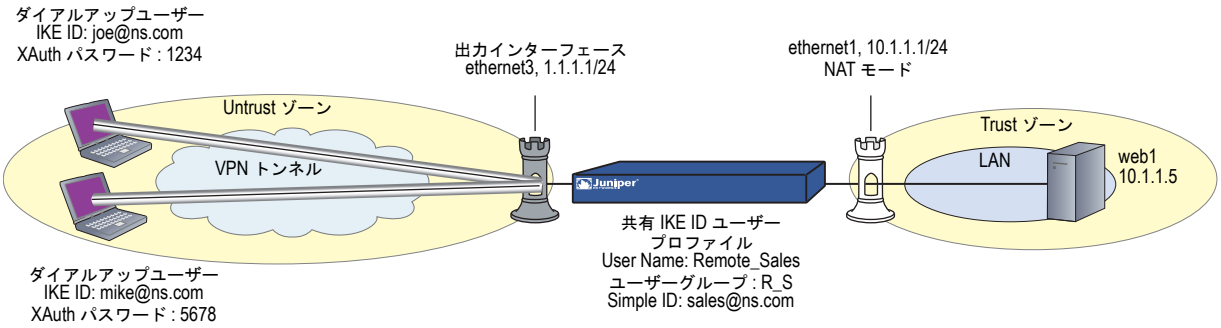
フェーズ 1 ネゴシエーションのアグレッシブ モードを使用してセキュリティ デバイスへの VPN トンネルを構成し、セキュリティ デバイスであらかじめ定義した事前共有鍵を入力します。それ以降、セキュリティ デバイスは、各リモート ユーザーを次のように認証します。

フェーズ 1 ネゴシエーションの間、セキュリティ デバイスは、まずクライアントが送信した IKE ID および事前共有鍵と セキュリティ デバイス上の IKE ID および事前共有鍵とを比較することによって、VPN クライアントを認証します。適合すれば、セキュリティ デバイスは XAuth を使用して個人ユーザーを認証します。フェーズ 1 とフェーズ 2 IKE ネゴシエーションの間に、リモート サイトのユーザーにログイン プロンプトを送信します。リモート ユーザーが正しいユーザー名とパスワードでログオンに成功すると、フェーズ 2 ネゴシエーションが始まります。

この例では、Remote_Sales という名前の新しいグループ IKE ID ユーザーを作成します。同じ事前共有鍵（abcd1234）を使用する VPN クライアントからのフェーズ 1 ネゴシエーションを最大 250 まで承認します。ダイアルアップ IKE ユーザーグループには、*R_S* という名前を付けます。さらに、2 人の XAuth ユーザー、Joe と Mike を構成します。

フェーズ 1 とフェーズ 2 の両方のネゴシエーションに対して、「Compatible」として事前に定義されたセキュリティ レベルを選択します。すべてのセキュリティゾーンは、trust-vr ルーティングドメインに存在します。

図 51: 共有 IKE ID (事前共有鍵)



WebUI

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24

次のように選択してから **OK** をクリックします。
Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

2. **アドレス**
Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: web1
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.5/32
Zone: Trust

3. **ユーザー**
Policy > Policy Elements > Users > Local > New: 次のように入力してから **OK** をクリックします。

User Name: Remote_Sales
Status: Enable
IKE User: (選択)
Number of Multiple Logins with same ID: 250
Simple Identity: (選択)
IKE Identity: sales@ns.com

Policy > Policy Elements > User Groups > Local > New: Group Name フィールドに **R_S** と入力し、次の手順を行ってから **OK** をクリックします。

Remote_sales を選択し、**<<** ボタンを使用してこのユーザーを Available Members 列から Group Members 列に移動します。

Policy > Policy Elements > Users > Local > New: 次のように入力してから **OK** をクリックします。

User Name: Joe
Status: Enable
XAuth User: (選択)
Password: 1234
Confirm Password: 1234

Policy > Policy Elements > Users > Local > New: 次のように入力してから **OK** をクリックします。

User Name: Mike
Status: Enable
XAuth User: (選択)
Password: 5678
Confirm Password: 5678

4. **VPN**

   VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

   Gateway Name: sales_gateway
   Security Level: Compatible (選択)
   Remote Gateway Type: Dialup Group (選択), R_S
   Preshared Key: abcd1234
   Outgoing Interface: ethernet3

   > Advanced: 次の詳細設定を入力してから **Return** をクリックして基本ゲートウェイ構成ページに戻ります。

   Enable XAuth: (選択)
   Local Authentication: (選択)
   Allow Any: (選択)

   VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

   VPN Name: Sales_VPN
   Security Level: Compatible
   Remote Gateway: Predefined: (選択) sales_gateway

   > Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

   Bind to: Tunnel Zone, Untrust-Tun

5. **ルート**

   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選択)
   Interface: ethernet3
   Gateway IP Address: 1.1.1.250

6. **ポリシー**

   Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Dial-Up VPN
   Destination Address:
   Address Book Entry: (選択), web1
   Service: HTTP
   Action: Tunnel
   Tunnel VPN: Sales_VPN
   Modify matching bidirectional VPN policy: (オフ)
   Position at Top: (選択)

CLI

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. アドレス

```
set address trust web1 10.1.1.5/32
```

3. ユーザー

```
set user Remote_Sales ike-id sales@ns.com share-limit 250
set user-group R_S user Remote_Sales
set user Joe password 1234
set user Joe type xauth
set user Mike password 5678
set user Mike type xauth
```

4. VPN

```
set ike gateway sales_gateway dialup R_S aggressive outgoing-interface ethernet3
    preshare abcd1234 sec-level compatible
set ike gateway sales_gateway xauth
set vpn sales_vpn gateway sales_gateway sec-level compatible
set vpn sales_vpn bind zone untrust-tun
```

5. ルート

```
set route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

6. ポリシー

```
set policy top from untrust to trust “Dial-Up VPN” web1 http tunnel vpn sales_vpn
save
```

NetScreen-Remote セキュリティポリシーエディタ

この例では、Joe という名前のユーザーに対する構成を示します。

1. **Options > Secure > Specified Connections** をクリックします。
2. **Add a new connection** をクリックし、表示された新しい接続アイコンの横に **web1** と入力してください。
3. 接続オプションを次のように構成します。

   Connection Security: Secure
   Remote Party ID Type: IP Address
   IP Address: 10.1.1.5
   Connect using Secure Gateway Tunnel: (**選択**)
   ID Type: IP Address; 1.1.1.1

4. web1 アイコンの左にある 「+」シンボルをクリックして接続ポリシーを拡張します。
5. **Security Policy** アイコンをクリックして、**Aggressive Mode** を選択し、**Enable Perfect Forward Secrecy (PFS)** をオフにします。

6. **My Identity** をクリックします。**Pre-shared Key > Enter Key** をクリックします。**abcd1234** と入力して、**OK** をクリックします。

   ID Type: (**E-mail Address** を選択し)、**sales@ns.com** を入力します。

7. Security Policy アイコンの左にある + シンボルをクリックしてから、Authentication (Phase 1) と Key Exchange (Phase 2) の左にある + シンボルをクリックし、ポリシーをさらに拡張します。

8. **Authentication (Phase 1) > Proposal 1** をクリックします。次の暗号化およびデータ保全性アルゴリズムを選択します。

   Authentication Method: Pre-Shared Key; Extended Authentication
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Key Group: Diffie-Hellman Group 2

9. **Authentication (Phase 1) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

   Authentication Method: Pre-Shared Key; Extended Authentication
   Encrypt Alg: Triple DES
   Hash Alg: MD5
   Key Group: Diffie-Hellman Group 2

10. **Authentication (Phase 1) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Authentication Method: Pre-Shared Key; Extended Authentication
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Key Group: Diffie-Hellman Group 2

11. **Authentication (Phase 1) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Authentication Method: Pre-Shared Key; Extended Authentication
    Encrypt Alg: DES
    Hash Alg: MD5
    Key Group: Diffie-Hellman Group 2

12. **Key Exchange (Phase 2) > Proposal 1** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: Triple DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel

13. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: Triple DES
    Hash Alg: MD5
    Encapsulation: Tunnel

14. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel

15. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: DES
    Hash Alg: MD5
    Encapsulation: Tunnel

16. **File > Save Changes** をクリックします。

第 6 章

レイヤー 2 トンネリングプロトコル

本章では L2TP (レイヤー 2 トンネリングプロトコル) について単体としての使用および IPSec のサポートを受けた場合の使用、そして L2TP と L2TP-over-IPSec の構成例を紹介しています。本章のセクションは、以下のようになります。

- 205 ページの「L2TP について」
- 208 ページの「パケットのカプセル化と脱カプセル化」
  - 208 ページの「カプセル化」
  - 209 ページの「脱カプセル化」
- 211 ページの「L2TP パラメータの設定」
- 213 ページの「L2TP と L2TP-Over-IPSec」
  - 213 ページの「L2TP 構成」
  - 218 ページの「L2TP-over-IPSec を構成する」
  - 226 ページの「双方向の L2TP-over-IPSec」

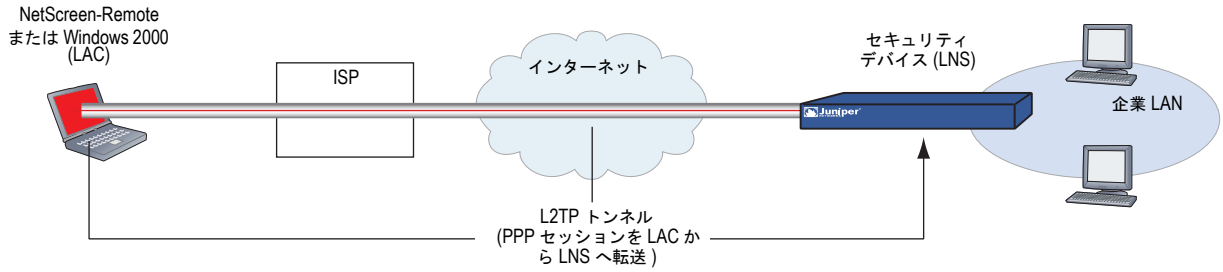
L2TP について

L2TP (レイヤー 2 トンネリングプロトコル) は、ダイヤルアップユーザーが LNS (L2TP ネットワークサーバー) への仮想 PPP (ポイントツーポイントプロトコル) 接続を確立する手段を提供しています。LNS はセキュリティデバイスの場合があります。L2TP は LAC (L2TP アクセスコンセントレータ) と LNS をつなぐトンネルを通して PPP フレームを送信します。

本来 L2TP は、ISP サイトにある LAC が他の ISP や企業サイト の LNS にトンネル接続できるよう設計されたものです。L2TP トンネルはダイヤルアップユーザーのコンピュータまで完全に延びてはおらず、ダイヤルアップユーザーのローカル ISP の LAC までしか到達していませんでした (これは強制的な L2TP 構成と呼ばれる場合もあります)。

Windows 2000 や Windows NT の NetScreen-Remote クライアント、または Windows 2000 クライアント自体が LAC として動作できます。L2TP トンネルはダイヤルアップユーザーのコンピュータまで直接延長されるため、エンドツーエンドトンネリングが可能となります (このアプローチは任意 L2TP 構成と呼ばれる場合もあります。

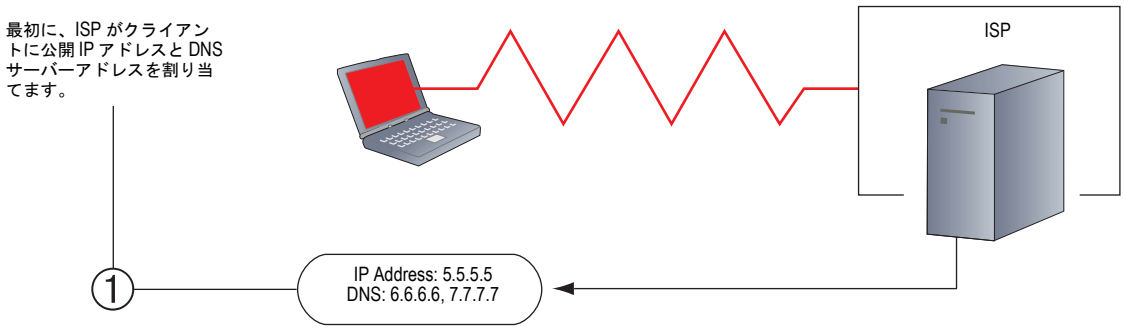
図 52: VPN クライアント (LAC) とセキュリティデバイス (LNS) 間の L2TP トンネル



PPP リンクはダイヤルアップユーザーからインターネットを経由して セキュリティデバイス (LNS) まで延びているため、ローカルデータベースまたは外部認証サーバー (RADIUS、SecurID、LDAP など) からクライアントに IP アドレス、DNS、WINS サーバーアドレスを割り当て、ユーザー認証するのは ISP ではなくセキュリティデバイスです。

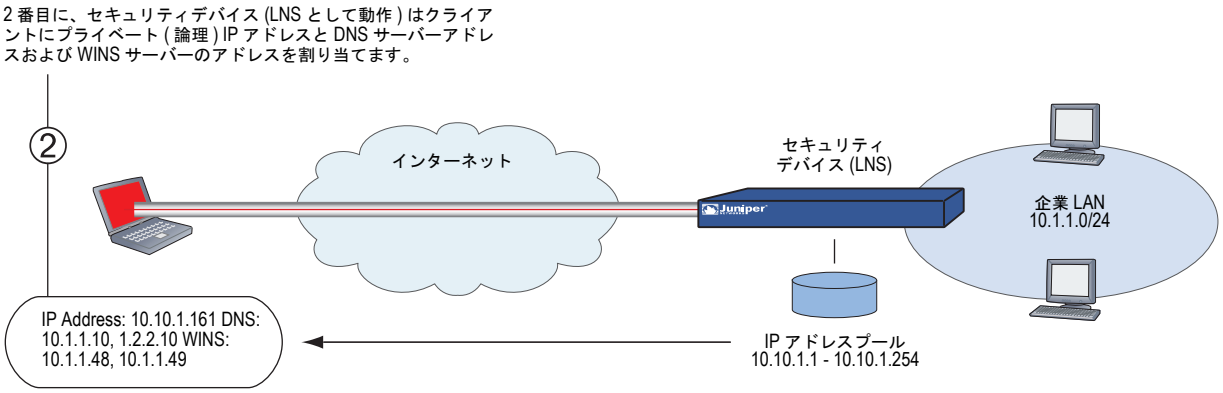
クライアントは 2 つの IP アドレスを受け取ります。1 つは ISP への物理的接続用、もう 1 つは LNS からの論理アドレスです。クライアンが PPP を使用して ISP に接続する際には、ISP が IP と DNS の割り当てを行い、クライアントを認証します。これによりユーザーは L2TP トンネルの外部 IP アドレスとなる公開 IP アドレスを使用してインターネットに接続できるようになります。

図 53: ISP からの IP と DNS の割り当て



L2TP トンネルがカプセル化 PPP フレームを セキュリティデバイスに転送すると、セキュリティデバイスはクライアントに IP アドレス、DNS と WINS の設定を割り当てます。インターネットで使用されていないプライベートアドレスのセットにある IP アドレスを使用することもできます。このアドレスは、L2TP トンネルの内部 IP アドレスになります。

図 54: LNS からの IP と DNS の割り当て



注 : L2TP クライアントに割り当てられる IP アドレスは、企業 LAN の IP アドレスとは異なるサブネットに存在する必要があります。

最新の ScreenOS では次の L2TP サポートを提供しています。

- Windows 2000 管理ホストを起点とする L2TP トンネル

注 : デフォルトにより Windows 2000 は、L2TP-over-IPSec を実行します。L2TP のみを使用するように設定するには、レジストリにある ProhibitIPSec キーを検索し、**0** (L2TP-over-IPSec) から **1** (L2TP のみ) に変更する必要があります (この変更を実施する前にレジストリのバックアップを取っておくことをお勧めします)。**スタート > ファイル名を指定して実行**をクリックし、**regedit** と入力します。**HKEY_LOCAL_MACHINE > System > CurrentControlSet > Services > RasMan > Parameters** の順にダブルクリックします。**ProhibitIPSec** をダブルクリックします。**1** を値のデータフィールドに入力し、**Hexadecimal** (16 進) を基礎値として選択して、**OK** をクリックします。その後再起動してください (そのようなエントリがレジストリに発見できなかった場合は、エントリを作成する方法について Microsoft Windows のマニュアルを参照してください)。

- L2TP と IPSec をトランスポートモードで連結 (L2TP-over-IPSec)
  - NetScreen-Remote の場合 : 証明書を使用したメインモードのネゴシエーションによる L2TP-over-IPSec、および事前共有鍵あるいは証明書を使用したアグレッシブモードのネゴシエーションによる L2TP-over-IPSec
  - Windows 2000 の場合 : 証明書を使用したメインモードのネゴシエーションによる L2TP-over-IPSec
- L2TP および L2TP-over-IPSec トンネルの出力ダイヤルアップポリシー (出力ダイヤルアップポリシーは、入力ポリシーと対になって、双方向トンネルを実現します。)
- ローカルデータベースや外部認証サーバー (RADIUS、SecurID、LDAP など) からの PAP (パスワード認証プロトコル) および CHAP (チャレンジハンドシェイク式認証プロトコル) を使用したユーザー認証

注： ローカルデータベースおよび RADIUS サーバーは、PAP と CHAP の両方をサポートしています。SecurID および LDAP サーバーは PAP だけをサポートしています。

- ローカルデータベースや RADIUS サーバーからのダイヤルアップユーザーの IP アドレス、DNS (ドメイン名システム) サーバー、および WINS (Windows インターネットネーミングサービス) サーバーの割り当て
- ルートシステムおよび仮想システム用の L2TP トンネルおよび L2TP-over-IPSec トンネル

注： L2TP を使用するには、セキュリティデバイスがレイヤー 3 で動作しており、セキュリティゾーンインターフェースを NAT モードまたはルートモードで使用している必要があります。セキュリティデバイスがレイヤー 2 で動作しており、セキュリティゾーンインターフェースが透過モードの場合、L2TP 関連資料が WebUI に表示され、L2TP 関連の CLI コマンドがエラーメッセージを引き出します。

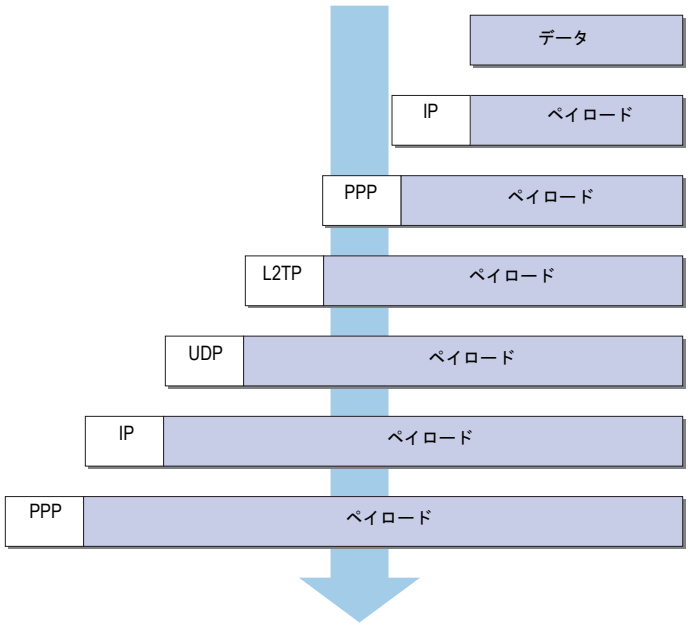
パケットのカプセル化と脱カプセル化

L2TP では PPP フレームを LAC から LNS へ移動する手段としてパケットのカプセル化を使用しています。L2TP および L2TP-over-IPSec のセットアップの具体例を見る前に、L2TP の処理に含まれるカプセル化および脱カプセル化の概要を説明します。

カプセル化

IP ネットワーク上のダイヤルアップユーザーが L2TP を経由してデータを送信する際、LAC は一連のレイヤー 2 フレーム、レイヤー 3 パケット、およびレイヤー 4 セグメント内の IP パケットをカプセル化します。ダイヤルアップユーザーが PPP リンクを経由してローカル ISP に接続したと仮定した場合、カプセル化は 209 ページの図 55 のように進行します。

図 55: L2TP パケットカプセル化

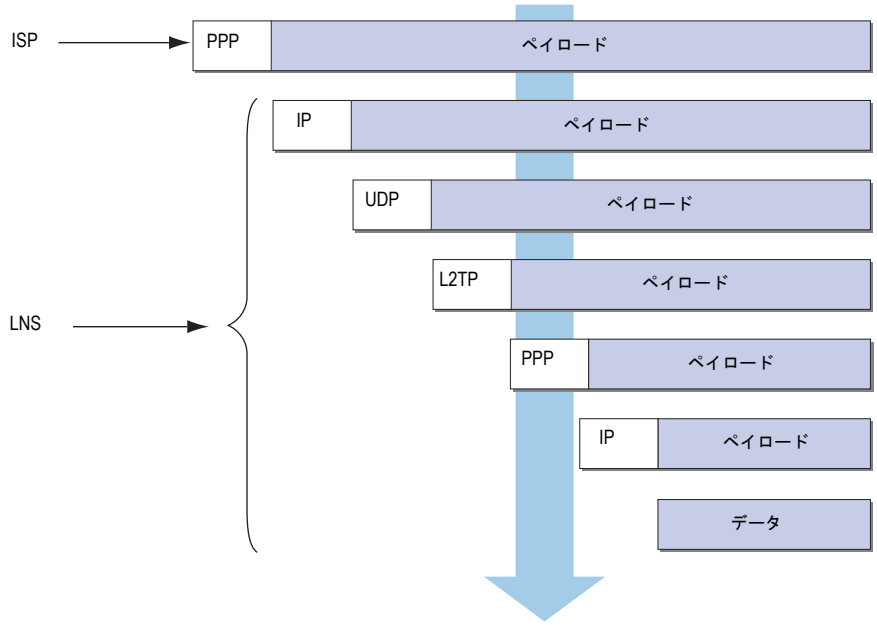


1. データは IP ペイロードに置かれます。
2. IP パケットは PPP フレーム内にカプセル化されます。
3. PPP フレームは L2TP フレーム内にカプセル化されます。
4. L2TP フレームは UDP セグメント内にカプセル化されます。
5. UDP セグメントは IP パケット内にカプセル化されます。
6. ダイヤルアップユーザーと ISP との物理的な接続を構築するため、IP パケットは PPP フレーム内にカプセル化されます。

脱カプセル化

LAC が ISP に接続する PPP リンクを開始する際、ネストされたコンテンツの脱カプセル化と転送は 210 ページの図 56 のように行われます。

図 56: L2TP パケット脱カプセル化



1. ISP は PPP リンクを確立し、ユーザーのコンピュータに IP アドレスを割り当てます。

   PPP ペイロードの内部には IP パケットが含まれています。

2. ISP は PPP ヘッダーを削除し、IP パケットを LNS に転送します。

3. LNS は IP ヘッダーを削除します。

   IP ペイロード内には、ポート 1701 を指定する UDP セグメントが含まれています。このポート番号は、L2TP のために予約されています。

4. LNS は UDP ヘッダーを削除します。

   UDP ペイロード内部には L2TP フレームが含まれています。

5. LNS は L2TP フレームを処理し、L2TP ヘッダー内トンネル ID、コール ID を使用して特定の L2TP トンネルを識別します。次に LNS は L2TP ヘッダーを削除します。

   L2TP ペイロードの内部には PPP フレームが含まれています。

6. LNS は PPP フレームを処理し、ユーザーのコンピュータに論理 IP アドレスを割り当てます。

   PPP ペイロードの内部には IP パケットが含まれています。

7. LNS は IP パケットを最終的な宛先へ導きます。最終的な宛先では IP ヘッダーが削除され、IP パケット内のデータが抽出されます。

L2TP パラメータの設定

LNS は L2TP を使用して、通常 ISP から接続するダイヤルアップユーザーの PPP 設定を行います。設定は次のとおりです。

- IPアドレス - セキュリティデバイスが IP アドレスのプールからアドレスを 1 つ選択し、ダイヤルアップユーザーのコンピュータに割り当てます。IP アドレスプールから周期的に選択プロセスが実施されます。IP アドレスプールから周期的に選択プロセスが実施されます。10.10.1.1 から 10.10.1.3 のプールの場合、10.10.1.1 - 10.10.1.2 - 10.10.1.3 - 10.10.1.1 - 10.10.1.2 … という周期でアドレスが選択されます。
- DNS プライマリおよびセカンダリサーバー IP アドレス - セキュリティデバイスはダイヤルアップユーザーのコンピュータにアドレスを提供します。
- WINDS プライマリおよびセカンダリサーバー IP アドレス - セキュリティデバイスはダイヤルアップユーザーのコンピュータにもアドレスを提供します。

LNS はまた、ユーザー名やパスワードを使用してユーザーを認証します。ユーザーをローカルデータベースや外部認証サーバー (RADIUS、SecurID、LDAP など) に入力することも可能です。

注 : L2TP ユーザーの認証に使用する RADIUS または SecurID サーバーは、ネットワークユーザーに使用したサーバーと同じサーバーか、異なるサーバーを使用することができます。

さらに PPP 認証には次のスキームの 1 つを指定することができます。

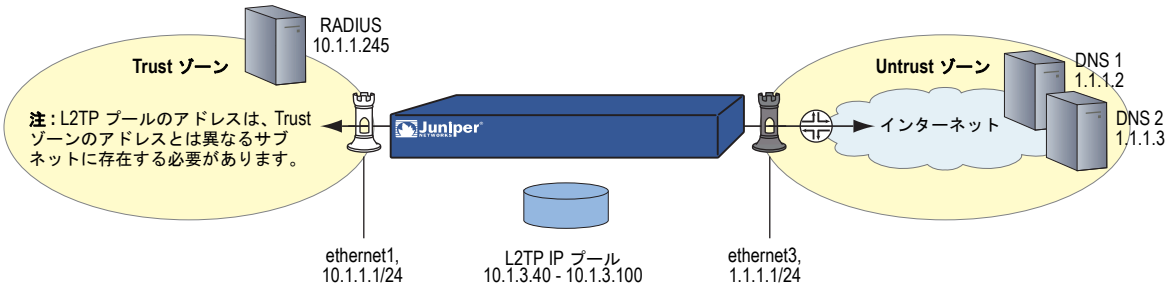
- CHAP (チャレンジハンドシェイク式認証プロトコル): ダイヤルアップユーザーが PPP リンク要求を出した後、セキュリティデバイスがチャレンジ (暗号化鍵) をダイヤルアップユーザーに送信し、ユーザーはその鍵で自分のログイン名、パスワードを暗号化します。ローカルデータベースおよび RADIUS サーバーは CHAP をサポートしています。
- PAP (パスワード認証プロトコル): ダイヤルアップユーザーのパスワードを暗号化せずに PPP リンク要求とともに送信します。ローカルデータベースおよび RADIUS、SecurID、LDAP サーバーは PAP をサポートしています。
- 「ANY」は、セキュリティデバイスが CHAP とネゴシエートし、失敗した場合は PAP とネゴシエートすることを意味しています。

ダイヤルアップユーザーやダイヤルアップユーザーグループに、L2TP デフォルト構成ページ (VPNs > L2TP > Default Settings) または **set l2tp default** コマンド設定を使用して構成したデフォルト L2TP パラメータを適用できます。ユーザー構成ページ (Users > Users > Local > New) または **set user** *name_str* **remote-settings** コマンドを使用して L2TP ユーザー専用に構成した L2TP パラメータを適用することも可能です。ユーザー指定 L2TP 設定はデフォルト L2TP 設定に置き換えられます。

212 ページの図 57 に示すように、10.1.3.40 から 10.1.3.100 の範囲のアドレスを持つ IP アドレスプールを定義します。DNS サーバー IP アドレスは 1.1.1.2 (プライマリ) と 1.1.1.3 (セカンダリ) に指定します。セキュリティデバイスは CHAP を使用して PPP 認証を実行します。

注 : L2TP トンネルごとに認証サーバーを指定します。

図 57: IP プールと L2TP デフォルト設定



WebUI

1. **IP プール**
   Objects > IP Pools > New: 次のように入力してから **OK** をクリックします。

   IP Pool Name: Sutro
   Start IP: 10.1.3.40
   End IP: 10.1.3.100

2. **L2TP デフォルト設定**
   VPNs > L2TP > Default Settings: 以下を入力して **Apply** をクリックします。

   IP Pool Name: Sutro
   PPP Authentication: CHAP
   DNS Primary Server IP: 1.1.1.2
   DNS Secondary Server IP: 1.1.1.3
   WINS Primary Server IP: 0.0.0.0
   WINS Secondary Server IP: 0.0.0.0

CLI

1. **IP プール**
   set ippool sutro 10.1.3.40 10.1.3.100

2. **L2TP デフォルト設定**
   set l2tp default ippool sutro
   set l2tp default ppp-auth chap
   set l2tp default dns1 1.1.1.2
   set l2tp default dns2 1.1.1.3
   save

L2TP と L2TP-Over-IPSec

ダイヤルアップユーザーは CHAP または PAP を利用して認証を受けることが可能ですが、L2TP トンネルは暗号化されていないため真の VPN トンネルではありません。L2TP の目的はただ単に、ローカルセキュリティデバイス管理者が IP アドレスをリモートダイヤルアップユーザーに割り当てることを許可することです。そしてこれらのアドレスはポリシーで参照できます。

L2TP トンネルを暗号化するには L2TP トンネルの暗号化スキームを適用する必要があります。L2TP は LAC と LNS の間のネットワークが IP であると想定しているため、暗号化に IPSec を使用することができます。この組み合わせは L2TP-over-IPSec と呼ばれています。L2TP-over-IPSec は L2TP トンネルおよび IPSec トンネルを同じ端点でセットアップし、ポリシーでリンクさせることが必要です。L2TP-over-IPSec はまたトンネル端点アドレスを暗号化せずに残しておくことができるよう IPSec トンネルをトランスポートモードにする必要があります。(トランスポートおよびトンネルモードの詳細については、4 ページの「モード」を参照してください。)

Windows 2000 のレジストリ設定を変更することで、L2TP トンネルをセキュリティデバイスと Windows 2000 管理ホストの間に作成することができます (レジストリの変更方法については、207 ページの注を参照してください) 。

L2TP-over-IPSec トンネルは、セキュリティデバイスと次の VPN クライアントのいずれかの間に作成できます。

- Windows 2000 あるいは Windows NT オペレーティングシステムの NetScreen-Remote 管理ホスト
- Windows 2000 (NetScreen-Remote 非装備) 管理ホスト

注 : NetScreen-Remote を装備していない Windows 2000 を使用して認証を行う場合は、証明書を使用する必要があります。

L2TP 構成

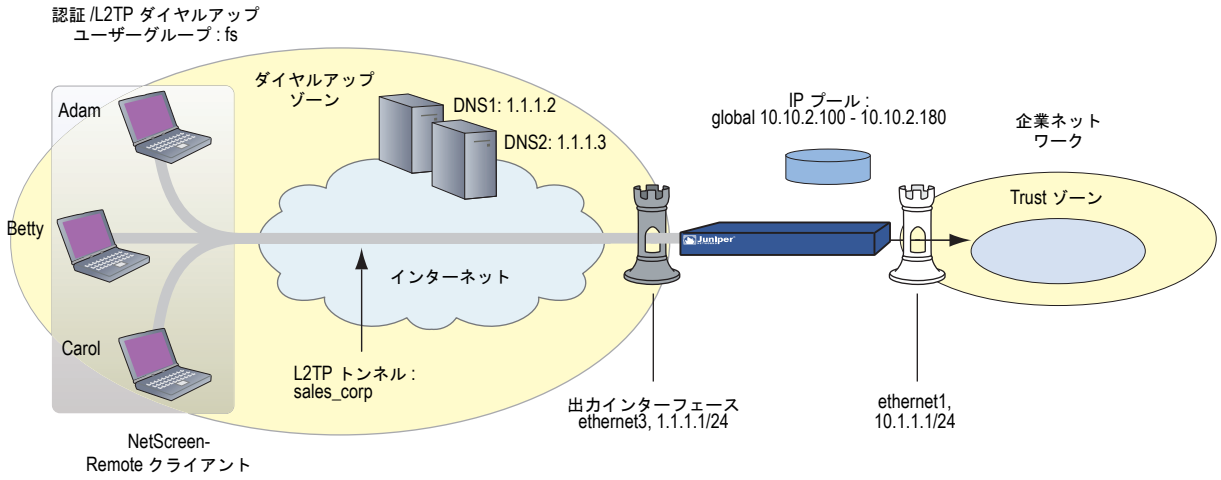
この例では、214 ページの図 58 に示すように、「fs」(field-sales の略) と呼ばれるダイヤルアップユーザーグループを作成し、ethernet3 (Untrust ゾーン) を L2TP トンネルの出力インターフェースとして使用して「sales_corp」と呼ばれる L2TP トンネルを構成します。セキュリティデバイスは次のデフォルト L2TP トンネル設定をダイヤルアップユーザーのグループに適用します。

- L2TP ユーザーはローカルデータベース経由で認証されます。
- PPP 認証には CHAP を使用します。
- 「global」と名づけられた IP プールのアドレスの範囲は 10.10.2.100 から 10.10.2.180 となります。
- DNS サーバーは 1.1.1.2 (プライマリ) と 1.1.1.3 (セカンダリ) です。

注： L2TP のみの構成は安全とは言えません。デバッグ目的の場合のみ使用するようお勧めします。

L2TP IP プール内のアドレスは、企業ネットワーク内のアドレスとは異なるサブネットに存在する必要があります。

図 58: L2TP 構成



リモート L2TP クライアントは Windows 2000 オペレーティングシステム上に存在します。リモートクライアント上に L2TP を構成する方法については、Windows 2000 のマニュアルを参照してください。L2TP トンネルのセキュリティデバイス側の構成だけを次に示します。

WebUI

1. **インターフェース**

   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24

   次のように選択してから **OK** をクリックします。

   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. **L2TP ユーザー**

   Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

   User Name: Adam
   Status: Enable
   L2TP User: (選択)
   User Password: AJbioJ15
   Confirm Password: AJbioJ15

   Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

   User Name: Betty
   Status: Enable
   L2TP User: (選択)
   User Password: BviPsoJ1
   Confirm Password: BviPsoJ1

   Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

   User Name: Carol
   Status: Enable
   L2TP User: (選択)
   User Password: Cs10kdD3
   Confirm Password: Cs10kdD3

3. **L2TP ユーザーグループ**

   Objects > User > Local Groups > New: Group Name フィールドに **fs** と入力し、次を実行して **OK** をクリックします。

   Adam を選択し、< < ボタンを使用して、Available Members 列から Group Members 列へ移動します。

   Betty を選択し、< < ボタンを使用して、Available Members 列から Group Members 列へ移動します。

   Carol を選択し、< < ボタンを使用して、Available Members 列から Group Members 列へ移動します。

4. **L2TP デフォルト設定**

   Objects > IP Pools > New: 次のように入力してから **OK** をクリックします。

   IP Pool Name: global
   Start IP: 10.10.2.100
   End IP: 10.10.2.180

   VPNs > L2TP > Default Settings: 次のように入力してから **OK** をクリックします。

   IP Pool Name: global
   PPP Authentication: CHAP
   DNS Primary Server IP: 1.1.1.2
   DNS Secondary Server IP: 1.1.1.3
   WINS Primary Server IP: 0.0.0.0
   WINS Secondary Server IP: 0.0.0.0

5. L2TP トンネル

VPNs > L2TP > Tunnel > New: 次のように入力してから **OK** をクリックします。

Name: sales_corp
Use Custom Settings: (選択)
Authentication Server: Local
Dialup Group: Local Dialup Group - fs
Outgoing Interface: ethernet3
Peer IP: 0.0.0.0
Host Name (optional): LAC として機能しているコンピュータ名を入力します。
Secret (optional): LAC と LNS の間の共有秘密を入力します。
Keep Alive: 60

Peer IP: ピアの ISP は動的にピアに IP アドレスを割り当てるため、上の例では **0.0.0.0** を入力します。

LAC: Windows 2000 を実行しているコンピュータの名前を確認するには次の手順を実行します。**スタート > 設定 > コントロール パネル > システム**をクリックします。システムプロパティのダイアログボックスが表示されます。**ネットワーク ID** タブをクリックし、**フル コンピュータ名**に続くエントリを参照してください。

L2TP トンネル認証用 LAC にパスワードを 追加するためには Windows 2000 のレジストリを以下のように変更する必要があります。

1. **スタート > ファイル名を指定して実行** をクリックして、**regedit** と入力します。レジストリ エディタが開きます。
2. **HKEY_LOCAL_MACHINE** をクリックします。
3. **システム**を右クリックし、表示されるポップアップメニューから**検索**を選択します。
4. **ms_l2tpminiport** と入力し、**次を検索**をクリックします。
5. 編集メニューの**新規**をハイライトし、**文字列**を選択します。
6. **Password** と入力します。
7. **Password** をダブルクリックします。文字列の編集ダイアログボックスが表示されます。
8. パスワードを値のデータフィールドに入力します。これはセキュリティデバイスの L2TP Tunnel Configuration Secret フィールドに入力したパスワードと同じ語句でなければなりません。
9. Windows 2000 を実行しているコンピュータを再起動します。

Windows 2000 のデフォルトである L2TP-over-IPSec を使用しているときにはトンネル認証は必要ありません。すべての L2TP メッセージは暗号化され、IPSec 内部で認証されます。

Keep-Alive: キープアライブの値はセキュリティデバイスが L2TP Hello 信号を LAC に送信するまでの無活動の秒数です。

6. ルート

Network > Routing > Routing Entries > New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

7. ポリシー

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Dial-Up VPN
Destination Address:
Address Book Entry: (選択), Any
NAT: Off
Service: ANY
Action: Tunnel
Tunnel L2TP: sales_corp
Position at Top: (選択)

CLI

1. ダイヤルアップユーザー

```
set user adam type l2tp
set user adam password AJbioJ15
unset user adam type auth
set user betty type l2tp
set user betty password BviPsoJ1
unset user betty type auth
set user carol type l2tp
set user carol password Cs10kdD3
unset user carol type auth
```

注 : ユーザーにパスワードを定義すると、そのユーザーは自動的に認証ユーザーとして分類されます。このため、ユーザータイプを L2TP として厳密に定義するには、認証ユーザータイプの設定を解除する必要があります。

2. L2TP ユーザーグループ

```
set user-group fs location local
set user-group fs user adam
set user-group fs user betty
set user-group fs user carol
```

3. L2TP デフォルト設定

```
set ippool global 10.10.2.100 10.10.2.180
set l2tp default ippool global
set l2tp default auth server Local
set l2tp default ppp-auth chap
set l2tp default dns1 1.1.1.2
set l2tp default dns2 1.1.1.3
```

4. **L2TP トンネル**
   set l2tp sales_corp outgoing-interface ethernet3
   set l2tp sales_corp auth server Local user-group fs

5. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

6. **ポリシー**
   set policy top from untrust to trust “Dial-Up VPN” any any tunnel l2tp sales_corp save

L2TP-over-IPSec を構成する

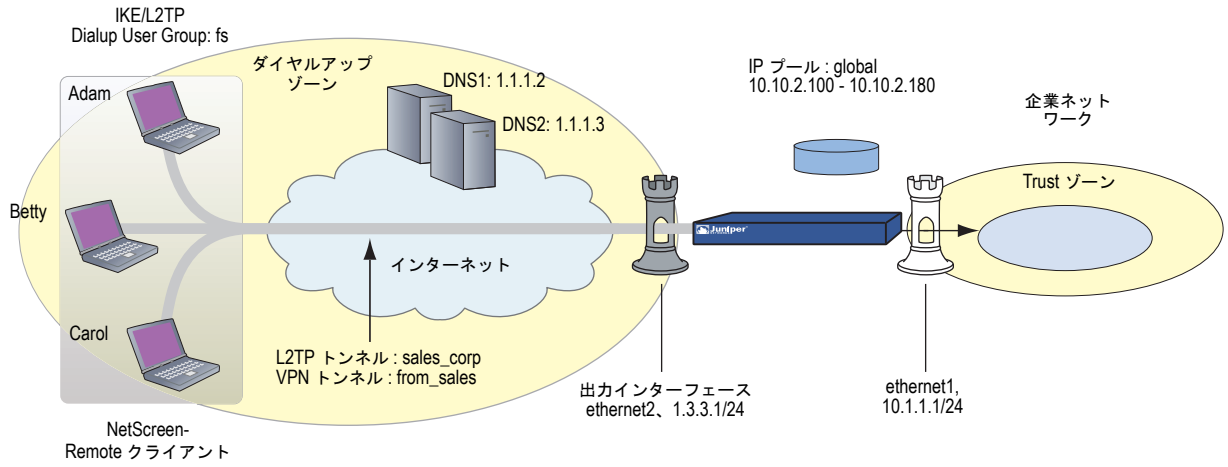
この例では前の例 (213 ページの「L2TP 構成」) 作成したのと同じ L2TP トンネルを使用します。それに加えて、暗号化を行うために IPSec トンネルを L2TP トンネルにかぶせます。IPSec トンネルは、あらかじめロードされた RSA 証明書、3DES 暗号化、および SHA -1 認証を使用して、アグレッシブモードでフェーズ 1 のネゴシエートを行います。CA (認証局) は Verisign です。(証明書の入手とローディングに関しては、第 2 章、「公開鍵暗号化」を参照してください)。フェーズ 2 のネゴシエーションではフェーズ 2 の提案に対して「互換性」があると事前に定義されたセキュリティレベルを使用します。IPSec トンネルはトランスポートモードです。

定義済み Trust ゾーンとユーザー定義ダイヤルアップゾーンは trust-vr ルーティングドメインに存在します。ダイヤルアップゾーンおよび Trust ゾーンのインターフェースはそれぞれ ethernet2 (1.3.3.1/24)、ethernet1 (10.1.1.1/24) です。Trust ゾーンは NAT モードです。

ダイヤルアップユーザーの Adam、Betty、Carol は、Windows 2000 オペレーティングシステム上の NetScreen-Remote クライアントを使用します。次の内容にはダイヤルアップユーザー Adam の NetScreen-Remote 構成も含まれています (他の 2 人のダイヤルアップユーザーの NetScreen-Remote 構成は Adam 用の構成と同じです)。

注 : Windows 2000 (NetScreen-Remote 非装備) に L2TP-over-IPSec トンネルを構成するには、フェーズ 1 のネゴシエーションはメインモードであり、IKE ID タイプは ASN1-DN である必要があります。

図 59: L2TP-over-IPSec を構成する



WebUI

1. **ユーザー定義ゾーン**
   Network > Zones > New: 次のように入力してから **OK** をクリックします。

   Zone Name: Dialup
   Virtual Router Name: Trust-vr
   Zone Type: Layer 3 (選択)
   Block Intra-Zone Traffic: (選択)
   TCP/IP Reassembly for ALG:（オフ）

注 : Trust ゾーンは事前に構成されています。新しく作成する必要はありません。

2. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように選択してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

   Zone Name: Dialup
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.3.3.1/24

3. **IKE /L2TP ユーザー**
   Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

   User Name: Adam
   Status: Enable
   IKE User: (選択)

Simple Identity: (選択)
IKE Identity: ajackson@abc.com
L2TP User: (選択)
User Password: AJbioJ15
Confirm Password: AJbioJ15

注 : NetScreen-Remote クライアントが送信した IKE ID と同じ IKE ID を入力する必要があります。これはクライアントが認証に使用している証明書に記載されている E メールアドレスです。

Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

User Name: Betty
Status: Enable
IKE User: (選択)
Simple Identity: (選択)
IKE Identity: bdavis@abc.com
L2TP User: (選択)
User Password: BviPsoJ1
Confirm Password: BviPsoJ1

Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

User Name: Carol
Status: Enable
IKE User: (選択)
Simple Identity: (選択)
IKE Identity: cburnet@abc.com
L2TP User: (選択)
User Password: Cs10kdD3
Confirm Password: Cs10kdD3

4. IKE/L2TP ユーザーグループ

Objects > Users > Local Groups > New: Group Name フィールドに **fs** と入力し、次を実行して **OK** をクリックします。

Adam を選択し、< < ボタンを使用して、Available Members 列から Group Members 列へ移動します。

Betty を選択し、< < ボタンを使用して、Available Members 列から Group Members 列へ移動します。

Carol を選択し、< < ボタンを使用して、Available Members 列から Group Members 列へ移動します。

5. IP プール

Objects > IP Pools > New: 次のように入力してから **OK** をクリックします。

IP Pool Name: global
Start IP: 10.10.2.100
End IP: 10.10.2.180

6. L2TP デフォルト設定

VPNs > L2TP > Default Settings: 以下を入力して **Apply** をクリックします。

IP Pool Name: global
PPP Authentication: CHAP

DNS Primary Server IP: 1.1.1.2
DNS Secondary Server IP: 1.1.1.3
WINS Primary Server IP: 0.0.0.0
WINS Secondary Server IP: 0.0.0.0

7. L2TP トンネル

VPNs > L2TP > Tunnel > New: 次のように入力してから **OK** をクリックします。

Name: sales_corp
Dialup Group: (**選択**), Local Dialup Group - fs
Authentication Server: Local
Outgoing Interface: ethernet2
Peer IP: 0.0.0.0

Host Name (optional): 特定のホストへの L2TP トンネルを規制する場合、LAC として動作しているコンピュータの名前を入力します。

Secret (optional): LAC と LNS の間の共有秘密を入力します。

Keep Alive: 60

LAC: Windows 2000 を実行しているコンピュータの名前を確認するには次の手順を実行します。**スタート > 設定 > コントロール パネル > システム**をクリックします。システムプロパティのダイアログボックスが表示されます。**ネットワーク ID** タブをクリックし、**フル コンピュータ名**に続くエントリを参照してください。

Secret: L2TP トンネル認証用 LAC にパスワードを追加するためには Windows 2000 のレジストリを以下のように変更する必要があります。

1. **スタート > ファイル名を指定して実行** をクリックして、**regedit** と入力します。レジストリ エディタが開きます。
2. **HKEY_LOCAL_MACHINE** をクリックします。
3. **システム**を右クリックし、表示されるポップアップメニューから**検索**を選択します。
4. **ms_l2tpminiport** と入力し、**次を検索**をクリックします。
5. 編集メニューの**新規**をハイライトし、**文字列**を選択します。
6. **Password** と入力します。
7. **Password** をダブルクリックします。文字列の編集ダイアログボックスが表示されます。
8. パスワードを値のデータフィールドに入力します。これはセキュリティデバイスの L2TP Tunnel Configuration Secret フィールドに入力したパスワードと同じ語句でなければなりません。
9. Windows 2000 を実行しているコンピュータを再起動します。

Windows 2000 のデフォルトである L2TP-over-IPSec を使用しているときにはトンネル認証は必要ありません。すべての L2TP メッセージは暗号化され、IPSec 内部で認証されます。

Keep-Alive: キープアライブの値はセキュリティデバイスが L2TP Hello 信号を LAC に送信するまでの無活動の秒数です。

注 : ホスト名および秘密設定は通常無視することができます。これらの設定は上級ユーザーだけが使用されるようお勧めします。

---

8. VPN トンネル

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: field
Security Level: Custom
Remote Gateway Type:
    Dialup User Group: (**選択**), Group: fs
Outgoing Interface: ethernet2

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: User Defined: Custom
Phase 1 Proposal: rsa-g2-3des-sha
Mode (Initiator): Aggressive
Preferred Certificate (optional):
Peer CA: Verisign
Peer Type: X509-SIG

注 : Windows 2000 (NetScreen-Remote 非装備) はメインモードネゴシエーションだけをサポートしています。

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

Name: from_sales
Security Level: Compatible
Remote Gateway: Predefined: field

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Security Level: Compatible
Transport Mode: (**選択**)

9. ポリシー

Policies > (From: Dialup, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (**選択**), Dial-Up VPN
Destination Address:
    Address Book Entry: (**選択**), Any
Service: ANY
Action: Tunnel
Tunnel VPN: from_sales
    Modify matching bidirectional VPN policy:（**オフ**）
L2TP: sales_corp
Position at Top: (**選択**)

CLI

1. ユーザー定義ゾーン

```
set zone name dialup
set zone dialup vrouter trust-vr
set zone dialup block
```

2. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet2 zone dialup
set interface ethernet2 ip 1.3.3.1/24
```

3. L2TP/IKE ユーザー

```
set user adam type ike l2tp
set user adam password AJbioJ15
unset user adam type auth
set user adam ike-id u-fqdn ajackson@abc.com
set user betty type ike l2tp
set user betty password BviPsoJ1
unset user betty type auth
set user betty ike-id u-fqdn bdavis@abc.com
set user carol type ike l2tp
set user carol password Cs10kdD3
unset user carol type auth
set user carol ike-id u-fqdn cburnet@abc.com
```

4. IKE/L2TP ユーザーグループ

```
set user-group fs location Local
set user-group fs user adam
set user-group fs user betty
set user-group fs user carol
```

5. IP プール

```
set ippool global 10.10.2.100 10.10.2.180
```

6. L2TP デフォルト設定

```
set l2tp default ippool global
set l2tp default ppp-auth chap
set l2tp default dns1 1.1.1.2
set l2tp default dns2 1.1.1.3
```

7. L2TP トンネル

```
set l2tp sales_corp outgoing-interface ethernet2
set l2tp sales_corp auth server Local user-group fs
```

8. VPN トンネル

```
set ike gateway field dialup fs aggressive outgoing-interface ethernet2 proposal
    rsa-g2-3des-sha
set ike gateway field cert peer-ca1
set ike gateway field cert peer-cert-type x509-sig
set vpn from_sales gateway field transport sec-level compatible
```

注： Windows 2000 (NetScreen-Remote 非装備) はメインモードネゴシエーションだけをサポートしています。

番号 1 は、CA ID 番号を示します。CA の ID 番号を調べるには、**get pki x509 list ca-cert** コマンドを使用してください。.

9. ポリシー

```
set policy top from dialup to trust “Dial-Up VPN” any any tunnel vpn from_sales
    l2tp sales_corp
save
```

NetScreen-Remote セキュリティポリシーエディタ (Adam)

Betty と Carol の NetScreen-Remote クライアント用 L2TP-over-IP Sec トンネルを構成する場合も、ここで Adam 用に説明した手順に従います。

1. **Options > Secure > Specified Connections** をクリックします。
2. **Add a new connection** をクリックします。表示される新規接続アイコンの横に **AJ** と入力します。
3. 接続オプションを次のように構成します。

   Connection Security: Secure
   Remote Party ID Type: IP Address
   IP Address: 1.3.3.1
   Protocol: UDP
   Port: L2TP
   Connect using Secure Gateway Tunnel:（**オフ**）

4. AJ アイコンの左側にある「＋」記号をクリックして接続ポリシーを拡張表示します。
5. **My Identity** をクリックし、次の構成を行います。

   Select Certificate ドロップダウンリストから、セキュリティデバイスでユーザーの IKE ID として指定されている E メールアドレスが含まれた証明書を選択します。

   ID Type: E-**mail Address**
   Port: L2TP

注： 証明書の E メールアドレスは、自動的に識別フィールドに表示されます。

6. **Security Policy** アイコンをクリックし、**Aggressive Mode** を選択します。
7. Security Policy アイコンの左にある「＋」シンボルをクリックしてから、Authentication (Phase 1) と Key Exchange (Phase 2) の左にある「＋」シンボルをクリックし、ポリシーをさらに拡張します。

8. **Authentication (Phase 1) > Proposal 1** をクリックします。次の認証方法およびアルゴリズムを選択します。

   Authentication Method: Pre-Shared Key
   (または)
   Authentication Method: RSA Signatures
   Hash Alg: SHA-1
   Key Group: Diffie-Hellman Group 2

9. **Key Exchange (Phase 2) > Proposal 1** をクリックします。次の IPSec プロトコルを選択します。

   Encapsulation Protocol (ESP): (**選択**)
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Encapsulation: Transport

10. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: Triple DES
    Hash Alg: MD5
    Encapsulation: Transport

11. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Encapsulation: Transport

12. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: DES
    Hash Alg: MD5
    Encapsulation: Transport

13. **File > Save Changes** をクリックします。

14. ネットワークの接続ウィザードを使用して、Windows 2000 オペレーティングシステムのネットワーク接続をセットアップする必要があります。

注 : ネットワークの接続ウィザードで構成を行う際には宛先ホスト名や IP アドレスを入力する必要があります。**1.3.3.1** を入力してください。その後、接続を開始してユーザー名とパスワードの入力を促すメッセージが表示されたら adam と **AJbioJ15** を入力します。詳細については、Microsoft Windows 2000 のマニュアルを参照してください。

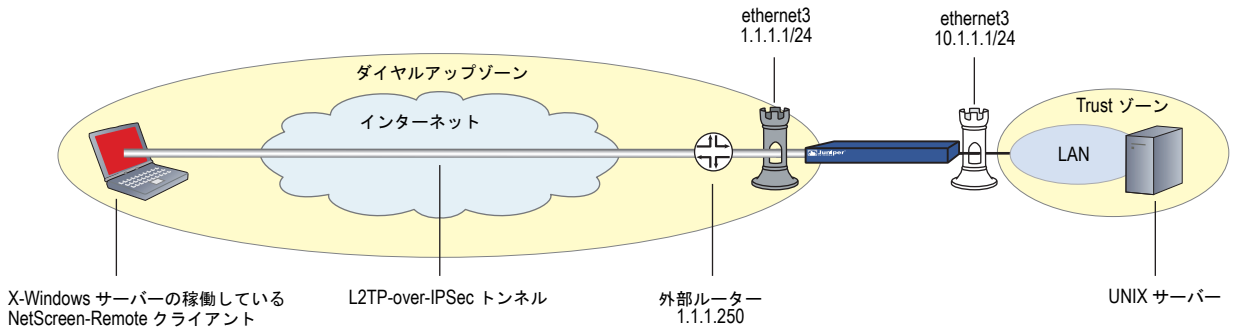
双方向の L2TP-over-IPSec

この例では、ethernet1 (10.1.1.1/24) が Trust ゾーンインターフェースで NAT モードになっており、ethernet3 (1.1.1.1/24) が Untrust ゾーンインターフェースです。NetScreen-Remote ダイヤルアップユーザーと企業 LAN との間に L2TP-over-IPSec トンネルを作成します。リモートユーザーは X-Windows アプリケーションが稼働しており、双方向ポリシーが必要です。

IKE ID *jf@ns.com* を持つ IKE ユーザー *dialup-j* に *VPN_dial* という名前のダイヤルアップ AutoKey IKE VPN トンネルの入力ポリシーと出力ポリシーを、そして tun1 という名前の L2TP トンネルを設定します。IKE ユーザーは、Trust ゾーンの企業サーバーに到達するために、Untrust ゾーンから セキュリティデバイスへの IPSec 接続を開始します。この時点では、L2TP 通信だけが許可されています。L2TP/PPP ネゴシエーションが完了すると、L2TP トンネルが確立されます。双方向ポリシーを設定すると、トラフィックはトンネルのどちらの端からでも送信できます。

ダイヤルアップユーザー *dialup-j* は、Windows 2000 OS オペレーティングシステム上では NetScreen-Remote クライアントを使用します。ダイヤルアップユーザー *dialup-j* 用の NetScreen-Remote の設定は、226 ページの図 60 の後で示します。

図 60: 双方向の L2TP-over-IPSec



注： Windows 2000 (NetScreen-Remote 非装備) に L2TP-over-IPSec トンネルを構成するには、フェーズ 1 のネゴシエーションはメインモードであり、IKE ID タイプは ASN1-DN である必要があります。

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24

   次のように選択してから **OK** をクリックします。

   Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Trust_net
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Trust

3. L2TP/IKE ユーザー

Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

User Name: dialup-j
Status: Enable
IKE User: (選択)
Simple Identity: (選択)
IKE Identity: jf@ns.com
Authentication User: (選択)
L2TP User: (選択)
User Password: abc123
Confirm Password: abc123

注 : NetScreen-Remote クライアントが送信した IKE ID と同じ IKE ID を入力する必要があります。これはクライアントが認証に使用している証明書に記載されている E メールアドレスです。

---

4. L2TP

VPNs > L2TP > Tunnel > New: 次のように入力してから **OK** をクリックします。

Name: Tun1
Use Default Settings: (選択)
Secret: netscreen
Keepalive: 60

5. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: dialup1
Security Level: (選択) Standard
Remote Gateway Type: Dialup User; (選択する), dialup-j
Preshared Key: n3TsCr33N
Outgoing Interface: (選択) ethernet3

> Advanced: 次のように入力して、**Return** をクリックし、基本 AutoKey IKE Gateway 構成ページに戻ります。

Mode (Initiator): Aggressive
Enable NAT-Traversal: (選択)
UDP Checksum: (選択)
Keepalive Frequency: 5

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: VPN_dial
Remote Gateway: Predefined: (選択), dialup1

> Advanced: 次のように入力して、**Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Security Level: Standard (選択)
Transport Mode (For L2TP-over-IPSec only): (選択)

6. ルート

Network > Routing > Routing Entries > New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

7. ポリシー

Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Dial-Up VPN
Destination Address:
Address Book Entry: (選択), trust_net
Service: ANY
Action: Tunnel
トンネル VPN: VPN_dial
Modify matching bidirectional VPN policy: (選択)
L2TP: (選択) tun1

Policies > (From: Trust, To: Untrust) > New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), trust_net
Destination Address:
Address Book Entry: (選択), Dial-Up VPN
Service: ANY
Action: Tunnel
Tunnel VPN: vpn_dial
Modify matching bidirectional VPN policy: (選択)
L2TP: tun1

CLI

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. アドレス

```
set address trust trust_net 10.1.1.0/24
```

3. L2TP/IKE ユーザー

```
set user dialup-j ike-id u-fqdn jf@ns.com
set user dialup-j type auth ike l2tp
set user dialup-j password abc123
```

4. L2TP

```
set L2TP tun1 outgoing-interface ethernet3 secret "netscreen" keepalive 60
```

5. VPN

```
set ike gateway dialup1 dialup "dialup-j" aggressive outgoing-interface ethernet3
    preshare n3TsCr33N sec-level standard
set ike gateway dialup1 nat-traversal udp-checksum
set ike gateway dialup1 nat-traversal keepalive-frequency 5
set vpn VPN_dial gateway dialup1 no-replay transport idletime 0 sec-level standard
```

6. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

7. ポリシー

```
set policy from untrust to trust “dial-Up VPN” trust_net any tunnel vpn VPN_dial
    tun1
set policy from trust to untrust trust_net “dial-Up VPN” any tunnel vpn VPN_dial
    l2tp tun1
save
```

NetScreen-Remote セキュリティポリシーエディタ (ユーザー 「dialup-j」用)

1. **Options > Secure > Specified Connections** をクリックします。
2. **Add a new connection** をクリックし、表示された新しい接続アイコンの横に **dialup-j** と入力します。
3. 接続オプションを次のように構成します。

   Connection Security: Secure
   Remote Party ID Type: IP Address
   IP Address: 1.1.1.1
   Protocol: UDP
   Port: L2TP
   Connect using Secure Gateway Tunnel:（**オフ**）

4. UNIX アイコンの左にある 「+」シンボルをクリックして接続ポリシーを拡張します。

5. **My Identity** をクリックし、次の構成を行います。

   Select Certificate ドロップダウンリストから、セキュリティデバイスでユーザーの IKE ID として指定されている E メールアドレスが含まれた証明書を選択します。

   ID Type: E**-mail Address**
   Port: L2TP

注： 証明書の E メールアドレスは、自動的に識別フィールドに表示されます。

6. **Security Policy** アイコンをクリックし、**Aggressive Mode** を選択します。

7. Security Policy アイコンの左にある「+」シンボルをクリックしてから、Authentication (Phase 1) と Key Exchange (Phase 2) の左にある「+」シンボルをクリックし、ポリシーをさらに拡張します。

8. **Authentication (Phase 1) > Proposal 1** をクリックします。次の認証方法およびアルゴリズムを選択します。

   Authentication Method: Pre-Shared Key
   (**または**)
   Authentication Method: RSA Signatures
   Hash Alg: SHA-1
   Key Group: Diffie-Hellman Group 2

注： PFS (Perfect Forwarding Secrecy) を セキュリティデバイス (DF グループ 1、2、または 5) 上で有効した場合は、NetScreen Remote の VPN クライアントも有効にしなければなりません。

9. **Key Exchange (Phase 2) > Proposal 1** をクリックします。次の IPSec プロトコルを選択します。

   Encapsulation Protocol (ESP): (**選択**)
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Encapsulation: Transport

10. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: Triple DES
    Hash Alg: MD5
    Encapsulation: Transport

11. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Encapsulation: Transport

12. **Key Exchange (Phase 2) > Create New Proposal** をクリックします。次の IPSec プロトコルを選択します。

    Encapsulation Protocol (ESP): (**選択**)
    Encrypt Alg: DES
    Hash Alg: MD5
    Encapsulation: Transport

13. **File > Save Changes** をクリックします。

ネットワークの接続ウィザードを使用して、Windows 2000 オペレーティングシステムのネットワーク接続をセットアップする必要があります。

注 : ネットワークの接続ウィザードで構成を行う際には宛先ホスト名や IP アドレスを入力する必要があります。1.1.1.1 と入力してください。その後、接続を開始してユーザー名とパスワードの入力を促すメッセージが表示されたら dialup-j と abc123 を入力します。詳細については、Microsoft Windows 2000 のマニュアルを参照してください。

第 7 章

高度な仮想プライベート ネットワーク機能

本章では、以下の VPN（仮想プライベートネットワーク）技術の使用法を説明します。

- 234 ページの「NAT-Traversal」
  - 235 ページの「NAT の精査」
  - 237 ページの「NAT デバイスのトラバース」
  - 239 ページの「UDP チェックサム」
  - 240 ページの「キープアライブパケット」
  - 240 ページの「イニシエータ / 受信側シンメトリー」
  - 241 ページの「NAT-Traversal を使用可能にする」
  - 242 ページの「NAT-Traversal との IKE ID の使用」
- 243 ページの「VPN の監視」
  - 244 ページの「再入力および最適化オプション」
  - 245 ページの「ソースインターフェースおよび宛先アドレス」
  - 246 ページの「ポリシー考慮事項」
  - 247 ページの「VPN 監視機能の構成」
  - 255 ページの「SNMP VPN 監視オブジェクトおよびトラップ」
- 256 ページの「1 つのトンネルインターフェースに対する複数のトンネル」
  - 257 ページの「ルートからトンネルへのマッピング」
  - 259 ページの「リモートピアのアドレス」
  - 260 ページの「手動および自動テーブルエントリ」

- 294 ページの「冗長 VPN ゲートウェイ」
  - 295 ページの「VPN グループ」
  - 296 ページの「監視機構」
  - 300 ページの「TCP SYN-Flag チェック」
- 306 ページの「VPN 対向の作成」
- 313 ページの「ハブアンドスポーク方式 VPN の作成」

NAT-Traversal

NAT (ネットワークアドレス変換機能) および NAPT (ネットワークアドレスポート変換機能) は、LAN (ローカルエリアネットワーク) で内部トラフィック用の IP アドレスのセット、および外部トラフィック用のアドレスのセットを使用できるようにするインターネット規格です。NAT デバイスは、IP アドレスの所定のプールからこれらの外部アドレスを生成します。

IPSec トンネルをセットアップする場合、データパスに沿う NAT デバイスを配置しても、フェーズ 1 と 2 IKE ネゴシエーションには効果がありません。IPSec トンネリングは常に、UDP (ユーザーデータグラムプロトコル) セグメント内で IKE パケットをカプセル化しています。しかしながら、フェーズ 2 ネゴシエーションの完了後に IPSec パケット上で NAT を実行すると、トンネルが正常に機能しません。NAT が IPSec を混乱させる原因は多数ありますが、その原因の 1 つとして、ESP (カプセル化されたセキュリティペイロード) に対して、NAT デバイスがポート変換用にレイヤー 4 ヘッダーの位置を識別できない (暗号化されているため) ことが挙げられます。AH (認証ヘッダー) プロトコルに対して、NAT デバイスはポート番号を変更できますが、IPSec パケット全体が含まれる認証確認は正常に実行できません。

注 : 非互換性 IPSec/NAT のリストは、Bernard Aboba の *draft-ietf-ipsec-nat-regts-00.txt* を参照してください。

この問題を解決するために、セキュリティ デバイスおよび NetScreen-Remote クライアント（バージョン 6.0 以上）では、NAT-T（NAT-Traversal）機能を作動させることができます。NAT-T は、フェーズ 1 の交換中にデータパスに沿って NAT デバイスを 1 つ以上検出すると、IETF ドラフトの最新バージョン同様 *draft-ietf-ipsec-nat-t-ike-00.txt* および *draft-ietf-ipsec-udp-encaps-00.txt* に規定されているように 、IPSec パケットに UDP カプセル化のレイヤーを追加します。

注 : NetScreen-Remote 6 および NetScreen-Remote 7 は、*draft-ietf-ipsec-nat-t-ike-00.txt* と *draft-ietf-ipsec-udp-encaps-00.txt* に規定されているように、NAT-T をサポートします。NetScreen-Remote 8.2 は、*ドラフト 02* をサポートしています。

NAT デバイスが IKE/IPSec 対応で、IKE ポート番号が 500 かまたは IPSec プロトコル番号が 50 (ESP の場合) または 51 (AH の場合) のパケットを処理しようとすると、別の問題が起こる可能性があります。そのような IKE パケットの中間処理を回避するために、前述の IETF ドラフトのバージョン 2 では、IKE 用の UDP

ポート番号を 500 から 4,500 に移行（または「フローティング」）することを提案しています。IPSec パケットの中間処理を回避するため、ドラフト 0 と 2 の両方では、外部 IP ヘッダーと ESP または AH ヘッダーの間に UDP ヘッダーを挿入するように規定しています。それにより、プロトコル フィールドの値が 50 または 51（それぞれ ESP、AH の場合）から 17（UDP の場合）に変わります。さらに、挿入した UDP ヘッダーはポート 4500 も使用します。ScreenOS の現行バージョンは、バージョン 0 同様、*draft-ietf-ipsec-nat-t-ike-02.txt* および *draft-ietf-ipsec-udp-encaps-02.txt* に基づく NAT-T をサポートしています。

注 : ScreenOS は、手動鍵トンネル用の NAT-T と、AH を使用する IPSec トラフィック用の NAT-T はどちらもサポートしていません。ESP を使用する AutoKey IKE トンネル用の NAT-T のみサポートしています。

NAT の精査

VPN トンネルの両端が NAT-T をサポートしているかをチェックするため、ScreenOS は、フェーズ 1 ネゴシエーションの最初の 2 つ（1 つはドラフト 0 のタイトル、もう 1 つはドラフト 2 のタイトル）の交換時にベンダー ID ペイロードの 2 つの MD-5 ハッシュを送信します。

- “4485152d 18b6bbcd 0be8a846 9579ddcc” - “draft-ietf-ipsec-nat-t-ike-00” の MD-5 ハッシュ
- “90cb8091 3ebb696e 086381b5 ec427b1f” - ”draft-ietf-ipsec-nat-t-ike-02” の MD-5 ハッシュ

どちらのピアも、ベンダーペイロード ID の上記の値の少なくとも 1 つを送受信して、NAT-T 精査を続けなければなりません。両方のドラフトのハッシュを送信する場合、ScreenOS はドラフト 2 の NAT-T 実装を使用します。

各端点にあるデバイスが NAT-T をサポートしていると、3 番目と 4 番目のフェーズ 1 交換 (メインモード) または 2 番目と 3 番目の交換 (アグレッシブモード) で 相互に NAT-D (NAT discovery) ペイロードを送信します。NAT-D (NAT discovery) ペイロードは、NAT-T の IKE ペイロードタイプです。NAT-D ペイロードタイプの番号は 0130 です。これ以外の IKE ペイロードタイプの一覧については、12 ページの「IKE パケット」を参照してください。

注 : ScreenOS は、IKE ネゴシエーションで複数の NAT-Discovery (NAT-D) ペイロードを処理できます。

NAT-D ペイロードには、次の情報のネゴシエートされたハッシュが含まれています。

- 宛先 NAT-D ハッシュ :
  - 開始側の cookie (CKY-I)
  - 受信側の cookie (CKY-R)
  - リモート (宛先) IKE ピアの IP アドレス
  - 宛先ポート番号

- ソース NAT-D ハッシュ (1 つ以上):
  - 開始側の cookie (CKY-I)
  - 受信側の cookie (CKY-R)
  - ローカル (ソース) IKE ピアの IP アドレス
  - ソースポート番号

注 : NAT-T は、複数のインターフェースおよび出力インターフェースを指定していない実装を持つデバイスの、複数のソース NAT-D ハッシュをサポートしています。

各ピアが送信や受信のハッシュを比較すると、ハッシュ間でアドレス変換が行われたかどうかを知らせることができます。変更されたパケットを識別すると、次のように NAT デバイスの場所も示します。

何が	一致する場合	その対処法
ローカルピアの宛先ハッシュ	リモートピアのソースハッシュの少なくとも 1 つ	アドレス変換は行われません。
ローカルピアのソースハッシュの少なくとも 1 つ	リモートピアの宛先ハッシュ	アドレス変換は行われません。

何が	一致しない場合	その対処法
ローカルピアの宛先ハッシュ	リモートピアのソースハッシュの少なくとも 1 つ	アドレス変換は行われません。
ローカルピアのソースハッシュの少なくとも 1 つ	リモートピアの宛先ハッシュ	アドレス変換は行われません。

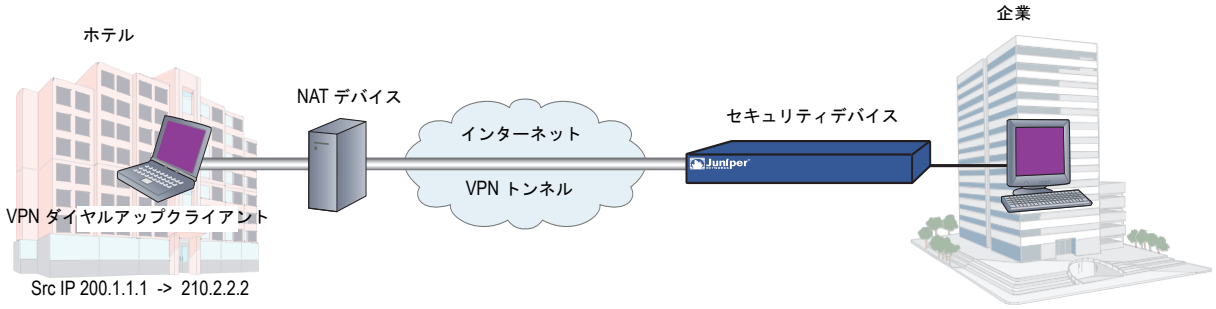
IKE キープアライブは、NAT デバイスの背後のピアから開始しなければならないため、NAT デバイスの位置を知ることが重要です。240 ページの「キープアライブパケット」を参照してください。

両方のピアが IETF ドラフト 2 をサポートしている場合、フェーズ 1 のネゴシエーション中、ピア間に NAT デバイスが検出されるとすぐに、IKE ポート番号を 500 から 4500 に変更します。メインモードでは、フェーズ 1 の 5 番目と 6 番目の変換、そしてフェーズ 2 のすべての変換で、ポート番号を 4500 に変更します。アグレッシブモードでは、フェーズ 1 の 3 番目と最後の変換、そしてフェーズ 2 のすべての変換で、ポート番号を 4500 に変更します。ピアは、それ以降のすべての IPSec トラフィックの UDP ポート番号にも 4500 を使用します。

NAT デバイスのトラバース

図 61 では、ホテルの LAN 周辺にある NAT デバイスが、ホテルによって割り当てられた IP アドレス 2.1.1.5 を使用する VPN ダイヤルアップ クライアントからのパケットを受け取ります。すべてのアウトバウンドトラフィックに対して、NAT デバイスは外部ヘッダーの本来のソース IP アドレスを新しいアドレス 2.2.2.2 に置き換えます。フェーズ 1 ネゴシエーションの間に VPN クライアントおよびセキュリティ デバイスは、双方の VPN 参加者が NAT-T をサポートしていること、そして NAT デバイスがデータ パスに沿って存在し VPN クライアントの前に配置されていることを検出します。

図 61: NAT-Traversal



UDP パケット内の IPSec パケットをカプセル化することによって（VPN クライアントとセキュリティ デバイスの両方が行う）、認証チェックが失敗するという問題を解決します。NAT デバイスはそれらを UDP パケットとして処理し、UDP ヘッダーのソースポートを変更して AH または ESP ヘッダーの SPI を無変更に保ちます。VPN 参加者は UDP レイヤーを取り除いて IPSec パケットを処理しますが、認証済みコンテンツがいずれも変更されていないため、このパケットは認証確認をパスします。

NAT デバイスが IKE/IPSec に対応している場合、別の問題が起こる可能性があります。IKE/IPSec 対応の NAT デバイスは、IKE/IPSec トラフィックを転送するのではなく、処理しようとすることがあります。そのような中間処理を防ぐために、NAT-T (v2) は IKE の ソースおよび宛先 UDP ポート番号を 500 から 4500 に変更します。また、ペイロードの直前に、UDP ヘッダーに非 ESP マーカーを挿入します。IPSec トラフィックでは、NAT-T (v0 および 2) は、外部 IP ヘッダーと ESP ヘッダーの間に UDP ヘッダーを挿入します。また、UDP パケットは、ソースと宛先の両方のポート番号に 4500 を使用します。

前述したように、NAT-T (v2) は、ヘッダーと UDP セグメントの間に非 ESP マーカーを追加して、ISAKMP パケットをカプセル化します。非 ESP マーカーとは、4 バイトの 0 (0000) で、UDP セグメントに追加して、マーカーのついていないカプセル化された ISAKMP パケットとカプセル化された ESP パケットを識別します。非 ESP マーカーがないと、どちらのパケットの UDP ヘッダーにも 4500 が使われているため、受信側はカプセル化されたパケットが ISAKMP なのか ESP なのかが分かりません。このマーカーを使用すると、カプセル化されたパケットの正しいタイプが分かるため、受信側はそのパケットを正確に多重分離することができます。

238 ページの図 62 に示されるように、データ パスで NAT デバイスを検出すると、IKE パケットの UDP ヘッダーにあるソースおよび宛先ポート番号は、500 から 4,500 に変更されます。また、VPN トンネルの端点は、UDP ヘッダーとペイロードの間に非 ESP マーカーを挿入して、カプセル化された ISAKMP パケットと ESP パケットを識別できるようにします。受信側は、このマーカーを使用することにより、カプセル化された ISAKMP パケットと ESP パケットを識別し、そのパケットを正確に多重分離します。

図 62: IKE パケット（フェーズ 1 と 2 の場合）

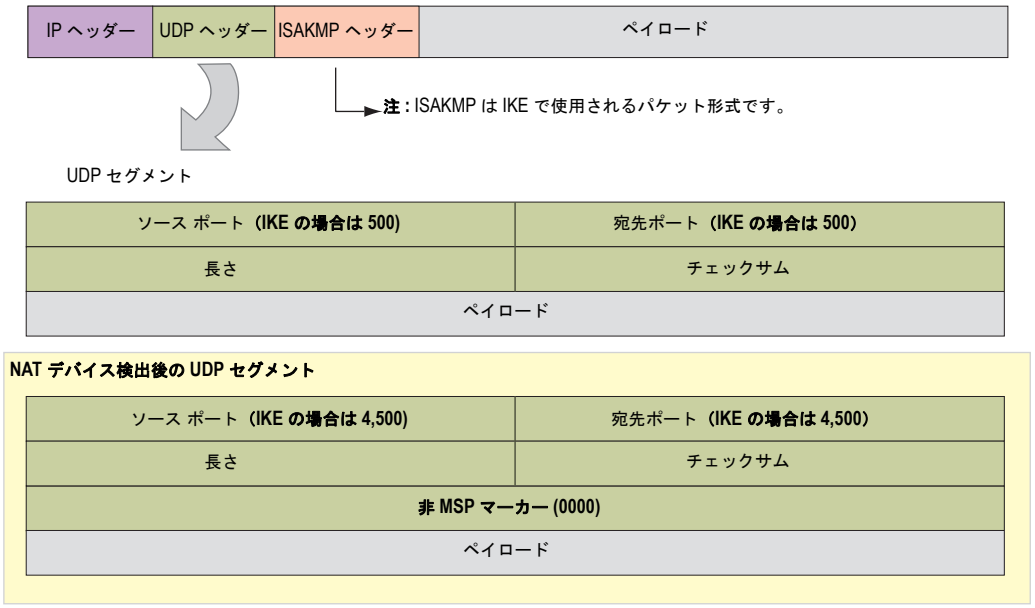
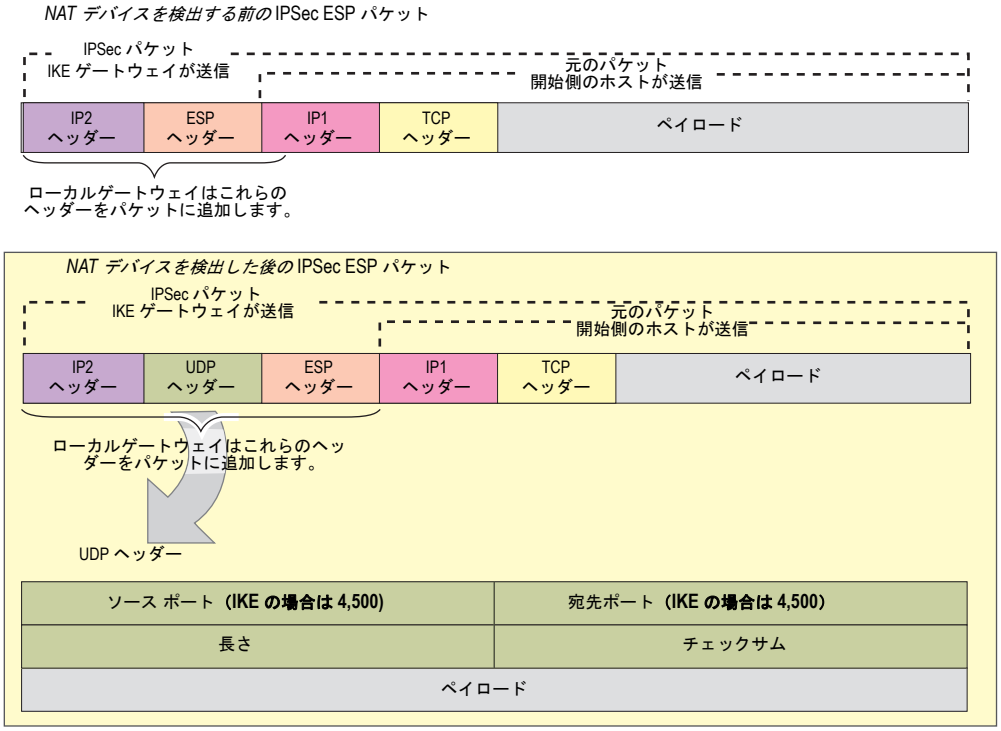


図 63 では、データ パスで NAT デバイスを検出すると、VPN トンネルの端点は IPSec パケットの外部 IP アドレスと ESP ヘッダーの間に UDP ヘッダーを追加挿入します。非 ESP マーカーが付いてないため、受信側はカプセル化された ESP パケットと ISAKMP パケットを識別し、ESP パケットを正確に多重分離することができます。

図 63: NAT デバイスを検出する前後の IPSec ESP パケット



UDP チェックサム

全ての UDP パケットには、UDP チェックサム、つまり UDP パケットに送信エラーのないことを保証する計算値が含まれます。セキュリティ デバイスでは NAT-T に対して UDP チェックサムを使用することを必須としていないため、WebUI および CLI にオプション設定としてチェックサムが存在します。ただし、いくつかの NAT デバイスはチェックサムを要求するため、この設定の有効化または無効化が必要となることもあります。デフォルトでは、NAT-T が有効になると UDP チェックサムが含まれます。

WebUI

VPNs > AutoKey Advanced > Gateway > New:

77 ページの「サイト間 VPN (仮想プライベートネットワーク)」または 157 ページの「ダイヤルアップ仮想プライベート ネットワーク」の説明に従って新しいトンネル ゲートウェイの必要なパラメータを入力します。次のように入力してから **OK** をクリックします。

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Enable NAT-Traversal: (選択)
UDP Checksum: Enable

CLI

set ike gateway *name* nat-traversal udp-checksum
unset ike gateway *name* nat-traversal udp-checksum

キープアライブパケット

NAT デバイスはホストに IP アドレスを割り当てる際に、トラフィックが全く発生しないときに新規アドレスが有効に保たれる期間を決定します。たとえば、NAT デバイスは、20 秒間未使用の状態にある任意の生成済み IP アドレスを無効化することも考えられます。そのため、通常 IPSec 参加者は、フェーズ 1 およびフェーズ 2 の SA の有効期限が切れるまで NAT マッピングが変更されないようにするために、キープアライブ パケット（空の UDP パケット）を NAT デバイスを介して定期的に送信する必要があります。

注： NAT デバイスが持つセッションタイムアウト間隔は、製造メーカーおよびモデルによって異なります。NAT デバイス用の間隔を特定し、キープアライブの周期値をその値より低く設定することが重要です。

イニシエータ / 受信側シンメトリー

2 つのセキュリティ デバイスが、NAT デバイスなしにトンネルを設定する場合、いずれかのセキュリティ デバイスがイニシエータまたは受信側としての機能を果たすことができます。ただし、いずれかのホストが NAT デバイスの背後に存在すれば、そのようなイニシエータ / 受信側シンメトリーが不可能となることもあります。この問題は NAT デバイスが動的に IP アドレスを生成する場合は常に発生します。

図 64: NAT デバイスの背後で動的に割り当てられた IP アドレスを持つセキュリティ デバイス

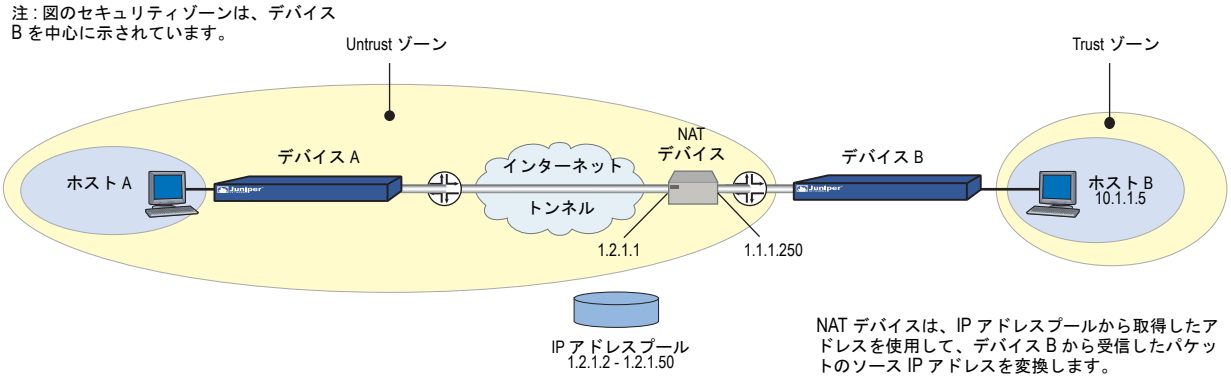


図 64 では、デバイス B は NAT デバイスの背後に位置するサブネット内に存在します。NAT デバイスが、デバイス B から（IP アドレスのプールから動的に取得することにより）パケットの新しいソース IP アドレスを生成すると、デバイス A はデバイス B を明確に識別できなくなります。そのため、デバイス A はデバイス B とのトンネルを正常に開始できません。デバイス A が受信側、デバイス B がイニシエータとなり、両者はアグレッシブ モードでフェーズ 1 ネゴシエーションを実行する必要があります。

ただし、NAT デバイスが MIP（マップ IP）またはその他の 1 対 1 アドレッシング方法を使用して新しい IP アドレスを生成すると、デバイス A はデバイス B を明確に識別できます。結果的に、デバイス A またはデバイス B のどちらかがイニシエータとなることができ、フェーズ 1 でメイン モードまたはアグレッシブ モードを使用できます。

注 : 受信側として機能するセキュリティ デバイス上で NAT-T を使用可能にし、これをメイン モードでの IKE ネゴシエーションを実行するように構成すると、このデバイス、および同じ出力インターフェース上で構成される次のタイプのピアは、互いに示された同じ順序で同じフェーズ 1 プロポーザルを使用する必要があります。

動的ピア（動的に割り当てられた IP アドレスを持つピア）
ダイヤルアップ VPN ユーザー
NAT デバイス背後の静的 IP アドレスを持つピア

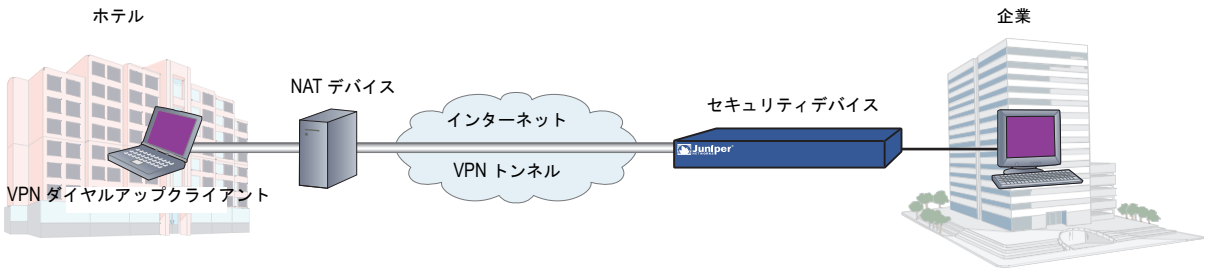
フェーズ 1 をメイン モードでネゴシエートする際は、最後の 2 つのメッセージまでピアを識別できないため、フェーズ 1 プロポーザルはすべて同じものとし、IKE ネゴシエーションが続行できるようにする必要があります。

セキュリティ デバイスは自動的に、すべてのフェーズ 1 プロポーザルが同一で、メイン モードでの IKE を同じ出力インターフェース上の前述のピア タイプのいずれか 1 つに設定したときと同じ順序であるかをチェックします。プロポーザルが同一でない場合、セキュリティ デバイスはエラー メッセージを生成します。

NAT-Traversal を使用可能にする

In 図 65 では、ホテル LAN 周辺の NAT デバイスは、会議に出席しているセールスマンの Jozef が使用する VPN ダイヤルアップ クライアントにアドレスを割り当てます。Jozef がダイヤルアップ VPN トンネルを介して企業 LAN に到達するには、セキュリティ デバイス上で構成されたリモート ゲートウェイ「jozef」用、および VPN ダイヤルアップ クライアント上で構成されたリモート ゲートウェイ用に NAT-T の機能を使用可能にする必要があります。セキュリティ デバイスで、伝送時に UDP チェックサムを含み、キープアライブの周期が 8 秒となるように設定することもできます。

図 65: NAT-Traversal を使用可能にする



WebUI

VPNs > AutoKey Advanced > Gateway > New: 第 4 章、「サイト間 VPN (仮想プライベートネットワーク)」、または第 5 章、「ダイヤルアップ仮想プライベート ネットワーク」、の説明に従って、新しいトンネル ゲートウェイの必要なパラメータを入力し、次のように入力してから **OK** をクリックします。

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Enable NAT-Traversal: (選択)
UDP Checksum: Enable
Keepalive Frequency: 8 秒 (0-300 秒)

注： CLI からダイヤルアップ VPN を設定すると、セキュリティ デバイスは自動的に NAT-Traversal を有効にします。

CLI

```
set ike gateway jozef nat-traversal
set ike gateway jozef nat-traversal udp-checksum
set ike gateway jozef nat-traversal keepalive-frequency 8
save
```

NAT-Traversal との IKE ID の使用

2 つの VPN ゲートウェイがメインモードでネゴシエートすると、互いを識別しトンネルをアクティブ化するため、IP アドレスを交換します。しかしながら、トンネルのどちらか一方または両方の端のデバイスに IP アドレスが動的に割り当てられている場合、トンネルの両端のデバイス上で IKE ID（ローカル ID およびピア ID）を構成しなければなりません。IKE ID は、静的なままであるユニークな識別子です。IKE ゲートウェイを構成すると、IKE ID はそのフェーズの間にセットアップされます。リモート IP アドレスの代わりに IKE ID を構成します。

NAT-T なしで、ローカル側のローカル ID およびリモート側のピア ID だけを使用して、VPN トンネルをアクティブ化できます。しかし、証明書を使用してメインモードで動的な VPN と NAT-Traversal を使用するとき、VPN トンネルの両側でローカル ID およびピア ID を設定しなければなりません。次の例は、互いに識別しその間のトンネルをアクティブ化できるように、firewall1 と firewall2 でのローカル ID およびピア ID の構成方法を示します。

WebUI

firewall1 で、以下を入力します。

VPNs > AutoKey IKE Advanced > Gateway > New (次のように入力して Advanced をクリックします。

```
Gateway Name: test_gw
Address/Hostname: 0.0.0.0
Peer-ID: firewall2
```

Advanced をクリックして、以下を入力します。

```
Security Level: Standard
Local-ID: firewall1
Outgoing Interface: ethernet0/0
Mode: Main
Security Level: Standard
```

firewall2 で、以下を入力します。

VPNs > AutoKey IKE Advanced > Gateway > New (次のように入力して Advanced をクリックします。

```
Gateway Name: gw_bap15_p1
Address/Hostname: 1.1.1.1
Peer-ID: firewall1
```

Advanced をクリックして、以下を入力します。

Security Level: Standard
Local-ID: firewall2
Outgoing Interface: ethernet0/0
Mode: Main
Security Level: Standard

CLI

firewall1 で、以下を入力します。

```
set ike gateway test-gw address 0.0.0.0 id firewall2 main local-id firewall1
    outgoing-interface ethernet0/0 proposal standard
```

firewall2 で、以下を入力します。

```
set ike gateway gw_bap15_p1 address 1.1.1.1 id firewall1 main local-id firewall2
    outgoing-interface ethernet0/0 proposal standard
```

VPN の監視

特定のトンネルに対して VPN 監視を使用可能にすると、セキュリティ デバイスは指定された間隔（秒単位で構成される）でそのトンネルを介して ICMP エコー要求（または「pings」）を送信し、そのトンネルを介したネットワーク接続を監視します。

注 : ping 間隔を変更するには、以下の CLI コマンドを使用します。**set vpnmonitor interval** *number* デフォルトは 10 秒です。

ping のアクティビティによって VPN 監視状態に変化が生じたことが示された場合、セキュリティ デバイスは次の SNMP（簡易ネットワーク管理プロトコル）トラップのいずれか 1 つを起動します。

- **Up to Down:** トンネルの VPN 監視の状態がアップ（作動中）であっても、指定された数の ICMP エコー要求が連続して応答を引き出せず、またその他に受信する VPN トラフィックが存在しない場合にこのトラップが発生します。すると停止状態へと変化します。
- **Down to Up:** トンネルに対する VPN 監視の状態が停止中であっても ICMP エコー要求が 1 つの応答を引き出すと、状態は作動中に変化します。停止中から作動中へのトラップは、再入力オプションが使用不可に設定されていて、ICMP エコー要求がトンネルを介して応答を引き出した際にフェーズ 2 SA が依然としてアクティブである場合にのみ発生します。

注 : CLI コマンド **set vpnmonitor threshold** *number* を使用すると、連続して失敗する ICMP エコー要求数のしきい値を変更できます。デフォルトは、10 連続要求です。

VPN 監視が提供する SNMP データに関する詳細については、255 ページの「SNMP VPN 監視オブジェクトおよびトラップ」を参照してください。

VPN 監視は VPN オブジェクト単位で適用すれば良く、VPN トンネル単位で行う必要はありません。VPN オブジェクトは、**set vpn** コマンドか、それと同等の WebUI で定義します。VPN オブジェクトを 1 つ定義すると、そのオブジェクトは 1 つ以上のポリシーで参照することができます (ポリシーベース VPN を作成)。ScreenOS は、VPN オブジェクトと他のポリシーパラメータからポリシーベース VPN トンネルを取得するため、単体の VPN オブジェクトが多数の VPN トンネルの要素となります。この VPN オブジェクトと VPN トンネルの違いは重要で、監視最適化を有効にしない場合は、VPN 監視を 100 個以下の VPN トンネルに適用するようお勧めします。監視最適化を有効にする場合は、VPN 監視を適用できる VPN トンネル数に制限はありません。監視オプションについては、244 ページの「再入力および最適化オプション」を参照してください。

注 : VPN 監視最適化は、オブジェクトごとに動作します。すべての VPN オブジェクトで有効にすることも、一部の VPN オブジェクトに対してだけ有効にすることもできます。

再入力および最適化オプション

再入力オプションを使用可能にすると、セキュリティ デバイスはトンネル構成が完成した直後に ICMP エコー要求の送信を開始し、無期限に送信し続けます。エコー要求によって、トンネルに対する VPN 監視の状態が作動中になるまで、VPN トンネルを設定するための IKE ネゴシエーションの開始試行が発生します。その後、セキュリティ デバイスは、VPN 監視を目的として ping を使用します。トンネルに対する VPN 監視の状態がアップからダウンへ変化すると、セキュリティ デバイスはそのピアに対するフェーズ 2 SA（セキュリティ アソシエーション）を非アクティブにします。セキュリティ デバイスは定義された間隔でそのピアにエコー要求を送信し続け、成功するまで IKE フェーズ 2 ネゴシエーション、および必要な場合はフェーズ 1 ネゴシエーションの再開試行を発生させます。この時点で、セキュリティ デバイスはフェーズ 2 SA を再度アクティブにし、新しい鍵を生成してトンネルを再設定します。正常な再入力オペレーションが発生したことを知らせるメッセージがイベントログに現れます。

注 : セキュリティ デバイスが DHCP クライアントの場合は、DHCP を異なるアドレスに更新すると IKE は再入力を実行します。しかしながら、DHCP を同じアドレスに更新しても IKE 再入力動作は発生しません。

再入力オプションを使用して AutoKey IKE トンネルが常に作動中であることを保証し、リモートサイトのデバイスを監視したり、動的ルーティングプロトコルでリモートサイトのルートを取得しトンネルを介してメッセージを伝送したりすることも可能です。再入力オプションを用いて VPN 監視を適用するもう 1 つの用途としては、複数の VPN トンネルが単一のトンネルインターフェースにバインドされている場合に、NHTB テーブル (次のホップトンネルのバインディングテーブル) およびルートテーブルの自動母集団統計があります。この用途の例については、256 ページの「1 つのトンネルインターフェースに対する複数のトンネル」を参照してください。

再入力オプションを使用不可にすると、セキュリティ デバイスは、ユーザー生成トラフィックでトンネルがアクティブな場合に限り、VPN 監視を実行します。

デフォルトでは、VPN 監視最適化は使用不可です。使用可能にすると (**set vpn** *name* **monitor optimized**)、VPN 監視の動作は次のように変化します。

- セキュリティ デバイスは、VPN トンネルを介して受信するトラフィックを ICMP エコー応答と同等に扱います。受信トラフィックを ICMP エコー応答として承認することによって、トンネルを介したトラフィックが重くエコー応答が伝達されない場合に誤ってアラームが発生する現象を少なくすることができます。

- VPN トンネルを介した受信および出力トラフィックの両方が存在する場合、セキュリティ デバイスは VPN 監視 ping の総数を抑制します。そうすることによってネットワークトラフィックの低減が可能になります。

VPN 監視最適化にはいくつかの利点がありますが、最適化オプションがアクティブな際には、VPN ネットワーク遅延時間などの正確な SNMP 統計データが利用できなくなることに注意が必要です。また、VPN 監視を使用してトンネルのリモートエンドにおける特定の宛先 IP アドレスの可用性をトラッキングしている場合は、最適化機能によって誤った結果が得られることもあります。

ソースインターフェースおよび宛先アドレス

デフォルトでは、VPN 監視機能は、ローカルな出力インターフェースの IP アドレスをソースアドレスとして、そしてリモートゲートウェイの IP アドレスを宛先アドレスとして使用します。リモート ピアが内部 IP アドレスを持つ VPN ダイヤルアップ クライアント（NetScreen-Remote など）の場合、セキュリティ デバイスは自動的にその内部アドレスを検出し、そのアドレスを宛先として使用します。VPN クライアントになれるのは、割り当てられた内部 IP アドレスを持つ XAuth ユーザー、または内部 IP アドレスを持つ VPN ユーザーかダイアルアップ VPN グループのメンバーです。主に、VPN トンネルの他方のエンドがセキュリティ デバイスでない場合に VPN 監視のサポートを可能にする目的で、VPN 監視に対する他のソースおよび宛先 IP アドレスの用途を指定することもできます。

VPN 監視はローカルおよびリモートサイトで独立して動作するため、トンネルの一方の端のデバイス上に構成されたソースアドレスは、もう一方の端のデバイス上に構成された宛先アドレスである必要はありません。実際に、トンネルの両端または片方の端で VPN 監視を使用可能にすることができます。

図 66: VPN 監視用ソースおよび宛先アドレス

デバイス A -> デバイス B

デバイス A は、出力インターフェースからリモートゲートウェイに、つまり デバイス A の Untrust ゾーンインターフェースから デバイス B の Untrust ゾーンインターフェースに ping を送信します。

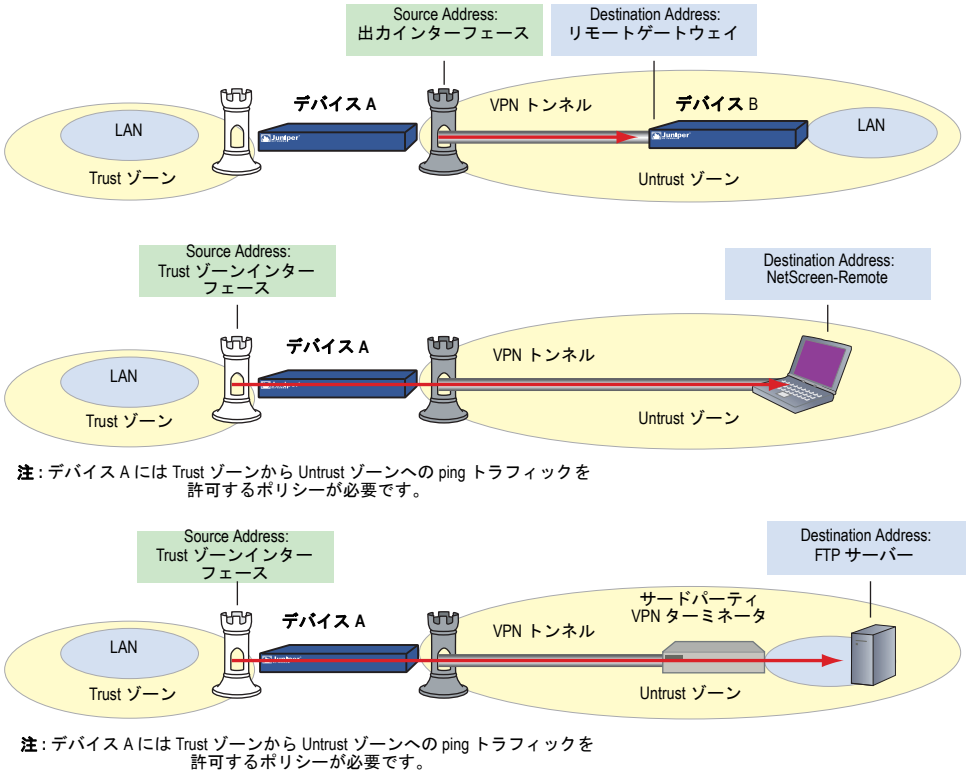
(デフォルト動作)

デバイス A -> NetScreen-Remote

デバイス A は Trust ゾーンインターフェースから NetScreen-Remote に ping を送信します。NetScreen-Remote はリモートゲートウェイの背後のアドレス、つまり デバイス A の Untrust ゾーンのインターフェースの背後からのインバウンド ICMP トラフィックを許可するポリシーを必要とします。

デバイス A -> サードパーティ VPN ターミネータ

デバイス A は Trust ゾーンインターフェースからリモートゲートウェイの背後のデバイスに ping を送信します。これは、リモートピアがインバウンド ping トラフィックをサポートするにもかかわらず、ping に応答しない場合に必要となることがあります。



注 : もう一方のトンネル端が XAuth を介してアドレスを受信する NetScreen-Remote VPN クライアントであれば、セキュリティ デバイスは、デフォルトで XAuth が割り当てた IP アドレスを VPN 監視の宛先として使用します。XAuth については、9-66 ページの「XAuth ユーザーとユーザーグループ」を参照してください。

ポリシー考慮事項

次のような場合、ソースインターフェースを含むゾーンから宛先アドレスを含むゾーンに向けて、ping に VPN トンネルを通過させるためのポリシーを送信デバイス上で作成する必要があります。

- ソース インターフェースは宛先アドレスと異なるゾーンに存在します。
- ソース インターフェースは宛先アドレスと同じゾーンに存在し、イントラゾーン ブロッキングが使用可能になっています。

次のような場合、ソースアドレスを含むゾーンから宛先アドレスを含むゾーンに向けて、ping に VPN トンネルを通過させるためのポリシーを受信デバイス上で作成する必要があります。

- 宛先アドレスはソース アドレスと異なるゾーンに存在します。

- 宛先アドレスはソース アドレスと同じゾーンに存在し、イントラゾーン ブロッキングが使用可能になっています。

注 : 受信デバイスが ICMP エコー要求に応答しないサードパーティ製品の場合は、ICMP エコー要求に応答するリモートピアの LAN の内部ホストに宛先を変更します。リモートピアのファイアウォールは、ICMP エコー要求の通過を許可するポリシーをもつ必要があります。

VPN 監視機能の構成

VPN 監視を使用可能にするには、次の手順に従います。

WebUI

VPNs > AutoKey IKE > New: VPN を構成し、**Advanced** をクリックして次のように入力し、**Return** をクリックして基本 VPN 構成ページに戻ってから **OK** をクリックします。

VPN モニター : この VPN トンネルの VPN 監視を使用可能に選択します。

Source Interface: ドロップダウンリストからインターフェースを選択します。**default** を選択すると、セキュリティデバイスは出力インターフェースを使用します。

Destination IP: 宛先 IP アドレスを入力します。何も入力しなければ、セキュリティ デバイスはリモート ゲートウェイ IP アドレスを使用します。

Rekey: トンネル状態がアップからダウンに変化した際に、セキュリティデバイスで IKE フェーズ 2 ネゴシエーション（および、必要であれば IKE フェーズ 1 ネゴシエーション）を試行する場合はこのオプションを選択します。このオプションを選択すると、トンネルの構成が完了した直後に、セキュリティ デバイスは IKE ネゴシエーションを試行し、トンネルを設定して VPN 監視を開始します。

トンネル状態がアップからダウンへ変化した際に、セキュリティ デバイスに IKE ネゴシエーションを試行させない場合は、このオプションをクリアします。再入力オプションが使用不可の場合、トンネル状態がアップからダウンに変化した際に、ユーザー生成トラフィックが IKE ネゴシエーションを発生させて停止した後に、VPN 監視が始まります。

(または)

VPNs > Manual Key > New: VPN を構成し、**Advanced** をクリックして次のように入力し、**Return** をクリックして基本 VPN 構成ページに戻ってから **OK** をクリックします。

VPN モニター : この VPN トンネルの VPN 監視を使用可能に選択します。

Source Interface: ドロップダウンリストからインターフェースを選択します。**default** を選択すると、セキュリティデバイスは出力インターフェースを使用します。

Destination IP: 宛先 IP アドレスを入力します。何も入力しなければ、セキュリティ デバイスはリモート ゲートウェイ IP アドレスを使用します。

CLI

```
set vpnmonitor frequency number
set vpnmonitor threshold number
set vpn name_str monitor [ source-interface interface [ destination-ip ip_addr ] ]
    [optimized] [ rekey ]
save
```

注： VPN 監視周期は秒単位です。デフォルト設定は 10 秒間隔です。

VPN 監視しきい値は、VPN トンネルを通じてリモート ゲートウェイに到達するかどうかを決定する ICMP エコー要求の成功もしくは失敗の連続回数です。デフォルトしきい値は、10 回連続の成功または不成功の ICMP エコー要求です。

ソース インターフェースを選択しない場合、セキュリティ デバイスは出力インターフェースをデフォルトとして使用します。

宛先 IP アドレスを選択しない場合、セキュリティ デバイスはリモート ゲートウェイの IP アドレスを使用します。

再入力オプションは、手動鍵 VPN トンネルに対しては使用できません。

この例では、2 台の セキュリティ デバイス（デバイス A および デバイス B）の間に AutoKey IKE VPN トンネルを構成します。デバイス A 上で、その Trust ゾーン インターフェース（ethernet1）からデバイス B 上の Trust ゾーン インターフェース（10.2.1.1./24）への VPN 監視をセットアップします。デバイス B 上で、その Trust ゾーン インターフェース（ethernet1）からデバイス A の背後の企業イントラネット サーバー（10.1.1.5）への VPN 監視をセットアップします。

デバイス A	デバイス B
ゾーンおよびインターフェース	
■ ethernet1 ■ Zone: Trust ■ IP address: 10.1.1.1/24 ■ Interface Mode: NAT ■ ethernet3 ■ Zone: Untrust ■ IP address: 1.1.1.1/24	■ ethernet1 ■ Zone: Trust ■ IP address: 10.2.1.1/24 ■ Interface Mode: NAT ■ ethernet3 ■ Zone: Untrust ■ IP address: 2.2.2.2/24
ルートベース自動鍵 IKE トンネルパラメータ	
■ フェーズ 1 ■ Gateway Name: gw1 ■ Gateway static IP address: 2.2.2.2 ■ Security level: Compatible[1] ■ Preshared Key: Ti82g4aX ■ 出力インターフェース : ethernet3 ■ Mode: Main ■ フェーズ 2 ■ VPN tunnel name: vpn1 ■ Security level: Compatible[2] ■ VPN Monitoring: src = ethernet1; dst = 10.2.1.1 ■ Bound to Interface: Tunnel.1	■ フェーズ 1 ■ Gateway Name: gw1 ■ Gateway static IP address: 1.1.1.1 ■ Proposals: Compatible ■ Preshared Key: Ti82g4aX ■ 出力インターフェース : ethernet3 ■ Mode: Main ■ フェーズ 2 ■ VPN tunnel name: vpn1 ■ Security Level: Compatible ■ VPN Monitoring: src = ethernet1; dst = 10.1.1.5 ■ Bound to Interface: Tunnel.1

1.フェーズ 1 セキュリティ レベルの Compatible は次のプロポーザルを含んでいます :
pre-g2-3des-sha、pre-g2-3des-md5、pre-g2-des-sha、および pre-g2-des-md5
2.フェーズ 2 セキュリティ レベルの Compatible は次のプロポーザルを含んでいます :
nopfs-esp-3des-sha、nopfs-esp-3des-md5、nopfs-esp-des-sha、および nopfs-esp-des-md5

デバイス A	デバイス B
ルート	
0.0.0.0/0 へは ethernet3、ゲートウェイ 1.1.1.250 を使用する	0.0.0.0/0 へは ethernet3、ゲートウェイ 2.2.2.250 を使用する
10.2.1.0/24 へは tunnel.1 を使用しゲートウェイは使用しない	10.1.1.0/24 へは tunnel.1 を使用しゲートウェイは使用しない
(Null ルート - tunnel.1 が停止している場合、10.2.1.0/24 へのトラフィックをドロップする) 10.2.1.0/24 へは Null インターフェースを使用し、メトリック値は 10 とする	(Null ルート - tunnel.1 が停止している場合、10.1.1.0/24 へのトラフィックをドロップする) 10.1.1.0/24 へは Null インターフェースを使用し、メトリック値は 10 とする

両方のデバイスが各自の Trust ゾーンのインターフェースから Untrust ゾーンのアドレスへ ping を実行するため、VPN トンネルの両端の管理者はゾーン間で ping の通過を許可するポリシーを設定する必要があります。

注： この例では、VPN ターミネータはどちらもセキュリティ デバイスであるため、VPN 監視用にデフォルトのソースおよび宛先アドレスが使用できます。その他のオプションの用途は、それらを使用するためにセキュリティ デバイスでどのように構成するかを説明するためにのみ付け加えています。

WebUI (デバイス A)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24
次のように入力してから **OK** をクリックします。
Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Tunnel IF New: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): Trust (trust-vr)
Unnumbered: (選択)
Interface: ethernet1(trust-vr)

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Trust_LAN
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Remote_LAN
IP Address/Domain Name:
IP/Netmask: (選択), 10.2.1.0/24
Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway:
Create a Simple Gateway: (選択)

Gateway Name: gw1
Type:
Static IP: (選択), Address/Hostname: 2.2.2.2
Preshared Key: Ti82g4aX
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface, tunnel.1
Proxy-ID: (選択)
Local IP / Netmask: 10.1.1.0/24
Remote IP / Netmask: 10.2.1.0/24
Service: ANY
VPN Monitor: (選択)
Source Interface: ethernet1
Destination IP: 10.2.1.1
Rekey:（オフ）

4. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.2.1.0/24
Gateway: (選択)
Interface: Tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.2.1.0/24
Gateway: (選択)
Interface: Null
Gateway IP Address: 0.0.0.0
Metric: 10

5. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Trust_LAN
Destination Address:
Address Book Entry: (選択), Remote_LAN
Service: ANY
Action: Permit
Position at Top: (選択)

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), Remote_LAN
Destination Address:
    Address Book Entry: (選択), Trust_LAN
Service: ANY
Action: Permit
Position at Top: (選択)

WebUI (デバイス B)

1. **インターフェース**

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.2.1.1/24
次のように入力してから **OK** をクリックします。
Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > Tunnel IF New: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): Trust (trust-vr)
Unnumbered: (選択)
    Interface: ethernet1(trust-vr)

2. **アドレス**

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Trust_LAN
IP Address/Domain Name:
    IP/Netmask: (選択), 10.2.1.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Remote_LAN
IP Address/Domain Name:
    IP/Netmask: (選択), 10.1.1.0/24
Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway:
Create a Simple Gateway: (選択)
Gateway Name: gw1
Type:
Static IP: (選択), Address/Hostname: 1.1.1.1
Preshared Key: Ti82g4aX
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface, tunnel.1
Proxy-ID: (選択)
Local IP / Netmask: 10.2.1.0/24
Remote IP / Netmask: 10.1.1.0/24
Service: ANY
VPN Monitor: (選択)
Source Interface: ethernet1
Destination IP: 10.1.1.5
Rekey:（オフ）

4. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 2.2.2.250

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
Gateway: (選択)
Interface: Tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
Gateway: (選択)
Interface: Null
Gateway IP Address: 0.0.0.0
Metric: 10

5. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Trust_LAN
Destination Address:
Address Book Entry: (選択), Remote_LAN
Service: ANY
Action: Permit
Position at Top: (選択)

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Remote_LAN
Destination Address:
Address Book Entry: (選択), Trust_LAN
Service: ANY
Action: Permit
Position at Top: (選択)

CLI (デバイス A)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface ethernet1
```

2. アドレス

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust Remote_LAN 10.2.1.0/24
```

3. VPN

```
set ike gateway gw1 address 2.2.2.2 main outgoing-interface ethernet3 preshare
    Ti82g4aX sec-level compatible
set vpn vpn1 gateway gw1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.1.0/24 any
set vpn vpn1 monitor source-interface ethernet1 destination-ip 10.2.1.1
```

4. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.2.1.0/24 interface tunnel.1
set vrouter trust-vr route 10.2.1.0/24 interface null metric 10
```

5. ポリシー

```
set policy top from trust to untrust Trust_LAN Remote_LAN any permit
set policy top from untrust to trust Remote_LAN Trust_LAN any permit
save
```

CLI (デバイス B)

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.2.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 2.2.2.2/24
   set interface tunnel.1 zone trust
   set interface tunnel.1 ip unnumbered interface ethernet1

2. **アドレス**
   set address trust Trust_LAN 10.2.1.0/24
   set address untrust Remote_LAN 10.1.1.0/24

3. **VPN**
   set ike gateway gw1 address 1.1.1.1 main outgoing-interface ethernet3 preshare Ti82g4aX sec-level compatible
   set vpn vpn1 gateway gw1 sec-level compatible
   set vpn vpn1 bind interface tunnel.1
   set vpn vpn1 proxy-id local-ip 10.2.1.0/24 remote-ip 10.1.1.0/24 any
   set vpn vpn1 monitor source-interface ethernet1 destination-ip 10.1.1.5

4. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
   set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
   set vrouter trust-vr route 10.1.1.0/24 interface null metric 10

5. **ポリシー**
   set policy top from trust to untrust Trust_LAN Remote_LAN any permit
   set policy top from untrust to trust Remote_LAN Trust_LAN any permit
   save

SNMP VPN 監視オブジェクトおよびトラップ

ScreenOS は、SNMP (簡易ネットワーク管理プロトコル) VPN 監視オブジェクトおよびトラップを使用して、アクティブ VPN の状況と状態を確認する機能を提供します。VPN 監視 MIB は、各 ICMP エコー要求が応答を引き出すかどうか、正常な応答の移動平均、応答の待ち時間、および過去 30 試行の平均待ち時間を監視します。

注 : SNMP マネージャ アプリケーションに VPN 監視 MIB を認識させるには、ScreenOS 専用の MIB エクステンション ファイルをアプリケーションにインポートする必要があります。MIB エクステンション ファイルは、セキュリティ デバイスに同梱されたドキュメンテーション CD にあります。

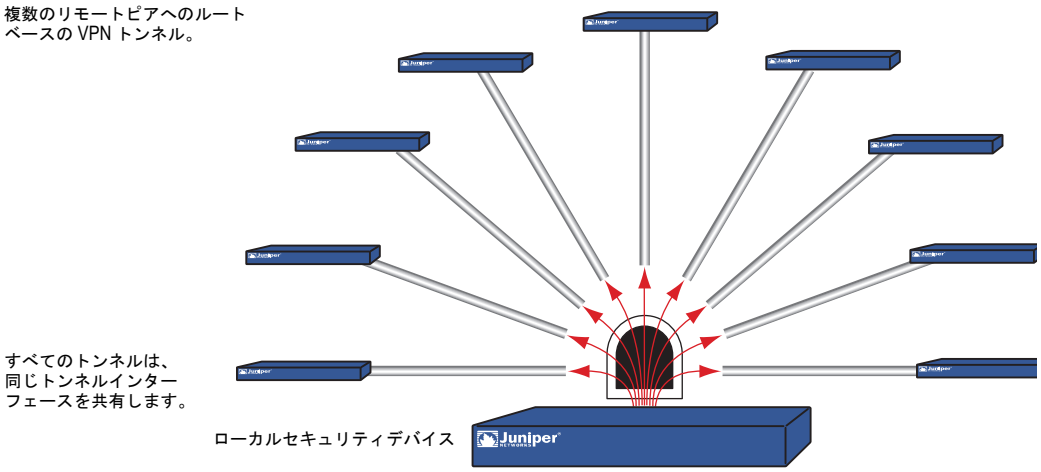
AutoKey IKE または手動鍵 VPN トンネル上の VPN 監視機能を使用可能にすることによって、セキュリティ デバイスは、次の事項に関するデータを含む SNMP VPN 監視オブジェクトをアクティブにします。

- アクティブな VPN セッションの総数
- 各セッションが開始した時刻
- 各セッションの SA (セキュリティアソシエーション) エレメント :
  - ESP 暗号化 (DES または 3DES) および認証アルゴリズム (MD5 または SHA-1) タイプ
  - AH アルゴリズムタイプ (MD5 または SHA-1)
  - 鍵交換プロトコル (AutoKey IKE または手動鍵)
  - フェーズ 1 認証方法 (事前共有鍵または証明書)
  - VPN タイプ (ダイヤルアップまたはピアツーピア)
  - ピアおよびローカルゲートウェイ IP アドレス
  - ピアおよびローカルゲートウェイ ID
  - SPI (セキュリティパラメータインデックス) 番号
- セッション状態パラメータ
  - VPN 監視状態 (アップまたはダウン)
  - トンネル状態 (アップまたはダウン)
  - フェーズ 1 と 2 の状態 (非アクティブまたはアクティブ)
  - フェーズ 1 と 2 の寿命 (再入力するまでの秒数; フェーズ 2 の寿命は、再入力するまでの残りバイト数でも報告されます)

1 つのトンネルインターフェースに対する複数のトンネル

単一のトンネルインターフェースに複数の IPSec VPN トンネルをバインドできます。同じトンネル インターフェースにバインドされた多数の VPN トンネルの中の 1 つに特定の宛先をリンクするために、セキュリティ デバイスは 2 つのテーブル、つまりルート テーブルおよび NHTB（ネクストホップ トンネル バインディング）テーブルを使用します。セキュリティ デバイスは、ルート テーブル エントリに指定されたネクストホップ ゲートウェイ IP アドレスを、NHTB テーブルに指定された特定の VPN トンネルにマッピングします。この技法によって、単一のトンネルインターフェースで多数の VPN トンネルがサポートできます (257 ページの「ルートからトンネルへのマッピング」を参照してください。)

図 67: 複数のトンネルにバウンドされた 1 つのトンネル インターフェース



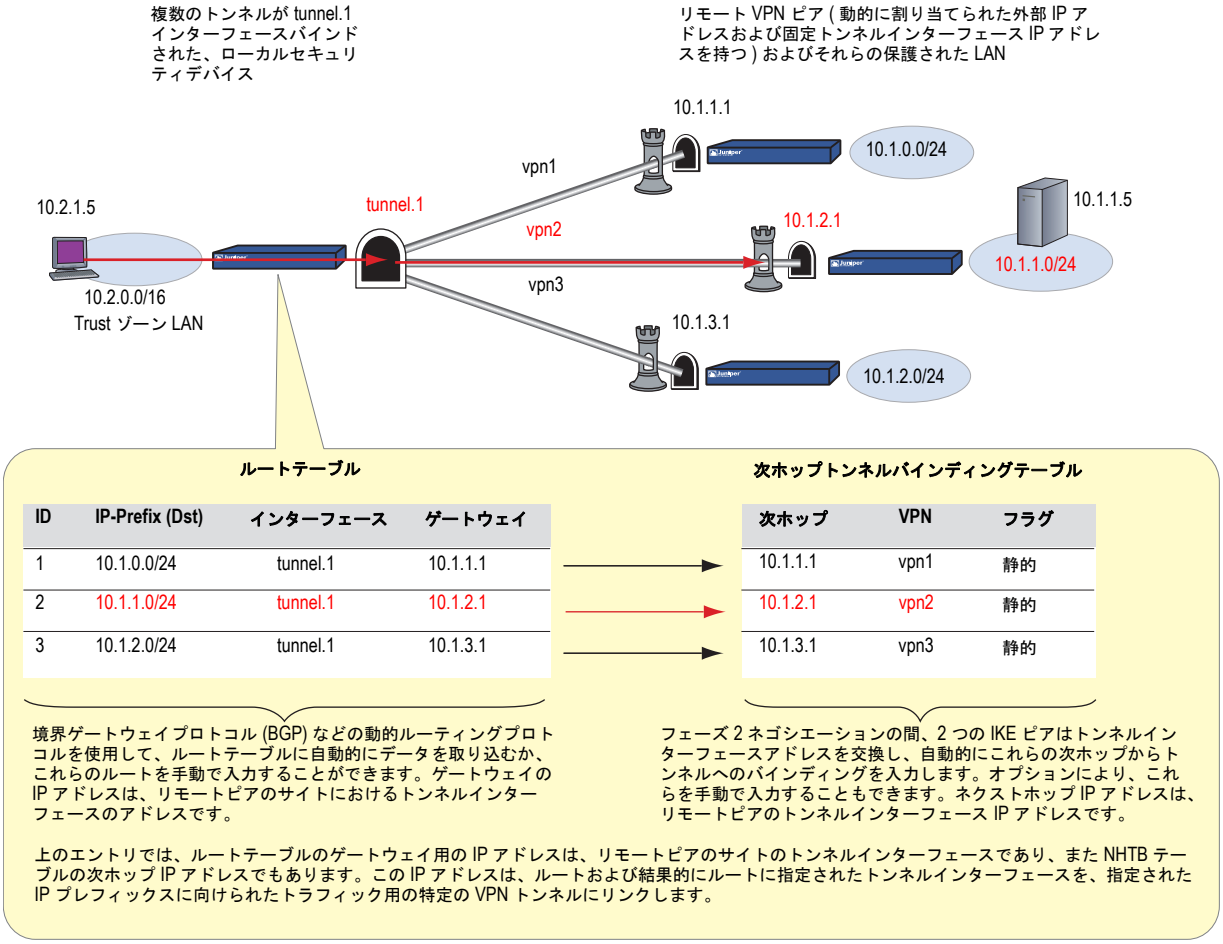
VPN トンネルの最大数は、作成するトンネルインターフェース数による制限は受けませんが、ルートテーブル容量または許可された専用の VPN トンネルの最大数 (どちらが小さくても) のいずれかによって制限されます。たとえば、セキュリティ デバイスが 4,000 のルートおよび 1,000 の専用 VPN トンネルをサポートする場合は、1,000 の VPN トンネルを作成してそれらを単一のトンネルインターフェースにバインドできます。セキュリティ デバイスが 8,192 のルートおよび 10,000 の専用 VPN トンネルをサポートする場合は、8,000 強の VPN トンネルを作成してそれらを単一のトンネル インターフェースにバインドできます。ご利用のセキュリティ デバイスの最大ルートおよびトンネル容量を確認するには、該当する製品データシートを参照してください。

注 : ルート テーブル容量が制限要因である場合は、セキュリティ ゾーン インターフェースによって自動的に生成されたルート、およびルートベース VPN トンネル用に利用可能な総数から定義が必要となるその他の静的ルート（デフォルト ゲートウェイへのルートなど）を差し引く必要があります。

ルートからトンネルへのマッピング

同じトンネル インターフェースにバインドされた複数の VPN トンネル間でトラフィックを振り分けるために、セキュリティ デバイスは、ルートに指定されたネクストホップ ゲートウェイ IP アドレスを特定の VPN トンネル名にマッピングします。ルートテーブルのエントリを NHTB テーブルのエントリにマッピングする方法を以下に示します。図 68 では、ローカル セキュリティ デバイスは 10.2.1.5 から 10.1.1.5 に送信されたトラフィックを、tunnel.1 インターフェースを経由してから vpn2 を経由するようにルーティングします。

図 68: ルート テーブルと NHTB（ネクストホップ トンネル バインディング）テーブル



セキュリティ デバイスは、リモート ピアのトンネル インターフェースの IP アドレスを、ゲートウェイおよびネクストホップ IP アドレスとして使用します。ルートを手動で入力するか、または動的ルーティングプロトコルを利用して、ルートテーブルとしてピアのトンネルインターフェース IP アドレスを参照するルートを自動的に入力することもできます。さらに、同じ IP アドレスを次のホップとして、該当する VPN トンネル名とともに NHTB テーブルに入力する必要があります。これにも、次の 2 つのオプションがあります。つまり手動で入力する方法と、セキュリティ デバイスを利用してフェーズ 2 ネゴシエーションの間にリモート ピアから取得して自動的に入力する方法です。

セキュリティ デバイスは、トンネル インターフェースを対応する VPN トンネルに結びつけるための共通要素として、ルート テーブル エントリのゲートウェイ IP アドレス、および NHTB テーブル エントリのネクストホップ IP アドレスを使用します。するとセキュリティ デバイスは、NHTB テーブルに指定された正しい VPN トンネルで、ルートに指定された IP プレフィックスに向けられたトラフィックを誘導できます。

リモートピアのアドレス

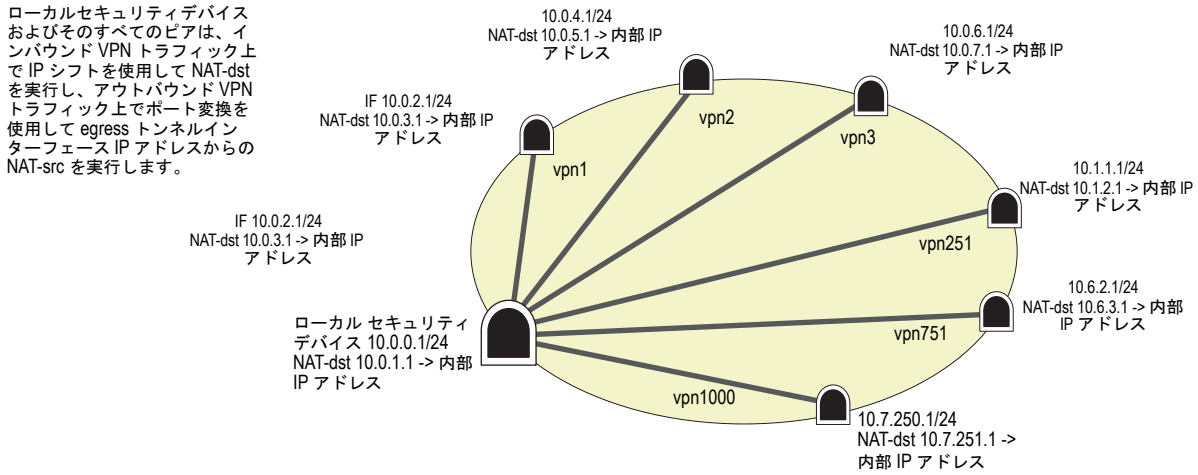
ルートベースの VPN を介して到達したすべてのリモートピアに対する内部アドレススキームは、互いに一意となる必要があります。これを可能にする方法の 1 つは、各リモートピアがソースおよび宛先アドレスに対して NAT (ネットワークアドレス変換機能) を実行することです。さらに、トンネルインターフェース IP アドレスは、すべてのリモートピアの間で一意であることが必要です。多数のリモートサイトに接続する予定であれば、アドレス計画が必須となります。最大 1000 VPN トンネルに対応可能なアドレス計画を次に示します。

ローカルルートテーブル内の宛先	ローカルトンネルインターフェース	ゲートウェイ / 次のホップ点 (ピアのトンネルインターフェース)	VPN トンネル
10.0.3.0/24	tunnel.1	10.0.2.1/24	vpn1
10.0.5.0/24	tunnel.1	10.0.4.1/24	vpn2
10.0.7.0/24	tunnel.1	10.0.6.1/24	vpn3
…	…	…	…
10.0.251.0/24	tunnel.1	10.0.250.1/24	vpn125
10.1.3.0/24	tunnel.1	10.1.2.1/24	vpn126
10.1.5.0/24	tunnel.1	10.1.4.1/24	vpn127
10.1.7.0/24	tunnel.1	10.1.6.1/24	vpn128
…	…	…	…
10.1.251.0/24	tunnel.1	10.1.250.1/24	vpn250
10.2.3.0/24	tunnel.1	10.2.2.1/24	vpn251
…	…	…	…
10.2.251.0/24	tunnel.1	10.2.250.1/24	vpn375
…	…	…	…
10.7.3.0/24	tunnel.1	10.7.2.1/24	vpn876
…	…	…	…
10.7.251.0/24	tunnel.1	10.7.250.1/24	vpn1000

ローカル セキュリティ デバイス上のトンネル インターフェースは、10.0.0.1/24 です。すべてのリモートホスト上に、IP アドレスを持つトンネルインターフェースが存在し、この IP アドレスはローカルルートテーブルおよび NHTB テーブル内のゲートウェイ / ネクストホップとして現れます。

アドレス変換を用いて単一のトンネルインターフェースにバインドされた複数のトンネルについては、262 ページの「オーバーラップするサブネットに対応する 1 つのトンネル インターフェースでの VPN の設定」を参照してください。

図 69: アドレス変換により単一のトンネル インターフェースにバウンドされた複数のトンネル



手動および自動テーブルエントリ

NHTB 内のエントリおよびルートテーブルを手動で作成できます。また、NHTB およびルートテーブルの入力を自動化することもできます。単一のトンネルインターフェースにバインドされた少数のトンネルに対しては、手動による方法が適しています。トンネルまたはインターフェースが、ハブサイトでのトンネルインターフェース上で利用できなくなった場合に、ルートが動的に自動調整を行うため、多数のトンネルに対しては、自動方法を使用すると管理設定およびメンテナンスの負担が低減できます。

手動テーブル入力

NHTB (ネクストホップトンネルバインディング) テーブル内のリモートピアのトンネルインターフェースの IP アドレスに、手動で VPN トンネルをマッピングできます。最初に、リモート管理者とコンタクトを取り、そのトンネル端のトンネルインターフェースに使用されている IP アドレスを取得することが必要です。すると、次のコマンドを使用して、NHTB テーブル内の VPN トンネル名にそのアドレスを関連付けることができます。

set interface tunnel.1 nhtb *peerís_tunnel_interface_addr* **vpn** *name_str*

その後に、そのトンネルインターフェース IP アドレスをゲートウェイとして使用するルートテーブル内に静的ルートを入力できます。WebUI または次の CLI コマンドのいずれかを介してルートを入力できます。

set vrouter *name_str* **route** *dst_addr* **interface tunnel.1 gateway** *peerís_tunnel_interface_addr*

自動テーブル入力

NHTB およびルートテーブルの両方の入力を自動化するには、次の条件を満たす必要があります。

- 単一のローカル トンネル インターフェースにバインドされたすべての VPN トンネルのリモート ピアは、ScreenOS 5.0.0 以降を実行するセキュリティ デバイスであることが必要です。
- 各リモートピアはそのトンネルをトンネルインターフェースにバインドする必要があり、そしてこのインターフェースは、すべてのピアトンネルインターフェースアドレス間で一意な IP アドレスを持つ必要があります。
- 各 VPN トンネルの両端で、再入力オプションを使用して VPN 監視を使用可能にするか、または各リモートゲートウェイの IKE ハートビート再接続オプションを使用可能にします。
- ローカルおよびリモートピアは、それらの接続トンネルインターフェース上で使用可能に設定された動的ルーティングプロトコルのインスタンスを持つことが必要です。

再入力オプションで VPN 監視を使用すると、トンネルの両端のセキュリティ デバイスは、ユーザーが作成した VPN トラフィックを待たずにトンネルをセットアップできるようになります。VPN トンネルの両端で再入力オプションを使用して VPN 監視を使用可能にすると、2 台のセキュリティ デバイスはフェーズ 1 およびフェーズ 2 IKE ネゴシエーションを実行してトンネルを設定します (詳細については、243 ページの「VPN の監視」を参照してください) 。

注 : トンネルインターフェース上で動的ルーティングプロトコルを実行している場合は、プロトコルによって生成されたトラフィックは、再入力オプションを使用して VPN 監視を使用可能にしなくても、または IKE ハートビート再接続オプションを使用可能にしなくても、IKE ネゴシエーションを起動できます。しかしながら、IKE ネゴシエーションの起動を動的ルーティング トラフィックに依存するのはお勧めできません。その代わりに、再入力オプションまたは IKE ハートビート再接続オプションで VPN 監視を使用します。

OSPF（オープン最短パス ファースト）では、ポイントツーマルチポイント インターフェースとしてローカル ピアにトンネル インターフェースを設定してから、インターフェースのルーティング プロトコルを有効にしてください。

動的に割り当てられた外部 IP アドレス、または動的 IP アドレスにマッピングされた FQDN（完全修飾ドメイン名）を持つリモート ピアの場合、リモート ピアは最初に IKE ネゴシエーションを開始する必要があります。しかしながら、ローカル セキュリティ デバイス上のフェーズ 2 SA はリモート ピアの動的に割り当てられた IP アドレスをキャッシュするため、どちらのピアも IKE ネゴシエーションを再開し、VPN 監視状態がアップからダウンに変更されているトンネルを再設定することができます。

フェーズ 2 ネゴシエーションの間、セキュリティ デバイスは互いにトンネル インターフェース IP アドレスを交換します。その後、各 IKE モジュールは、トンネルインターフェース IP アドレスおよびそれに対応する VPN トンネル名を NHTB テーブルに自動的に入力できます。

ローカル セキュリティ デバイスがリモート宛先へのルートを自動的にそのルート テーブルに入力できるようにするには、ローカルおよびリモート トンネル インターフェース上の BGP のインスタンスを使用可能にする必要があります。基本的な手順は次のとおりです。

1. 複数の VPN トンネルをバインドしたトンネルインターフェースを含む仮想ルーター上で、BGP ルーティングインスタンスを作成します。

2. 仮想ルーター上でルーティングインスタンスを使用可能にします。

3. BGP ピアにつながるトンネルインターフェース上で、ルーティングインスタンスを使用可能にします。

リモートピアもこれらの手順を実行します。

ローカル (またはハブ) デバイス上で、さらに、各ピアのトンネルインターフェース IP アドレスへのデフォルトルートおよび静的ルートを定義する必要があります。ピアのトンネルインターフェースへの静的ルートは、ハブデバイスが最初に正しい VPN トンネルを介して BGP 隣接ノードに到達するために必要です。

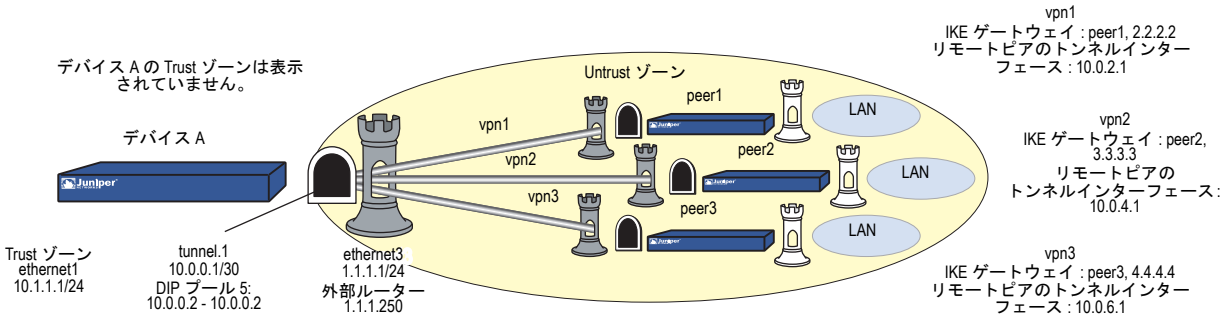
通信を設定すると、BGP 隣接ノードは、それぞれ自動的にルートテーブルを入力できるように、ルーティング情報を交換します。2 台のピアが両者の間に VPN トンネルを設定すると、リモートピアはローカルデバイスから出入りするルーティング情報を送受信できます。ローカル セキュリティ デバイス上の動的ルーティング インスタンスが、ローカル トンネル インターフェースを介してピアに向かうルートを取得する際に、ルート内のゲートウェイとしてピアのトンネル インターフェースの IP アドレスが同時に取得されます。

「ハブ」デバイスが NHTB およびルートテーブルを自動的に入力する、単一のトンネルインターフェースにバインドされた複数のトンネルの構成を示す例は、281 ページの「自動ルートおよび NHTB テーブル エントリのバインディング」を参照してください。

オーバーラップするサブネットに対応する 1 つのトンネル インターフェースでの VPN の設定

この例では、3 つのルートベース AutoKey IKE VPN トンネル、vpn1、vpn2、vpn3 を単一のトンネルインターフェース tunnel.1 にバインドします。トンネルはデバイス A から 3 台のリモート ピア、peer1、peer2、peer3 に繋がっています。3 台すべてのピアに対してデバイス A 上でルート テーブルおよび NHTB テーブル両方のエントリを手動で追加します。ルート テーブルおよび NHTB テーブルの入力を自動化する構成については、281 ページの「自動ルートおよび NHTB テーブル エントリのバインディング」を参照してください。

図 70: 3 つの VPN トンネルにバウンドされた Tunnel.1 インターフェース



各トンネルの両端での VPN トンネル構成には、以下のパラメータを使用します。

- AutoKey IKE
- 各ピアの事前共有鍵 :
  - ピア 1 は「netscreen1」を使用
  - ピア 2 は「netscreen2」を使用
  - ピア 3 は「netscreen3」を使用
- セキュリティ レベルは、フェーズ 1 とフェーズ 2 の両方のプロポーザルで「Compatible」として定義済み (これらのプロポーザルに関する詳細については、8 ページの「トンネルネゴシエーション」を参照してください)。

各デバイス上のすべてのセキュリティゾーンおよびインターフェースは、そのデバイスの trust-vr 仮想ルーティングドメイン内に存在します。

この例では、NAT-src および NAT-dst (ソースおよび宛先ネットワーク変換) を使用して IPSec ピア間のアドレス衝突を解決する方法を説明するために、すべての LAN に対して同じアドレス空間 10.1.1.0/24 を使用しています。NAT-src および NAT-dst の詳細については、*第 8 部 : アドレス変換* を参照してください。

WebUI (デバイス A)

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): Untrust (trust-vr)
Fixed IP: (選択)
IP Address/Netmask: 10.0.0.1/30

Network > Interfaces > Edit (tunnel.1) > DIP > New: 次のように入力してから **OK** をクリックします。

ID: 5
IP Address Range: (選択), 10.0.0.2 ~ 10.0.0.2
Port Translation: (選択)
In the same subnet as the interface IP or its secondary IPs: (選択)

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: corp
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: oda1
IP Address/Domain Name:
IP/Netmask: (選択), 10.0.1.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Peers
IP Address/Domain Name:
IP/Netmask: (選択), 10.0.0.0/16
Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: peer1
Type: Static IP: (選択), Address/Hostname: 2.2.2.2
Preshared Key: netscreen1
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface, tunnel.1
Proxy-ID: (選択)
Local IP/Netmask: 0.0.0.0/0
Remote IP/Netmask: 0.0.0.0/0
Service: ANY

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn2
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: peer2
Type: Static IP: (選択), Address/Hostname: 3.3.3.3
Preshared Key: netscreen2
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface, tunnel.1
Proxy-ID: (選択)
Local IP/Netmask: 0.0.0.0/0
Remote IP/Netmask: 0.0.0.0/0
Service: ANY

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn3
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: peer3
Type: Static IP: (選択), Address/Hostname: 4.4.4.4
Preshared Key: netscreen3
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface, tunnel.1
Proxy-ID: (選択)
Local IP/Netmask: 0.0.0.0/0
Remote IP/Netmask: 0.0.0.0/0
Service: ANY

4. ルート

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.1.0/24
Gateway: (選択)
Interface: ethernet1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.3.0/24
Gateway: (選択)
Interface: Tunnel.1
Gateway IP Address: 10.0.2.1

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.2.2/32
Gateway: (選択)
Interface: Tunnel.1
Gateway IP Address: 10.0.2.1

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.5.0/24
Gateway: (選択)
Interface: Tunnel.1
Gateway IP Address: 10.0.4.1

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.4.2/32
Gateway: (選択)
Interface: Tunnel.1
Gateway IP Address: 10.0.4.1

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.7.0/24
Gateway: (選択)
Interface: Tunnel.1
Gateway IP Address: 10.0.6.1

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.6.2/32
Gateway: (選択)
Interface: Tunnel.1
Gateway IP Address: 10.0.6.1

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.0.0/16
Gateway: (選択)
Interface: Null
Gateway IP Address: 0.0.0.0
Metric: 10

Network > Interfaces > Edit (tunnel.1) > NHTB > New: 次のように入力してから **Add** をクリックします。

New Next Hop Entry:
IP Address: 10.0.2.1
VPN: vpn1

Network > Interfaces > Edit (tunnel.1) > NHTB: 次のように入力してから **Add** をクリックします。

New Next Hop Entry:
IP Address: 10.0.4.1
VPN: vpn2

Network > Interfaces > Edit (tunnel.1) > NHTB: 次のように入力してから **Add** をクリックします。

New Next Hop Entry:
IP Address: 10.0.6.1
VPN: vpn3

5. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book: (選択), corp
Destination Address:
Address Book: (選択), peers
Service: ANY
Action: Permit
Position at Top: (選択)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

NAT:
Source Translation: (選択)
DIP On: 5 (10.0.0.2-10.0.0.2)/X-late

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), peers
Destination Address:
Address Book Entry: (選択), oda1
Service: ANY
Action: Permit
Position at Top: (選択)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

NAT:
Destination Translation: (選択)
Translate to IP Range: (選択する), 10.1.1.0 - 10.1.1.254

CLI (デバイス A)

1. **インターフェース**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.0.0.1/30
set interface tunnel.1 dip 5 10.0.0.2 10.0.0.2
```

2. **アドレス**

```
set address trust corp 10.1.1.0/24
set address trust oda1 10.0.1.0/24
set address untrust peers 10.0.0.0/16
```

3. **VPN**

```
set ike gateway peer1 address 2.2.2.2 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway peer1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set ike gateway peer2 address 3.3.3.3 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
set vpn vpn2 gateway peer2 sec-level compatible
set vpn vpn2 bind interface tunnel.1
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set ike gateway peer3 address 4.4.4.4 outgoing-interface ethernet3 preshare
    netscreen3 sec-level compatible
set vpn vpn3 gateway peer3 sec-level compatible
set vpn vpn3 bind interface tunnel.1
set vpn vpn3 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. **ルート**

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.0.1.0/24 interface ethernet1
set vrouter trust-vr route 10.0.3.0/24 interface tunnel.1 gateway 10.0.2.1
set vrouter trust-vr route 10.0.2.2/32 interface tunnel.1 gateway 10.0.2.1
set vrouter trust-vr route 10.0.5.0/24 interface tunnel.1 gateway 10.0.4.1
set vrouter trust-vr route 10.0.4.2/32 interface tunnel.1 gateway 10.0.4.1
set vrouter trust-vr route 10.0.7.0/24 interface tunnel.1 gateway 10.0.6.1
set vrouter trust-vr route 10.0.6.2/32 interface tunnel.1 gateway 10.0.6.1
set vrouter trust-vr route 10.0.0.0/16 interface null metric 10
set interface tunnel.1 nhtb 10.0.2.1 vpn vpn1
set interface tunnel.1 nhtb 10.0.4.1 vpn vpn2
set interface tunnel.1 nhtb 10.0.6.1 vpn vpn3
```

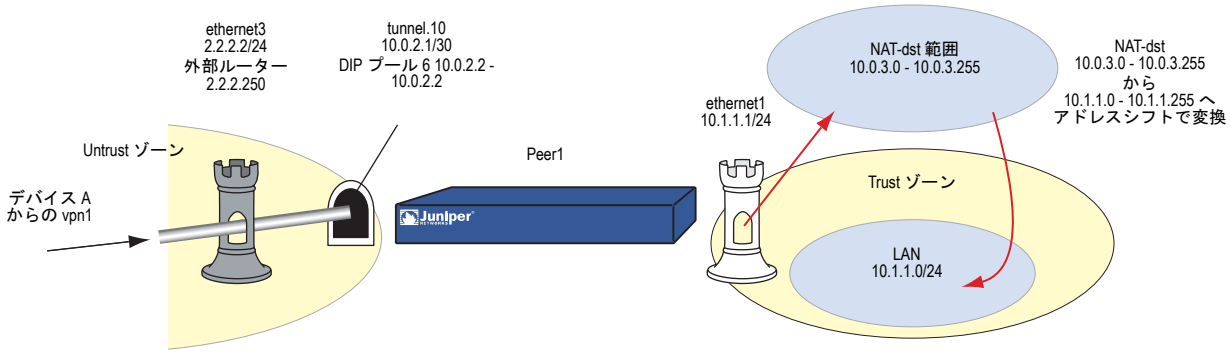
5. **ポリシー**

```
set policy from trust to untrust corp peers any nat src dip-id 5 permit
set policy from untrust to trust peers oda1 any nat dst ip 10.1.1.0 10.1.1.254
    permit
save
```

Peer1

次の構成は、図 71 に示されるように、peer1 サイトのセキュリティ デバイスのリモート管理者が、企業サイトのデバイス A への VPN トンネルを作成するために入力する必要のある項目です。内部アドレスは企業 LAN（10.1.1.0/24）内のアドレスと同じアドレス空間に存在するため、リモート管理者は、ソースおよび宛先 NAT（NAT-src および NAT-dst）を実行するように、セキュリティ デバイスを構成します。Peer1 は、VPN1 を介してデバイス A にトラフィックを送信する際に、DIP プール 6 を使用して NAT-src を実行し、すべての内部ソース アドレスを 10.0.2.2 に変換します。Peer1 はデバイス A から送信された VPN トラフィック上で NAT-dst を実行し、実際のアドレス シフトを使用してアドレスを 10.0.3.0/24 から 10.1.1.0/24 に変換します。

図 71: NAT-Dst を実行する Peer1



注 : NAT-src および NAT-dst の詳細については、*第 8 部 : アドレス変換* を参照してください。

WebUI (Peer1)

1. **インターフェース**

   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 2.2.2.2/24

   Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

   Tunnel Interface Name: Tunnel.10
   Zone (VR): Untrust (trust-vr)
   Fixed IP: (選択)
   IP Address/Netmask: 10.0.2.1/30

Network > Interfaces > Edit (tunnel.10) > DIP > New: 次のように入力してから **OK** をクリックします。

ID: 6
IP Address Range: (選択), 10.0.2.2 ～ 10.0.2.2
Port Translation: (選択)
In the same subnet as the interface IP or its secondary IPs: (選択)

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: lan
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: oda2
IP Address/Domain Name:
IP/Netmask: (選択), 10.0.3.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: To_corp
IP Address/Domain Name:
IP/Netmask: (選択), 10.0.1.0/24
Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: fr_corp
IP Address/Domain Name:
IP/Netmask: (選択), 10.0.0.2/32
Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: corp
Type: Static IP: (選択), Address/Hostname: 1.1.1.1
Preshared Key: netscreen1
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface, tunnel.10
Proxy-ID: (選択)

Local IP/Netmask: 0.0.0.0/0
Remote IP/Netmask: 0.0.0.0/0
Service: ANY

4. ルート

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 2.2.2.250
Metric: 1

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.3.0/24
Gateway: (選択)
Interface: ethernet1
Gateway IP Address: 0.0.0.0
Metric: 1

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.0.0/8
Gateway: (選択)
Interface: Tunnel.10
Gateway IP Address: 0.0.0.0
Metric: 10

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.0.0/8
Gateway: (選択)
Interface: Null
Gateway IP Address: 0.0.0.0
Metric: 12

5. ポリシー

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), fr_corp
Destination Address:
Address Book Entry: (選択), oda2
Service: ANY
Action: Permit
Position at Top: (選択)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

NAT:
Destination Translation: (選択)
Translate to IP Range: (選択する), 10.1.1.0 - 10.1.1.254

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), lan
Destination Address:
Address Book Entry: (**選択**), to_corp
Service: ANY
Action: Permit
Position at Top: (**選択**)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

NAT:
Source Translation: (**選択**)
DIP On: 6 (10.0.2.2-10.0.2.2)/X-late

CLI (Peer1)

1. **インターフェース**
```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface tunnel.10 zone untrust
set interface tunnel.10 ip 10.0.2.1/30
set interface tunnel.10 dip 6 10.0.2.2 10.0.2.2
```

2. **アドレス**
```
set address trust lan 10.1.1.0/24
set address trust oda2 10.0.3.0/24
set address untrust to_corp 10.0.1.0/24
set address untrust fr_corp 10.0.0.2/32
```

3. **VPN**
```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway corp sec-level compatible
set vpn vpn1 bind interface tunnel.10
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

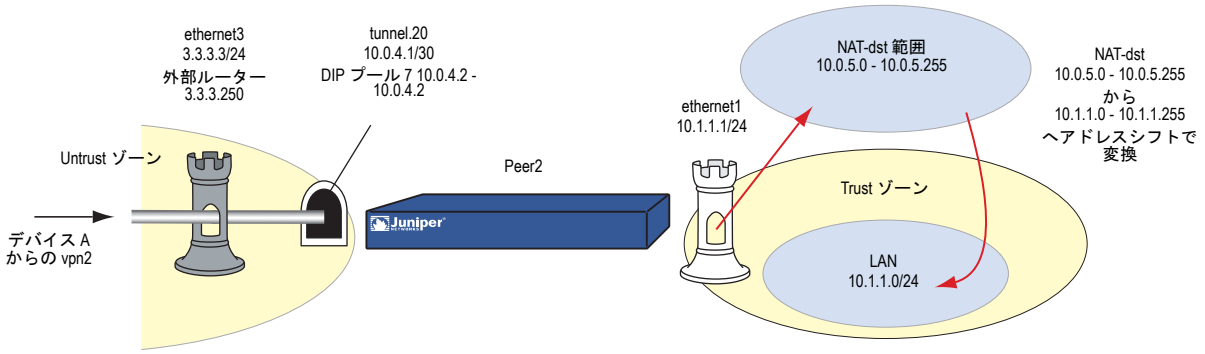
4. **ルート**
```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
    metric 1
set vrouter trust-vr route 10.0.3.0/24 interface ethernet1 metric 1
set vrouter trust-vr route 10.0.0.0/8 interface tunnel.10 metric 10
set vrouter trust-vr route 10.0.0.0/8 interface null metric 12
```

5. **ポリシー**
```
set policy from trust to untrust lan to_corp any nat src dip-id 6 permit
set policy from untrust to trust fr_corp oda2 any nat dst ip 10.1.1.0 10.1.1.254
    permit
save
```

Peer2

次の構成は、図 72 に示されるように、peer2 サイトのセキュリティ デバイスのリモート管理者が、企業サイトのデバイス A への VPN トンネルを作成するために入力する必要のある項目です。内部アドレスは企業 LAN（10.1.1.0/24）内のアドレスと同じアドレス空間に存在するため、リモート管理者は、ソースおよび宛先 NAT（NAT-src および NAT-dst）を実行するように、セキュリティ デバイスを構成します。Peer2 は、VPN2 を介して デバイス A にトラフィックを送信する際に、DIP プール 7 を使用して NAT-src を実行し、すべての内部ソース アドレスを 10.0.4.2 に変換します。Peer2 は デバイス A から送信された VPN トラフィック上で NAT-dst を実行し、実際のアドレス シフトを使用してアドレスを 10.0.5.0/24 から 10.1.1.0/24 に変換します。

図 72: Peer2



注 : NAT-src および NAT-dst の詳細については、*第 8 部 : アドレス変換* を参照してください。

WebUI (Peer2)

1. **インターフェース**

   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 3.3.3.3/24

   Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

   Tunnel Interface Name: Tunnel.20
   Zone (VR): Untrust (trust-vr)
   Fixed IP: (選択)
   IP Address/Netmask: 10.0.4.1/30

Network > Interfaces > Edit (tunnel.20) > DIP > New: 次のように入力してから **OK** をクリックします。

ID: 7
IP Address Range: (選択), 10.0.4.2 ～ 10.0.4.2
Port Translation: (選択)
In the same subnet as the interface IP or its secondary IPs: (選択)

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: lan
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: oda3
IP Address/Domain Name:
IP/Netmask: (選択), 10.0.5.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: To_corp
IP Address/Domain Name:
IP/Netmask: (選択), 10.0.1.0/24
Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: fr_corp
IP Address/Domain Name:
IP/Netmask: (選択), 10.0.0.2/32
Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn2
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: corp
Type: Static IP: (選択), Address/Hostname: 1.1.1.1
Preshared Key: netscreen2
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface, tunnel.20
Proxy-ID: (選択)

Local IP/Netmask: 0.0.0.0/0
Remote IP/Netmask: 0.0.0.0/0
Service: ANY

4. ルート

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: ethernet3
Gateway IP Address: 3.3.3.250
Metric: 1

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.5.0/24
Gateway: (**選択**)
Interface: ethernet1
Gateway IP Address: 0.0.0.0
Metric: 1

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.1.0/24
Gateway: (**選択**)
Interface: Tunnel.20
Gateway IP Address: 0.0.0.0
Metric: 10

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.1.0/24
Gateway: (**選択**)
Interface: Null
Gateway IP Address: 0.0.0.0
Metric: 12

5. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), lan
Destination Address:
Address Book Entry: (**選択**), to_corp
Service: ANY
Action: Permit
Position at Top: (**選択**)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

NAT:
Source Translation: (**選択**)
DIP On: 7 (10.0.4.2ñ10.0.4.2)/X-late

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), fr_corp
Destination Address:
Address Book Entry: (**選択**), oda3
Service: ANY
Action: Permit
Position at Top: (**選択**)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

NAT:
Destination Translation: (**選択**)
Translate to IP Range: (**選択する**), 10.1.1.0 - 10.1.1.254

CLI (Peer2)

1. **インターフェース**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24
set interface tunnel.20 zone untrust
set interface tunnel.20 ip 10.0.4.1/30
set interface tunnel.20 dip 7 10.0.4.2 10.0.4.2
```

2. **アドレス**

```
set address trust lan 10.1.1.0/24
set address trust oda3 10.0.5.0/24
set address untrust to_corp 10.0.1.0/24
set address untrust fr_corp 10.0.0.2/32
```

3. **VPN**

```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
set vpn vpn2 gateway corp sec-level compatible
set vpn vpn2 bind interface tunnel.20
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. **ルート**

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 3.3.3.250
    metric 1
set vrouter trust-vr route 10.0.5.0/24 interface ethernet1 metric 1
set vrouter trust-vr route 10.0.0.0/8 interface tunnel.20 metric 10
set vrouter trust-vr route 10.0.0.0/8 interface null metric 12
```

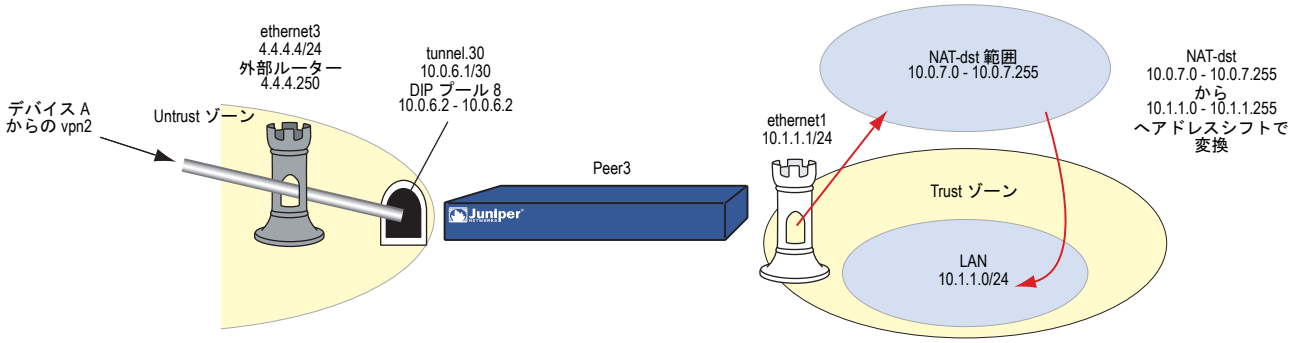
5. **ポリシー**

```
set policy from trust to untrust lan to_corp any nat src dip-id 7 permit
set policy from untrust to trust fr_corp oda3 any nat dst ip 10.1.1.0 10.1.1.254
    permit
save
```

Peer3

次の構成は、図 73 に示されるように、peer3 サイトのセキュリティ デバイスのリモート管理者が、企業サイトのデバイス A への VPN トンネルを作成するために入力する必要のある項目です。内部アドレスは企業 LAN（10.1.1.0/24）内のアドレスと同じアドレス空間に存在するため、リモート管理者は、ソースおよび宛先 NAT（NAT-src および NAT-dst）を実行するように、セキュリティ デバイスを構成します。Peer3 は、VPN3 を介して デバイス A にトラフィックを送信する際に、DIP プール 8 を使用して NAT-src を実行し、すべての内部ソース アドレスを 10.0.6.2 に変換します。Peer3 は デバイス A から送信された VPN トラフィック上で NAT-dst を実行し、実際のアドレス シフトを使用してアドレスを 10.0.7.0/24 から 10.1.1.0/24 に変換します。

図 73: Peer3



注 : NAT-dst に関する詳細については*第 8 部: アドレス変換*を参照してください。

WebUI (Peer3)

1. **インターフェース**

   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 4.4.4.4/24

   Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

   Tunnel Interface Name: Tunnel.30
   Zone (VR): Untrust (trust-vr)
   Fixed IP: (選択)
   IP Address/Netmask: 10.0.6.1/30

Network > Interfaces > Edit (tunnel.30) > DIP > New: 次のように入力してから **OK** をクリックします。

ID: 7
IP Address Range: (選択), 10.0.6.2 ～ 10.0.6.2
Port Translation: (選択)
In the same subnet as the interface IP or its secondary IPs: (選択)

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: lan
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: oda4
IP Address/Domain Name:
IP/Netmask: (選択), 10.0.7.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: To_corp
IP Address/Domain Name:
IP/Netmask: (選択), 10.0.1.0/24
Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: fr_corp
IP Address/Domain Name:
IP/Netmask: (選択), 10.0.0.2/32
Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn3
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: corp
Type: Static IP: (選択), Address/Hostname: 1.1.1.1
Preshared Key: netscreen3
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface, tunnel.30
Proxy-ID: (選択)
Local IP/Netmask: 0.0.0.0/0
Remote IP/Netmask: 0.0.0.0/0
Service: ANY

4. **ルート**

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: ethernet3
Gateway IP Address: 4.4.4.250
Metric: 1

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.7.0/24
Gateway: (**選択**)
Interface: ethernet1
Gateway IP Address: 0.0.0.0
Metric: 1

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.0.0/8
Gateway: (**選択**)
Interface: Tunnel.20
Gateway IP Address: 10.0.0.1
Metric: 10

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.0.0.0/8
Gateway: (**選択**)
Interface: Null
Gateway IP Address: 10.0.0.1
Metric: 12

5. **ポリシー**

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), lan
Destination Address:
Address Book Entry: (**選択**), to_corp
Service: ANY
Action: Permit
Position at Top: (**選択**)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

NAT:
Source Translation: (**選択**)
DIP On: 8 (10.0.6.2ñ10.0.6.2)/X-late

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), fr_corp

Destination Address:
Address Book Entry: (選択), oda4
Service: ANY
Action: Permit
Position at Top: (選択)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

NAT:
Destination Translation: (選択)
Translate to IP Range: (選択する), 10.1.1.0 - 10.1.1.254

CLI (Peer3)

1. **インターフェース**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 4.4.4.4/24
set interface tunnel.30 zone untrust
set interface tunnel.30 ip 10.0.6.1/30
set interface tunnel.30 dip 8 10.0.6.2 10.0.6.2
```

2. **アドレス**

```
set address trust lan 10.1.1.0/24
set address trust oda4 10.0.7.0/24
set address untrust to_corp 10.0.1.0/24
set address untrust fr_corp 10.0.0.2/32
```

3. **VPN**

```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3 preshare
    netscreen3 sec-level compatible
set vpn vpn3 gateway corp sec-level compatible
set vpn vpn3 bind interface tunnel.30
set vpn vpn3 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. **ルート**

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 3.3.3.250 metric
    1
set vrouter trust-vr route 10.0.7.0/24 interface ethernet1 metric 1
set vrouter trust-vr route 10.0.0.0/8 interface tunnel.30 metric 10
set vrouter trust-vr route 10.0.0.0/8 interface null metric 12
```

5. **ポリシー**

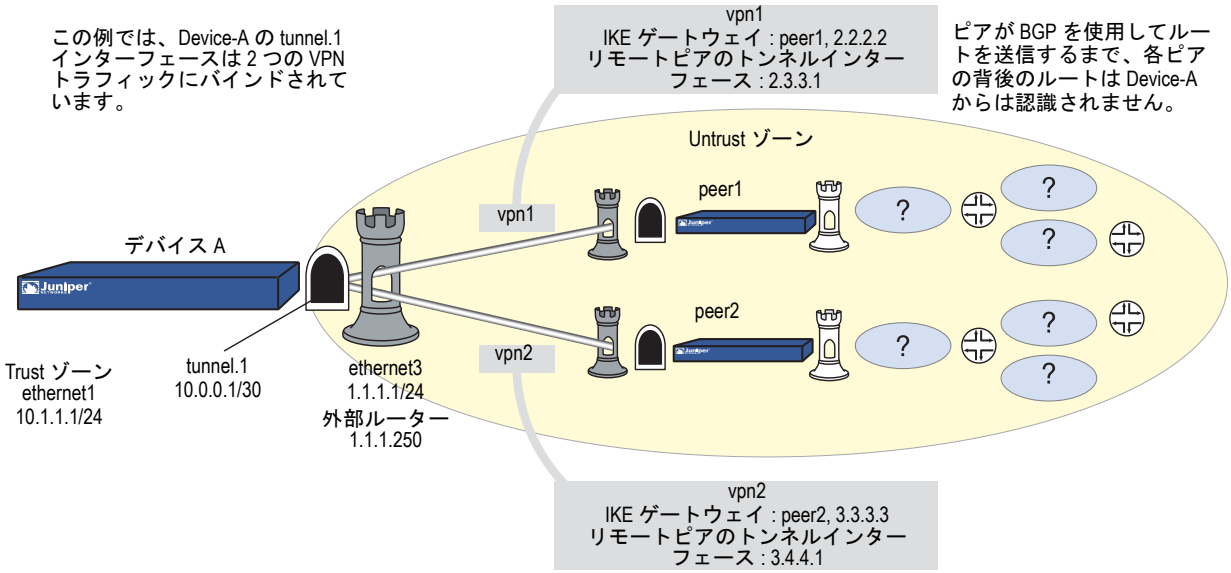
```
set policy from trust to untrust lan to_corp any nat src dip-id 8 permit
set policy from untrust to trust fr_corp oda4 any nat dst ip 10.1.1.0 10.1.1.254
    permit
save
```

自動ルートおよび NHTB テーブル エントリのバインディング

281 ページの図 74 では、2 つのルートベース AutoKey IKE VPN トンネル vpn1、vpn2 を、企業サイトのデバイス A 上の単一のトンネル インターフェース tunnel.1 にバインドします。各リモートピアが保護するネットワークは、接続されたルートの背後に複数のルートを持ちます。ピアは BGP（境界ゲートウェイ プロトコル）を使用して、各自のルートをデバイス A に伝達します。この例ではデバイス A 背後の企業サイトからピア サイトへの VPN トラフィックを許可しています。

注 : この例のルーティングプロトコルとしては、BGP の代わりに OSPF (Open Shortest Path First) を使用することもできます。See OSPF の設定の詳細については、292 ページの「自動ルー テーブル エントリでの OSPF の使用方法」を参照してください。

図 74: 自動ルートおよび NHTB テーブル エントリ（デバイス A）



各トンネルの両端での VPN トンネル構成には、以下のパラメータを使用します。すなわち、AutoKey IKE、事前共有鍵 (peer1 は「netscreen1」、peer2 は「netscreen2」)、ならびにフェーズ 1 と 2 のプロポーザルの「Compatible」として定義済みのセキュリティレベルを使用します (これらのプロポーザルに関する詳細については、8 ページの「トンネルネゴシエーション」を参照してください)。

次の 2 つの機能を構成すると、デバイス A は NHTB およびルート テーブルを自動的に入力できるようになります。

- 再入力オプション (または、IKE ハートビート再接続オプション) を使用した VPN 監視
- tunnel.1 上での BGP 動的ルーティング

注： トンネルインターフェース上で動的ルーティングプロトコルを実行している場合は、プロトコルによって生成されたトラフィックは、再入力オプションを使用して VPN 監視を使用可能にしなくても、または IKE ハートビート再接続オプションを使用可能にしなくても、IKE ネゴシエーションを起動できます。しかしながら、IKE ネゴシエーションの起動を動的ルーティングトラフィックに依存するのはお勧めできません。その代わりに、再入力オプションまたは IKE ハートビート再接続オプションで VPN 監視を使用します。

トンネル インターフェース上で BGP を実行している場合は、BGP によって生成されたトラフィックは、再入力オプションを使用して VPN 監視を使用可能にしなくても、または IKE ハートビート再接続オプションを使用可能にしなくても、IKE ネゴシエーションを起動できます。しかしながら、IKE ネゴシエーションの起動を BGP トラフィックに依存するのはお勧めできません。その代わりに、再入力オプションまたは IKE ハートビート再接続オプションで VPN 監視を使用します。

AutoKey IKE VPN トンネルに対して、再入力オプションを使用して VPN 監視を使用可能にすると、リモート サイトのユーザーと管理者がトンネルの構成を完了した直後に、デバイス A はそのリモート ピアと VPN 接続を確立します。デバイスは、ユーザーが生成した VPN トラフィックが IKE ネゴシエーションを実行するのを待ちません。フェーズ 2 ネゴシエーションの間、デバイス A が自動的に NHTB テーブルに VPN からネクストホップへのマッピングを作成できるように、セキュリティ デバイスは各自のトンネル インターフェース IP アドレスを交換します。

再入力オプションによって、フェーズ 1 と 2 の鍵寿命が期限切れになった際に、デバイスが人の作業を必要とせず自動的に新しい鍵の生成をネゴシエートすることが保証されます。再入力オプションを使用可能にした VPN 監視は、基本的に、ユーザー生成のトラフィックが存在しない場合でも VPN トンネルをアップの状態に保つ手段を提供するものです。これは、ユーザーとリモート管理者がトンネルの両端のトンネル インターフェース上で作成して使用可能にした BGP 動的ルーティング インスタンスが、デバイス A にルーティング情報を送信し、トラフィックを誘導して VPN トンネルを経由させるのに必要なルートがユーザー生成トラフィックに必要となる前に、それらのルートをルート テーブルに自動的に入力するために必要です (ただし、ピアサイトの管理者は、各サイトのトンネルインターフェースを介して仮想プライベートネットワークのその他に向かう単一の静的ルートを入力する必要があります)。

正しい VPN トンネルを介して BGP 隣接ノードに到達するために、デバイス A 上でデフォルト ルートおよび静的ルートを入力します。各デバイス上のすべてのセキュリティゾーンおよびインターフェースは、そのデバイスの trust-vr 仮想ルーティングドメイン内に存在します。

WebUI (デバイス A)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24
次のように入力してから **OK** をクリックします。
Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): Untrust (trust-vr)
Fixed IP: (選択)
IP Address/Netmask: 10.0.0.1/30

2. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: peer1
Type: Static IP: (選択), Address/Hostname: 2.2.2.2
Preshared Key: netscreen1
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface, tunnel.1
Proxy-ID: (選択)
Local IP/Netmask: 0.0.0.0/0
Remote IP/Netmask: 0.0.0.0/0
Service: ANY
VPN Monitor: (選択)
Rekey: (選択)

注 : Source Interface および Destination IP オプションは変更せずデフォルト設定にしておきます。これらのオプションについては、243 ページの「VPN の監視」を参照してください。

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn2
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: peer2
Type: Static IP: (選択), Address/Hostname: 3.3.3.3
Preshared Key: netscreen2
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface, tunnel.1
Proxy-ID: (選択)
Local IP/Netmask: 0.0.0.0/0
Remote IP/Netmask: 0.0.0.0/0
Service: ANY
VPN Monitor: (選択)
Rekey: (選択)

注 : Source Interface および Destination IP オプションは変更せずデフォルト設定にしておきます。これらのオプションについては、243 ページの「VPN の監視」を参照してください。

3. 静的ルート

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 2.3.3.1/32
Gateway: (選択)
Interface: Tunnel.1
Gateway IP Address: 2.3.3.1

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 3.4.4.1/32
Gateway: (選択)
Interface: Tunnel.1
Gateway IP Address: 3.4.4.1

4. 動的ルーティング

Network > Routing > Virtual Routers > Edit (trust-vr) > Create BGP Instance: 次のように入力してから **OK** をクリックします。

AS Number (必須): 99
BGP Enabled: (選択)

Network > Interfaces > Edit (for tunnel.1) > BGP: **Protocol BGP** チェックボックスをオンにして **OK** をクリックします。

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Neighbors: 次のように入力してから **Add** をクリックします。

AS Number: 99
Remote IP: 2.3.3.1
Outgoing Interface: Tunnel.1

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Neighbors: 次のように入力してから **Add** をクリックします。

AS Number: 99
Remote IP: 3.4.4.1
Outgoing Interface: Tunnel.1

5. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book: (選択), Any
Destination Address:
    Address Book: (選択), Any
Service: ANY
Action: Permit

CLI (デバイス A)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.0.0.1/30
```

2. VPN

```
set ike gateway peer1 address 2.2.2.2 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway peer1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set vpn vpn1 monitor rekey
set ike gateway peer2 address 3.3.3.3 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
set vpn vpn2 gateway peer2 sec-level compatible
set vpn vpn2 bind interface tunnel.1
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set vpn vpn2 monitor rekey
```

3. 静的ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 2.3.3.1/32 interface tunnel.1 gateway 2.3.3.1
set vrouter trust-vr route 2.4.4.1/32 interface tunnel.1 gateway 2.4.4.1
```

4. **動的ルーティング**

```
device-> set vrouter trust-vr protocol bgp 99
device-> set vrouter trust-vr protocol bgp enable
device-> set interface tunnel.1 protocol bgp
device-> set vrouter trust-vr
device(trust-vr)-> set protocol bgp
device(trust-vr/bgp)-> set neighbor 2.3.3.1 remote-as 99 outgoing interface
    tunnel.1
device(trust-vr/bgp)-> set neighbor 2.3.3.1 enable
device(trust-vr/bgp)-> set neighbor 3.4.4.1 remote-as 99 outgoing interface
    tunnel.1
device(trust-vr/bgp)-> set neighbor 3.4.4.1 enable
device(trust-vr/bgp)-> exit
device(trust-vr)-> exit
```

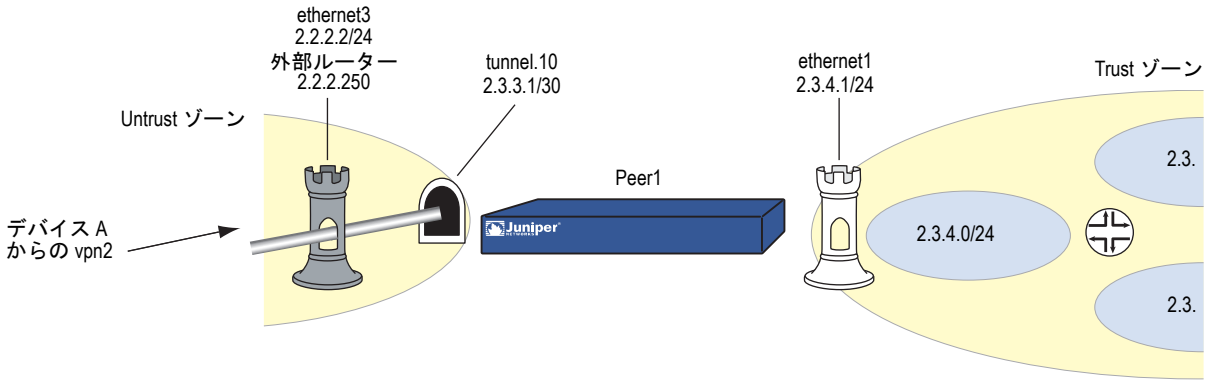
5. **ポリシー**

```
set policy from trust to untrust any any any permit
save
```

Peer1

次の構成は、286 ページの図 75 に示されるように、peer1 サイトのセキュリティ デバイスのリモート管理者が、企業サイトのデバイス A への VPN トンネルを作成するために入力する必要のある項目です。リモート管理者は、企業サイトからのインバウンド トラフィックを許可するようにセキュリティ デバイスを構成します。さらに、この管理者は vpn1 を介して内部ルートを BGP 隣接ノードに伝達するようにセキュリティ デバイスを構成します。

図 75: Peer1



WebUI (Peer1)

1. **インターフェース**

   Network > Interfaces > Edit (ethernet1): 次のように入力してから **OK** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 2.3.4.1/24

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.10
Zone (VR): Untrust (trust-vr)
Fixed IP: (選択)
IP Address/Netmask: 2.3.3.1/30

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: corp
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: corp
Type: Static IP: (選択), Address/Hostname: 1.1.1.1
Preshared Key: netscreen1
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface, tunnel.10
Proxy-ID: (選択)
Local IP/Netmask: 0.0.0.0/0
Remote IP/Netmask: 0.0.0.0/0
Service: ANY

4. 静的ルート

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 2.2.2.250
Metric: 1

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
Gateway: (選択)
Interface: Tunnel.10
Gateway IP Address: 0.0.0.0
Metric: 1

5. **動的ルーティング**
Network > Routing > Virtual Routers > Edit (trust-vr) > Create BGP Instance: 次のように入力してから **OK** をクリックします。

AS Number (必須): 99
BGP Enabled: (選択)

Network > Interfaces > Edit (tunnel.10) > BGP: **Protocol BGP** チェックボックスをオンにして **OK** をクリックします。

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Neighbors: 次のように入力してから **Add** をクリックします。

AS Number: 99
Remote IP: 10.0.0.1
Outgoing Interface: Tunnel.10

6. **ポリシー**
Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), corp
Destination Address:
Address Book Entry: (選択), Any
Service: ANY
Action: Permit

CLI (Peer1)

1. **インターフェース**
```
set interface ethernet1 zone trust
set interface ethernet1 ip 2.3.4.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface tunnel.10 zone untrust
set interface tunnel.10 ip 2.3.3.1/30
```

2. **アドレス**
```
set address untrust corp 10.1.1.0/24
```

3. **VPN**
```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway corp sec-level compatible
set vpn vpn1 bind interface tunnel.10
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. **静的ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250 metric 1
   set vrouter trust-vr route 10.1.1.0/24 interface tunnel.10 metric 1

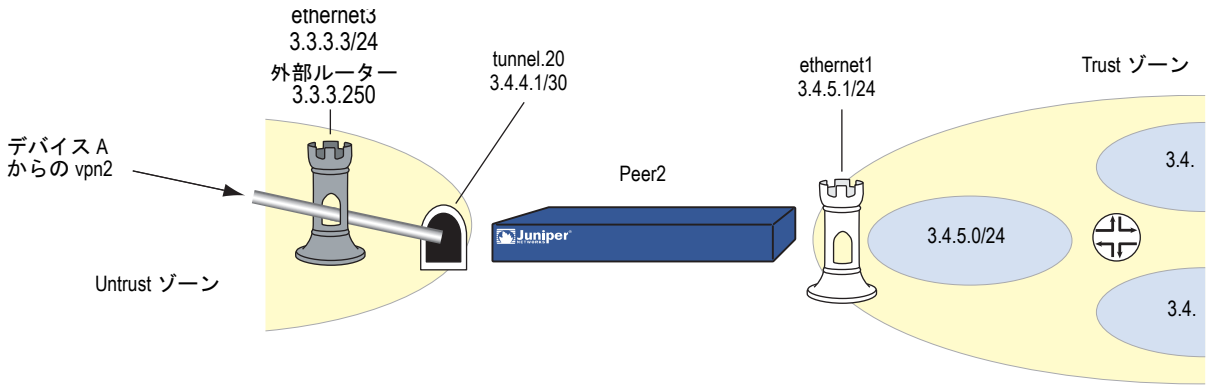
5. **動的ルーティング**
   device-> set vrouter trust-vr protocol bgp 99
   device-> set vrouter trust-vr protocol bgp enable
   device-> set interface tunnel.10 protocol bgp
   device-> set vrouter trust-vr
   device(trust-vr)-> set protocol bgp
   device(trust-vr/bgp)-> set neighbor 10.0.0.1 remote-as 99 outgoing interface tunnel.10
   device(trust-vr/bgp)-> set neighbor 10.0.0.1 enable
   device(trust-vr/bgp)-> exit
   device(trust-vr)-> exit

6. **ポリシー**
   set policy from untrust to trust corp any any permit
   save

Peer2

次の構成は、図 76 に示されるように、peer2 サイトのセキュリティ デバイスのリモート管理者が、企業サイトのデバイス A への VPN トンネルを作成するために入力する必要のある項目です。リモート管理者は、企業サイトからのインバウンド トラフィックを許可するようにセキュリティ デバイスを構成します。さらに、この管理者は vpn2 を介して内部ルートを BGP 隣接ノードに伝達するようにセキュリティ デバイスを構成します。

図 76: Peer2



WebUI (Peer2)

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 次のように入力してから **OK** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 2.3.4.1/24

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 3.3.3.3/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.20
Zone (VR): Untrust (trust-vr)
Fixed IP: (選択)
IP Address/Netmask: 3.4.4.1/30

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: corp
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn2
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: corp
Type: Static IP: (選択), Address/Hostname: 1.1.1.1
Preshared Key: netscreen2
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to: Tunnel Interface, tunnel.20
Proxy-ID: (選択)
Local IP/Netmask: 0.0.0.0/0
Remote IP/Netmask: 0.0.0.0/0
Service: ANY

4. 静的ルート

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 3.3.3.250
Metric: 1

Network > Routing > Routing Entries > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
Gateway: (選択)
Interface: Tunnel.20
Gateway IP Address: 0.0.0.0
Metric: 1

5. 動的ルーティング

Network > Routing > Virtual Routers > Edit (trust-vr) > Create BGP Instance: 次のように入力してから **OK** をクリックします。

AS Number (必須): 99
BGP Enabled: (選択)

Network > Interfaces > Edit (tunnel.20) > BGP: **Protocol BGP** チェックボックスをオンにして **OK** をクリックします。

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Neighbors: 次のように入力してから **Add** をクリックします。

AS Number: 99
Remote IP: 10.0.0.1
Outgoing Interface: Tunnel.20

6. ポリシー

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), corp
Destination Address:
Address Book Entry: (選択), Any
Service: ANY
Action: Permit

CLI (Peer2)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 3.4.5.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24
set interface tunnel.20 zone untrust
set interface tunnel.20 ip 3.4.4.1/30
```

2. アドレス

```
set address untrust corp 10.1.1.0/24
```

3. VPN

```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
set vpn vpn1 gateway corp sec-level compatible
set vpn vpn1 bind interface tunnel.20
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. **静的ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 3.3.3.250 metric 1
   set vrouter trust-vr route 10.1.1.0/24 interface tunnel.20 metric 1

5. **動的ルーティング**
   device-> set vrouter trust-vr protocol bgp 99
   device-> set vrouter trust-vr protocol bgp enable
   device-> set interface tunnel.20 protocol bgp
   device-> set vrouter trust-vr
   device(trust-vr)-> set protocol bgp
   device(trust-vr/bgp)-> set neighbor 10.0.0.1 remote-as 99 outgoing interface tunnel.20
   device(trust-vr/bgp)-> set neighbor 10.0.0.1 enable
   device(trust-vr/bgp)-> exit
   device(trust-vr)-> exit

6. **ポリシー**
   set policy from untrust to trust corp any any permit
   save

自動ルー テーブル エントリでの OSPF の使用方法

ピアに対し、BGP 動的ルーティングの代わりに OSPF を設定して、デバイス A へのルートを伝達することができます。デバイス A の tunnel.1 が そのピアと隣接する OSPF を形成するためには、ポイントツーマルチポイント インターフェースとして、トンネル インターフェースを設定しなければなりません。各デバイスの OSPF 動的ルーティングの設定を以下に示します。

WebUI (デバイス A)

動的ルーティング (OSPF)

Network > Routing > Virtual Routers > Edit (trust-vr) > Create OSPF Instance: **OSPF Enabled** を選択し、**Apply** をクリックします。

Area > Configure (エリア 0.0.0.0): **< <** **Add** をクリックして、tunnel.1 インターフェースを Available Interface(s) リストから Selected Interface(s) リストに移動させ、**OK** をクリックします。

Network > Interfaces > Edit (tunnel.1) > OSPF: 以下を入力して **Apply** をクリックします。

Bind to Area: (選択)、ドロップダウンリストから 0.0.0.0 を選択します。
Protocol OSPF: Enable
Link Type: Point-to-Multipoint (選択)

CLI (デバイス A)

動的ルーティング (OSPF)

device-> set vrouter trust-vr protocol ospf
device-> set vrouter trust-vr protocol ospf enable
device-> set interface tunnel.1 protocol ospf area 0
device-> set interface tunnel.1 protocol ospf link-type p2mp
device-> set interface tunnel.1 protocol ospf enable
device-> save

WebUI (Peer1)

動的ルーティング (OSPF)

Network > Routing > Virtual Routers > Edit (trust-vr) > Create OSPF Instance: **OSPF Enabled** を選択し、**Apply** をクリックします。

Area > Configure (エリア 0.0.0.0): **< <** **Add** をクリックして、tunnel.1 インターフェースを Available Interface(s) リストから Selected Interface(s) リストに移動させ、**OK** をクリックします。

Network > Interfaces > Edit (tunnel.1) > OSPF: 以下を入力して **Apply** をクリックします。

Bind to Area: (選択)、ドロップダウンリストから 0.0.0.0 を選択します。
Protocol OSPF: Enable

CLI (Peer1)

動的ルーティング (OSPF)

```
device-> set vrouter trust-vr protocol ospf
device-> set vrouter trust-vr protocol ospf enable
device-> set interface tunnel.1 protocol ospf area 0
device-> set interface tunnel.1 protocol ospf enable
device-> save
```

WebUI (Peer2)

動的ルーティング (OSPF)

Network > Routing > Virtual Routers > Edit (trust-vr) > Create OSPF Instance: **OSPF Enabled** を選択し、**Apply** をクリックします。

Area > Configure (エリア 0.0.0.0): **< <** **Add** をクリックして、tunnel.1 インターフェースを Available Interface(s) リストから Selected Interface(s) リストに移動させ、**OK** をクリックします。

Network > Interfaces > Edit (tunnel.1) > OSPF: 以下を入力して **Apply** をクリックします。

Bind to Area: (選択)、ドロップダウンリストから 0.0.0.0 を選択します。
Protocol OSPF: Enable

CLI (Peer2)

動的ルーティング (OSPF)

```
device-> set vrouter trust-vr protocol ospf
device-> set vrouter trust-vr protocol ospf enable
device-> set interface tunnel.1 protocol ospf area 0
device-> set interface tunnel.1 protocol ospf enable
device-> save
```

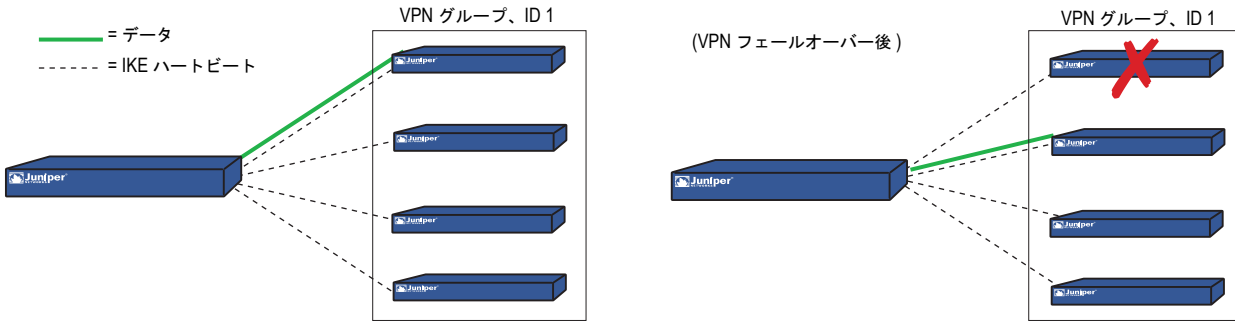
冗長 VPN ゲートウェイ

冗長ゲートウェイ機能は、サイト間フェールオーバーの間およびその後の、継続した VPN 接続性に対するソリューションを提供します。VPN グループを作成して、ポリシーベースのサイト間またはサイト間動的ピア AutoKey IKE IPSec VPN トンネルが接続可能な最大 4 台の冗長ゲートウェイからなるセットを構築します。セキュリティ デバイスは、VPN グループを参照するポリシーにマッチングするトラフィックを受信すると、そのグループのすべてのメンバーとフェーズ 1 およびフェーズ 2 の IKE ネゴシエーションを実行します。セキュリティ デバイスは、そのグループ内の最高の優先順位、つまりウェイトで、VPN トンネルを介してゲートウェイへデータを送信します。グループのその他のすべてのゲートウェイに対しては、セキュリティ デバイスはフェーズ 1 と 2 の SA を維持し、トンネルを介して IKE キープアライブ パケットを送信することによってトンネルをアクティブな状態に維持します。アクティブ VPN トンネルに障害が発生すると、トンネルはグループ内で 2 番目に高い優先度を持つトンネルおよびゲートウェイにフェールオーバーすることができます。

注： VPN グループは、L2TP、L2TP-over-IPSec、ダイヤルアップ、手動鍵、またはルートベース VPN トンネルタイプをサポートしていません。サイト間動的ピア配列では、VPN グループを監視するセキュリティ デバイスの Untrust IP アドレスは動的に割り当てられたものであることが必要ですが、VPN グループ メンバーの untrust IP アドレスは静的なものであることが必要です。

このスキームでは、データがすべてのサイトのホストの間でミラーリングできるように、冗長ゲートウェイの背後のサイトが接続されていると仮定しています。さらに、HA（高可用性）専用の各サイトは、HA モードで稼動するセキュリティ デバイスからなる冗長クラスタを装備しています。したがって、VPN フェールオーバーしきい値は、デバイスフェールオーバーしきい値よりも高く設定する必要があり、そうしないと VPN フェールオーバーが不必要に発生することがあります。

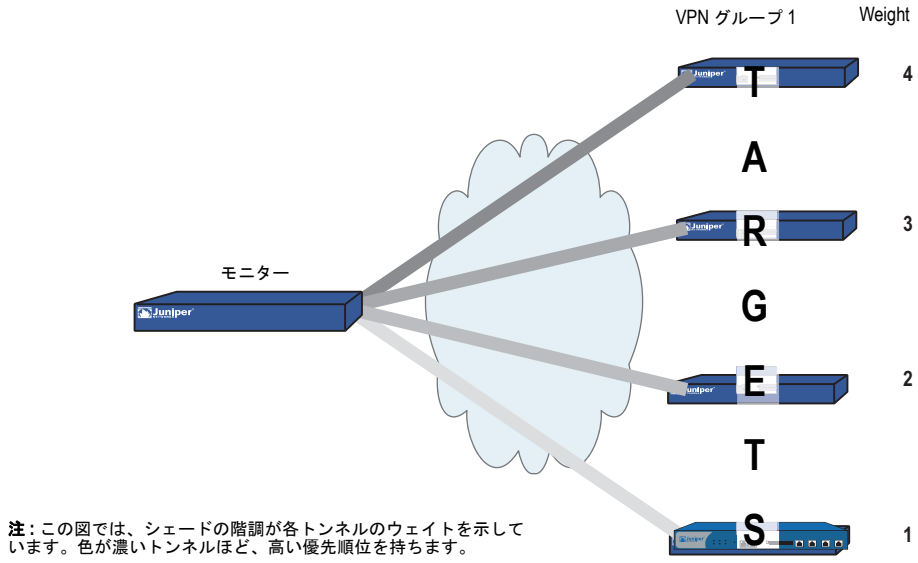
図 77: VPN トンネル フェールオーバーの冗長 VPN ゲートウェイ



VPN グループ

VPN グループとは、最大 4 台のターゲットリモートゲートウェイに対する VPN トンネル構成のセットです。1 つのグループの各トンネルに対するフェーズ 1 と 2 SA (セキュリティアソシエーション) パラメータは、異なっていても同一でもかまいません (リモートゲートウェイの IP アドレスは例外で、明確に異なるものであることが必要です)。VPN グループは、295 ページの図 78 に示すように、固有の ID 番号を持ち、グループの各メンバには、アクティブ トンネルとなる優先度ランクの位置を示す固有のウェイトが割り当てられます。値 1 は、最低すなわち最も優先度の低いランクを示します。

図 78: ターゲット リモート ゲートウェイ



VPN グループ メンバーと通信するセキュリティデバイス、およびメンバー自身はモニターとターゲットの関係を持つことが必要です。監視デバイスは、各ターゲットデバイスの接続状態と動作状態を絶えず監視します。監視を行うためにモニターが使用するツールは、次のとおりです。

- IKE ハートビート
- IKE 復旧試行

これらのツールについては、次のセクション 投 *f* 視機構 ,i ページ 296 で扱います。

注 : モニターとターゲットの関係は、一方向である必要はありません。監視デバイスは VPN グループのメンバーでも可能で、他の監視デバイスのターゲットとなることも可能です。

監視機構

2 つの機構は、VPN グループのメンバーを監視し、メンバーが VPN トラフィックを終了できることを確認します。

- IKE ハートビート
- IKE 復旧試行

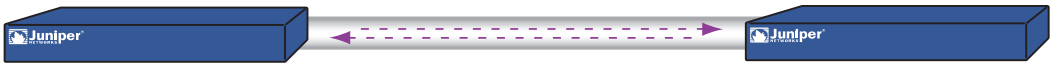
これら 2 つのツールに加えて TCP アプリケーション フェールオーバー オプション（300 ページの「TCP SYN-Flag チェック」を参照してください）を使用しているため、セキュリティ デバイスは、VPN フェールオーバーが必要となるときを検出し、VPN サービスを中断させずにトラフィックを新しいトンネルにシフトできます。

IKE ハートビート

IKE ハートビートは、確立した第 1 段階 SA (セキュリティアソシエーション) の保護の下で、IKE ピアが互いに送信し、相手の接続性と動作性を確認するハローメッセージです。たとえば、device_m (「モニター」) が device_t (「ターゲット」) から指定された数 (デフォルトは 5) のハートビートを受信しなければ、device_m は device_t がダウン状態であると判断します。device_m は対応する第 1 および第 2 SA (セキュリティアソシエーション) を SA キャッシュからクリアし、IKE 復旧手順を開始します (298 ページの「IKE 復旧手順」を参照) さらに、device_t は SA をクリアします。

注： IKE ハートビート機能は、VPN グループ内の VPN トンネルの両端のデバイス上で使用可能に設定されていることが必要です。device_ t 上ではなく、device_m 上で使用可能に設定されいる場合、device_m は IKE ハートビート伝送を抑圧し、イベントログにメッセージ「Heartbeats have been disabled because the peer is not sending them.」を生成します。

図 79: 双方向の IKE ハートビート フロー



IKE ハートビートは VPN トンネルを両方向に流れる必要があります。

IKE ハートビート間隔、および特定の VPN トンネルのしきい値 (デフォルトは 5) を定義するには、次のようにします。

WebUI

VPNs > AutoKey Advanced > Gateway > Edit (IKE ハートビートしきい値を変更するゲートウェイ) > Advanced: Heartbeat Hello および Heartbeat Threashold フィールドに新しい値を入力してから **OK** をクリックします。

CLI

set ike gateway *name_str* heartbeat hello *number*
set ike gateway *name_str* heartbeat threshold *number*

DPD（デッド ピア検出）

DPD は、ネットワーク デバイスによって使用されるプロトコルであり、現在他のピア デバイスが存在しているか、また利用可能か確認します。

DPD を、(前述の）IKE ハートビート機能の代わりに使用することができます。しかし、両方の機能を同時に使用することはできません。さらに、IKE ハートビートは、デバイスで構成されているすべての IKE ゲートウェイに影響するグローバル設定として設定できます。また、IKE ハートビート設定は、個々のゲートウェイのみに影響する、個別 IKE ゲートウェイ コンテキストに適用することもできます。それとは対照的に、DPD は個別 IKE ゲートウェイ コンテキストのみに構成することができ、グローバル パラメータとしては構成できません。

デバイスは、暗号化された IKE フェーズ 1 通知ペイロード（R-U-THERE）をピアに送信し、ピアからの DPD 確認応答（R-U-THERE-ACK）を待つことで DPD 検証を行います。デバイスは、指定した DPD 間隔以内にピアからトラフィックを受信しなかった場合はその場合に限り、R-U-THERE 要求を送信します。もし DPD が有効なデバイスがトンネル上のトラフィックを受信した場合、デバイスはそのトンネルに対する R-U-THERE カウンタをリセットし、これによって新しい間隔が開始されます。デバイスは、この間隔以内にピアから R-U-THERE-ACK を受信した場合は、ピアがアライブであると見なします。デバイスは、この間隔以内に R-U-THERE-ACK 応答を受信しなかった場合は、ピアがデッドであると見なします。

デバイスは、ピア デバイスがデッドであると見なしたときは、ピアへのフェーズ 1 SA およびすべてのフェーズ 2 SA を削除します。

CLI または WebUI のどちらかから、以下の DPD パラメータを構成することができます。

- **interval** パラメータは、DPD 間隔を指定します。この間隔は、ピアがデッドであるとデバイスが見なすまでの許容経過時間です（秒単位）。
- **always-send** パラメータは、ピアとの IPSec トラフィックの有無に関わらず、DPD 要求を送信するようデバイスに指示します。
- **retry** パラメータは、ピアがデッドであるとデバイスが見なすまでの間に、R-U-THERE 要求を送信できる最大回数を指定します。IKE ハートビート構成では、デフォルトの送信回数は 5 回で、指定可能な範囲は 1 ～ 128 回です。ゼロに設定すると、DPD は無効になります。

以下の例では、5 秒の DPD 間隔を使用したゲートウェイを作成します。

WebUI

VPNs > AutoKey Advanced > Gateway > Edit: 以下の値を入力してゲートウェイを作成し、**OK** をクリックします。

Gateway Name: our_gateway
Security Level: Standard
Remote Gateway Type: Static IP Address
IP Address/Hostname: 1.1.1.1
Preshared Key: jun9345

VPNs > AutoKey Advanced > Gateway > Edit (our_gateway): 次の値を入力してから **OK** をクリックします。

Predefined: Standard (選択)
DPD:
Interval: 5

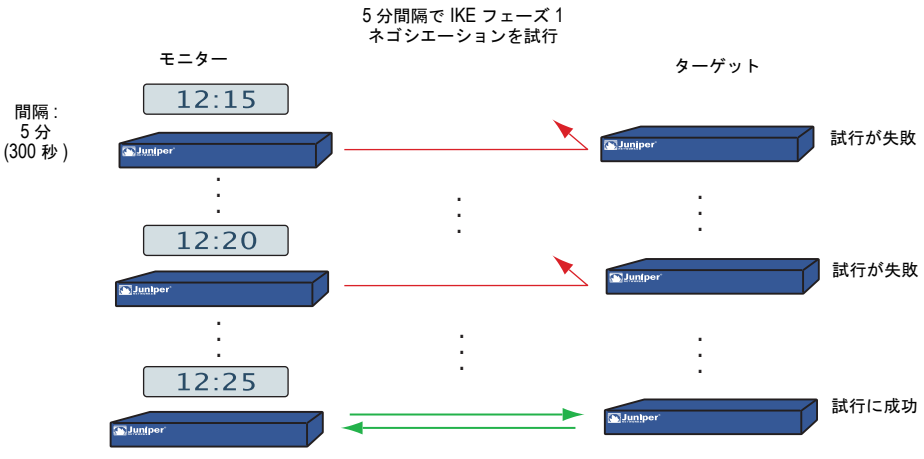
CLI

```
set ike gateway "our_gateway" address 1.1.1.1 main outgoing-interface "untrust"
    preshare "jun9345" sec-level standard
set ike gateway "our_gateway" dpd interval 5
```

IKE 復旧手順

監視セキュリティ デバイスが、ターゲット デバイスがダウン状態にあると判断すると、モニターは IKE ハートビートの送信を停止し、そのピアの SA を SA キャッシュから削除します。定義された間隔を経た後に、モニターは障害を発生したピアでフェーズ 1 ネゴシエーションの開始を試みます。最初の試行が成功しなければ、ネゴシエーションが成功するまで、モニターは一定の間隔でフェーズ 1 ネゴシエーションの試行を継続します。

図 80: 繰り返される IKE フェーズ 1 ネゴシエーション試行



特定の VPN トンネルの IKE 復旧間隔 (最小設定は 60 秒) を定義するには、次のいずれかを行います。

WebUI

VPNs > AutoKey Advanced > Gateway > Edit (IKE ハートビートしきい値を変更するゲートウェイ) > Advanced: Heartbeat Reconnect フィールドに秒単位で値を入力してから **OK** をクリックします。

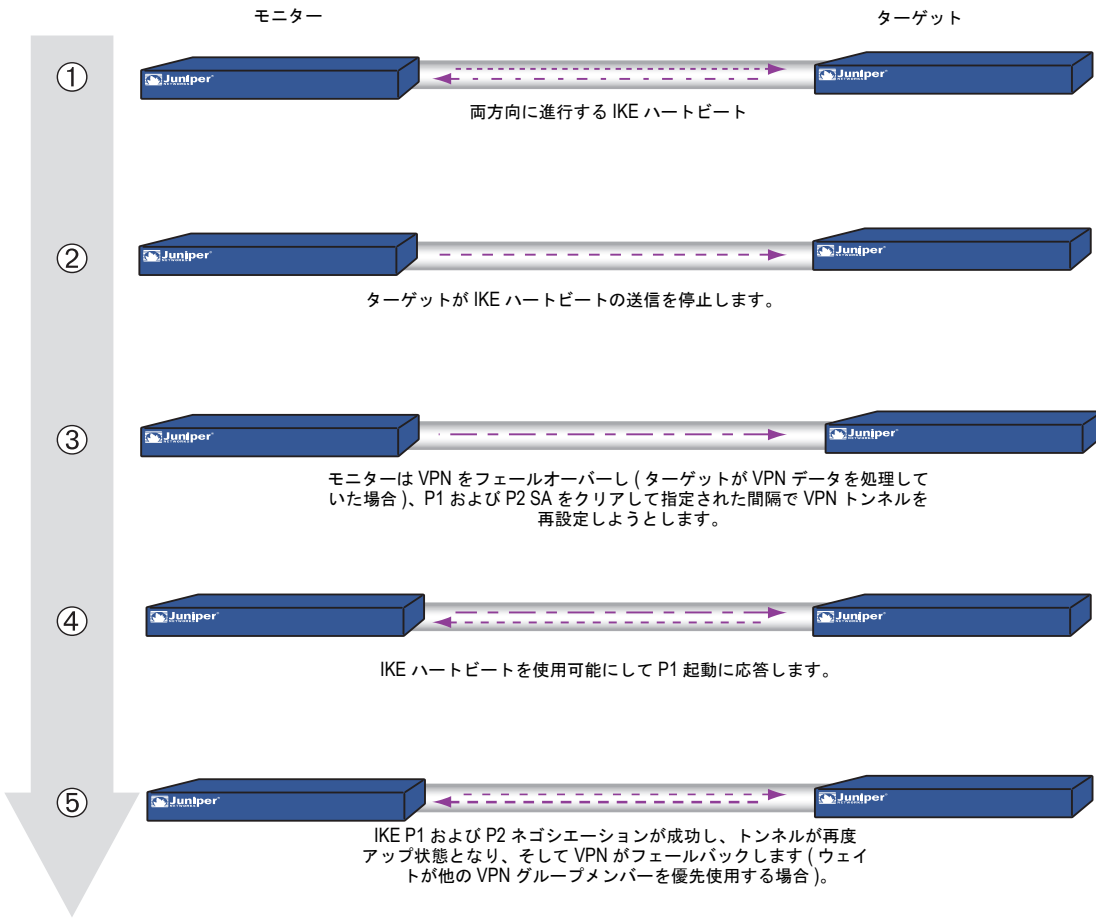
CLI

set ike gateway *name_str* heartbeat reconnect *number*

最も高いウェイトを持つ VPN グループメンバーが、トンネルを他のグループメンバーにフェールオーバーしてから監視デバイスを再接続すると、トンネルは再度最初のメンバーに自動的にフェールオーバーします。ウェイトシステムは、可能であれば常に、VPN データを扱うのに最適なグループ内のゲートウェイをランキングします。

299 ページの図 81 は、ターゲット ゲートウェイからの消失ハートビートが障害しきい値を越えた際に、VPN グループのメンバーが行う手順を示しています。

図 81: フェールオーバーとその後の復旧



TCP SYN-Flag チェック

VPN フェールオーバーを透過的に行うには、TCP セッション処理に対処する必要があります。フェールオーバー後に新しいアクティブゲートウェイが、既存の TCP セッションでパケットを受信すると、新しいゲートウェイはそれを新しい TCP セッションの最初のパケットとして扱い、パケットヘッダーに SYN フラグが設定されているかチェックします。このパケットは、実際に既存セッションの一部分であるため、SYN フラグは設定されていません。結果的に、新しいゲートウェイはパケットを拒否します。TCP SYN フラグチェックを使用可能にすると、すべての TCP アプリケーションはフェールオーバーの発生後に再接続する必要があります。

この問題を解決するために、次のように VPN トンネル内の TCP セッションに対する SYN-flag チェックを使用不可にすることができます。

WebUI

WebUI を介して SYN-flag チェックを使用不可にすることはできません。

CLI

unset flow tcp-syn-check-in-tunnel

注： デフォルトでは、SYN-flag チェックは使用可能になっています。

冗長 VPN ゲートウェイの作成

この例では、企業サイトにはデータセンターへの VPN トンネル、およびバックアップデータセンターへのトンネルがあります。すべてのデータは、2 箇所のデータセンターサイトの間でリース回線接続を介してミラーリングされています。終日の電源停止や自然災害などの重度の障害の際に継続してサービスを提供できるように、データセンターは物理的に分割されています。

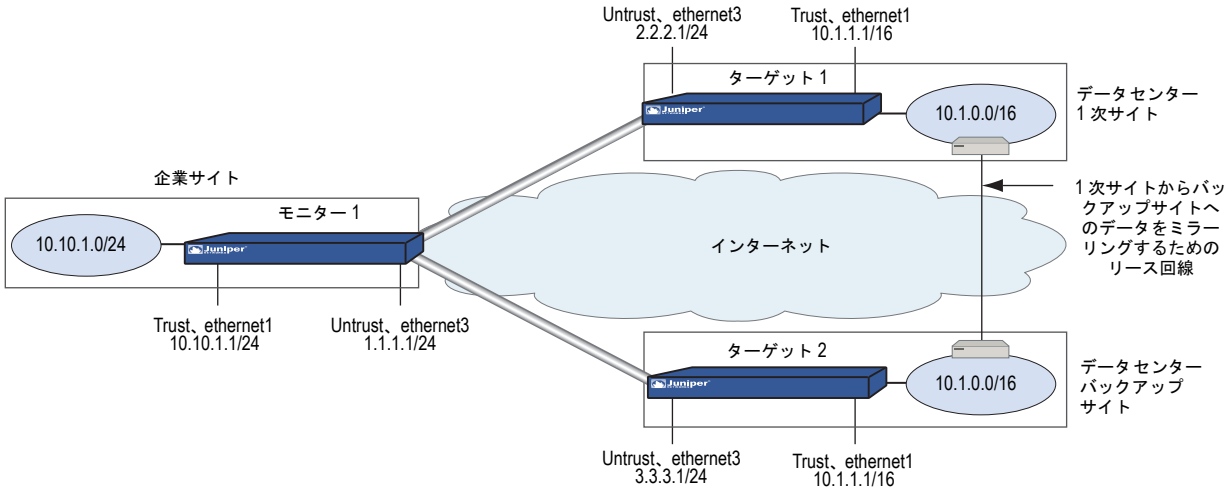
デバイスの配置と名前、Trust および Untrust ゾーンの物理インターフェースと IP アドレス、そして各セキュリティ デバイスの VPN グループ ID とウェイトは、次のとおりです。

デバイス場所	デバイス名前	物理インターフェースおよび IP アドレス (Trust ゾーン)	物理インターフェース、IP アドレス、デフォルトゲートウェイ (Untrust ゾーン)	VPN グループ ID およびウェイト
企業	モニター 1	ethernet1, 10.10.1.1/24	ethernet3, 1.1.1.1/24, (GW) 1.1.1.2	--
データセンター (1 次)	ターゲット 1	ethernet1, 10.1.1.1/16	ethernet3, 2.2.2.1/24, (GW) 2.2.2.2	ID = 1, ウェイト = 2
データセンター (バックアップ)	ターゲット 2	ethernet1, 10.1.1.1/16	ethernet3, 3.3.3.1/24, (GW) 3.3.3.2	ID = 1, ウェイト = 1

注： 両データセンターサイトの内部アドレス空間は、同一であることが必要です。

セキュリティゾーンはすべて trust-vr ルーティングドメインにあります。すべてのサイト間 AutoKey IKE トンネルは、フェーズ 1 と 2 のプロポーザルの両方に対して、「Compatible」として定義済みのセキュリティレベルを使用します。事前共有鍵で参加者を認証します。

図 82: 冗長 VPN ゲートウェイ



WebUI (モニター 1)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.10.1.1/24
次のように入力してから **OK** をクリックします。
Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: in_trust
IP Address/Domain Name:
IP/Netmask: (選択), 10.10.1.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: data_ctr
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.0.0/16
Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > VPN Group: VPN Group ID フィールドに **1** を入力してから **Add** をクリックします。

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: Target1
Security Level: Compatible
Remote Gateway Type: Static IP Address: (選択), IP Address: 2.2.2.1
Preshared Key: SLi1yoo129
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Compatible
Mode (Initiator): Main (ID 保護)
Heartbeat:
Hello: 3 Seconds
Reconnect: 60 seconds
Threshold: 5

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: To_target1
Security Level: Compatible
Remote Gateway: Predefined: (選択), target1

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

VPN Group: VPN Group-1
Weight: 2

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: Target2
Security Level: Compatible
Remote Gateway Type: Static IP Address: (選択), IP Address: 3.3.3.1
Preshared Key: CMFwb7oN23
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Compatible
Mode (Initiator): Main (ID 保護)
Heartbeat:
Hello: 3 Seconds
Reconnect: 60 seconds
Threshold: 5

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: To_target2
Security Level: Compatible
Remote Gateway: Predefined: (選択), target2

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

VPN Group: VPN Group-1
Weight: 1

4. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.2(untrust)

5. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), in_trust
Destination Address:
Address Book Entry: (選択), data_ctr
Service: ANY
Action: Tunnel
VPN: vPN Group-1
Modify matching bidirectional VPN policy: (選択)
Position at Top: (選択)

WebUI (ターゲット 1)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/16
次のように入力してから **OK** をクリックします。
Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 2.2.2.1/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: in_trust
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.1.0.0/16
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: corp
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.10.1.0/24
Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: monitor1
Security Level: Compatible
Remote Gateway Type:
Static IP Address: (**選択**), IP Address/Hostname: 1.1.1.1
Preshared Key: SLi1yoo129
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Compatible
Mode (Initiator): Main (ID **保護**)
Heartbeat:
Hello: 3 Seconds
Reconnect: 0 seconds

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

Name: To_monitor1
Security Level: Compatible
Remote Gateway: Predefined: (**選択**), monitor1

4. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: ethernet3
Gateway IP Address: 2.2.2.2

5. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), in_trust
Destination Address:
    Address Book Entry: (選択), corp
Service: ANY
Action: Tunnel
Tunnel VPN: monitor1
Modify matching bidirectional VPN policy: (選択)
Position at Top: (選択)

WebUI (ターゲット 2)

注 : ターゲット 1 の構成手順に従ってターゲット 2 を構成します。ただし、Untrust ゾーンインターフェース IP アドレスを 3.3.3.1/24、デフォルトゲートウェイ IP アドレスを 3.3.3.2 として定義し、CMFwb7oN23 を使用して事前共有鍵を生成します。

CLI (モニター 1)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.10.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. アドレス

```
set address trust in_trust 10.10.1.0/24
set address untrust data_ctr 10.1.0.0/16
```

3. VPN

```
set ike gateway target1 address 2.2.2.1 main outgoing-interface ethernet3
    preshare SLi1yoo129 sec-level compatible
set ike gateway target1 heartbeat hello 3
set ike gateway target1 heartbeat reconnect 60
set ike gateway target1 heartbeat threshold 5
set vpn to_target1 gateway target1 sec-level compatible
set ike gateway target2 address 3.3.3.1 main outgoing-interface ethernet3
    preshare CMFwb7oN23 sec-level compatible
set ike gateway target2 heartbeat hello 3
set ike gateway target2 heartbeat reconnect 60
set ike gateway target2 heartbeat threshold 5
set vpn to_target2 gateway target2 sec-level compatible
set vpn-group id 1 vpn to_target1 weight 2
set vpn-group id 1 vpn to_target2 weight 1
unset flow tcp-syn-check-in-tunnel
```

4. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.2
```

5. ポリシー

```
set policy top from trust to untrust in_trust data_ctr any tunnel "vpn-group 1"
set policy top from untrust to trust data_ctr in_trust any tunnel "vpn-group 1"
save
```

CLI (ターゲット 1)

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/16
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 2.2.2.1/24

2. **アドレス**
   set address trust in_trust 10.1.0.0/16
   set address untrust corp 10.10.1.0/24

3. **VPN**
   set ike gateway monitor1 address 1.1.1.1 main outgoing-interface ethernet3
   preshare SLi1yoo129 sec-level compatible
   set ike gateway monitor1 heartbeat hello 3
   set ike gateway monitor1 heartbeat threshold 5
   set vpn to_monitor1 gateway monitor1 sec-level compatible

4. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.2

5. **ポリシー**
   set policy top from trust to untrust in_trust corp any tunnel vpn to_monitor
   set policy top from untrust to trust corp in_trust any tunnel vpn to_monitor
   save

CLI (ターゲット 2)

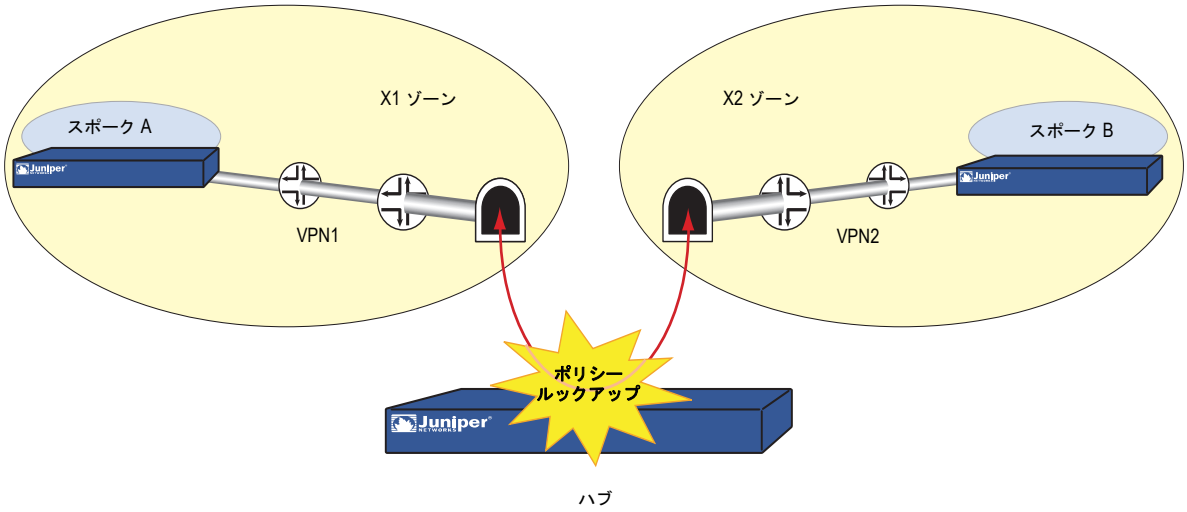
注 : ターゲット 1 の構成手順に従ってターゲット 2 を構成します。ただし、Untrust ゾーンインターフェース IP アドレスを 3.3.3.1/24、デフォルトゲートウェイ IP アドレスを 3.3.3.2 として定義し、CMFwb7oN23 を使用して事前共有鍵を生成します。

VPN 対向の作成

別のゾーンにスポークサイトを設置することによって、1 つの VPN トンネルからもう 1 つの VPN トンネルへ向かうトラフィックのインターゾーンポリシーを、ハブサイトで強化することができます。それらは異なるゾーンに存在するため、ハブのセキュリティ デバイスは、1 つのトンネルから他のトンネルにトラフィックをルーティングする前に、ポリシー ルックアップを行う必要があります。スポーク サイト間の VPN トンネルを介して流れるトラフィックを制御できます。このような方法を、*VPN 対向*と呼びます。

注 : オプションでイントラゾーンブロッキングを使用可能にし、同じゾーン内の 2 つのトンネルインターフェース間のトラフィックを制御するイントラゾーンポリシーを定義することもできます。

図 83: VPN 対向



VPN 対向の主な利点は次のとおりです。

- 作成する必要がある VPN 数を節約できます。たとえば、周辺サイト A はハブ、および周辺サイト B、C、D にリンクできますが、A が設定する必要があるのは 1 つの VPN トンネルのみです。特に NetScreen-5XP ユーザーは最大 10 個の VPN トンネルを使用できるため、ハブアンドスポーク方式を利用することによって、VPN オプションと能力を大幅に向上させることができます。
- ハブデバイスの管理者（admin）は、周辺サイト間の VPN トラフィックを完全に制御できます。たとえば、
  - 管理者は HTTP トラフィックフローのみを許可し、B から A へは任意のトラフィックフローを許可します。
  - 管理者は A から発信され C に到達するトラフィックを許可し、C から発信される A に到達するトラフィックを拒否することもできます。
  - 管理者は A の特定のホストが D ネットワーク全体に到達するのを許可する一方で、D の特定のホストのみが A の異なるホストに到達するのを許可することができます。
- ハブデバイスの管理者は、全ての周辺ネットワークからのアウトバウンドトラフィックを完全に制御できます。各ペリミターサイトに、最初に、カスタマイズ VPN からハブに全ての発信トラフィックをトンネルするポリシーがなければなりません。例えば : **set policy top from trust to untrust any any any tunnel vpn** *name_str* (ここで *name_str* は、各ペリミターサイトからハブへの特定の VPN トンネルを定義します。ハブでは、管理者は特定の種類のトラフィック（HTTP のみなど）を許可し、不適切な Web サイトへの URL ブロックを実行してインターネットのアクセスを制御できます。
- 地域ハブはスポークトンネルを介して使用し相互に接続でき、1 つの地域のスポークサイトが別の地域のスポークサイトに到達するのを可能にします。

次の例は 313 ページの「ハブアンドスポーク方式 VPN の作成」と似ていますが、ニューヨークのハブ サイトのセキュリティ デバイスが、東京とパリの支社への 2 つのトンネル間でルーティングするトラフィック上で、ポリシー チェックを実行するという点が異なります。各リモートサイトを異なるゾーンに配置することによって、VPN トラフィックをハブで制御します。

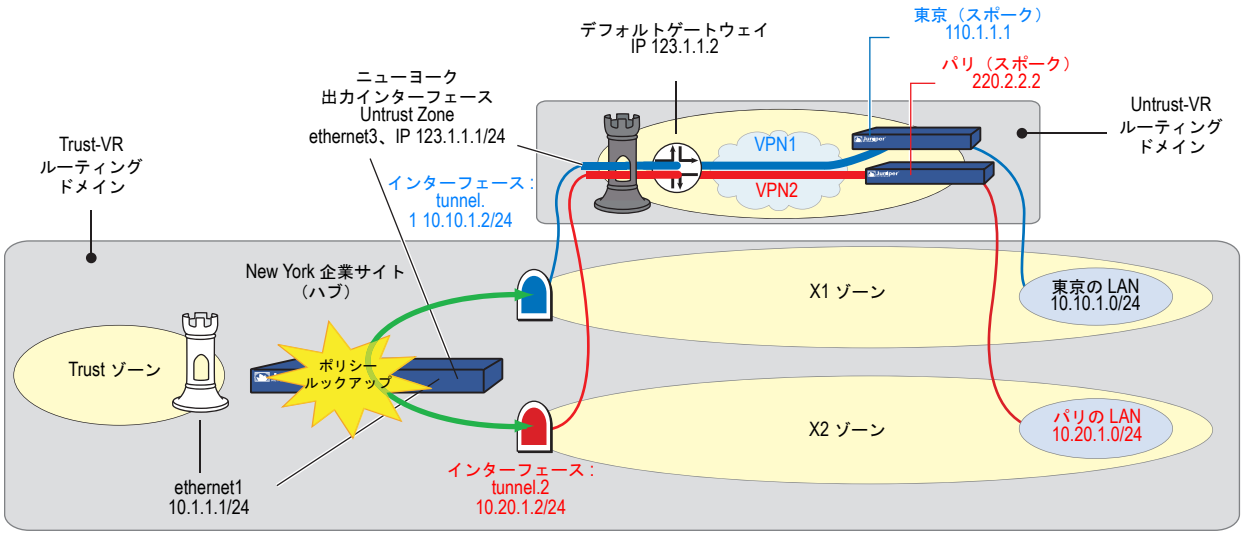
東京の LAN アドレスはユーザー定義の X1 ゾーン内にあり、パリの LAN アドレスはユーザー定義の X2 ゾーン内にあります。両方のゾーンは、Trust-VR ルーティングドメインにあります。

注： ユーザー定義ゾーンを作成するには、まずセキュリティ デバイスのゾーン ソフトウェア キーを入手しロードする必要があります。

VPN1 トンネルを tunnel.1 インターフェースに、VPN2 トンネルを tunnel.2 インターフェースにバインドします。X1 と X2 ゾーンインターフェースには IP アドレスを割り当てませんが、両方のトンネルインターフェースにはアドレスを与えます。これらのインターフェースのルートは、Trust-VR ルーティングテーブルに自動的に表示されます。トンネルインターフェースの IP アドレスを宛先のアドレスと同じサブネットに配置することによって、そのサブネットに宛てたトラフィックは、トンネルインターフェースにルーティングされます。

出力インターフェースは、Untrust ゾーンにバインドされた ethernet3 です。図 84 から、両方のトンネルが Untrust ゾーンで終了していることがわかります。ただし、トンネルを利用するトラフィックの端点は X1 および X2 ゾーンに存在します。トンネルは事前共有鍵とともに AutoKey IKE を使用します。フェーズ 1 と 2 プロポーザルの両方に対し、「Compatible」として定義済みのセキュリティレベルを選択します。untrust-vr に Untrust ゾーンをバインドします。トンネルはルーティングベースであるため (正しいトンネルは、ポリシーで指定されたトンネル名ではなくルーティングで決定されます)、プロキシ ID は各トンネルの構成に含まれています。

図 84: 2 つのルーティング ドメインと複数のセキュリティ ゾーンを持つ VPN 対向



WebUI

1. セキュリティゾーンと仮想ルーター

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

IP Address/Netmask: 0.0.0.0/0
Manage IP: 0.0.0.0

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Null

Network > Zones > Edit (Untrust): 次のように入力してから **OK** をクリックします。

Virtual Router Name: untrust-vr
Block Intra-Zone Traffic: (選択)

Network > Zones > New: 次のように入力してから **OK** をクリックします。

Zone Name: X1
Virtual Router Name: Trust-vr
Block Intra-Zone Traffic: (選択)

Network > Zones > New: 次のように入力してから **OK** をクリックします。

Zone Name: X2
Virtual Router Name: Trust-vr
Block Intra-Zone Traffic: (選択)

2. インターフェース

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 123.1.1.1/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): X1 (trust-vr)
Fixed IP: (選択)
IP Address/Netmask: 10.10.1.2/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.2
Zone (VR): X2 (trust-vr)
Fixed IP: (選択)
IP Address/Netmask: 10.20.1.2/24

3. 東京オフィスの VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vPN1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: Tokyo
Type: Static IP: (選択), Address/Hostname: 110.1.1.1
Preshared Key: netscreen1
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Proxy-ID: (選択)
Local IP / Netmask: 10.20.1.0/24
Remote IP / Netmask: 10.10.1.0/24
Service: ANY

注 : 東京オフィスとパリ オフィスを保護するセキュリティ デバイス上で VPN トンネルを構成する場合は、次のいずれかを行います。

（ルーティングベース VPN）**Enable Proxy-ID** チェックボックスをオンにし、ローカル IP およびネットマスク用に **10.10.1.0/24**（東京）および **10.20.1.0/24**（パリ）、リモート IP およびネットマスク用に **10.20.1.0/24**（東京）および **10.10.1.0/24**（パリ）を入力します。

（ポリシーベース VPN）Trust ゾーン アドレス帳内に 10.10.1.0/24（東京）および 10.20.1.0/24（パリ）、Untrust ゾーン アドレス帳内に 10.20.1.0/24（東京）および 10.10.1.0/24（パリ）に対応するエントリを作成します。これらを、ハブサイトへの VPN トンネルを参照するポリシーのソースおよび宛先アドレスとして使用します。

---

4. パリオフィスの VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vPN2
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: paris
Type: Static IP: (選択), Address/Hostname: 220.2.2.2
Preshared Key: netscreen2
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Proxy-ID: (選択)
Local IP / Netmask: 10.10.1.0/24
Remote IP / Netmask: 10.20.1.0/24
Service: ANY

5. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Next Hop Virtual Router Name: (選択), untrust-vr

Network > Routing > Routing Entries > untrust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 123.1.1.2

6. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Tokyo LAN
IP Address/Domain Name:
IP/Netmask: (選択), 10.10.1.0/24
Zone: X1

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Paris LAN
IP Address/Domain Name:
IP/Netmask: (選択), 10.20.1.0/24
Zone: X2

7. ポリシー

Policies > (From: X1, To: X2) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Tokyo LAN
Destination Address:
Address Book Entry: (選択), Paris LAN
Service: ANY
Action: Permit
Position at Top: (選択)

Policies > (From: X2, To: X1) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Paris LAN
Destination Address:
Address Book Entry: (選択), Tokyo LAN
Service: ANY
Action: Permit
Position at Top: (選択)

CLI

1. **セキュリティゾーンと仮想ルーター**
   unset interface ethernet3 ip
   unset interface ethernet3 zone
   set zone untrust vrouter untrust-vr
   set zone untrust block
   set zone name x1
   set zone x1 vrouter trust-vr
   set zone x1 block
   set zone name x2
   set zone x2 vrouter trust-vr
   set zone x2 block

2. **インターフェース**
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 123.1.1.1/24
   set interface tunnel.1 zone x1
   set interface tunnel.1 ip 10.10.1.2/24
   set interface tunnel.2 zone x2
   set interface tunnel.2 ip 10.20.1.2/24

3. **東京オフィスの VPN**
   set ike gateway Tokyo address 110.1.1.1 outgoing-interface ethernet3 preshare netscreen1 sec-level compatible
   set vpn VPN1 gateway Tokyo sec-level compatible
   set vpn VPN1 bind interface tunnel.1
   set vpn VPN1 proxy-id local-ip 10.20.1.0/24 remote-ip 10.10.1.0/24 any

---

注 : 東京オフィスとパリ オフィスを保護するセキュリティ デバイス上で VPN トンネルを構成する場合は、次のいずれかを行います。

(ルートベース VPN) 次のコマンドを入力します。**set vpn VPN1 proxy-id local-ip 10.20.1.0/24 remote-ip 10.10.1.0/24**（東京）および **set vpn VPN1 proxy-id local-ip 10.10.1.0/24 remote-ip 10.20.1.0/24**（パリ）

（ポリシーベース VPN）Trust ゾーン アドレス帳内に 10.10.1.0/24（東京）および 10.20.1.0/24（パリ）、Untrust ゾーン アドレス帳内に 10.20.1.0/24（東京）および 10.10.1.0/24（パリ）に対応するエントリを作成します。ハブサイトへの VPN トンネルを参照するポリシーのソースおよび宛先アドレスとして、これらのエントリを使用します。

---

4. **パリオフィスの VPN**
   set ike gateway Paris address 220.2.2.2 outgoing-interface ethernet3 preshare netscreen2 sec-level compatible
   set vpn VPN2 gateway Paris sec-level compatible
   set vpn VPN2 bind interface tunnel.2
   set vpn VPN2 proxy-id local-ip 10.10.1.0/24 remote-ip 10.20.1.0/24 any

5. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
   set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 123.1.1.2

6. **アドレス**
   set address x1 "Tokyo LAN" 10.10.1.0/24
   set address x2 "Paris LAN" 10.20.1.0/24

7. **ポリシー**
   set policy top from x1 to x2 "Tokyo LAN" "Paris LAN" any permit
   set policy top from x2 to x1 Paris LAN" "Tokyo LAN" any permit
   save

注 : トンネルインターフェースが NAT モードであるため、次のメッセージが表示されますが、無視できます :

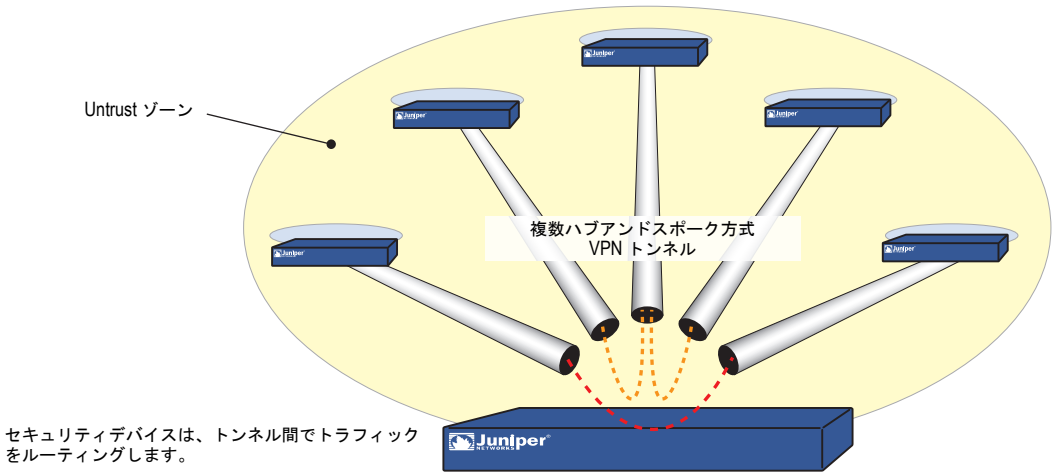
警告 : *zone_name* ゾーンのインターフェースには、NAT モードになっているものもあります。トラフィックはそこを通過できません !

ハブアンドスポーク方式 VPN の作成

セキュリティ デバイスで終了する 2 つの VPN トンネルを作成すると、セキュリティ デバイスが 1 つのトンネルから出たトラフィックをもう 1 つのトンネルに誘導できるように、ルートのペアを設定することができます。両方のトンネルが 1 つのゾーンに含まれている場合は、1 つのトンネルからもう 1 つのトンネルへトラフィックが通過するのを許可するポリシーを作成する必要はありません。必要なのは、ルートを定義することだけです。このような方法は、*ハブアンドスポーク方式 VPN* と呼ばれます。

1 つのトンネルに複数の VPN を構成し、任意の 2 つのトンネル間でトラフィックをルーティングすることもできます。

図 85: ハブアンドスポーク方式 VPN 構成における複数トンネル



この例では、東京とパリの 2 つの支社が VPN のトンネル、VPN1 および VPN2 のペアを介して、互いに通信します。各トンネルは、リモートサイトから始まりニューヨークの企業サイトで終結します。企業サイトのセキュリティ デバイスは、1 つのトンネルから出るトラフィックをもう 1 つのトンネルにルーティングします。

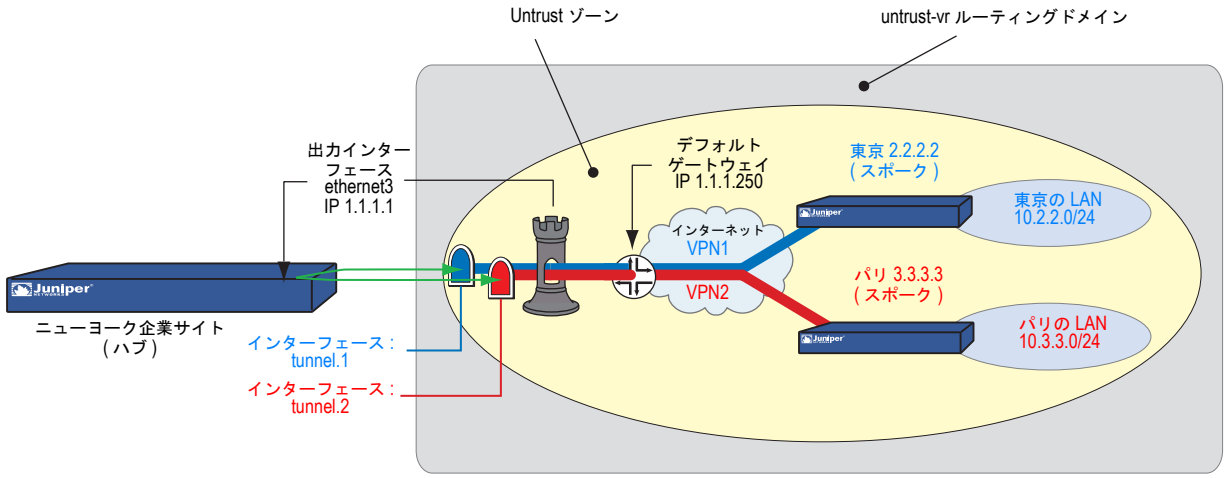
イントラゾーン ブロッキングを使用不可にすることによって、企業サイトのセキュリティ デバイスは、リモート端点がともに同じゾーン（Untrust ゾーン）に存在するため、トンネル間でトラフィックを誘導する際にルート ルックアップのみを実行すれば十分となり、ポリシー ルックアップは必要ありません。

注： オプションで、イントラゾーンブロッキングを使用可能にし、2 つのトンネルインターフェース間のトラフィックを許可するイントラゾーンポリシーを定義することもできます。

トンネルインターフェース tunnel.1 および tunnel.2 (いずれも番号を与えられていない) に、トンネルをバインドします。トンネルは事前共有鍵をとともに、AutoKey IKE を使用します。フェーズ 1 と 2 プロポーザルの両方に対し、「Compatible」として定義済みのセキュリティレベルを選択します。untrust-vr に Untrust ゾーンをバインドします。Untrust ゾーンインターフェースは ethernet3 です。

注： 次の構成は、ルートベース VPN 用です。ポリシーベースのハブアンドスポーク方式 VPN を構成する場合は、ポリシーで Trust および Untrust ゾーンを使用する必要があり、ユーザー定義のセキュリティゾーンは使用できません。

図 86: ハブアンドスポーク方式 VPN



WebUI (ニューヨーク)

1. **セキュリティゾーンと仮想ルーター**

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   IP Address/Netmask: 0.0.0.0/0
   Manage IP: 0.0.0.0

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Null

   Network > Zones > Edit (Untrust): 次のように入力してから **OK** をクリックします。

   Virtual Router Name: untrust-vr
   Block Intra-Zone Traffic: (**オフ**)

2. インターフェース

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): Untrust (untrust-vr)
Unnumbered: (選択)
Interface: ethernet3 (untrust-vr)

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.2
Zone (VR): Untrust (untrust-vr)
Unnumbered: (選択)
Interface: ethernet3 (untrust-vr)

3. 東京オフィスの VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vPN1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: Tokyo
Type: Static IP: (選択), Address/Hostname: 2.2.2.2
Preshared Key: netscreen1
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Proxy-ID: (選択)
Local IP/Netmask: 0.0.0.0/0
Remote IP/Netmask: 0.0.0.0/0
Service: ANY

4. パリオフィスの VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vPN2
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: paris
Type: Static IP: (選択), Address/Hostname: 3.3.3.3
Preshared Key: netscreen2
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Proxy-ID: (選択)
Local IP/Netmask: 0.0.0.0/0
Remote IP/Netmask: 0.0.0.0/0
Service: ANY

5. ルート

Network > Routing > Routing Entries > untrust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.2.2.0/24
Gateway: (選択)
Interface: Tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > untrust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.3.3.0/24
Gateway: (選択)
Interface: Tunnel.2
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > untrust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

WebUI (東京)

1. セキュリティゾーンと仮想ルーター

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

IP Address/Netmask: 0.0.0.0/0
Manage IP: 0.0.0.0

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Null

Network > Zones > Edit (Untrust): 次のように入力してから **OK** をクリックします。

Virtual Router Name: untrust-vr
Block Intra-Zone Traffic: (選択)

2. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.2.2.1/24
次のように選択してから **OK** をクリックします。
Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): Untrust (untrust-vr)
Unnumbered: (選択)
Interface: ethernet3 (untrust-vr)

3. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Paris
IP Address/Domain Name:
IP/Netmask: (選択), 10.3.3.0/24
Zone: Untrust

4. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vPN1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: New York
Type: Static IP: (選択), Address/Hostname: 1.1.1.1
Preshared Key: netscreen1
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Proxy-ID: (選択)
Local IP/Netmask: 0.0.0.0/0
Remote IP/Netmask: 0.0.0.0/0
Service: ANY

5. **ルート**
   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Next Hop Virtual Router Name: (選択); untrust-vr

   Network > Routing > Routing Entries > untrust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選択)
   Interface: ethernet3
   Gateway IP Address: 2.2.2.250

   Network > Routing > Routing Entries > untrust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 10.3.3.0/24
   Gateway: (選択)
   Interface: Tunnel.1
   Gateway IP Address: 0.0.0.0

6. **ポリシー**
   Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Any
   Destination Address:
   Address Book Entry: (選択), Paris
   Service: ANY
   Action: Permit

WebUI (パリ)

1. **セキュリティゾーンと仮想ルーター**
   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   IP Address/Netmask: 0.0.0.0/0
   Manage IP: 0.0.0.0

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Null

   Network > Zones > Edit (Untrust): 次のように入力してから **OK** をクリックします。

   Virtual Router Name: untrust-vr
   Block Intra-Zone Traffic: (選択)

2. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.3.3.1/24
次のように選択してから **OK** をクリックします。
Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 3.3.3.3/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: Tunnel.1
Zone (VR): Untrust (untrust-vr)
Unnumbered: (選択)
Interface: ethernet3 (untrust-vr)

3. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Tokyo
IP Address/Domain Name:
IP/Netmask: (選択), 10.2.2.0/24
Zone: Untrust

4. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vPN2
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: New York
Type: Static IP: (選択), Address/Hostname: 1.1.1.1
Preshared Key: netscreen2
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Proxy-ID: (選択)
Local IP/Netmask: 0.0.0.0/0
Remote IP/Netmask: 0.0.0.0/0
Service: ANY

5. **ルート**
   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Next Hop Virtual Router Name: (選択); untrust-vr

   Network > Routing > Routing Entries > untrust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選択)
   Interface: ethernet3
   Gateway IP Address: 3.3.3.250

   Network > Routing > Routing Entries > untrust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 10.2.2.0/24
   Gateway: (選択)
   Interface: Tunnel.1
   Gateway IP Address: 0.0.0.0

6. **ポリシー**
   Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Any
   Destination Address:
   Address Book Entry: (選択), Tokyo
   Service: ANY
   Action: Permit

CLI (ニューヨーク)

1. **セキュリティゾーンと仮想ルーター**
   unset interface ethernet3 ip
   unset interface ethernet3 zone
   set zone untrust vrouter untrust-vr
   unset zone untrust block

2. **インターフェース**
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24
   set interface tunnel.1 zone untrust
   set interface tunnel.1 ip unnumbered interface ethernet3
   set interface tunnel.2 zone untrust
   set interface tunnel.2 ip unnumbered interface ethernet3

3. **東京オフィスの VPN**
   set ike gateway Tokyo address 2.2.2.2 outgoing-interface ethernet3 preshare
   netscreen1 sec-level compatible
   set vpn VPN1 gateway Tokyo sec-level compatible
   set vpn VPN1 bind interface tunnel.1
   set vpn VPN1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any

4. パリオフィスの VPN

```
set ike gateway Paris address 3.3.3.3 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
set vpn VPN2 gateway Paris sec-level compatible
set vpn VPN2 bind interface tunnel.2
set vpn VPN2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

5. ルート

```
set vrouter untrust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter untrust-vr route 10.3.3.0/24 interface tunnel.2
set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
save
```

CLI (東京)

1. セキュリティゾーンと仮想ルーター

```
unset interface ethernet3 ip
unset interface ethernet3 zone
set zone untrust vrouter untrust-vr
```

2. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

3. アドレス

```
set address untrust Paris 10.3.3.0/24
```

4. VPN

```
set ike gateway "New York" address 1.1.1.1 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn VPN1 gateway "New York" sec-level compatible
set vpn VPN1 bind interface tunnel.1
set vpn VPN1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

5. ルート

```
set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter untrust-vr route 10.3.3.0/24 interface tunnel.1
```

6. ポリシー

```
set policy from trust to untrust any Paris any permit
set policy from untrust to trust Paris any any permit
save
```

CLI (パリ)

1. **セキュリティゾーンと仮想ルーター**
   unset interface ethernet3 ip
   unset interface ethernet3 zone
   set zone untrust vrouter untrust-vr

2. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.3.3.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 3.3.3.3/24
   set interface tunnel.1 zone untrust
   set interface tunnel.1 ip unnumbered interface ethernet3

3. **アドレス**
   set address untrust Tokyo 10.2.2.0/24

4. **VPN**
   set ike gateway "New York" address 1.1.1.1 outgoing-interface ethernet3 preshare
   netscreen2 sec-level compatible
   set vpn VPN2 gateway "New York" sec-level compatible
   set vpn VPN2 bind interface tunnel.1
   set vpn VPN2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any

5. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
   set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 3.3.3.250
   set vrouter untrust-vr route 10.2.2.0/24 interface tunnel.1

6. **ポリシー**
   set policy from trust to untrust any Tokyo any permit
   set policy from untrust to trust Tokyo any any permit
   save

第 8 章

AutoConnect 仮想プライベートネットワーク

本章では、ScreenOS の AutoConnect 仮想プライベートネットワーク（AC-VPN）機能について記述し、それがハブアンドスポーク方式のネットワークトポロジーでどのように動作するかを説明し、それが使用される典型的なシナリオの構成例を提供します。

概要

仮想プライベートネットワーク（VPN）トンネルでそのリモートのサテライトサイトの安全を確保する小規模企業は、リモートサイトが本社だけでなく互いとも通信する必要があるので、通常はフルメッシュ VPN で全サイトを相互に接続しています。この種のネットワークでは、リモートサイトは通常、最高 25 個の VPN トンネルをサポートする、ローエンドのセキュリティデバイスを運用します。企業は、そのリモートサイトに、（相当な経費をかけて）容量がより大きいセキュリティデバイスを設置するか、フルメッシュからハブアンドスポーク方式のネットワークトポロジーへ切り換えなければなりません。

ハブアンドスポーク方式の構成は、スケーラビリティの問題を解決しますが、その主な欠点は、スポーク間の通信がすべてハブを通過しなければなりません。という点です。スポークの数が 1,000 を超えても、トラフィックが単純なデータであれば、これは通常、問題にはありません。しかしながら、トラフィックが動画または VoIP（音声 IP 化プロトコル）である場合、ハブでの処理オーバヘッドがレイテンシの原因となり、そのような用途では重大な問題となる場合があります。

AC-VPN は、必要に応じてスポークが互いの間で動的に直接 VPN トンネルを作成できるように、ハブアンドスポーク方式のネットワークを構成する方法を提供します。これは、スポーク間のレイテンシの問題を解決するだけでなく、ハブでの処理オーバヘッドを低減し、それにより全般的なネットワークのパフォーマンスを改善します。ネットワーク管理者は、静的な VPN トンネルの複雑なネットワークを維持するという時間のかかるタスクから解放されます。

機能

AC-VPN は、全スポークが VPN トンネルによってハブに接続されている、ハブアンドスポーク方式のネットワークで実装されるように設計されています。ハブとスポーク上に AC-VPN を構成し、NHRP（ネクストホップレゾリューションプロトコル）を有効にします。ハブは、パブリックアドレスとプライベートアドレスのマッピング、サブネットマスク長さ、およびルーティングおよびホップカウント情報など、各スポークに関する一連の情報を取得するために NHRP を使用します。これらの情報はハブがキャッシュします。次に、いずれかのスポークが別のスポークと（ハブを通して）通信を始めると、ハブは、スポークの AC-VPN 構成から取得した情報と組み合わせて、この情報を使用し、スポークが相互に AC-VPN トンネルをセットアップできるようにします。トンネルがネゴシエートされている間に、通信は、ハブを介して 2 つのスポーク間に流れ続けます。動的なトンネルがアクティブになると、ハブはリンクへの参加を取りやめ、トラフィックは 2 つのスポーク間を直接流れます。トラフィックが動的なトンネルを通過しなくなると、トンネルはタイムアウトします。

NHRP メッセージ

NHRP では、ハブアンドスポーク方式ネットワークのハブは、ネクストホップサーバー（NHS）と呼ばれ、スポークはネクストホップクライアント（NHC）と呼ばれます。NHS と NHC の間の NHRP 通信は、NHRP メッセージの正式な交換を通して発生します。NBMA (Nonbroadcast Multi Access) ネクストホップレゾリューションプロトコル（RFC 2332）は、7 つの NHRP メッセージを定義しています。これらの 7 つのメッセージに、ScreenOS はさらに 2 つを追加しました。これらの 9 つのメッセージおよび AC-VPN ハブアンドスポーク方式ネットワークでのその動作は、以下のように定義されます。

- **Registration Request** - 静的な VPN トンネルが NHC とその NHS の間でアクティブになった後、NHC は、NHS に NHRP 登録要求メッセージを送信します。メッセージには、多くのクライアント情報エントリー（CIE）が含まれます。これには、NHC のパブリックアドレスからプライベートアドレスへのマッピング、サブネットマスク長、およびルーティング情報やホップカウント情報などが含まれます。

注： 現在の ScreenOS 実装では、NHRP は、そのピアへルートを再分配しません。また、BGP と OSPF は、そのピアへ NHRP ルートを再分配しません。

- **Registration Reply** - NHS は､登録要求に対して ACK または NAK で応答できます。NHS がパケットを認識できない場合、パケットは承認されず（NAK）破棄されます。登録が成功すると、NHS は、登録要求に含まれていた CIE をキャッシュし、登録応答 ACK を送信します。

- **Resolution Request**, **Resolution Reply** - ScreenOS 専用の Resolution-set および Resolution-ack メッセージの導入により、NHRP の Resolution Request および Resolution Reply メッセージのペアは、NHS 上のキャッシュされた CIE を最新の状態に維持するよう委託されます。NHC は、NHS で構成された保持時間と共にこれを行います。これは、各 NHC についてキャッシュされたエントリの寿命を指定します。NHS がそのサブネットに関して最新の情報を持っているように、NHC は、定期的に NHS へ Resolution Request メッセージを送信します。デバイスが、サブネットに追加されたりサブネットから削除された場合、その情報は Resolution Request メッセージに含まれ、NHS はそのキャッシュを更新して、Resolution Reply を送信します。

- **Purge Request**, **Purge Reply** - 管理者が NHC をシャットダウンすると、デバイスは NHS に Purge Request メッセージを送信します。Purge Request を受信すると、NHS は、その NHC についてキャッシュされたエントリをすべて削除し、Purge Reply を送信します。NHC でシステム障害が発生しオフラインになった場合、NHS は、キャッシュの構成された寿命が期限切れになった後、デバイスについてキャッシュされたエントリを削除します。
- **Error Indication** - このメッセージは、NHRP エラー条件をログに記録します。

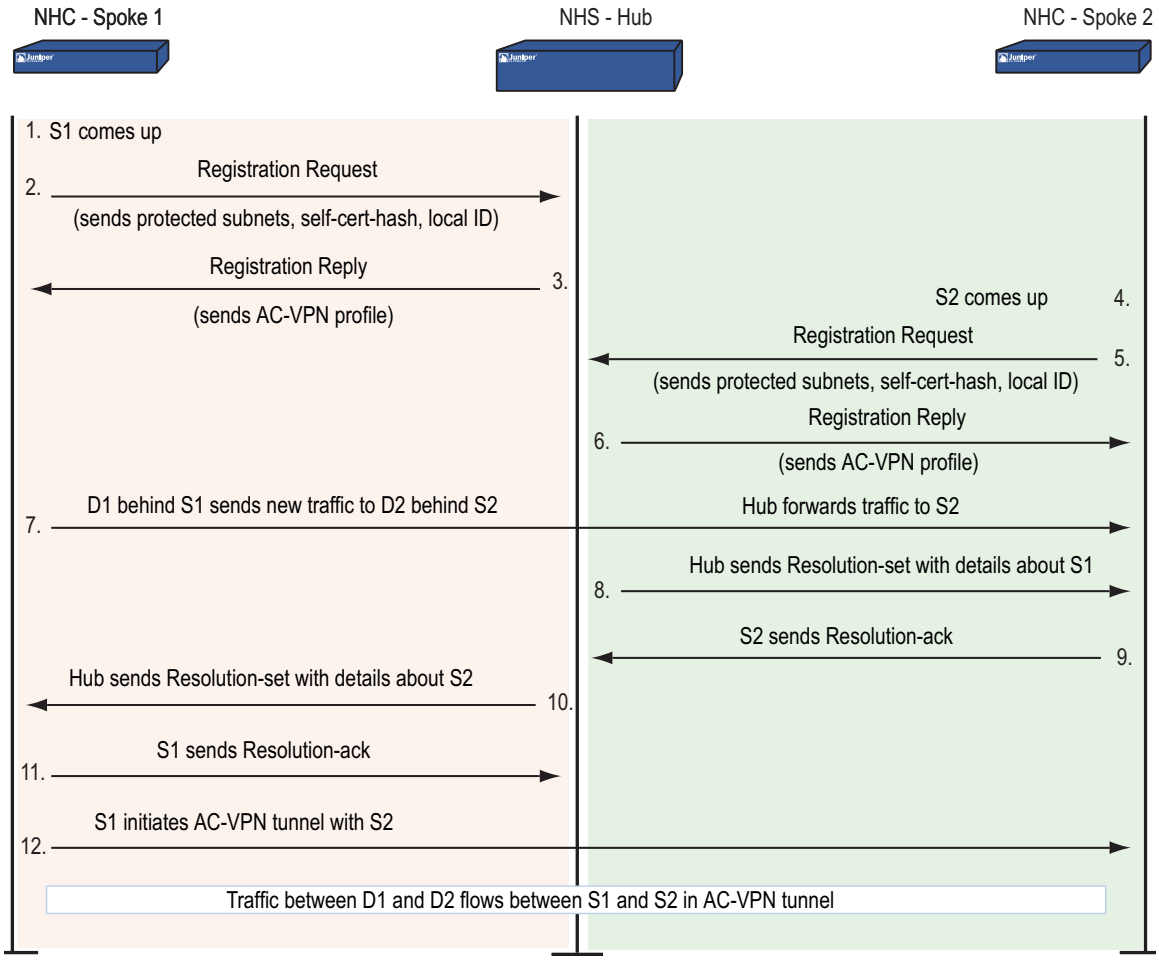
AC-VPN をサポートするため、ScreenOS は次のメッセージペアを追加しました。

- **Resolution-set**, **Resolution-ack** - NHS は、ある静的な VPN トンネルから別の VPN トンネルへのトラフィックを検出すると、各静的トンネルの端にある NHC に Resolution-set メッセージを送信します。これらのメッセージには、各 NHC が AC-VPN トンネルをセットアップするのに必要な、相手に関する情報がすべて含まれています。NHC が Resolution-ack メッセージで応答すると、NHS は、NHC の 1 つに ACVPN トンネルネゴシエーションを開始するよう指示します。

ACVPN トンネルの開始

図 87 は、NHRP Registration Request および Registration Reply メッセージ、さらには ScreenOS 独自の Resolution-set および Resolution-ack メッセージを使用して、ScreenOS が ACVPN トンネルのセットアップをトリガする様子を示しています。簡略化のために、図では、Resolution Request および Resolution Reply メッセージの交換、および Purge メッセージと Error メッセージを示していません。(省略形 S1 および S2 は スポーク 1 およびスポーク 2 をそれぞれ表し、D1 と D2 は、それらのスポークの背後にある宛先を指します。)

図 87: NHRP による AC-VPN のセットアップ



AC-VPN の構成

次の一般的な制限が適用されます。

- ハブの方向へ構成される VPN トンネルはすべて、ルートベースでなければなりません。
- フェーズ 1 の自動鍵管理は、アグレッシブモードで行う必要があります。
- 認証方式は、自己署名証明書および汎用 PKI でなければなりません。
- スポークはすべて、ハブ上の 1 つのゾーンに接続されていなければなりません。
- 仮想ルーターの複数のインスタンスでの NHRP の構成は、NHS でのみサポートされます。
- 動的ルーティングプロトコルは、NHC から NHS への登録についてはサポートされません。スポークを構成する場合、**set protocol nhrp cache *ip_addr/mask*** コマンドを使用してルートを追加しなければなりません。

ネットワークアドレス変換

次の制限が NAT に適用されます。

- Nat-Traversal - スポークの 1 つが、ハブへ向かうパスの NAT デバイスの背後にある場合、AC-VPN は、2 つのスポーク間に動的なトンネルを作成できます。しかしながら、両方のスポークが NAT デバイスの背後にある場合、動的なトンネルは作成されません。スポーク間の通信はハブを介して続けられます。NAT-Traversal については、234 ページの「NAT-Traversal」を参照してください。
- NAT は、マップインターネットプロトコル (MIP) のアドレシングでのみサポートされます。
- ポートアドレス変換（PAT）は、1 つのスポークとハブの間でのみサポートされます。たとえば、1 つのスポークとハブの間に NAT デバイスを設置できます。また、動的なトンネルは、別のスポークとハブの間に NAT デバイスがない限り、そのスポークとその別のスポークの間で作成できます。このシナリオでは、ハブは、別のスポークへのトンネルを開始するよう NAT デバイスの背後のスポークに強制します。
- ハブの直前の PAT はサポートされます。
- スポークの間の PAT はサポートされません。

ハブでの構成

スポークの構成には以下が含まれます。

1. 静的なゲートウェイおよび VPN を作成する。
2. スポークへの静的なトンネルを作成し、VPN をトンネルにバインドする。
3. AC-VPN ゲートウェイプロフィールを作成する。
4. AC-VPN VPN プロフィールを作成する。
5. 仮想ルーターで NHRP を使用可能にする。
6. NHRP 用の ACVPN プロフィールを選択する。
7. トンネルインターフェースで NHRP を使用可能にする。
8. ルーティングを構成する。

各スポークでの構成

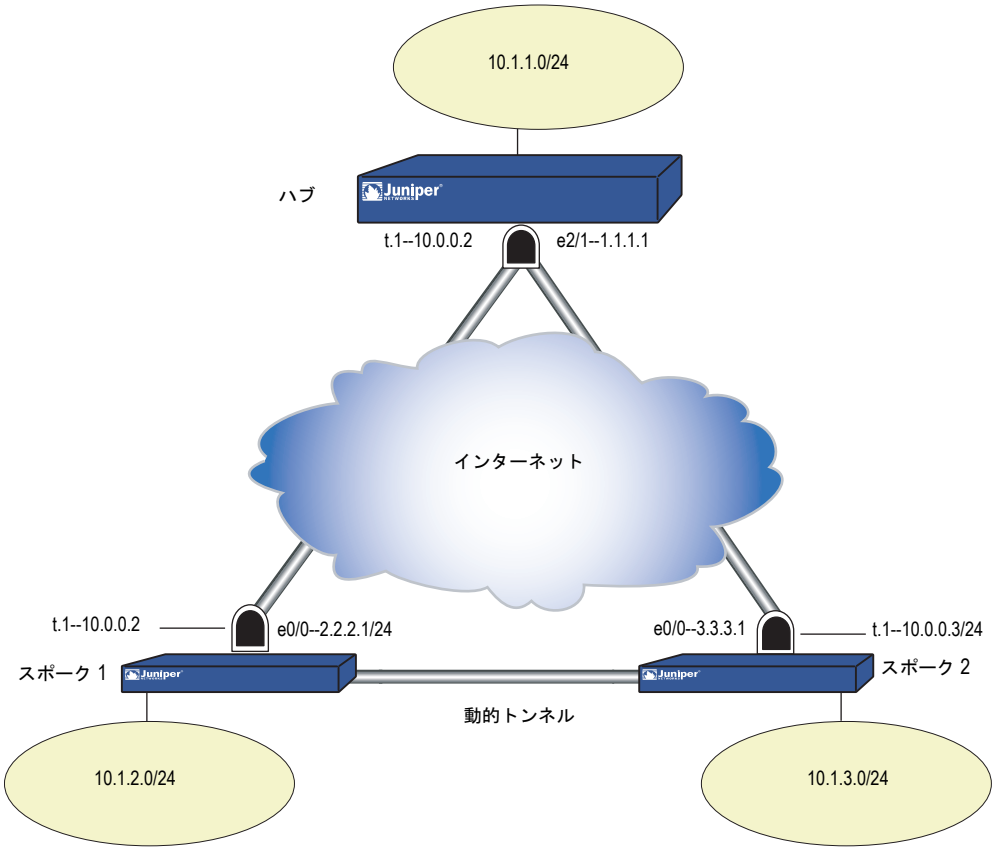
ハブには以下が含まれます。

1. ハブへの静的なトンネルを作成する。
2. ゲートウェイを作成する。
3. VPN ゲートウェイを作成する。
4. ACVPN 動的ゲートウェイを作成する。
5. ACVPN 動的 VPN を作成する。
6. 仮想ルーターで NHRP を使用可能にする。
7. NHS IP アドレスを構成する。
8. ローカルキャッシュを構成する。
9. トンネルインターフェースで NHRP を使用可能にする。
10. ルーティングを構成する。

例

この例では、AC-VPN 構成でネクストホップサーバー（NHS）として動作するように、ハブ内でハブとして動作するハイエンドのセキュリティデバイスを構成します。ここでは、Spoke1 および Spoke2（ローエンドのセキュリティデバイス）がネクストホップクライアント（NHC）になります。デバイス上のインターフェースを構成した後、ハブと各スポークの間の静的な VPN トンネルを構成します。次に、AC-VPN を構成し、接続インターフェースで NHRP を使用可能にします。この例ではオープンショーテストパスファースト（OSPF）ルーティングプロトコルを使用しますが、ScreenOS は AC-VPN について動的ルーティングプロトコルをすべてサポートします。

注 : AC-VPN は動的ホスト制御プロトコル（DHCP）もサポートします。



WebUI (ハブ)

メモ : ハブからスポークおよびスポークからハブまでの静的なゲートウェイおよび静的な VPN を構成した後、AC-VPN ウィザードを使用して、AC-VPN の構成を完了できます。

1. **インターフェース**
   Network > Interfaces > Edit (ethernet2/1): 以下を入力して **Apply** をクリックします。

   Zone Name: Untrust
   IP Address/Netmask: 1.1.1.1/24
   Interface Mode: Route

   Network > Interfaces > Edit (ethernet2/2): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   IP Address/Netmask: 10.1.1.1/24
   Interface Mode: NAT

Network > Interfaces > New (Tunnel IF): 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 1
Zone (VR): Trust-vr
Fixed IP
IP Address/Netmask: 10.0.0.1/24
Unnumbered
Interface:
NHRP Enable: (選択)

2. **スポーク 1 とスポーク 2 へのトンネルの構成**

VPNs > AutoKey Advanced > Gateway > New: IKE ゲートウェイを構成して、**Advanced** をクリックし、セキュリティレベルを設定します。次に、**Return** をクリックして、IKE ゲートウェイ構成ページに戻り、**OK** をクリックします。

Gateway Name: Spoke1
Remote Gateway: (選択)
Static IP Address: (選択) IPv4/v6 Address/Hostname: 2.2.2.1

Preshare key: Juniper
Outgoing interface: (選択) ethernet 2/1
Security Level: Standard

VPNs > AutoKey Advanced > Gateway > New: IKE ゲートウェイを構成して、**Advanced** をクリックし、セキュリティレベルを設定します。次に、**Return** をクリックして、IKE ゲートウェイ構成ページに戻り、**OK** をクリックします。

Gateway Name: Spoke2
Remote Gateway: (選択)
Static IP Address: (選択) IPv4/v6 Address/Hostname: 3.3.3.1

Preshare key: Juniper
Outgoing interface: (選択) ethernet 2/1
Security Level: Standard

3. **VPN スポークのゲートウェイへの構成**

VPNs > AutoKey IKE > New: IKE ゲートウェイを構成して、**Advanced** をクリックし、セキュリティレベルを設定します。次に、**Return** をクリックして、IKE ゲートウェイ構成ページに戻り、**OK** をクリックします。

VPN Name: spoke1
Remote Gateway: (選択) Predefined
(ドロップダウンメニューの定義済みリストから適切なゲートウェイ名を選択します。)
Security Level (選択) Standard
Bind To: (選択) Tunnel Interface
(ドロップダウンメニューから Tunnel.1 を選択します。)

VPNs > AutoKey IKE > New: IKE ゲートウェイを構成して、**Advanced** をクリックし、セキュリティレベルを設定します。次に、**Return** をクリックして、IKE ゲートウェイ構成ページに戻り、**OK** をクリックします。

VPN Name: spoke2
Remote Gateway: (選択) Predefined
(ドロップダウンメニューの定義済みリストから適切なゲートウェイ名を選択します。)

Security Level (選択) Standard
Bind To: (選択) Tunnel Interface
（ドロップダウンメニューから Tunnel.1 を選択します。）

4. ACVPN プロファイルの構成

VPNs > AutoKey Advanced > Gateway > New: IKE ゲートウェイを構成して、**Advanced** をクリックし、セキュリティレベルを設定します。次に、**Return** をクリックして、IKE ゲートウェイ構成ページに戻り、**OK** をクリックします。

Gatewary Name: ac-spoke-gw
ACVPN-Profile: (選択)

Security Level: (選択) Standard

VPNs > AutoKey IKE > New: ACVPN プロファイルを構成して、**Advanced** をクリックし、セキュリティレベルおよび再生保護を設定します。次に、**Return** をクリックして、VPN 構成ページに戻り、**OK** をクリックします。

VPN Name: ac-vpn
ACVPN-Profile: (選択)
Binding to tunnel: (選択) ac-spoke-gw

Security Level: (選択) Standard
Replay Protection: (選択)

5. vrouter の構成

Network > Routing > Virtual Router > (trust-vr) Edit: 以下を入力して **Apply** をクリックします。

Next Hop Resolution Protocol(NHRP) Support
NHRP: (設定) NHRP Setting
NHS Setting: (選択)
Profile: (選択) ACVPN-Profile name

6. トンネルインターフェースで NHRP を使用可能にする

Network > Interfaces > New (TunnelIF): 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 1
NHRP Enable: (選択)

7. ルーティングの構成

Network > Routing > Destination > New: 以下を入力して **Apply** をクリックします。

IP Address/netmask: 0.0.0.0
Gateway (選択)
Gateway IP Address: 1.1.1.2

CLI (ハブ)

```
set interface ethernet2/1 zone Untrust
set interface ethernet2/2 zone Trust
set interface tunnel.1 zone Trust

set interface ethernet2/1 ip 1.1.1.1/24
set interface ethernet2/1 route
set interface ethernet2/2 ip 10.1.1.1/24
```

```
set interface ethernet2/2 nat
set interface tunnel.1 ip 10.0.0.1/24

set ike gateway spoke2 address 3.3.3.1 Main outgoing-interface ethernet2/1
    preshare juniper== sec-level standard
set ike gateway spoke1 address 2.2.2.1 Main outgoing-interface ethernet2/1
    preshare juniper== sec-level standard

set vpn spoke2 gateway spoke2 no-replay tunnel idletime 0 sec-level standard
set vpn spoke2 id 1 bind interface tunnel.1
set vpn spoke1 gateway spoke1 no-replay tunnel idletime 0 sec-level standard
set vpn spoke1 id 2 bind interface tunnel.1

set ike gateway ac-spoke-gw acvpn-profile sec-level standard
set vpn ac-vpn acvpn-profile ac-spoke-gw no-replay tunnel idletime 0 sec-level
    standard

set vrouter trust-vr
set protocol nhrp
set protocol nhrp acvpn-profile ac-vpn
exit
set interface tunnel.1 protocol nhrp enable

set vr trust protocol ospf
set vr trust protocol ospf enable
set vr trust protocol ospf area 10
set interface ethernet2/2 protocol ospf area 0.0.0.10
set interface ethernet2/2 protocol ospf enable
set interface tunnel.1 protocol ospf area 0.0.0.0
set interface tunnel.1 protocol ospf link-type p2mp
set interface tunnel.1 protocol ospf enable

set route 0.0.0.0/0 gateway 1.1.1.2
```

WebUI (スポーク 1)

1. **インターフェース**
   Network > Interfaces > Edit(ethernet0/0): 以下を入力して **Apply** をクリックします。

   Zone Name: Untrust
   IP Address/Netmask: 2.2.2.1/24
   Interface Mode: Route

   Network > Interfaces > Edit (bgroup0): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust

   Network > Interfaces > Edit (ethernet2/2): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   IP Address/Netmask: 10.1.2.1/24
   Interface Mode: NAT

Network > Interfaces > Edit (ethernet2/2) Bind Port を選択し、以下を入力して **Apply:** をクリックします。

ethernet0/2 bgroup0: (選択) Bind to Current Bgroup

Network > Interfaces > New (Tunnel IF): 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 1
Zone (VR): Trust-vr
Fixed IP
IP Address/Netmask: 10.0.0.2/24
NHRP Enable: (選択)

2. ハブへのトンネルの構成

VPNs > AutoKey Advanced > Gateway > New: IKE ゲートウェイを構成して、**Advanced** をクリックし、セキュリティレベルを設定します。次に、**Return** をクリックして、IKE ゲートウェイ構成ページに戻り、**OK** をクリックします。

Gateway Name: hub-gw
Remote Gateway: (選択)
Static IP Address: (選択) IPv4/v6 Address/Hostname: 1.1.1.1

Preshare key: Juniper
Outgoing interface: (選択) ethernet 2/1
Security Level: Standard

3. VPN スポークのゲートウェイへの構成

VPNs > AutoKey IKE > New: IKE ゲートウェイを構成して、**Advanced** をクリックし、セキュリティレベルを設定します。次に、**Return** をクリックして、IKE ゲートウェイ構成ページに戻り、**OK** をクリックします。

VPN Name: vpn-hub
Remote Gateway: (選択) Predefined
（ドロップダウンメニューの定義済みリストから適切なゲートウェイ名を選択します）

Security Level (選択) Standard
Bind To: (選択) Tunnel Interface
（ドロップダウンメニューから Tunnel.1 を選択します）

4. ACVPN-Dynamic の構成

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gatewary Name: ac-hub-gw
ACVPN-Dynamic: (選択)

VPNs > AutoKey > New: 次のように入力してから **OK** をクリックします。

VPN Name: ac-hub-vpn
ACVPN-Dynamic: (選択)
Gateway (選択): ac-hub-gw
Tunnel Towards Hub: (選択) vpn-hub

5. 仮想ルーターの構成

Network > Routing > Virtual Router > (trust-vr) Edit: 以下を入力して **Apply** をクリックします。

Next Hop Resolution Protocol(NHRP) Support
NHRP Enable: (選択)
NHC Setting: (選択)
NHS IP Address: 10.1.1.1

6. トンネルインターフェースで NHRP を使用可能にする

Network > Interfaces > New (TunnelIF): 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 1
NHRP Enable: (選択)

7. ルーティングの構成

Network > Routing > Destination > New: 以下を入力して **Apply** をクリックします。

IP Address/netmask: 0.0.0.0
Gateway (選択)
Gateway IP Address: 2.2.2.2

CLI (スポーク 1)

```
set interface ethernet0/0 zone Untrust
set interface bgroup0 zone Trust
set interface bgroup0 port ethernet0/2
set interface tunnel.1 zone Trust

set interface ethernet0/0 ip 2.2.2.1/24
set interface ethernet0/0 route
set interface bgroup0 ip 10.1.2.1/24
set interface bgroup0 nat
set interface tunnel.1 ip 10.0.0.2/24

set ike gateway hub-gw address 1.1.1.1 Main outgoing-interface ethernet0/0
    preshare juniper== sec-level standard
set vpn vpn-hub id 1 bind interface tunnel.1

set ike gateway ac-hub-gw acvpn-dynamic
set vpn ac-hub-vpn acvpn-dynamic ac-hub-gw vpn-hub

set vrouter trust-vr
set protocol nhrp
set protocol nhrp nhs 10.0.0.1
set protocol nhrp cache 10.1.2.0/24
exit
set interface tunnel.1 protocol nhrp enable

set vr trust protocol ospf
set vr trust protocol ospf enable
set vr trust protocol ospf area 20

set interface bgroup0 protocol ospf area 0.0.0.20
set interface bgroup0 protocol ospf enable
set interface tunnel.1 protocol ospf area 0.0.0.0
set interface tunnel.1 protocol ospf enable
set route 0.0.0.0/0 gateway 2.2.2.2
```

WebUI (スポーク 2)

1. インターフェース

Network > Interfaces > Edit(ethernet0/0): 以下を入力して **Apply** をクリックします。

Zone Name: Untrust
IP Address/Netmask: 3.3.3.1/24
Interface Mode: Route

Network > Interfaces > Edit (bgroup0): 以下を入力して **Apply** をクリックします。

Zone Name: Trust

Network > Interfaces > Edit (ethernet2/2): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
IP Address/Netmask: 10.1.3.1/24
Interface Mode: NAT

Network > Interfaces > Edit (ethernet2/2) Bind Port を選択し、以下を入力して **Apply:** をクリックします。

ethernet0/2 bgroup0: (選択) Bind to Current Bgroup

Network > Interfaces > New (Tunnel IF): 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 1
Zone (VR): Trust-vr
Fixed IP
IP Address/Netmask: 10.0.0.3/24
NHRP Enable: (選択)

2. ハブへのトンネルの構成

VPNs > AutoKey Advanced > Gateway > New: IKE ゲートウェイを構成して、**Advanced** をクリックし、セキュリティレベルを設定します。次に、**Return** をクリックして、IKE ゲートウェイ構成ページに戻り、**OK** をクリックします。

Gateway Name: hub-gw
Remote Gateway: (選択)
Static IP Address: (選択) IPv4/v6 Address/Hostname: 1.1.1.1

Preshare key: Juniper
Outgoing interface: (選択) ethernet 2/1
Security Level: Standard

3. **VPN スポークのゲートウェイへの構成**
   VPNs > AutoKey IKE > New: IKE ゲートウェイを構成して、**Advanced** をクリックし、セキュリティレベルを設定します。次に、**Return** をクリックして、IKE ゲートウェイ構成ページに戻り、**OK** をクリックします。

   VPN Name: vpn-hub
   Remote Gateway: (選択) Predefined
   （ドロップダウンメニューの定義済みリストから適切なゲートウェイ名を選択します。）

   Security Level (選択) Standard
   Bind To: (選択) Tunnel Interface
   （ドロップダウンメニューから Tunnel.1 を選択します。）

4. **ACVPN-Dynamic の構成**
   VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

   Gatewary Name: ac-hub-gw
   ACVPN-Dynamic: (選択)

   VPNs > AutoKey > New: 次のように入力してから **OK** をクリックします。

   VPN Name: ac-hub-vpn
   ACVPN-Dynamic: (選択)
   Gateway (選択): ac-hub-gw
   Tunnel Towards Hub: (選択) vpn-hub

5. **vrouter の構成**
   Network > Routing > Virtual Router > (trust-vr) Edit: 以下を入力して **Apply** をクリックします。

   Next Hop Resolution Protocol(NHRP) Support
   NHRP Enable: (選択)
   NHC Setting: (選択)
   NHS IP Address: 1.1.1.1

6. **トンネルインターフェースで NHRP を使用可能にする**
   Network > Interfaces > New (TunnelIF): 以下を入力して **Apply** をクリックします。

   Tunnel Interface Name: 1
   NHRP Enable: (選択)

7. **ルーティングの構成**
   Network > Routing > Destination > New: 以下を入力して **Apply** をクリックします。

   IP Address/netmask: 0.0.0.0
   Gateway (選択)
   Gateway IP Address: 3.3.3.3

CLI (スポーク 2)

```
set interface ethernet0/0 zone Untrust
set interface bgroup0 zone Trust
set interface bgroup0 port ethernet0/2
set interface tunnel.1 zone Trust

set interface ethernet0/0 ip 3.3.3.1/24
set interface ethernet0/0 route
set interface bgroup0 ip 10.1.3.1/24
set interface bgroup0 nat
set interface tunnel.1 ip 10.0.0.3/24

set ike gateway hub-gw address 1.1.1.1 Main outgoing-interface ethernet0/0
    preshare juniper== sec-level standard
set vpn vpn-hub id 1 bind interface tunnel.1

set ike gateway ac-hub-gw acvpn-dynamic
set vpn ac-hub-vpn acvpn-dynamic ac-hub-gw vpn-hub

set vrouter trust-vr
set protocol nhrp
set protocol nhrp nhs 10.0.0.1
set protocol nhrp cache 10.1.3.0/24
exit

set interface tunnel.1 protocol nhrp enable

set vr trust protocol ospf
set vr trust protocol ospf enable
set vr trust protocol ospf area 30
set interface bgroup0 protocol ospf area 0.0.0.30
set interface bgroup0 protocol ospf enable
set interface tunnel.1 protocol ospf area 0.0.0.0
set interface tunnel.1 protocol ospf enable
set route 0.0.0.0/0 gateway 3.3.3.3
```

索引

数字

3DES 6

A

AES 6
AES (次世代標準暗号)AES 6
AH 3, 6

C

CA 証明書 22, 25
CHAP 207, 211
CRL
    CRL (証明書の取り消しリスト) を参照

D

DES 6
Diffie-Hellman 10
DIP プール
    VPN の NAT 137
    拡張インターフェース 137
DN 182
DNS、L2TP 設定 211

E

ESP 3, 6
    暗号化と認証 52, 58
    暗号化のみ 52
    認証のみ 52

H

HMAC 6
HMAC (ハッシュベースメッセージ認証コード) 6

I

IKE 7, 84, 93, 159
    IKE ID 49, 50, 55, 56
    IKE ID に関するアドバイス 68
    IKE ID、Windows 2000 ..... 220, 227
    共有 IKE ID ユーザー 197–203
    グループ IKE ID ユーザー 182–197
    グループ IKE ID、コンテナ 185
    グループ IKE ID、ワイルドカード 185
    冗長ゲートウェイ 294, 306
    第 1 段階提案、定義済み 9
IKE（続き）
    第 2 段階提案、定義済み 11
    ハートビート 296
    ハローメッセージ 296
    プロキシ ID 11
    リモート ID、ASN1-DN 185
IP (インターネットプロトコル) アドレス
    IP アドレスを参照
IP アドレス
    拡張 137
IP セキュリティ
    IPSec を参照
IPSec
    AH 2, 51, 57
    ESP 2, 51, 57
    L2TP-over-IPSec 4
    SA 2, 8, 11
    SPI 2
    デジタル署名 20
    トランスポートモード 4, 207, 213, 218
    トンネル 2
    トンネルネゴシエーション 8
    トンネルモード 4
セキュリティアソシエーション
    SA を参照

K

keys
    事前共有 159
    手動 116, 122

L

L2TP 205–231
    Hello 信号 216, 222
    RADIUS サーバー 211
    ScreenOS サポート 207
    SecurID サーバー 211
    Windows 2000 で L2TP のみを使用 207
    Windows 2000 トンネル認証 216, 221
    アクセスコネクター
    カプセル化 L2TP 208
    キープアライブ 216, 222
    強制構成 205
    双方向 207
    脱カプセル化 209

L2TP（続き）
デフォルトパラメータ 211
動作モード 208
トンネル 213
任意構成 205
ネットワークサーバー
L2TP-over-IPSec 4, 213, 218
双方向 207
トンネル 213
LAC 205
LAC を参照
NetScreen-Remote 5.0 205
Windows 2000 205
LNS
LNS を参照

M

MD5 6
MIB ファイル、インポート 255
MIP、VPN 138

N

NAT
IPSec および NAT 234
NAT サーバー 234
NAT-dst
VPN 138
NAT-Src
VPN 140
NAT-T 234–242
IKE パケット 237
IPSec パケット 238
NAT の精査 235–236
VPN の障 Q 物 237
イニシエータとレスポンダ 240
キープアライブの周期 240
使用可能 241
NAT-Traversal
NAT-T を参照
NetScreen-Remote
NAT-T オプション 234
VPN AutoKey IKE 159
動的ピア 164, 171
NHTB テーブル 256–261
アドレス計画 259
自動入力 261
手動入力 260
ルートをトンネルにマッピングする 257
Null ルート 83

O

OCSP (オンライン証明書ステータスプロトコル) 34
レスポンダ 34

P

PAP 207, 211
PFS 11, 51, 57
PKI (公開鍵基盤) 22
PPP 206

R

RADIUS
L2TP 211

S

SA 8, 11
パケットフローのチェック 63
SCEP (簡易認証送受信プロトコル) 30
SecurID
L2TP 211
SHA-1 6
SNMP
MIB ファイル、インポート 255
VPN 監視 255

T

TCP
SYN フラグチェック 300

U

UDP
NAT-T のカプセル化 234
チェックサム 239

V

Verisign 34
VPN
AutoKey IKE 7
Diffie-Hellman グループ 10
Diffie-Hellman の鍵交換 10
FQDN エイリアス 128
MIP 138
NAT-dst 138
NAT-Src 140
SA 8
VPN 監視および再入力 244
VPN グループ 294
アグレッシブモード 10
暗号オプション 46, 59
オーバーラップしているアドレスの NAT ... 137, 148
ゲートウェイの FQDN 127–137
構成のヒント 66–68
再生保護 12
冗長グループ、復旧手順 298
冗長ゲートウェイ 294–306
トランスポートモード 4

VPN（続き）
トンネルインターフェース 1 つあたりに複数のトンネル 256–292
トンネルの常時作動 244
パケットフロー 61–66
フェーズ 1 9
フェーズ 2 11
プロキシ ID、一致 67
メインモード 9
両方向のポリシー 123
ルートベースとポリシーベース 59
VPN AutoKey IKE 7
管理 7
VPN 監視
ICMP エコー要求 255
SNMP 255
宛先アドレス 245–248
宛先アドレス、XAuth 246
再入力オプション 244, 261
出力インターフェース 245–248
状態変化 243, 247
ポリシー 246
ルーティング設計 68

W

WINS
L2TP 設定 211

X

XAuth
VPN 監視 246

あ

アグレッシブモード 10
暗号オプション 46–59
ESP 52, 58
トンネルモード 58
IKE ID 49, 50, 55, 56
IPSec プロトコル 51, 57
PFS 51, 57
暗号化アルゴリズム 49–55, 58
鍵方式 47
再生防止チェック 50, 57
サイトツーサイト 46–53
サイトツーサイト VPN の推奨オプション 53
証明書のビット長 48, 54
ダイヤルアップ 53–59
ダイヤルアップ VPN の推奨オプション 59
トランスポートモード 58
認証アルゴリズム 49, 52, 55, 59
認証タイプ 48, 54
フェーズ 1 モード 47, 54
暗号化
アルゴリズム 6, 49, 52–58

い

インターネット鍵交換
IKE を参照
インターフェース
null 83
拡張 137

か

完全転送機密保持
PFS を参照

き

キープアライブ
L2TP 216
周期、NAT-T 240

く

グループ IKE ID
事前共有鍵 197
証明書 191
事前共有鍵 191
証明書 182

こ

公開鍵基盤
PKI を参照
公開鍵 / 秘密鍵ペア 23
攻撃
再生 12
コンテナ 185

さ

再生防止チェック 50, 57
再生保護 12
再入力オプション、VPN 監視 244

し

識別名（DN） 182
事前共有鍵 7, 159
手動鍵 116, 122
管理 7
冗長ゲートウェイ 294–306
SYN フラグチェック 300
復旧手順 298
証明書 7
CA 22, 25
E メール経由 25
CRL のローディング 23
取り消し 24, 34
要求 25
ローカル 25
ローディング 28

証明書の取り消しリスト
(CRL: Certificate Revocation List) 23, 34
ローディング 23

せ

セキュアハッシュアルゴリズム -1
SHA-1 を参照
セキュリティペイロードのカプセル化
ESP を参照

ち

チャレンジハンドシェイク式認証プロトコル
CHAP を参照

て

提案
フェーズ 1 ..... 9, 66
フェーズ 2 ..... 11, 66
データ暗号化規格 (DES) 6
デジタル署名 20

と

トランスポートモード 4, 207, 213, 218
トリプル DES
3DES を参照
トンネルモード 4
トンネル
特定の 243

に

認証
アルゴリズム 6, 49, 52, 55, 59
認証ヘッダー (AH) 6

は

パケットフロー
アウトバウンド VPN 63
インバウンド VPN 63–65
ポリシーベース VPN 65–66
ルートベース VPN 61–65
パスワード認証プロトコル
PAP を参照

ふ

フェーズ 1 9
提案 9
定義済み 9
フェーズ 2 11
提案 11
定義済み 11
プライベート 137
プロキシ ID 11
一致 60, 67
プロトコル
CHAP 207
PAP 207
PPP 206

ほ

ポイントツーポイントプロトコル
PPP を参照
ポリシー
両方向 VPN 123
ポリシーベース VPN 59

め

メインモード 9
メッセージダイジェストバージョン 5 (MD5) 6

も

モード
Tunnel 4, 58
L2TP 動作 208
Main 9
アグレッシブ 10
トランスポート 4, 58, 207, 213, 218
フェーズ 1 暗号 47, 54
モジュラス 10

ゆ

ユーザー
共有 IKE ID 197–203
グループ IKE ID 182–197

る

ルート
null 83
ルートベース VPN 59–61

れ

レイヤー 2 トンネリングプロトコル
L2TP を参照

ろ

ローカル証明書 25

わ

ワイルドカード 185



概念と用例
ScreenOS リファレンス ガイド

第 6 部 :
音声 IP 化

リリース 6.0.0、改訂 02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

品番 : 530-017772-01-JP, 改訂 02

Copyright Notice

Copyright © 2007 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

目次

本編について **vii**

ドキュメントの規則 vii
Web ユーザーインターフェースの規則 viii
コマンドラインインターフェースの規則 viii
ネーミング規則および文字タイプ ix
説明図の規則 x
技術ドキュメントおよびテクニカルサポート xi

第 1 章 H.323 アプリケーションレイヤーゲートウェイ **1**

概要 1
例 2
例 : Trust ゾーンのゲートキーパー 2
例 : Untrust ゾーンのゲートキーパー 3
例 : NAT での発信コール 5
例 : NAT での受信コール 8
例 : NAT での Untrust ゾーン内のゲートキーパー 10

第 2 章 セッション起動プロトコル アプリケーション レイヤーゲートウェイ **13**

概要 13
SIP 要求方法 14
SIP 応答のクラス 16
SIP アプリケーションレイヤーゲートウェイ 17
セッション記述プロトコルのセッション 18
ピンホールの作成 19
セッション無活動タイムアウト 21
SIP 攻撃保護 21
例 : SIP 保護拒否 22
例 : シグナリングおよびメディア無活動タイムアウト 22
例 : UDP フラッディング保護 22
例 : SIP 接続の最大数 23

ネットワークアドレス変換での SIP 23
出力コール 24
受信コール 24
転送されたコール 25
コールの終了 25
コールの Re-INVITE メッセージ 25
コールセッションタイマー 26
コールのキャンセル 26
フォーク 26
SIP メッセージ 26
SIP ヘッダー 27
SIP ボディ 28
SIP NAT の手順 29
例 31
SIP Registrar を使用する受信 SIP コールのサポート 32
例 : 受信コール (インターフェース DIP) 33
例 : 受信コール (DIP プール) 36
例 : MIP での受信コール 38
例 : プライベートゾーン内のプロキシ 40
例 : パブリックゾーン内のプロキシ 43
例 : 3 つのゾーン、DMZ 内のプロキシ 45
例 : Untrust ゾーン内 48
例 : Trust ゾーン内 52
例 : フルメッシュ VPN での SIP 54
VoIP サービスの帯域幅管理 63

第 3 章 メディアゲートウェイ制御プロトコルのアプリケーションレイヤーゲートウェイ 67

概要 67
MGCP セキュリティ 68
MGCP について 69
MGCP 内のエンティティ 69
端点 69
接続 69
コール 69
コールエージェント 70
コマンド 70
応答コード 73
例 74
加入者の自宅におけるメディアゲートウェイ - ISP でのコールエージェント 74
ISP ホストサービス 76

第 4 章 スキニィクライアント制御プロトコルのアプリケーションレイヤーゲートウェイ 81

概要 81
SCCP セキュリティ 82

SCCP について 82
SCCP のコンポーネント 83
SCCP クライアント 83
コールマネージャ 83
クラスタ 83
SCCP トランザクション 84
クライアントの初期化 84
クライアント登録 84
コールの設定 85
メディアの設定 85
SCCP 制御メッセージと RTP フロー 86
SCCP メッセージ 87
例 88
例 : Trust ゾーンのコールマネージャ /TFTP サーバー 88
例 : Untrust ゾーン内のコールマネージャ /TFTP サーバー 90
例 : 3 ゾーン、DMZ 内のコールマネージャ /TFTP サーバー 92
例 : ゾーン内、Trust ゾーンのコールマネージャ /TFTP サーバー ... 96
例 : ゾーン内、Untrust ゾーンのコールマネージャ /TFTP サーバー 99
例 : フルメッシュ VPN での SCCP 102

索引 ..... IX-I

本編について

*第 6 部 : 音声 IP 化*では、サポートされる VoIP ALG (アプリケーションレイヤーゲートウェイ) について説明し、次の章が含まれています。

- 第 1 章「H.323 アプリケーションレイヤー ゲートウェイ」では、H.323 プロトコルについて解説し、一般的なシナリオを例示します。
- 第 2 章「セッション起動プロトコル アプリケーション レイヤーゲートウェイ」では、SIP（セッション起動プロトコル）について解説し、SIP ALG がルートモードおよび NAT（ネットワークアドレス変換）モードのコールを処理する方法について説明します。SIP のアーキテクチャの要約に続いて、一般的なシナリオを例示します。
- 第 3 章「メディアゲートウェイ制御プロトコルの アプリケーションレイヤーゲートウェイ」では、MGCP (メディアゲートウェイ制御プロトコル) ALG の概要を説明し、実装できるファイアウォールセキュリティ機能のリストを示します。MGCP のアーキテクチャの要約に続いて、一般的なシナリオを例示します。
- 第 4 章「スキニィクライアント制御プロトコルの アプリケーションレイヤーゲートウェイ」では、SCCP（スキニィクライアント制御プロトコル）ALG の概要を説明し、実装できるファイアウォールセキュリティ機能のリストを示します。SCCP のアーキテクチャの要約に続いて、一般的なシナリオを例示します。

ドキュメントの規則

このドキュメントは、次のセクションで説明されている規則を使用しています。

- 展 eb ユーザーインターフェースの規則 ,î ページ viii
- 塔 R マンドラインインターフェースの規則 ,î ページ viii
- ix ページの「ネーミング規則および文字タイプ」
- x ページの「説明図の規則」

Web ユーザーインターフェースの規則

WebUI（Web ユーザーインターフェース）では、各作業の操作指示は、操作手順と構成設定値に分かれています。構成設定を入力できる WebUI ページを開くには、画面の左側にあるナビゲーション ツリーのメニュー項目をクリックして、そのページに移動します。先へ進むと、ナビゲーション パスが画面の上部に表示されます。各ページは角括弧で分離されています。

WebUI のパスおよびアドレスを定義するためのパラメータは、以下のとおりです。

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.2.2.5/32
Zone: Untrust

構成設定のオンラインヘルプを開くには、画面の左上にある疑問符（?）をクリックします。

ナビゲーションツリーにも、Help > Config Guide 構成ページがあり、セキュリティポリシーおよび IPSec （インターネットプロトコルセキュリティ）の構成に役立ちます。ドロップダウンメニューからオプションを選択して、そのページの指示に従います。構成設定のオンラインヘルプを開くには、左上にある **?** 文字をクリックします。

コマンドラインインターフェースの規則

次の規則は、例とテキストにおいて、コマンドラインインターフェース（CLI）コマンドの構文を示すために使用されます。

例においては、次のように使用されます。

- 角括弧 [ ] 内にあるものはすべてオプションです。
- 中括弧 { } 内にあるものはすべて必須です。
- 選択肢が複数ある場合、各選択肢はパイプ (|) で区切られています。例えば、次のように表示されます。

  set interface { ethernet1 | ethernet2 | ethernet3 } manage

- 変数は*斜体*で表示されます。

  set admin user *name1* password *xyz*

テキストにおいては、コマンドは**太字**で、変数は*斜体*で表示されます。

注： キーワード入力時には、単語を間違いなく識別できる数の文字を入力すれば十分です。**set admin user wheezer j12fmt54** というコマンドを入力する際には、**set adm u whee j12fmt54** と入力するだけで十分です。ただし、本編に記載されたコマンドはすべて本来の形式で記載されています。

ネーミング規則および文字タイプ

ScreenOS はオブジェクトの名前 (アドレス、管理ユーザー、認証サーバー、IKE ゲートウェイ、仮想システム、VPN トンネルおよびゾーンなど、ScreenOS 構成に定義されているもの) に関して、次の規則に従います。

- 名前文字列に 1 つまたは複数のスペースが含まれる場合、文字列全体を二重引用符で囲む必要があります。例 :

  set address trust “local LAN” 10.1.1.0/24

- 二重引用符で囲まれた文字列の先頭または末尾のスペースを取り除きます。たとえば、**「 local LAN 」**は**「local LAN」**となります。

- 連続した複数のスペースは、一つのスペースとして扱われます。

- CLI キーワードの多くはケースセンシティブではありませんが、名前文字列はケースセンシティブです。たとえば、**「local LAN」**は**「local lan」**とは異なります。

ScreenOS は、次の文字タイプをサポートします。

- 1 バイト文字セット (SBCS) およびマルチバイト文字セット (MBCS)。SBCS の例に、ASCII、欧州言語、およびヘブライ語があります。2 バイト文字セット (DBCS) とも呼ばれる MBCS の例に、中国語、韓国語、および日本語があります。

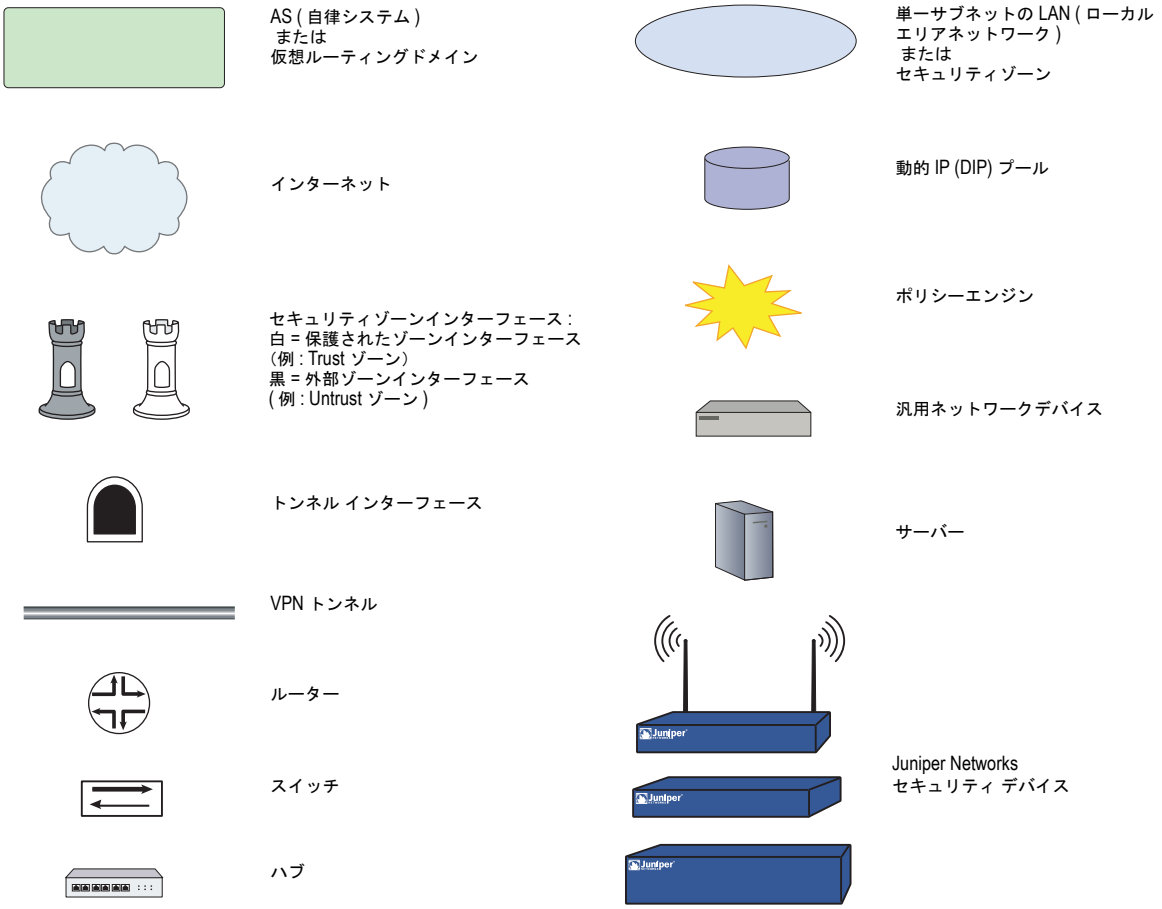
- ASCII 文字の 32（16 進数の 0x20）から 255（0xff)。ただし二重引用符 (“) は、スペースを含む名前文字列の先頭と末尾を示す特殊な意味をもつため、例外とします。

注 : コンソール接続では、SBCS のみがサポートされます。ご利用のブラウザがサポートする文字セットに応じて、WebUI は SBCS および MBCS の両方をサポートします。

説明図の規則

次の図は、本編を通して説明図に使用されている画像の基本的なものです。

図 1: 説明図の画像



技術ドキュメントおよびテクニカルサポート

Juniper Networks 製品のいずれかの技術ドキュメントを入手するには、www.juniper.net/techpubs/ をご覧になってください。

テクニカルサポートについては、http://www.juniper.net/customers/support/ にある Case Manager を使って事例サポートを開くか、1-888-314-JTAC (米国内) か 1-408-745-9500 (その他の国) までお問い合わせください。

本書に間違いや欠落があった場合は、techpubs-comments@juniper.net までお知らせください。

第 1 章

H.323 アプリケーションレイヤーゲートウェイ

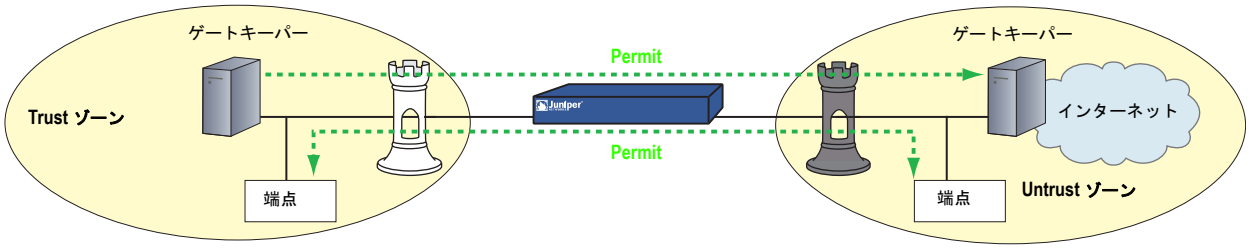
本章では、H.323 プロトコルについて説明し、Juniper Networks セキュリティデバイスの H.323 ALG（アプリケーションレイヤーゲートウェイ）を設定する方法を例で示します。本章のセクションは、以下のようになります。

- 本ページの 「概要」
- 2 ページの「例」

概要

H.323 ALG（アプリケーションレイヤーゲートウェイ）を使用すると、IP 電話やマルチメディアデバイスなどのターミナルホスト間で、セキュア VoIP（音声 IP 化）通信が可能になります。そのような電話システムでは、ゲートキーパーデバイスが VoIP コールのコール登録、アクセス許可、およびコール状態を管理します。ゲートキーパーは、2 つの異なるゾーンまたは同じゾーンで存在可能です。

図 2: H.323 プロトコル



注： 本章の図では例示を目的として IP 電話を使用していますが、NetMeeting マルチメディアデバイスなどの VoIP プロトコルを使用するホストも構成できます。

例

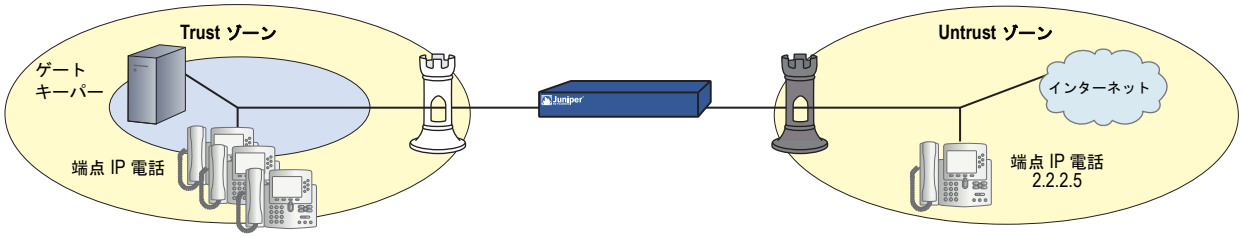
このセクションには、以下の構成例があります。

- 本ページの 「例 : Trust ゾーンのゲートキーパー」
- 3 ページの「例 : Untrust ゾーンのゲートキーパー」
- 5 ページの「例 : NAT での発信コール」
- 8 ページの「例 : NAT での受信コール」
- 10 ページの「例 : NAT での Untrust ゾーン内のゲートキーパー」

例: Trust ゾーンのゲートキーパー

次の例では、Trust ゾーン内の IP 電話ホストやゲートキーパーと、Untrust ゾーン内の IP 電話アドレス 2.2.2.5 の IP 電話との間の通過を H.323 トラフィックに許可するように、2 つのポリシーを設定します。この例では、セキュリティデバイスは、透過モードあるいはルートモードのいずれかです。Trust と Untrust セキュリティゾーンはともに、trust-vr ルーティングドメインに存在します。

図 3: H.323 Trust ゾーンのゲートキーパー



WebUI

1. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: IP_Phone
   IP Address/Domain Name:
   IP/Netmask: (選択), 2.2.2.5/32
   Zone: Untrust

2. **ポリシー**
   Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Any
   Destination Address:
   Address Book Entry: (選択), IP_Phone
   Service: H.323
   Action: Permit

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), IP_Phone
Destination Address:
Address Book Entry: (選択), Any
Service: H.323
Action: Permit

CLI

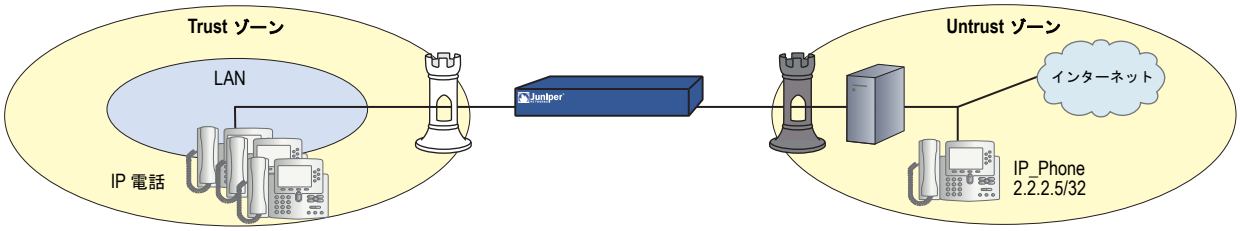
1. **アドレス**
   set address untrust IP_Phone 2.2.2.5/32
2. **ポリシー**
   set policy from trust to untrust any IP_Phone h.323 permit
   set policy from untrust to trust IP_Phone any h.323 permit
   save

例 : Untrust ゾーンのゲートキーパー

透過モードとルートモードにはいかなる種類のアドレスマッピングも必要ないため、Untrust ゾーン内のゲートキーパー用セキュリティデバイス構成は通常、Trust ゾーン内のゲートキーパー用構成と完全に一致します。

次の例では、Trust ゾーン内の IP 電話ホストと、Untrust ゾーン内の IP アドレス 2.2.2.5 にある IP 電話 (やゲートキーパー) との間の通過を H.323 トラフィックに許可するように、2 つのポリシーを設定します。デバイスは、透過モードあるいはルートモードで動作が可能です。Trust と Untrust セキュリティゾーンはともに、trust-vr ルーティングドメインに存在します。

図 4: H.323 Untrust ゾーンのゲートキーパー



WebUI

1. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: IP_Phone
   IP Address/Domain Name:
   IP/Netmask: (選択), 2.2.2.5/32
   Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Gatekeeper
IP Address/Domain Name:
IP/Netmask: (選択), 2.2.2.10/32
Zone: Untrust

2. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

ソースアドレス :
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), IP_Phone
Service: H.323
Action: Permit

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), IP_Phone
Destination Address:
Address Book Entry: (選択), Any
Service: H.323
Action: Permit

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), Gatekeeper
Service: H.323
Action: Permit

CLI

1. アドレス

```
set address untrust IP_Phone 2.2.2.5/32
set address untrust gatekeeper 2.2.2.10/32
```

2. ポリシー

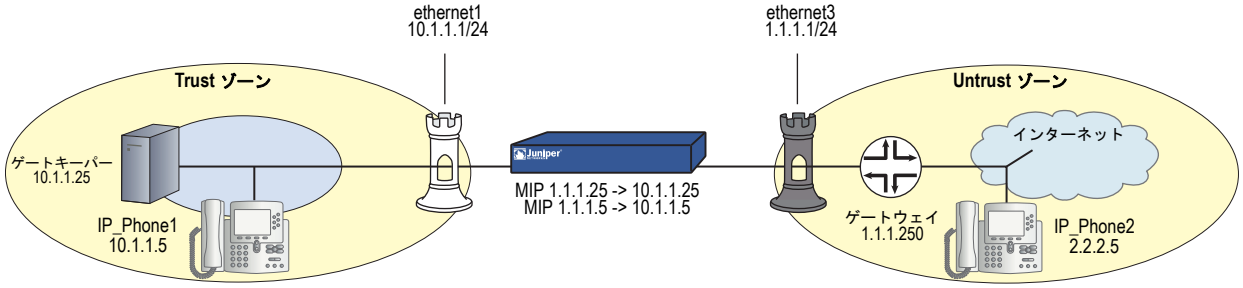
```
set policy from trust to untrust any IP_Phone h.323 permit
set policy from trust to untrust any gatekeeper h.323 permit
set policy from untrust to trust IP_Phone any h.323 permit
set policy from untrust to trust gatekeeper any h.323 permit
save
```

例 : NAT での発信コール

セキュリティデバイスが NAT (ネットワークアドレス変換機能) モードを使用する場合、ゲートキーパーあるいは端点デバイスは、Trust ゾーンにある場合はプライベートアドレスを所有し、Untrust ゾーンにある場合はパブリックアドレスを所有します。セキュリティデバイスを NAT モードに設定する場合、プライベートアドレス付きの入ってくるトラフィックを受信する必要がある各デバイスに、パブリック IP アドレスをマッピングする必要があります。

この例では、Trust ゾーンのデバイスとして、端点ホスト (10.1.1.5) とゲートキーパーデバイス (10.1.1.25) があります。IP_Phone2 (2.2.2.5) は Untrust ゾーンにあります。Trust ゾーンの端点ホスト IP_ Phone1 およびゲートキーパーと、Untrust ゾーンの端点ホスト IP_Phone2 との間のトラフィックを許可するように、セキュリティデバイスを構成します。Trust と Untrust セキュリティゾーンはともに、trust-vr ルーティングドメインに存在します。

図 5: ネットワークアドレス変換 - 発信コール



WebUI

1. **インターフェース**

   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように選択してから **OK** をクリックします。
   Interface mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. **アドレス**

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: IP_Phone1
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.5/32
   Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Gatekeeper
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.25/32
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: IP_Phone2
IP Address/Domain Name:
IP/Netmask: (選択), 2.2.2.5/32
Zone: Untrust

3. マップ IP アドレス

Network > Interfaces > Edit (for ethernet3) > MIP > New: 次のように入力してから **OK** をクリックします。

Mapped IP: 1.1.1.5
Netmask: 255.255.255.255
Host IP Address: 10.1.1.5
Host Virtual Router Name: trust-vr

Network > Interfaces > Edit (for ethernet3) > MIP > New: 次のように入力してから **OK** をクリックします。

Mapped IP: 1.1.1.25
Netmask: 255.255.255.255
Host IP Address: 10.1.1.25
Host Virtual Router Name: trust-vr

4. ルート

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

5. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), IP_Phone1
Destination Address:
Address Book Entry: (選択), IP_Phone2
Service: H.323
Action: Permit

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Gatekeeper

Destination Address:
Address Book Entry: (選択), IP_Phone2
Service: H.323
Action: Permit

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), IP_Phone2
Destination Address:
Address Book Entry: (選択), MIP(1.1.1.5)
Service: H.323
Action: Permit

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), IP_Phone2
Destination Address:
Address Book Entry: (選択), MIP(1.1.1.25)
Service: H.323
Action: Permit

CLI

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **アドレス**
   set address trust IP_Phone1 10.1.1.5/32
   set address trust gatekeeper 10.1.1.25/32
   set address untrust IP_Phone2 2.2.2.5/32

3. **マップ IP アドレス**
   set interface ethernet3 mip 1.1.1.5 host 10.1.1.5
   set interface ethernet3 mip 1.1.1.25 host 10.1.1.25

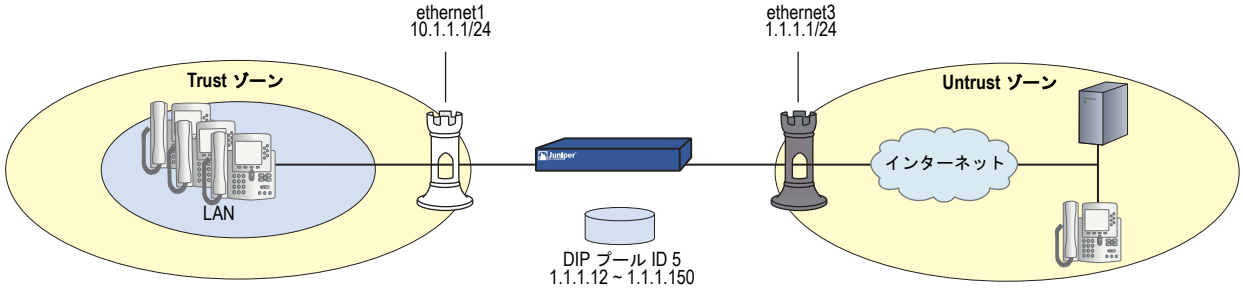
4. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

5. **ポリシー**
   set policy from trust to untrust IP_Phone1 IP_Phone2 h.323 permit
   set policy from trust to untrust gatekeeper IP_Phone2 h.323 permit
   set policy from untrust to trust IP_Phone2 mip(1.1.1.5) h.323 permit
   set policy from untrust to trust IP_Phone2 mip (1.1.1.25) h.323 permit
   save

例 : NAT での受信コール

この例では、セキュリティデバイスを構成して、NAT 境界を通過する受信コールを承認します。承認するには、動的に割り当てる宛先アドレスの DIP アドレスプールを作成します。通常の構成はこの例とは違って、DIP プールがソースアドレスのみを提供する構成となっています。

図 6: ネットワークアドレス変換 - 受信コール



DIP プール名はユーザー定義の DIP(*id_num*) です。DIP プールがインターフェース IP アドレスと同じアドレスを使用する場合には DIP(*interface*) となります。ポリシーにある宛先アドレスなどのアドレスエントリは、H.323、SIP、その他 VoIP (音声 IP 化) プロトコルなどのサービスと一緒に使用すると、受信コールをサポートできます。

以下の例では、H.323 VoIP 構成内で DIP を使用します。キーワード 妬 ncomingE は、グローバルゾーンに DIP とインターフェースアドレスを追加するようデバイスに指示します。

WebUI

1. **インターフェース**

   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. **受信 NAT での DIP**

   Network > Interfaces > Edit (ethernet3) > DIP > New: 次のように入力してから **OK** をクリックします。

   ID: 5
   IP Address Range: (選択), 1.1.1.12 ~ 1.1.1.150
   Port Translation: (選択)
   In the same subnet as the interface IP or its secondary IPs: (選択)
   Incoming NAT: (選択)

3. **アドレス**
   Policy > Policy Elements > Addresses > List > New (Trust): 次のように入力してから **OK** をクリックします。

   Address Name: IP_Phone1
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.5/24
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New (Untrust): 次のように入力してから **OK** をクリックします。

   Address Name: IP_Phone2
   IP Address/Domain Name:
   IP/Netmask: (選択), 2.2.2.5/32
   Zone: Untrust

4. **ポリシー**
   Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), IP_Phone1
   Destination Address:
   Address Book Entry: (選択), Any
   Service: H.323
   Action: Permit

   Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), IP_Phone2
   Destination Address:
   Address Book Entry: (選択), DIP(5)
   Service: H.323
   Action: Permit

CLI

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **受信 NAT での DIP**
   set interface ethernet3 dip 5 1.1.1.12 1.1.1.150 incoming

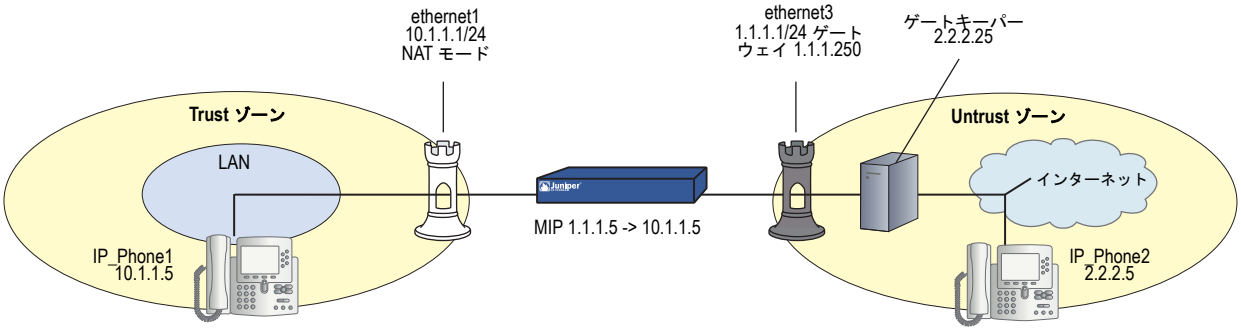
3. **アドレス**
   set address trust IP_Phones1 10.1.1.5/24
   set address untrust IP_Phone2 2.2.2.5/32

4. **ポリシー**
   set policy from trust to untrust IP_Phones1 any h.323 nat src dip 5 permit
   set policy from untrust to trust IP_Phone2 dip(5) h.323 permit
   save

例 : NAT での Untrust ゾーン内のゲートキーパー

この例では、ゲートキーパーデバイス (2.2.2.25) とホスト IP_Phone2 (2.2.2.5) は Untrust ゾーンに存在し、ホスト IP_Phone1 (10.1.1.5) は Trust ゾーンに存在します。セキュリティデバイスを構成して、Trust ゾーン内のホスト IP_Phone1 と Untrust ゾーン内のホスト IP_Phone2 (やゲートキーパー) との間のトラフィックを許可します。Trust と Untrust セキュリティゾーンはともに、trust-vr ルーティングドメインに存在します。

図 7: Untrust ゾーンのゲートキーパー



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: IP_Phone1
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.5/32
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: Gatekeeper
   IP Address/Domain Name:
   IP/Netmask: (選択), 2.2.2.25/32
   Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: IP_Phone2
IP Address/Domain Name:
IP/Netmask: (選択), 2.2.2.5/32
Zone: Untrust

3. マップ IP アドレス

Network > Interfaces > Edit (for ethernet3) > MIP > New: 次のように入力してから **OK** をクリックします。

Mapped IP: 1.1.1.5
Netmask: 255.255.255.255
Host IP Address: 10.1.1.5

4. ルート

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

5. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), IP_Phone1
Destination Address:
Address Book Entry: (選択), IP_Phone2
Service: H.323
Action: Permit

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), IP_Phone1
Destination Address:
Address Book Entry: (選択), Gatekeeper
Service: H.323
Action: Permit

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), IP_Phone2
Destination Address:
Address Book Entry: (選択), MIP(1.1.1.5)
Service: H.323
Action: Permit

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Gatekeeper
Destination Address:
Address Book Entry: (選択), MIP(1.1.1.5)
Service: H.323
Action: Permit

CLI

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **アドレス**
   set address trust IP_Phone1 10.1.1.5/32
   set address untrust gatekeeper 2.2.2.25/32
   set address untrust IP_Phone2 2.2.2.5/32

3. **マップ IP アドレス**
   set interface ethernet3 mip 1.1.1.5 host 10.1.1.5

4. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

5. **ポリシー**
   set policy from trust to untrust IP_Phone1 IP_Phone2 h.323 permit
   set policy from trust to untrust IP_Phone1 gatekeeper h.323 permit
   set policy from untrust to trust IP_Phone2 mip(1.1.1.5) h.323 permit
   set policy from untrust to trust gatekeeper mip(1.1.1.5) h.323 permit
   save

第 2 章

セッション起動プロトコル アプリケーション レイヤーゲートウェイ

本章では、SIP (セッション起動プロトコル) ALG (アプリケーションレイヤーゲートウェイ) について説明し、次のセクションが含まれています。

- 13 ページの「概要」
- 23 ページの「ネットワークアドレス変換での SIP」
- 31 ページの「例」

概要

SIP (セッション起動プロトコル) とは、インターネットを介してマルチメディアセッションを開始、変更、および終了するための IETF (Internet Engineering Task Force、インターネット技術標準化タスクフォース) 規格のプロトコルです。そのようなセッションには、ネットワーク環境でのインスタントメッセージおよびアプリケーションレベルモビリティなどの機能を備えた会議やテレフォニー、マルチメディアなどがあると考えられます。

Juniper Networks セキュリティデバイスは SIP をサービスとしてサポートし SIP トラフィックを選別できるため、構成したポリシーに基づいて SIP トラフィックの許可および拒否を行うことができます。SIP は ScreenOS に定義済みのサービスで、宛先ポートとしてポート 5060 を使用します。

SIP の基本機能は、セッション記述情報の配布、およびセッション中におけるセッションのパラメータのネゴシエーションと変更を行うことです。SIP はマルチメディアセッションを終了するためにも使用されます。

セッション記述情報は INVITE メッセージと ACK メッセージに含められ、たとえば音声やビデオなど、マルチメディアの種類を示します。SIP はさまざまな記述プロトコルを使用してセッションを記述できますが、Juniper Networks SIP ALG では SDP（セッション記述プロトコル）のみがサポートされます。

SDP は、システムがマルチメディアセッションに参加するのに使用する情報を提供します。SDP には、IP アドレス、ポート番号、時刻、日付などのような情報が含まれると考えられます。SDP ヘッダーの IP アドレスとポート番号（それぞれ、“c=”と “m=”フィールド）は、クライアントがマルチメディアスト

リームを受信するときに使用するアドレスとポートであり、SIP 要求が発生する IP アドレスとポート番号ではないことに注意してください（ただし、一致する場合もあります）。詳細は 18 ページの「セッション記述プロトコルのセッション」を参照してください。

SIP メッセージは、クライアントからサーバーへ送られる要求、およびその要求に対して、セッション (またはコール) を確立する目的でサーバーからクライアントへ送られる応答からなります。ユーザーエージェント（UA）はコールの端点で動作するアプリケーションで、ユーザーに代わって SIP 要求を送信するユーザーエージェントクライアント（UAC）と、応答に注意を向け、応答が到着した際にユーザーに通知するユーザーエージェントサーバー（UAS）との 2 部分からなります。UA の例としては、SIP プロキシサーバーや電話があります。

SIP 要求方法

SIP トランザクションモデルには、いくつかの要求メッセージや応答メッセージが含まれており、各メッセージにはその要求の目的を示す *method* フィールドが含まれています。ScreenOS は、以下のメソッドタイプと応答コードをサポートします。

- INVITE - ユーザーが他のユーザーにセッションへの参加を勧誘するために、INVITE 要求を送信します。INVITE 要求のボディには、セッションの記述が含まれる場合があります。NAT モードでは、ヘッダーフィールド Via:、From:、To:、Call-ID:、Contact:、Route:、および Record-Route: にある IP アドレスが、27 ページの表 2 で示すように変更されます。

- ACK - INVITE の作成元のユーザーは ACK 要求を送信することで、INVITE 要求に対する最終応答を受信したことを確認します。元の INVITE 要求にセッション記述が含まれない場合は、ACK 要求にセッション要求が含まれていることが必要です。NAT モードでは、ヘッダーフィールド Via:、From:、To:、Call-ID:、Contact:、Route:、および Record-Route: にある IP アドレスが、27 ページの表 2 で示すように変更されます。

- OPTIONS - ユーザーエージェント (UA) が使用して、SIP プロキシの機能についての情報を取得します。サーバーは、自身がサポートするメソッド、セッション記述プロトコル、およびメッセージ符号化についての情報とともに応答します。NAT モードでは、OPTIONS 要求が NAT 外の UA から NAT 内のプロキシに送信されると、SIP ALG が、Request-URL にあるアドレスと To: フィールドにある IP アドレスを、内部クライアントの適切な IP アドレスに変換します。UA が NAT 内にあり、プロキシが NAT 外にある場合には、SIP ALG は、From:、Via:、および Call-ID: フィールドを 27 ページの表 2 で示すように変換します。

- BYE - ユーザーが BYE 要求を送信し、セッションを廃棄します。ユーザーのいずれか 1 人からの BYE 要求によって、セッションが自動的に終了します。NAT モードでは、ヘッダーフィールド Via:、From:、To:、Call-ID:、Contact:、Route:、および Record-Route: にある IP アドレスが、27 ページの表 2 で示すように変更されます。

- CANCEL - ユーザーが CANCEL 要求を送信し、承認待ちの INVITE 要求をキャンセルします。INVITE を処理する SIP サーバーが CANCEL を受信する前に INVITE に対する最終応答を送信した場合、CANCEL 要求は無効となります。NAT モードでは、ヘッダーフィールド Via:、From:、To:、Call-ID:、Contact:、Route:、および Record-Route: にある IP アドレスが、27 ページの表 2 で示すように変更されます。

- REGISTER - ユーザーは REGISTER 要求を SIP *registrar* サーバーに送信し、現在の場所を通知します。SIP registrar サーバーは REGISTER 要求にある受信したすべての情報を記録し、ユーザーを配置しようとする任意の SIP サーバーでこの情報が利用できるようにします。NAT モードでは、REGISTER 要求は以下のとおりに処理されます。
  - REGISTER が外部のクライアントから内部の registrar に要求します。SIP ALG は、内部への REGISTER 要求を受信すると、Request-URL に IP アドレスがあればその IP アドレスを変換します。受信 REGISTER メッセージは、MIP アドレスまたは VIP アドレスのみに許可されます。外部へ発信する応答には変換は必要ありません。
  - 内部クライアントから外部 registrar への REGISTER 要求 - SIP ALG は外部への REGISTER 要求を受信すると、ヘッダーフィールド To:、From:、Via:、Call-ID:、および Contact: Via:、Contact:、および Record-Route: ヘッダーフィールドにある情報に基づいてネゴシエートされたポート番号です。受信する応答には、逆方向の変換が実行されます。
- Info - コールのシグナリングパスを経由する中間セッションシグナリング情報の通信に使用されます。NAT モードでは、ヘッダーフィールド Via:、From:、To:、Call-ID:、Contact:、Route:、および Record-Route: にある IP アドレスが、27 ページの表 2 で示すように変更されます。
- Subscribe - リモートノードから現在の状態と状態の更新を要求するのに使用されます。NAT モードでは、メッセージが外部のネットワークから内部のネットワークへ移動する場合に、Request-URL にあるアドレスをプライベート IP アドレスに変更します。ヘッダーフィールド Via:、From:、To:、Call-ID:、Contact:、Route:、および Record-Route: にある IP アドレスは、27 ページの表 2 で示すように変更されます。
- Notify - 購入者に、お持ちであるサービスの状態が変更されたことを通知します。NAT モードでは、メッセージが外部ネットワークから内部ネットワークに移動している場合に、Request-URI: ヘッダーフィールドにある IP アドレスをプライベート IP アドレスに変更します。ヘッダーフィールド Via:、From:、To:、Call-ID:、Contact:、Route:、および Record-Route: にある IP アドレスは、27 ページの表 2 で示すように変更されます。
- Refer - (Request-URL によって識別される) 受信者に、要求にあるサードパーティの連絡先情報を紹介します。NAT モードでは、メッセージが外部のネットワークから内部のネットワークへ移動している場合に、Request-URL にある IP アドレスをプライベート IP アドレスに変更します。ヘッダーフィールド Via:、From:、To:、Call-ID:、Contact:、Route:、および Record-Route: にある IP アドレスは、27 ページの表 2 で示すように変更されます。

  たとえば、プライベートネットワーク内のユーザー A がパブリックネットワーク内のユーザー B に同じプライベートネットワーク内のユーザー C を紹介すると、SIP ALG がユーザー C に新規の IP アドレスとポート番号を割り当てて、ユーザー C はユーザー B との連絡が可能になります。ただし、ユーザー C が r egistrar に登録されると、ユーザー C のポートマッピングは ALG NAT テーブルに保存されて、変換の実行に再利用されます。
- Update - 新規または更新された SDP 情報のピンホールをオープンするのに使用されます。ヘッダーフィールド Via:、From:、To:、Call-ID:、Contact:、Route:、および Record-Route: にある IP アドレスは、27 ページの表 2 で示すように変更されます。
- 1*xx*、202、2*xx*、3*xx*、4*xx*、5*xx*、6*xx* Response Codes トランザクションの状態を示します。ヘッダーフィールドは 27 ページの表 2 に示されるように変更されます。

SIP 応答のクラス

SIP 応答は SIP トランザクションのステータス情報を表示し、応答コードとリーズンフレーズを含んでいます。SIP 応答は次のクラスにグループ化されます。

- 通知（100 ～ 199）- 要求の受信、要求処理の継続
- 成功（200 ～ 299）- アクションの受信、解釈、承認が正常に行われた
- 転送（300 ～ 399）- 要求を完了するにはさらにアクションを起こす必要がある
- クライアントエラー（400 ～ 499）- 要求が不正な構文を含む、またはこのサーバーでは実行できない
- サーバーエラー（500 ～ 599）- サーバーが明らかに有効な要求の実行に失敗した
- グローバルエラー（600 ～ 699）- 要求がどのサーバーでも実行できない

表 1 に、現在のすべての SIP 応答を一覧表示します。これらのすべてが Juniper Networks セキュリティデバイスでサポートされています。

表 1: セッション開始プロトコルの応答

クラス	応答コード - リーズンフレーズ	応答コード - リーズンフレーズ	応答コード - リーズンフレーズ
通知	100 試行中	180 呼び出し中	181 呼を転送中
	182 キューに入れられた	183 セッションの進捗状況	
成功	200 OK	202 承認された	
転送	300 複数の選択肢がある	301 恒久的に移動した	302 一時的に移動した
	305 プロキシを使用せよ	380 代替サービス	
クライアントエラー	400 不正なリクエスト	401 認可されていない	402 料金支払いが必要
	403 禁止	404 見つからない	405 メソッドが許可されていない
	406 受け入れ不能	407 プロキシ認証が必要	408 リクエストがタイムアウトした
	409 重複する	410 リソースがもう存在しない	411 長さが必要
	413 要求のエンティティが大きすぎる	414 Request-URL が長すぎる	415 サポートされていないメディアタイプ
	420 不正な拡張	480 一時的に利用不可	481 呼またはトランザクションが存在しない
	482 ループが検知された	483 ホップが多すぎる	484 アドレスが不完全
	485 不明瞭	486 ここはビジー	487 要求をキャンセル
	488 ここでは受け入れ不能		
サーバーエラー	500 サーバー内部エラー	501 実装されていない	502 不正なゲートウェイ
	502 サービスを利用できない	504 サーバータイムアウト	505 サポートされていない SIP バージョン
グローバルエラー	600 どの場所もビジー	603 辞退	604 どこにも存在しない
	606 受け入れ不能		

SIP アプリケーションレイヤーゲートウェイ

SIP トラフィックには 2 つのタイプ、つまりシグナリングとメディアストリームがあります。SIP シグナリングトラフィックは、クライアントとサーバーとの間の要求メッセージと応答メッセージからなり、ユーザーデータグラムプロトコル（UDP）や伝送制御プロトコル（TCP）などのトランスポートプロトコルを使用します。メディアストリームはデータ（たとえば、オーディオデータ）の伝送を行い、UDP でのリアルタイムプロトコル（RTP）などのアプリケーションレイヤープロトコルを使用します。

Juniper Networks セキュリティデバイスは、ポート 5060 で SIP シグナリングメッセージをサポートします。SIP サービスを許可するポリシーを簡単に作成することができ、セキュリティデバイスは他のトラフィックタイプと同様に、SIP シグナリングトラフィックをフィルタリングして許可または拒否を行います。ただし、メディアストリームは、呼び出し中に何度か変更される可能性のある動的に割り当てられたポート番号を使用します。固定されたポートがなければ、メディアトラフィックを制御する静的なポリシーは作成できません。この場合、セキュリティデバイスは SIP ALG を呼び出します。SIP ALG は SIP メッセージおよび SDP コンテンツを読み込み、動的にピンホールを開けるのに必要なポート番号情報を取り出して、メディアストリームにセキュリティデバイスを行き来させます。

注 : ここでのピンホールとは、排他的トラフィックを許可するために限定されたポートを開くこと意味します。

SIP ALG は SIP トランザクションを監視して、これらのトランザクションから取り出した情報に基づいてピンホールを動的に作成し管理します。
Juniper Networks SIP ALG は、すべての SIP メソッドと応答をサポートしています。14 ページの「SIP 要求方法」および 16 ページの「SIP 応答のクラス」を参照してください)。SIP サービスを許可する静的ポリシーを作成することによって、SIP トランザクションに Juniper Networks ファイアウォールを行き来させることができます。このポリシーによって、セキュリティデバイスは SIP トラフィックを代行受信して、トラフィックを許可または拒否、または SIP ALG にピンホールを開かせてメディアストリームを通過させることができます。SIP ALG は、メディア情報 (SDP) を含む SIP 要求および応答に対してのみ、ピンホールをオープンする必要があります。SDP を含まない SIP メッセージに対しては、セキュリティデバイスは単純にそれらを通過させます。

SIP ALG は SDP を含む SIP メッセージを代行受信し、ピンホールを作成するのに必要な情報をパーサーを使用して抽出します。SIP ALG はパケットの SDP 部分を調べ、パーサーは IP アドレスやポート番号などの情報を抽出します。そして SIP ALG がこの情報をピンホールテーブルに記録します。SIP ALG はピンホールテーブルに記録された IP アドレスおよびポート番号を使用してピンホールをオープンし、メディアストリームがセキュリティデバイスを通過できるようにします。

注： Juniper Networks セキュリティデバイスは、暗号化された SDP はサポートしません。SDP が暗号化されている SIP メッセージをセキュリティデバイスが受信すると、SIP ALG はそのメッセージがファイアウォールを通過するのを許可しますが、ログメッセージを作成してパケットを処理できないことをユーザーに知らせます。SDP が暗号化されていると、SIP ALG はピンホールをオープンするのに必要な情報を SDP から抽出することができません。その結果、SDP が記述するメディアコンテンツはセキュリティデバイスを通過できません。

セッション記述プロトコルのセッション

SDP セッションの記述はテキストベースで、複数の行の 1 セットからなります。この中には、セッションレベル情報とメディアレベル情報が含まれています。セッションレベル情報はセッション全体に適用されますが、メディアレベル情報は特定のメディアストリームに適用されます。SDP セッション記述には、その最初の部分にセッションレベル情報が常に含まれ、またその後にメディアレベル情報が含まれることもあります。

注： SDP セッション記述では、メディアレベル情報は m = フィールドで始まります。

SDP 記述の多数のフィールドの中でも、トランスポートレイヤー情報を含むため SIP ALG に特に役立つものが 2 つあります。その 2 つのフィールドは次のとおりです。

- **c =** 接続情報用

  このフィールドは、セッションレベルまたはメディアレベルで表示されます。次のフォーマットで表示されます。

- c = < ネットワークタイプ > < アドレスタイプ > < 接続アドレス >

  現在セキュリティデバイスがサポートするのは、ネットワークタイプとして「IN」(インターネット用), アドレスタイプとして 「IP4」、宛先 (接続) IP アドレスとしてユニキャスト IP アドレス、またはドメイン名のみです。

注： 一般に宛先 IP アドレスはマルチキャスト IP アドレスになることができますが、NetScreen では現在、SIP でのマルチキャストをサポートしていません。

宛先 IP アドレスがユニキャスト IP アドレスである場合には、SIP ALG はメディア記述フィールド m = に指定された IP アドレスとポート番号を使用してピンホールを作成します。

- **m =** メディア通知用

  このフィールドはメディアレベルで表示され、メディアの説明が含まれています。次のフォーマットで表示されます。

  m = < メディア > < ポート > < トランスポート > < fmt リスト >

セキュリティデバイスで現在サポートしているのは、メディアとしての「audio」、およびアプリケーションレイヤトランスポートプロトコルとしての「RTP」のみです。ポート番号は、メディアストリームの発信元ではなく宛先を示します。フォーマットリスト (fmt リスト) には、メディアが使用するアプリケーションレイヤープロトコルに関する情報を記述します。

この ScreenOS のリリースでは、セキュリティデバイスは RTP および RTCP に対してのみポートをオープンします。すべての RTP セッションは、対応する RTCP（リアルタイムトランスポート制御プロトコル）セッションを持ちます。したがって、メディアストリームが RTP を使用する際は常に、SIP ALG は RTP および RTCP トラフィックの両方に対してポートを確保 (ピンホールを作成) する必要があります。デフォルトでは、RTCP のポート番号は RTP ポート番号よりも 1 つ大きくなります。

注 : 一般に宛先 IP アドレスはマルチキャスト IP アドレスになることができますが、NetScreen では現在、SIP でのマルチキャストをサポートしていません。

ピンホールの作成

RTP および RTCP トラフィック用のピンホールはともに、同じ宛先 IP アドレスを共有します。IP アドレスは SDP セッション記述の c= フィールドから取得します。c= フィールドは SDP セッション記述のセッションレベル部分またはメディアレベル部分のいずれかに表示されるため、次の規則に基づいて (SDP 規則に従って) パーサーが IP アドレスを決定します。

- まず SIP ALG パーサーは、メディアレベルに IP アドレスを含む c= フィールドが存在するかどうかを確認します。フィールドが存在すればパーサーがその IP アドレスを抽出し、SIP ALG がそのアドレスを使用してメディアのピンホールを作成します。
- メディアレベルに c= フィールドが存在しない場合は、SIP ALG パーサーがセッションレベルの c= フィールドから IP アドレスを抽出し、SIP ALG がそのアドレスを使用してメディアのピンホールを作成します。セッション記述のどちらのレベルにも c= フィールドが含まれない場合は、プロトコルスタックのエラーであるためセキュリティデバイスはパケットをドロップしてイベントをログに記録します。

次に示すリストは、ピンホールを作成するために SIP ALG が必要とする情報です。この情報は、セキュリティデバイスの SDP セッション記述とパラメータから得られます。

- Protocol: UDP
- Source IP: 不明
- Source port: 不明
- Destination IP: パーサーがメディアまたはセッションレベルの c= フィールドから宛先 IP アドレスを抽出します。
- Destination port: パーサーがメディアレベルの m= フィールドから RTP の宛先ポート番号を抽出し、次の公式を使って RTCP の宛先ポート番号を算出します。

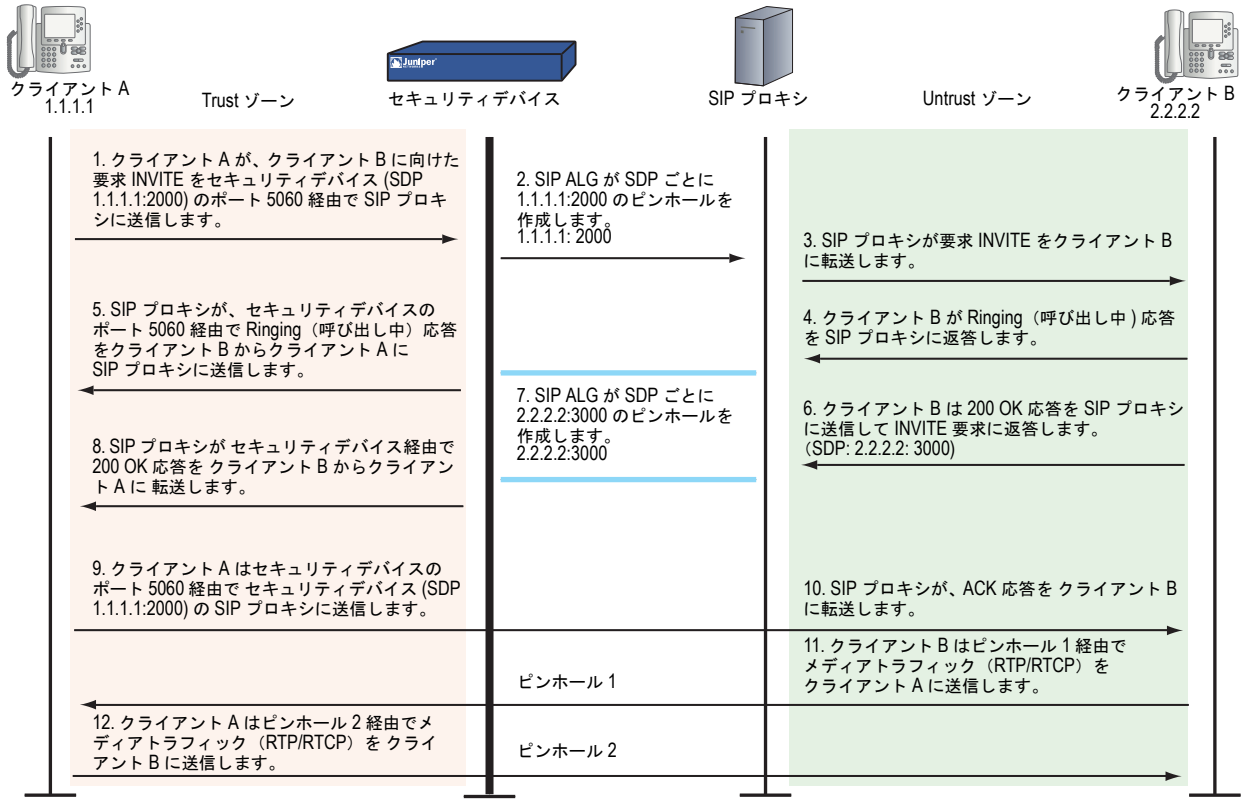
  RTP ポート番号 + 1

- Lifetime: この値は、ピンホールを開いてパケットを通過させることのできる時間の長さ（秒単位）を示します。パケットはピンホールが寿命に達するまでにピンホールを通過する必要があります。寿命に達すると SIP ALG はピンホールを削除します。

  パケットが寿命期間内にピンホールを通過すると、その直後に SIP ALG はパケットが入ってきた方向のピンホールを削除します。

  図 8 で、2 つの SIP クライアント間でのコール設定、および SIP ALG が RTP および RTCP トラフィックを許可するピンホールを作成する方法について説明します。この図では、セキュリティデバイスは SIP を許可するポリシーを持ち、SIP シグナリングメッセージ用のポート 5060 をオープンすると仮定しています。

図 8: SIP ALG コール設定



注： 宛先 IP アドレスが、セッションが保留中であることを示す 0.0.0.0 の場合、SIP ALG は RTP および RTCP トラフィックに対するピンホールを作成しませんたとえば、電話通信中にセッションを保留状態にするには、ユーザー (ユーザー A) 側から他のユーザー (ユーザー B) に宛先 IP アドレスが 0.0.0.0 である SIP メッセージを送信します。これによって、新しい通知が来るまでメディアを一切送信しないことがユーザー B に示されます。ユーザー B がメディアを送信した場合、そのパケットはドロップされます。

セッション無活動タイムアウト

通常は、クライアントの 1 つが BYE 要求または CANCEL 要求を送信するとコールが終了します。SIP ALG は BYE 要求または CANCEL 要求を代行受信し、そのコールについてのメディアセッションすべてを削除します。クライアントが BYE 要求または CANCEL 要求を行うのを阻止すると、電源障害などの原因や問題になることがあります。この例では、コールが無限に継続して、セキュリティデバイスのリソースが消費されるおそれがあります。無活動タイムアウト機能を利用すると、セキュリティデバイスはコールの活動を監視し、一定期間内に活動がない場合には呼び出しを終了させます。

コールは、1 つ以上の音声チャネルを持ちます。各音声チャネルには、RTP 用および RTCP 用の 2 つのセッション (または 2 つのメディアストリーム) があります。セキュリティデバイスはセッションを管理する際、各音声チャネルにあるセッションを 1 つのグループとみなします。そのため、無活動タイムアウトなどの設定は、各セッションではなくグループに適用されます。

グループの寿命を決定する無活動タイムアウトには、次の 2 つのタイプがあります。

- シグナリング無活動タイムアウトこのパラメータは、SIP シグナリングトラフィックなしの状態でコールがアクティブな状態を持続できる最大時間（秒単位）です。このタイムアウトは、コール内で SIP シグナリングメッセージが発生するたびにリセットされます。デフォルト設定値は 43200 秒 (12 時間) です。

- メディア無活動タイムアウトこのパラメータは、グループ内の SIP メディア (RTP または RTCP) トラフィックなしでコールがアクティブな状態を持続できる最大時間 (秒単位) を示します。このタイムアウトは、コール内で RTP または RTCP パケットが発生するたびにリセットされます。デフォルト設定値は 120 秒です。

これらのタイムアウトのいずれかが期限切れになると、セキュリティデバイスは、そのテーブルからコールのすべてのセッションを削除することによってコールを終了させます。

SIP 攻撃保護

一度拒否した SIP INVITE 要求が、悪意のあるエラーであるかクライアントやサーバー経由のエラーかにかかわらず繰り返されると、SIP プロキシサーバーのコール処理機能が影響を受ける可能性があります。このような要求による SIP プロキシサーバーへの攻撃を予防するには、**sip protect deny** コマンドを使用して、セキュリティデバイス側で INVITE 要求およびそれに対するプロキシサーバー応答を監視させます。応答に 3*xx*、4*xx*、または 5*xx* の応答コード (16 ページの「SIP 応答のクラス」を参照) が含まれる場合には、ALG によって、要求のソース IP アドレスとテーブル内プロキシサーバーの IP アドレスが保存されます。その後、セキュリティデバイスはこのテーブルを照合してすべての INVITE 要求をチェックし、設定可能な秒数（デフォルトは 3）の間、テーブル内のエントリに一致するパケットをすべて破棄します。また、宛先 IP アドレスを指定して特定のプロキシサーバーへの INVITE 要求を監視するようにセキュリティデバイスを構成することもできます。SIP 攻撃保護はグローバルに構成されます。

例 : SIP 保護拒否

次の例では、すでに拒否されているサービスへの INVITE 要求を繰り返す攻撃から単一の SIP プロキシサーバー (1.1.1.3/24) を保護するようにセキュリティデバイスを構成します。パケットは 5 秒間ドロップされます。その後セキュリティデバイスは、これらのソースからの INVITE 要求の転送を再開します。

WebUI

SIP プロキシサーバーを INVITE 要求による氾濫から保護するには、CLI を使用する必要があります。

CLI

```
set alg sip app-screen protect deny dst-ip 1.1.1.3/24
set alg sip protect deny timeout 5
save
```

例 : シグナリングおよびメディア無活動タイムアウト

この例では、シグナリング無活動タイムアウトを 30,000 秒に、メディア無活動タイムアウトを 90 秒に設定します。

WebUI

注 : SIP シグナリングまたはメディアの無活動タイムアウトを設定するには、CLI を使用する必要があります。

CLI

```
set alg sip signaling-inactivity-timeout 30000
set alg sip media-inactivity-timeout 90
save
```

例 : UDP フラッディング保護

ゾーンや宛先アドレスを指定して、UDP フラッディングからセキュリティデバイスを保護することができます。この例では、Untrust ゾーン内の IP アドレス 1.1.1.5 で受信する UDP パケット数のしきい値を 1 秒あたり 80,000 に設定します。この設定により、セキュリティデバイスはアラームを生成してからその秒での残りのパケットをドロップします。

注 : この例では、一般的な ScreenOS コマンドを使用します。また、この例は SIP 固有ではありません。UDP フラッド保護についての詳細、および有効な設定を決める方法についての詳細は **4**-50 ページの「UDP フラッド」を参照してください。

WebUI

Security > Screening > Screen: 以下を入力して **Apply** をクリックします。

Zone: Untrust
UDP Flood Protection (選択)

> Destination IP: 以下を入力してから、お使いのブラウザの戻る矢印をクリックして Screen 構成ページに戻ります。

Destination IP: 1.1.1.5
Threshold: 80000
Add: (選択)

CLI

set zone untrust screen udp-flood dst-ip 1.1.1.5 threshold 80000
save

例 : SIP 接続の最大数

この例では、単一の IP アドレスからの同時セッションの最大数を 20 に設定して、Untrust ゾーンにいる攻撃者からの SIP ネットワークへのフラッド攻撃を予防します。セキュリティデバイス側で同じ IP アドレスからの接続試行が 20 を超えたことを検出すると、それ以降の接続試行はドロップされ、セッション数が指定した最大数を下回るまでドロップされます。

注 : この例では、一般的な ScreenOS コマンドを使用します。また、この例は SIP 固有ではありません。ソースベースのセッションについての詳細、および有効な設定を決める方法についての詳細は **4**-30 ページの「ソースベースおよび宛先ベースセッション制限」を参照してください。

WebUI

Screening > Screen (Zone: Untrust): 次のように入力してから **OK** をクリックします。

Source IP Based Session Limit: (選択)
Threshold: 20 Sessions

CLI

set zone untrust screen limit-session source-ip-based 20
save

ネットワークアドレス変換での SIP

ネットワークアドレス変換 (NAT) プロトコルは、プライベートサブネット内の複数のホストを使用可能にして、単一のパブリック IP アドレスを共有してインターネットにアクセスできます。出力トラフィックについては、NAT はプライベートサブネット内のホストのプライベート IP アドレスをパブリック IP アドレスに置き換えます。受信トラフィックについては、パブリック IP アドレスが変換されて、プライベートサブネット内の適切なホストにルーティングされたプライベートアドレスとメッセージに戻されます。

SIP サービスと連携して NAT を使用すると、SIP メッセージには SIP ボディ内にだけでなく SIP ヘッダー内にも IP アドレスが含まれるため、複雑になります。SIP ヘッダーには呼び出し側と受信側についての情報が含まれます。セキュリティデバイスは、外部のネットワークに対してこの情報を隠します。SDP ボディには SDP (セッション記述プロトコル) 情報が含まれています。この情報には、メディア伝送についての IP アドレスとポート番号があります。セキュリティデバイスは、リソースを割り当ててメディアの送信および受信を可能にするために、SDP 情報を変換します。

SIP メッセージ内の IP アドレスとポート番号の置換手順は、メッセージの方向によって決まります。出力メッセージの場合は、クライアントのプライベート IP アドレスとポート番号が、Juniper Networks ファイアウォールのパブリック IP アドレスとポート番号に置き換えられます。受信メッセージの場合は、NetScreen ファイアウォールのパブリック IP アドレスが、クライアントのプライベートアドレスに置き換えられます。

INVITE メッセージをファイアウォール経由で外部に送信する場合、SIP ALG はメッセージヘッダーからの情報をコールテーブルに収集します。コールテーブルは、以降のメッセージを正しい端点へ転送するために使用されます。新しいメッセージ、たとえば ACK や 200 OK が到着すると、ALG は From:、To:、および Call-ID: フィールドをコールテーブルと比較して、メッセージのコールコンテキストを識別します。到着した新しい INVITE メッセージが既存のコールと一致する場合、ALG はこのメッセージを REINVITE として処理します。

SDP 情報を含むメッセージが到着すると、ALG はポートを割り当てて、割り当てられたポートと SDP 内のポートとをマッピングする NAT を作成します。SDP には RTP (リアルタイムプロトコル) チャネルと RTCP (リアルタイムトランスポート制御プロトコル) チャネルについての連続したポート番号が必要であるため、ALG は連続した偶数 / 奇数のポート番号を提供します。ポート番号のペアが見つからない場合、SIP メッセージは破棄されます。

出力コール

内部のネットワークから外部のネットワークへ向かう SIP 要求メッセージによって SIP コールが起動すると、NAT は SDP 内の IP アドレスとポート番号を置換し、その IP メッセージとポート番号を Juniper Networks ファイアウォールへマップするバインディングを作成します。Via:、Contact:、Route:、および Record-Route: ヘッダーフィールドが存在していれば、同様にファイアウォールの IP アドレスにバインドされます。SIP ヘッダーフィールドも存在していれば、同様にファイアウォールの IP アドレスにバインドされます。これらのマッピングは保存されて、再伝送および SIP 応答メッセージに使用されます。

次に SIP ALG がファイアウォールにピンホールを開けて、メディアのセキュリティデバイス通過を許可します。このセキュリティデバイスに動的に割り当てられているポート番号は、SDP にある情報と、Via:、Contact:、および Record-Route: ヘッダーフィールドにある情報に基づいてネゴシエートされたポート番号です。また、ピンホールによって、受信パケットが Contact:、Via:、および Record-Route: フィールド中の IP アドレスおよびポートへ到達することができます。ALG は返信トラフィックを処理する際に、元の SIP フィールド Contact:、Via:、Route:、および Record-Route: をパケットに挿入します。

受信コール

受信コールはプライベートネットワークから、パブリックマップ IP（MIP）アドレスへ、またはセキュリティデバイス上のインターフェース IP アドレスへ起動されます。MIP は、内部ホストを指す静的に構成された IP アドレスです。インターフェース IP アドレスについては、ALG が内部ホストから SIP Registrar に送信される REGISTER メッセージを監視しながら、動的に記録します。(詳細については、31 ページの「例」を参照してください)。セキュリティデバイスが SIP 受信パケットを受信すると、セッションを設定してパケットのペイロードを SIP ALG に転送します。

ALG が SIP 要求メッセージ (最初は INVITE から) を調べ、SDP 内の情報に基づいて、発信するメディアのゲートを開きます。SIP ALG は要求メッセージ 200 OK が到着すると、IP アドレスとポートに対して NAT を実行して、アウトバウンド方向にピンホールを開きます。(開いたゲートの time-to-live は短く、すぐに要求メッセージ 200 OK を受信しない場合にはタイムアウトになります。)

SIP プロキシは要求メッセージ 200 OK が到着すると、SDP 情報を調べ、各メディアセッションについての IP アドレスとポート番号を読み込みます。セキュリティデバイス上の SIP ALG は、アドレスとポート番号に対して NAT を実行し、アウトバウンドトラフック用にピンホールを開いて、インバウンド方向のゲートのタイムアウトをリフレッシュします。

ACK が 200 OK で到着する場合は、ACK は SIP ALG も通過します。メッセージに SDP 情報が含まれている場合、SIP ALG は、IP アドレスとポート番号が以前の INVITE から変更されていないかどうかを確認します。変更されている場合、ALG は古いピンホールを削除してから新規のピンホールを作成して、メディアの通過を許可します。ALG は、Via:、Contact:、および Record-Route: SIP フィールドも監視し、これらのフィールドが変更されたと判断した場合は新しいピンホールを開きます。

転送されたコール

たとえば、ネットワーク外部にいるユーザー A がネットワーク内部にいるユーザー B を呼び出して、ユーザー B がネットワーク外部にいるユーザー C にそのコールを転送する場合に、転送されたコールとなります。SIP ALG はユーザー A からの INVITE を、通常の受信コールとして処理します。一方、ユーザー B からネットワーク外部のユーザー C に転送されたコールを調べて、同じインターフェースを使用して B と C に到達することが判明した場合、メディアは A と C 間では直接やり取りされないため、ファイアウォールにピンホールが開きません。

コールの終了

コールの終了には、BYE メッセージが使用されます。セキュリティデバイスは BYE メッセージを受信すると、他のメッセージと同様にヘッダーフィールドを変換します。ただし、BYE メッセージは受信側で 200 OK と認識される必要があるため、200 OK が送信できるように ALG 側でコールの ティアダウン を 5 秒間遅延します。

コールの Re-INVITE メッセージ

Re-INVITE メッセージは、コールに新規メディアセッションを追加したり、既存のメディアセッションを削除するために使用されます。新規のメディアセッションをコールに追加すると、ファイアウォールに新しくピンホールを開いて、新規のアドレスバインディングを作成します。このプロセスは、元のコールの設定と同じです。1 つ以上のメディアセッションをコールから削除すると、ピンホールを閉じて、BYE メッセージの場合と同様にアドレスバインディングを解放します。

コールセッションタイマー

SIP ALG は Session-Expires 値を使用して、Re-INVITE メッセージや UPDATE メッセージが受信されない場合にセッションをタイムアウトします。Session-Expires 値が存在している場合には、INVITE への応答 200 OK からこの値を取得して、シグナリングタイムアウトにこの値を使用します。セッションがタイムアウトする前に別の INVITE を受信した場合には、すべてのタイムアウト値がこの INVITE またはデフォルトでの値にリセットされ、プロセスが繰り返されます。

SIP ALG は予防手段として、ハードタイムアウト値を使用して、コールが存在できる最大経過時間を設定します。これにより、以下のイベントが発生した場合にセキュリティデバイスが保護されます。

- コール中にエンドシステムがクラッシュして、BYE メッセージが受信されない。
- 悪意のあるユーザーが SIP ALG を攻撃しようとして、BYE が送信されない。
- SIP プロキシの実装が不十分で、Record-Route が処理されずに、BYE メッセージが送信されない。
- ネットワークに障害が発生して、BYE メッセージが受信されていない。

コールのキャンセル

どちら側からでも CANCEL メッセージを送信してコールをキャンセルできます。SIP ALG は、CANCEL メッセージを受信すると、ファイアウォールに開いているピンホールがあれば閉じて、アドレスバインディングを解放します。SIP ALG はリソースが解放される前に、制御チャネル age-out を約 5 秒間遅延して、最終の 200 OK が通過できるようにします。5 秒間のタイムアウトを過ぎると、到着する応答が 487 である場合や 200 以外である場合にかかわらず、コールが終了します。

フォーク

フォークによって、複数の宛先に対して同時に単一の INVITE を送信できる SIP プロキシが使用可能になり、単一のコールに対して複数の 200 OK 応答メッセージが到着すると、SIP ALG が解析を行いますが、コール情報の更新は受信した最初の 200 OK メッセージを使用します。

SIP メッセージ

SIP メッセージ形式は、SIP ヘッダーセクションと SIP ボディから成ります。要求メッセージの場合、ヘッダーセクションの最初の行は要求行です。この行には、メソッドタイプ、Request-URL、およびプロトコルバージョンが含まれています。応答メッセージの場合、最初の行はステータス行であり、ステータスコードがあります。SIP ヘッダーには、シグナリングに使用する IP アドレスとポート番号が含まれています。SIP ボディとヘッダーセクションは 1 行の空白で隔てられています。SIP ボディには、オプションでのセッション記述情報用に行が確保されています。Juniper Networks セキュリティデバイスは現在、SDP (セッション記述プロトコル) のみをサポートしています。SIP ボディには、メディアの転送に使用する IP アドレスとポート番号が含まれています。

NAT モードでは、セキュリティデバイスは SIP ヘッダー内の情報を変換して、外部のネットワークに対してこの情報を隠します。SIP ボディの情報に対して NAT が実行され、リソース、つまり受信するメディアのポート番号が割り当てられます。

SIP ヘッダー

以下の SIP 要求メッセージのサンプルでは、NAT によってヘッダーフィールドにある太字の IP アドレスが置換され、外部のネットワークに対してこの情報が隠されます。

INVITE bob@**10.150.20.5** SIP/2.0
Via: SIP/2.0/UDP **10.150.20.3**:5434
From: alice@**10.150.20.3**
To: bob@**10.150.20.5**
Call-ID: a12abcde@**10.150.20.3**
Contact: alice@**10.150.20.3**:5434
Route: <sip:netscreen@**10.150.20.3**:5060>
Record-Route: <sip:netscreen@**10.150.20.3**:5060>

IP アドレス変換の方法は、以下のいずれかのメッセージのタイプと方向によって決まります。

- インバウンド要求
- アウトバウンド応答
- アウトバウンド要求
- インバウンド応答

表 2 は、メッセージのタイプによる NAT の実行方法を示しています。いくつかのヘッダーフィールドについては、ALG 側でメッセージの発信元が内部ネットワークであるか外部のネットワークであるか以外の情報が必要になります。また、クライアントが開始するコールについての情報や、メッセージが要求または応答のどちらかであるかについての情報も必要です。

表 2: NAT でメッセージを要求

メッセージタイプ	フィールド	Action
インバウンド要求 (パブリックネットワークからプライベートネットワークへ)	宛先 :	ALG アドレスをローカルアドレスに置換
	From:	None
	Call-ID:	None
	Via:	None
	Request-URI:	ALG アドレスをローカルアドレスに置換
	Contact:	None
	Record-Route:	None
	Route:	None

メッセージタイプ	フィールド	Action
アウトバウンド応答 (プライベートネットワークからパブリックネットワークへ)	To:	ALG アドレスをローカルアドレスに置換
	From:	None
	Call-ID:	None
	Via:	None
	Request-URI:	なし
	Contact:	ローカルアドレスを ALG アドレスに置換
	Record-Route:	ローカルアドレスを ALG アドレスに置換
	Route:	None
アウトバウンド要求 (プライベートネットワークからパブリックネットワークへ)	To:	None
	From:	ローカルアドレスを ALG アドレスに置換
	Call-ID:	ローカルアドレスを ALG アドレスに置換
	Via:	ローカルアドレスを ALG アドレスに置換
	Request-URI:	None
	Contact:	ローカルアドレスを ALG アドレスに置換
	Record-Route:	ローカルアドレスを ALG アドレスに置換
	Route:	ALG アドレスをローカルアドレスに置換
アウトバウンド応答 (パブリックネットワークからプライベートネットワークへ)	To:	None
	From:	ALG アドレスをローカルアドレスに置換
	Call-ID:	ALG アドレスをローカルアドレスに置換
	Via:	ALG アドレスをローカルアドレスに置換
	Request-URI:	なし
	Contact:	None
	Record-Route:	ALG アドレスをローカルアドレスに置換
	Route:	ALG アドレスをローカルアドレスに置換

SIP ボディ

SIP ボディ内の SDP 情報には、ALG がメディアストリームのチャネルを作成する際に使用する IP アドレスが含まれています。また、SDP セクションの変換によって、リソース、つまりメディアを送信および受信するポート番号が割り当てられます。

次に示す例外は、サンプル SDP セクションで、リソースを割り当てるために変換されるフィールドです。

```
o=user 2344234 55234434 IN IP4 10.150.20.3
c=IN IP4 10.150.20.3
m=audio 43249RTP/AVP 0
```

SIP メッセージには、複数のメディアストリームを入れることができます。概念的には、E メールメッセージに複数のファイルを添付することに類似しています。たとえば、SIP クライアントから SIP サーバーに送信される INVITE メッセージには、以下のようなフィールドがあります。

c=IN IP4 **10.123.33.4**
m=audio **33445**RTP/AVP 0
c=IN IP4 **10.123.33.4**
m=audio **33447**RTP/AVP 0
c=IN IP4 **10.123.33.4**
m=audio **33449**RTP/AVP 0

Juniper Networks セキュリティデバイスは、最大で 6 つの SDP チャネルをサポートします。チャネルは各方向についてネゴシエートされるため、1 コールつき合計で 12 チャネルがサポートされます。詳細については、18 ページの「セッション記述プロトコルのセッション」を参照してください。

SIP NAT の手順

以下の図 9 では、ph1 が ph2 に SIP INVITE メッセージを送信します。太字で示されたヘッダーフィールド内 IP アドレスが変換される方法を確認してください。

INVITE メッセージの SDP セクションには、呼び出し側がメディアを受信する場所が示されています。Media ピンホールには、RTCP と RTP についてそれぞれ 2 つのポート番号 52002 と 52003 が割り当てられています。Via/Contact ピンホールでは、SIP シグナリングを行うためのポート番号 5060 が提供されます。

応答メッセージ 200 OK では、INVITE メッセージで実行される逆方向の変換について確認してください。このメッセージにあるパブリック IP アドレスは変換されません。ただし、ゲートは開かれて、メディアストリームがプライベートネットワークにアクセスできます。

図 9: SIP NAT の手順 1

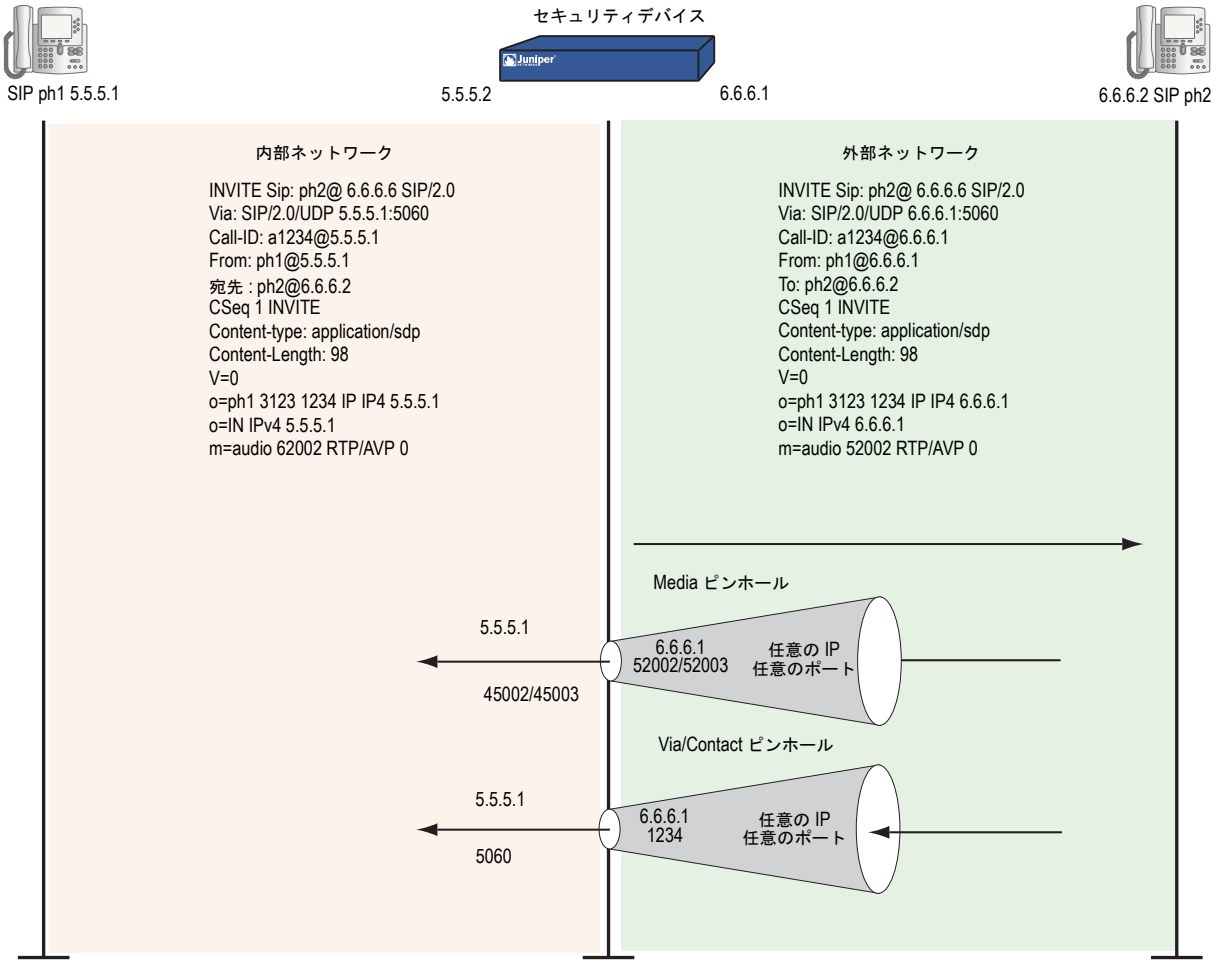
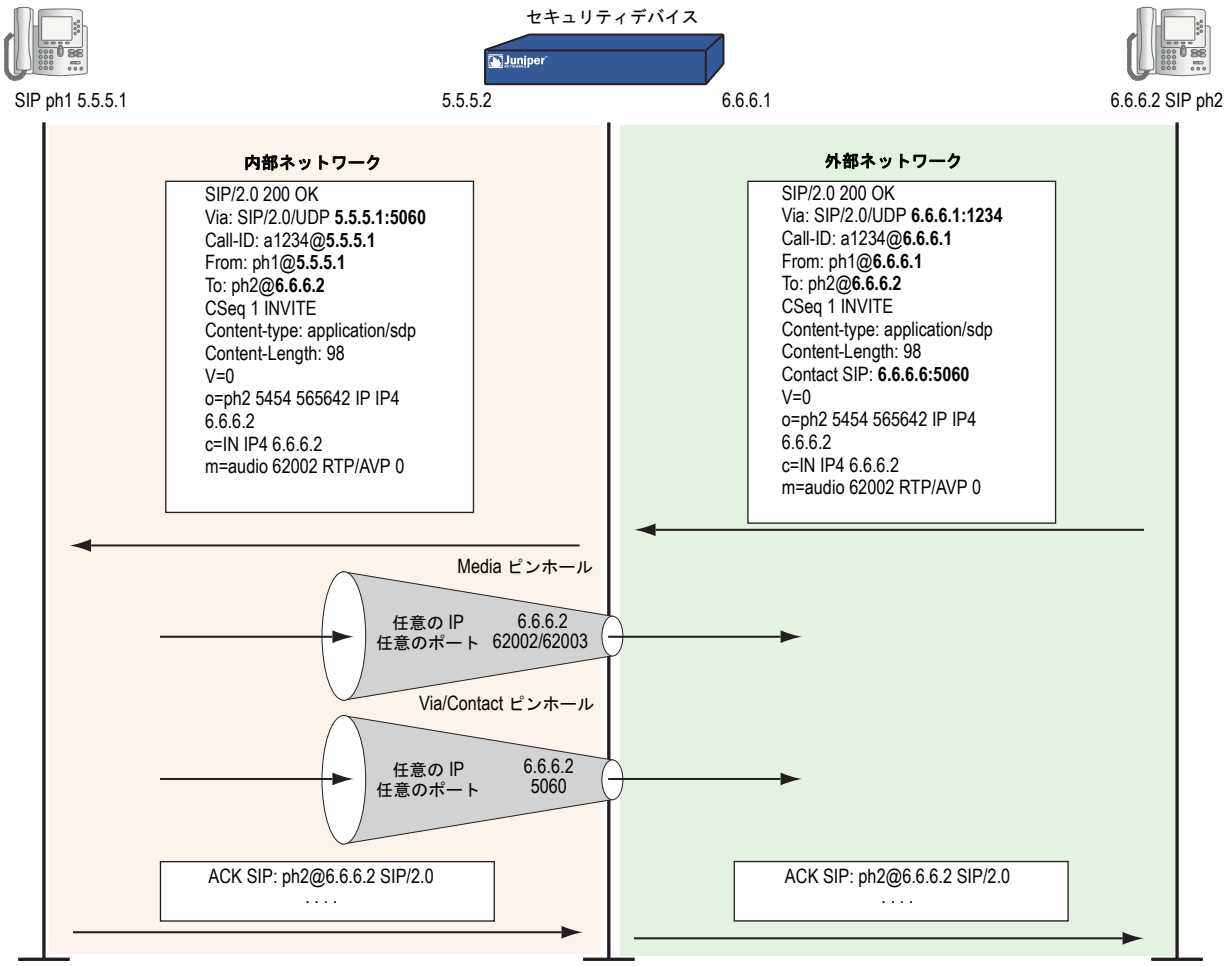


図 10: SIP NAT の手順 2



例

このセクションには、以下のサンプル例があります。

- 32 ページの「SIP Registrar を使用する受信 SIP コールのサポート」
- 38 ページの「例 : MIP での受信コール」
- 40 ページの「例 : プライベートゾーン内のプロキシ」
- 43 ページの「例 : パブリックゾーン内のプロキシ」
- 45 ページの「例 : 3 つのゾーン、DMZ 内のプロキシ」
- 48 ページの「例 : Untrust ゾーン内」
- 52 ページの「例 : Trust ゾーン内」
- 54 ページの「例 : フルメッシュ VPN での SIP」

SIP Registrar を使用する受信 SIP コールのサポート

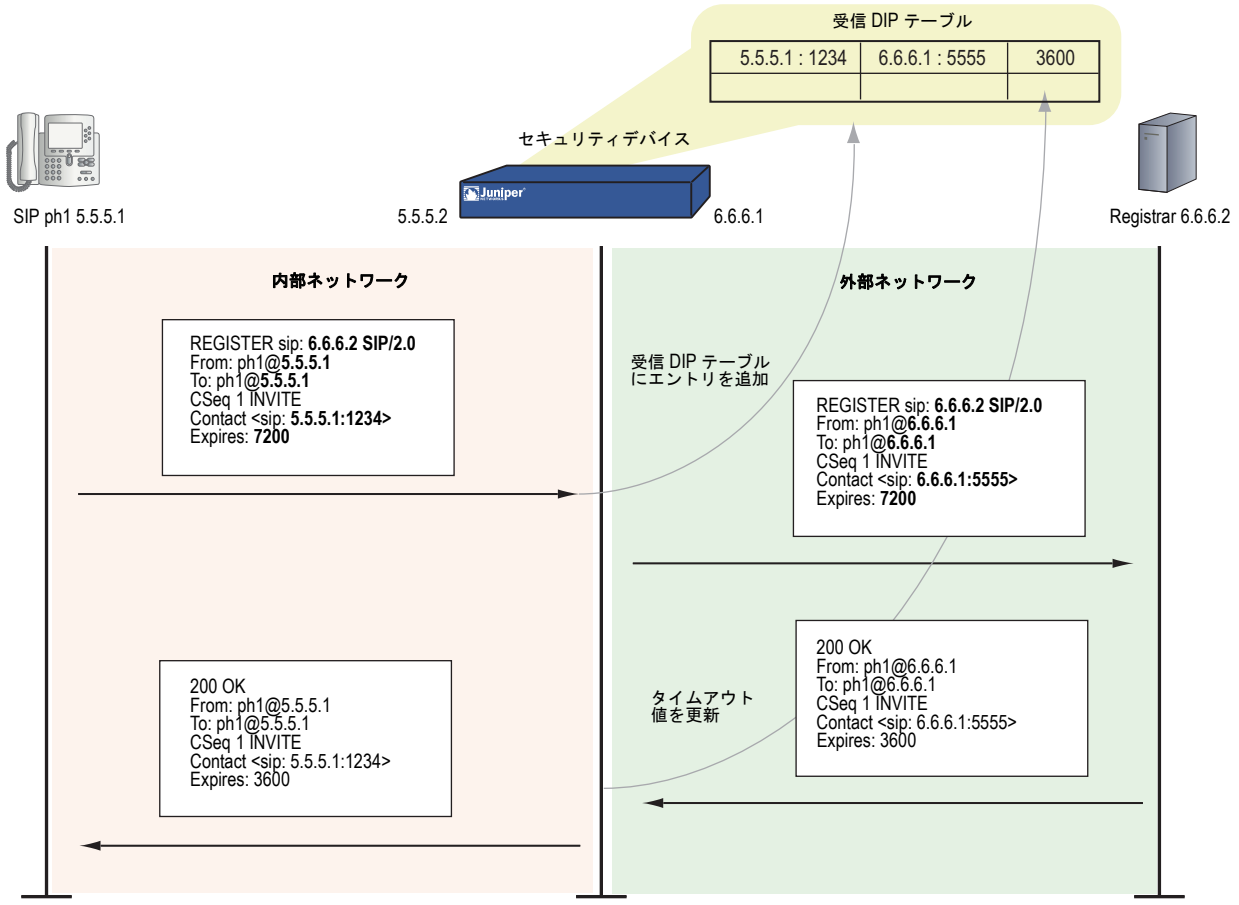
SIP 登録によって、検出機能が提供されます。この検出機能によって、SIP プロキシとロケーションサーバー側で、ユーザーが連絡しようとする場所を識別できます。ユーザーは、Registrar に REGISTER メッセージを送信して 1 つ以上の場所を登録します。REGISTER メッセージ内の To: フィールドと Contact: フィールドには、図 11 で示されるように、address-of-record URL と 1 つ以上の連絡先 URL が含まれています。登録によって、address-of-record アドレスを連絡先アドレスに関連付けるロケーションサービスにバインディングが作成されます。

セキュリティデバイスは、出力 REGISTER メッセージの監視、これらのアドレスについて NAT を実行、受信 DIP テーブルに情報を格納します。次に、ネットワークの外部から INVITE メッセージを受信すると、セキュリティデバイスは受信 DIP テーブルを使用して、INVITE メッセージのルーティング先である内部ホストを識別します。SIP プロキシ登録サービスを活用して、セキュリティデバイスの egress インターフェース上にあるインターフェース DIP や DIP プールを構成することによって受信コールを許可できます。小規模のオフィスで受信コールを処理するには、インターフェース DIP で十分です。規模の大きいネットワークや大企業では、DIP プールの設定が推奨されます。

注： インターフェース DIP や DIP プールを使用する受信コールのサポートは、SIP と H.323 サービスに限ってサポートされます。

受信コールについては、セキュリティデバイスは現在、UDP と TCP のみをサポートします。また現時点ではドメイン名解決がサポートされないため、図 11 に示すように、URL は IP アドレスにする必要があります。

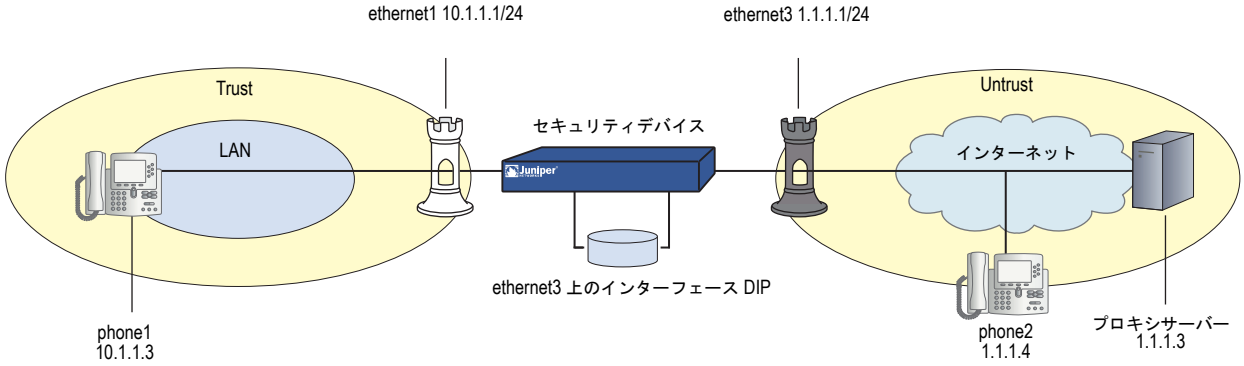
図 11: 受信 SIP



例 : 受信コール (インターフェース DIP)

この例では、phone1 が Trust ゾーン内の ethernet1 インターフェースにあり、phone2 とプロキシサーバーが Untrust ゾーン内の ethernet3 インターフェースにあります。ethernet3 インターフェース上にインターフェース DIP を設定して受信コールに対して NAT を実行してから、Untrust ゾーンから Trust ゾーンへの SIP トラフィックを許可するポリシーを作成してそのポリシー内の DIP を参照します。また、NAT を使用して Trust ゾーンから Untrust ゾーンへの SIP トラフィックを許可するポリシーも作成することもできます。これによって、Trust ゾーン内の phone1 が Untrust ゾーン内のプロキシに登録できます。受信 DIP が SIP 登録サービスと連携する詳細については、31 ページの「例」を参照してください。

図 12: ethernet3 インターフェース上のインターフェース DIP での受信コール



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24
   Interface mode: Route

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: phone1
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.3/24
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: phone2
   IP Address/Domain Name:
   IP/Netmask: (選択), 1.1.1.4/24
   Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: **プロキシ**
IP Address/Domain Name:
IP/Netmask: (**選択**), 1.1.1.3/24
Zone: Untrust

3. 受信 NAT での DIP

Network > Interfaces > Edit (ethernet3) > DIP > New: Incoming NAT オプションを選択してから **OK** をクリックします。

4. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address
Address Book Entry: (**選択**), phone1
Destination Address
Address Book Entry: (**選択**), any
Service: SIP
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: (**選択**)
(DIP on): None (Use Egress Interface IP)

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address
Address Book Entry: (**選択**), Any
Destination Address
Address Book Entry: (**選択**), DIP(ethernet3)
Service: SIP
Action: Permit

CLI

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
```

2. アドレス

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address untrust proxy 1.1.1.3/24
```

3. 受信 NAT での DIP

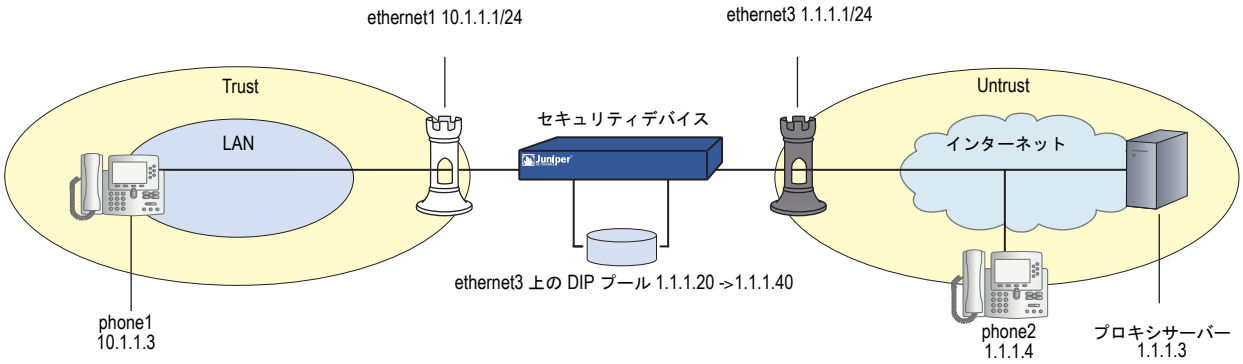
```
set interface ethernet3 dip interface-ip incoming
set dip sticky
```

4. **ポリシー**
   set policy from trust to untrust phone1 any sip nat src permit
   set policy from untrust to trust any dip(ethernet3) sip permit
   save

例 : 受信コール (DIP プール)

この例では、phone1 が Trust ゾーンに、phone2 とプロキシサーバーが Untrust ゾーンにあります。ethernet3 インターフェース上に DIP プールを設定して受信コールに対して NAT を実行してから、Untrust ゾーンから Trust ゾーンへの SIP トラフィックを許可するポリシーを作成して、そのポリシー内の DIP プールを参照します。また、NAT を使用して Trust ゾーンから Untrust ゾーンへの SIP トラフィックを許可するポリシーも作成することもできます。これによって、Trust ゾーン内の phone1 が Untrust ゾーン内のプロキシに登録できます。DIP が SIP 登録サービスと連携する詳細については、31 ページの「例」を参照してください。

図 13: 受信コール (DIP プール)



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24
   Interface mode: Route

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: phone1
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.3/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: phone2
IP Address/Domain Name:
IP/Netmask: (選択), 1.1.1.4/24
Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: proxy
IP Address/Domain Name:
IP/Netmask: (選択), 1.1.1.3/24
Zone: Untrust

3. 受信 NAT での DIP プール

Network > Interfaces > Edit (ethernet3) > DIP > New: 次のように入力してから **OK** をクリックします。

ID: 5
IP Address Range: (選択), 1.1.1.20 ~ 1.1.1.40
Port Translation: (選択)
In the same subnet as the interface IP or its secondary IPs: (選択)
Incoming NAT: (選択)

4. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address
Address Book Entry: (選択), phone1
Destination Address
Address Book Entry: (選択), Any
Service: SIP
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: (選択)
(DIP on): 5 (1.1.1.20-1.1.1.40)/port-xlate

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address
Address Book Entry: (**選択**), Any
Destination Address
Address Book Entry: (**選択**), DIP(5)
Service: SIP
Action: Permit

CLI

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24
   set interface ethernet3 route

2. **アドレス**
   set address trust phone1 10.1.1.3/24
   set address untrust phone2 1.1.1.4/24
   set address untrust proxy 1.1.1.3/24

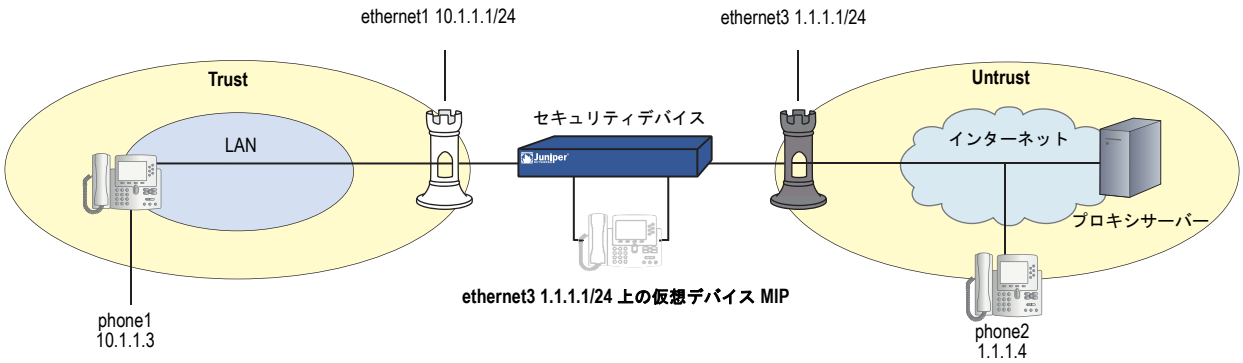
3. **受信 NAT での DIP プール**
   set interface ethernet3 dip 5 1.1.1.20 1.1.1.40 incoming
   set dip sticky

4. **ポリシー**
   set policy from trust to untrust phone1 any sip nat src dip 5 permit
   set policy from untrust to trust any dip(5) sip permit
   save

例 : MIP での受信コール

この例では、phone1 が Trust ゾーン内の ethernet1 インターフェースにあり、phone2 とプロキシサーバーが Untrust ゾーン内の ethernet3 インターフェースにあります。phone1 の ethernet3 インターフェース上に MIP を配置してから、Untrust ゾーンから Trust ゾーンへの SIP トラフィックを許可するポリシーを作成して、そのポリシー内の MIP を参照します。また、phone1 の Untrust ゾーン内のプロキシサーバーへの登録を許可するポリシーも作成します。この例は、前の 2 つの例に似ています (33 ページの「例 : 受信コール (インターフェース DIP)」および 36 ページの「例 : 受信コール (DIP プール)」を参照)。ただし、インターフェース DIP や DIP プールの場合には、1 つのインターフェースが複数のアドレスを使用できるのに対して、MIP を使用するには、Trust ゾーン内の各プライベートアドレスにつき 1 つのパブリックアドレスが必要になります。

図 14: MIP での受信コール



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone: Untrust
   IP Address/Netmask: 1.1.1.1/24
   Interface mode: Route

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: phone1
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.3/24
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: phone2
   IP Address/Domain Name:
   IP/Netmask: (選択), 1.1.1.4/24
   Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: proxy
IP Address/Domain Name:
IP/Netmask: (**選択**), 1.1.1.3/24
Zone: Untrust

3. **MIP**

Network > Interfaces > Edit (ethernet3) > MIP > New: 次のように入力してから **OK** をクリックします。

Mapped IP: 1.1.1.3
Netmask: 255.255.255.255
Host IP Address: 10.1.1.3

4. **ポリシー**

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), any
Destination Address:
Address Book Entry: (**選択**), MIP(1.1.1.3)
Service: SIP
Action: Permit

CLI

1. **インターフェース**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
```

2. **アドレス**

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address untrust proxy 1.1.1.3/24
```

3. **MIP**

```
set interface ethernet3 mip 1.1.1.3 host 10.1.1.3
```

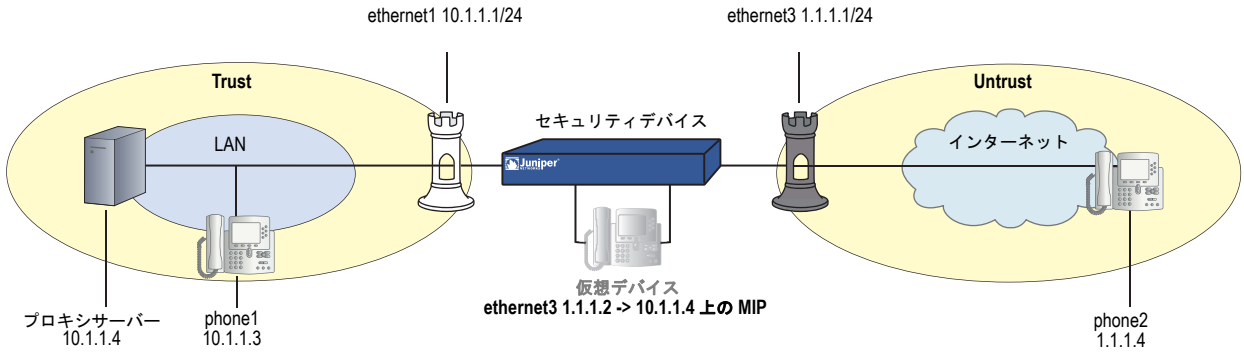
4. **ポリシー**

```
set policy from untrust to trust any mip(1.1.1.3) sip permit
save
```

例 : プライベートゾーン内のプロキシ

この例では、phone1 と SIP プロキシサーバーが Trust (プライベート) ゾーン内の ethernet1 インターフェースにあり、phone2 が Untrust ゾーン内の ethernet3 インターフェースにあります。プロキシサーバーに ethernet3 インターフェース上の MIP を配置すると、phone2 のプロキシサーバーへの登録が許可され、Untrust ゾーンから Trust ゾーンへの SIP トラフィックを許可するポリシーを作成して、そのポリシー内の MIP を参照します。また、phone1 の Trust ゾーンから Untrust ゾーンへの呼び出しを許可するポリシーも作成します。

図 15: プライベートゾーン内のプロキシ



WebUI

1. **インターフェース**

   Network > Interfaces > Edit (ethernet1): 次のように入力してから **OK** をクリックします。

   Zone: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone: Untrust
   IP Address/Netmask: 1.1.1.1/24
   Interface mode: Route

2. **アドレス**

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: phone1
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.3/24
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: phone2
   IP Address/Domain Name:
   IP/Netmask: (選択), 1.1.1.4/24
   Zone: Untrust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: proxy
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.4/24
   Zone: Trust

3. **MIP**

   Network > Interfaces > Edit (loopback.3) > MIP > New: 次のように入力してから **OK** をクリックします。

   Mapped IP: 1.1.1.2
   Netmask: 255.255.255.255
   Host IP Address: 10.1.1.4
   Host Virtual Router Name: trust-vr

4. **ポリシー**

   Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   　Address Book Entry: (選択), any
   Destination Address:
   　Address Book Entry: (選択), phone2
   Service: SIP
   Action: Permit

   > Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

   NAT:
   Source Translation: (選択)
   (DIP on): None (Use Egress Interface IP)

   Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   　Address Book Entry: (選択), phone2
   Destination Address:
   　Address Book Entry: (選択), MIP(1.1.1.2)
   Service: SIP
   Action: Permit

CLI

1. **インターフェース**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
```

2. **アドレス**

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address trust proxy 10.1.1.4/24
```

3. **MIP**

```
set interface ethernet3 mip 1.1.1.2 host 10.1.1.4
```

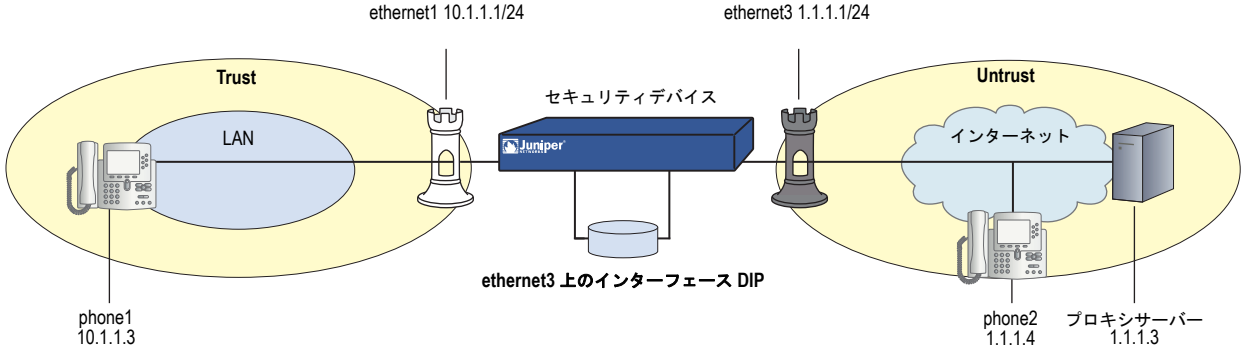
4. **ポリシー**

```
set policy from trust to untrust any phone2 sip nat src permit
set policy from untrust to trust phone2 mip(1.1.1.2) sip permit
save
```

例 : パブリックゾーン内のプロキシ

この例では、phone1 が Trust ゾーン内の ethernet1 インターフェースにあり、phone2 とプロキシサーバーが Untrust (パブリック) ゾーン内の ethernet3 インターフェースにあります。Untrust インターフェース上にインターフェース DIP を設定してから、Untrust ゾーンから Trust ゾーンへの SIP トラフィックを許可するポリシーを作成して、そのポリシー内の DIP を参照します。また、Trust ゾーンから Untrust ゾーンへポリシーを作成して、phone1 の Untrust ゾーン内プロキシサーバーへの登録を許可できます。この例は、Untrust インターフェースで DIP または MIP を使用できるという点で、前の受信コールについての例と似ています (36 ページの「例 : 受信コール (DIP プール)」、および 38 ページの「例 : MIP での受信コール」を参照)。

図 16: パブリックゾーン内のプロキシ



WebUI

1. **インターフェース**

   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone: Untrust
   IP Address/Netmask: 1.1.1.1/24
   Interface mode: Route

2. **アドレス**

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: phone1
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.3/24
   Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: phone2
IP Address/Domain Name:
IP/Netmask: (選択), 1.1.1.4/24
Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: proxy
IP Address/Domain Name:
IP/Netmask: (選択), 1.1.1.3/24
Zone: Untrust

3. インターフェース DIP

Network > Interface > Edit (ethernet3) > DIP: Incoming NAT チェックボックスをオンにします。

4. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択) phone1
Destination Address:
Address Book Entry: (選択) Any
Service: SIP
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: (選択)
(DIP on): None (Use Egress Interface IP)

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), DIP(ethernet3)
Service: SIP
Action: Permit

CLI

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. **アドレス**
   set address trust phone1 10.1.1.3/24
   set address untrust phone2 1.1.1.4/24
   set address untrust proxy 1.1.1.3/24

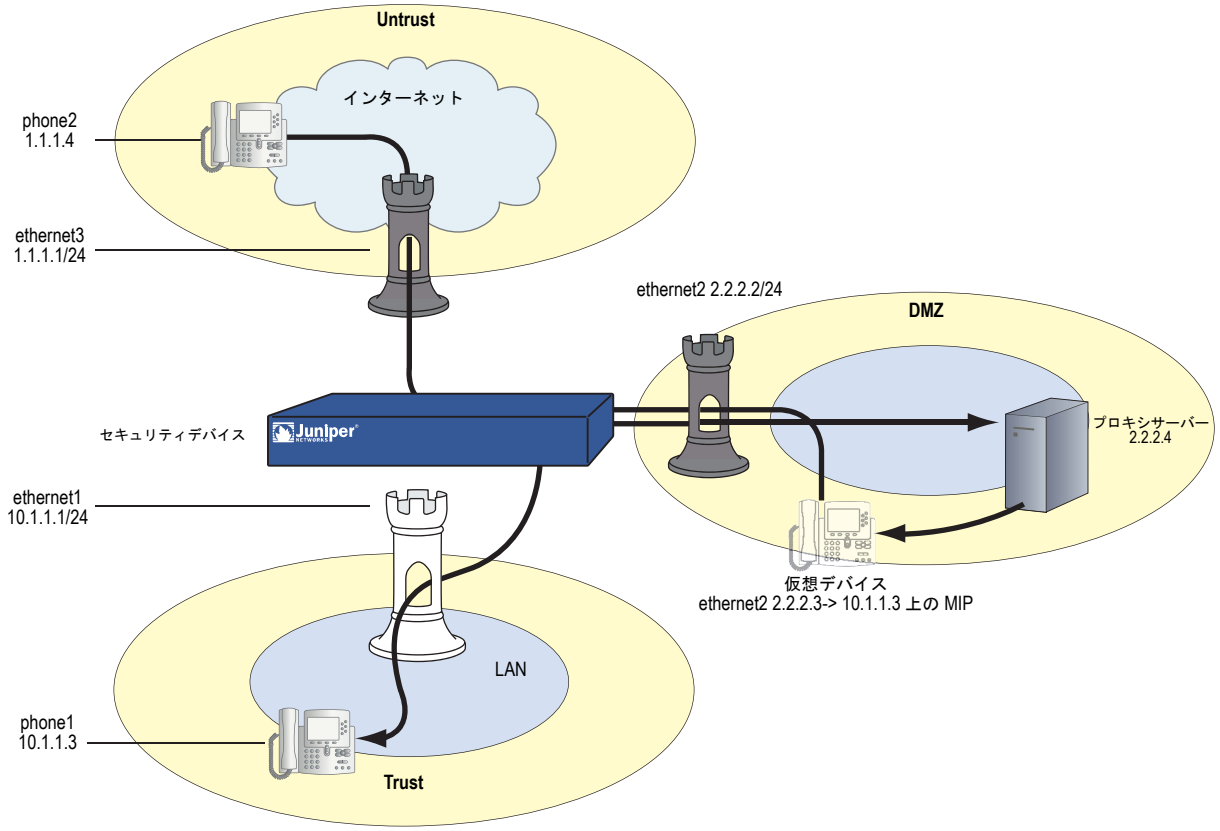
3. **インターフェース DIP**
   set interface ethernet3 dip interface-ip incoming

4. **ポリシー**
   set policy from trust to untrust phone1 any sip nat src permit
   set policy from untrust to trust any dip(ethernet3) sip permit
   save

例 : 3 つのゾーン、DMZ 内のプロキシ

この例では、phone1 が Trust ゾーン内の ethernet1 インターフェースにあり、phone2 が Untrust ゾーン内の ethernet3 インターフェースにあり、プロキシサーバーが DMZ 内の ethernet2 インターフェースにあります。Trust ゾーン内の phone1 の ethernet2 インターフェース上に MIP を配置し、DMZ から Trust ゾーンへのポリシーを作成して、そのポリシー内の MIP を参照します。実際に 3 つのゾーンを使用するには、ゾーン間の双方向ポリシーを作成する必要があります。図 17 の矢印は SIP シグナリングトラフィックの流れを示しています。この場合、Untrust ゾーン内の phone2 が Trust ゾーン内の phone1 を呼び出しています。セッションの開始後、メディアは phone1 と phone2 の間で直接やり取りされます。

図 17: DMZ のプロキシ



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface mode: NAT

   Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

   Zone Name: DMZ
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 2.2.2.2/24

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: phone1
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.3/24
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: phone2
   IP Address/Domain Name:
   IP/Netmask: (選択), 1.1.1.4/24
   Zone: Untrust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: proxy
   IP Address/Domain Name:
   IP/Netmask: (選択), 2.2.2.4/24
   Zone: DMZ

3. **MIP**
   Network > Interfaces > Edit (ethernet2) > MIP > New: 次のように入力してから **OK** をクリックします。

   Mapped IP: 2.2.2.3
   Netmask: 255.255.255.255
   Host IP Address: 10.1.1.3

4. ポリシー

Policies > (From: Trust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), phone1
Destination Address:
Address Book Entry: (選択), proxy
Service: SIP
Action: Permit

> Advanced: 以下を入力して、Return をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: Enable
(DIP on): None (Use Egress Interface IP)

Policies > (From: DMZ, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), proxy
Destination Address:
Address Book Entry: (選択), phone2
Service: SIP
Action: Permit

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), phone2
Destination Address:
Address Book Entry: (選択), phone1
Service: SIP
Action: Permit

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), phone2
Destination Address:
Address Book Entry: (選択), proxy
Service: SIP
Action: Permit

Policies > (From: DMZ, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), proxy
Destination Address:
Address Book Entry: (選択), MIP(2.2.2.3)
Service: SIP
Action: Permit

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), phone1
Destination Address:
Address Book Entry: (**選択**), phone2
Service: SIP
Action: Permit

> Advanced: 以下を入力して、Return をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: Enable
(DIP on): None (Use Egress Interface IP)

CLI

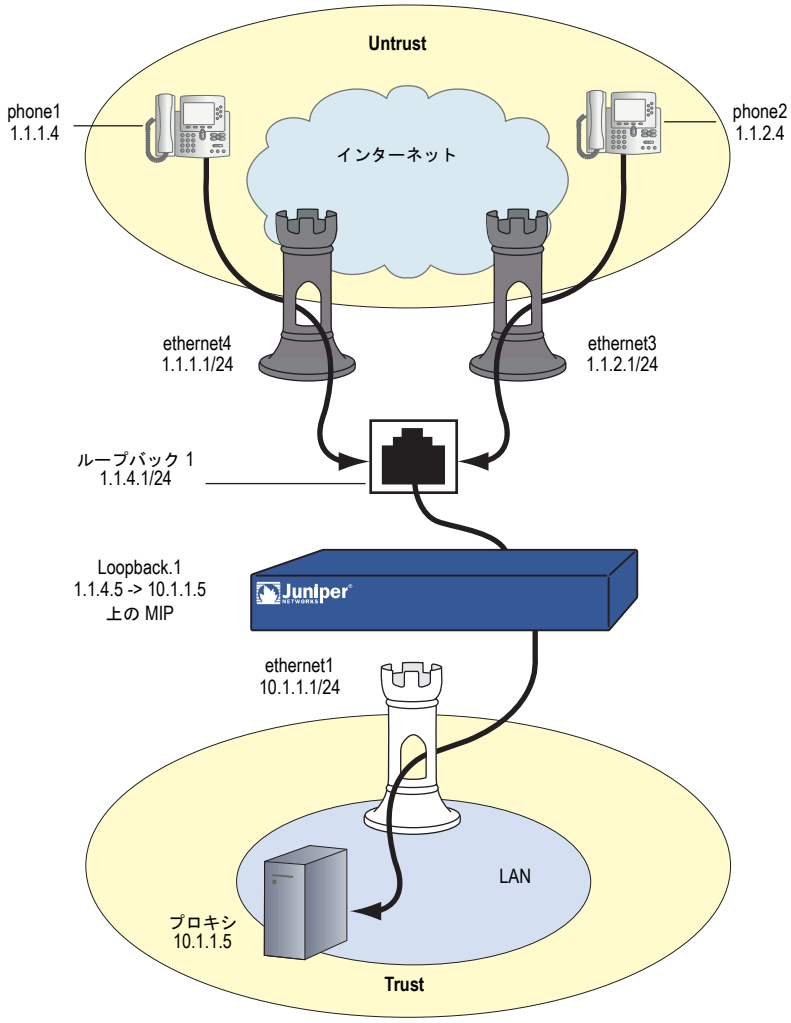
1. **インターフェース**
```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
set interface ethernet2 zone dmz
set interface ethernet2 ip 2.2.2.2/24
set interface ethernet2 route
```
2. **アドレス**
```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address dmz proxy 2.2.2.4
```
3. **MIP**
```
set interface2 mip 2.2.2.3 host 10.1.1.3
```
4. **ポリシー**
```
set policy from trust to dmz phone1 proxy sip nat src permit
set policy from dmz to untrust proxy phone2 sip permit
set policy from untrust to trust phone2 phone1 sip permit
set policy from untrust to dmz phone2 proxy sip permit
set policy from dmz to trust proxy mip(2.2.2.3) sip permit
set policy from trust to untrust phone1 phone2 sip nat src permit
save
```

例 : Untrust ゾーン内

この例では、phone1 が Untrust ゾーン内の ethernet4 インターフェースにあり、phone2 が Untrust ゾーン内 ethernet3 インターフェースのサブネット内にあり、プロキシサーバーが Trust ゾーン内の ethernet1 インターフェースにあります。Untrust ゾーンにある 2 台の電話間にゾーン内 SIP トラフィックを許可するには、ループバックインターフェースを作成して、ethernet3 と ethernet4 インターフェースをループバックグループに追加してから、プロキシサーバーの IP アドレスにループバックインターフェース上の MIP を配置します。ループバックインターフェースを作成すると、単一の MIP を使用して Trust ゾーン内のプロキシ

サーバーを運用できます。Untrust ゾーンではブロッキングがデフォルトでオンになっているため、ゾーン内の通信を許可するにはブロッキングをオフにする必要もあります。ループバックインターフェースを使用する詳細については、8-71 ページの「MIP とループバックインターフェース」を参照してください。

図 18: Untrust ゾーン内



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24

   次のように入力してから **OK** をクリックします。

   Interface mode: NAT

Network > Interfaces > Edit (ethernet4): 次のように入力してから **OK** をクリックします。

Zone: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.2.1/24

Network > Interfaces > New Loopback IF: 次のように入力してから **OK** をクリックします。

Interface Name: loopback.1
Zone: Untrust (trust-vr)
IP Address/Netmask: 1.1.4.1/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: proxy
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.5/32
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: phone1
IP Address/Domain Name:
IP/Netmask: (選択), 1.1.1.4/32
Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: phone2
IP Address/Domain Name:
IP/Netmask: (選択), 1.1.2.4/32
Zone: Untrust

3. ループバックグループ

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

As member of loopback group: (選択) loopback.1
Zone Name: Untrust

Network > Interfaces > Edit (ethernet4): 次のように入力してから **OK** をクリックします。

As member of loopback group: (選択) loopback.1
Zone Name: Untrust

4. MIP

Network > Interfaces > Edit (loopback.1) > MIP > New: 次のように入力してから **OK** をクリックします。

Mapped IP: 1.1.4.5
Netmask: 255.255.255.255
Host IP Address: 10.1.1.5
Host Virtual Router Name: trust-vr

5. ブロッキング

Network > Zones > Edit (Untrust): 次のように入力してから **OK** をクリックします。

Block Intra-Zone Traffic: (**オフ**)

6. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), proxy
Destination Address:
Address Book Entry: (**選択**), Any
Service: SIP
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: Enable
(DIP on): None (Use Egress Interface IP)

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), MIP(1.1.4.5)
Service: SIP
Action: Permit

CLI

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.2.1/24
set interface ethernet3 route
set interface ethernet4 zone untrust
set interface ethernet2 ip 1.1.1.1/24
set interface ethernet2 route
set interface loopback.1 zone untrust
set interface loopback.1 ip 1.1.4.1/24
set interface loopback.1 route
```

2. **アドレス**
   set address trust proxy 10.1.1.5/32
   set address untrust phone1 1.1.1.4/32
   set address untrust phone2 1.1.2.4/32

3. **ループバックグループ**
   set interface ethernet3 loopback-group loopback.1
   set interface ethernet4 loopback-group loopback.1

4. **MIP**
   set interface loopback.1 mip 1.1.4.5 host 10.1.1.5

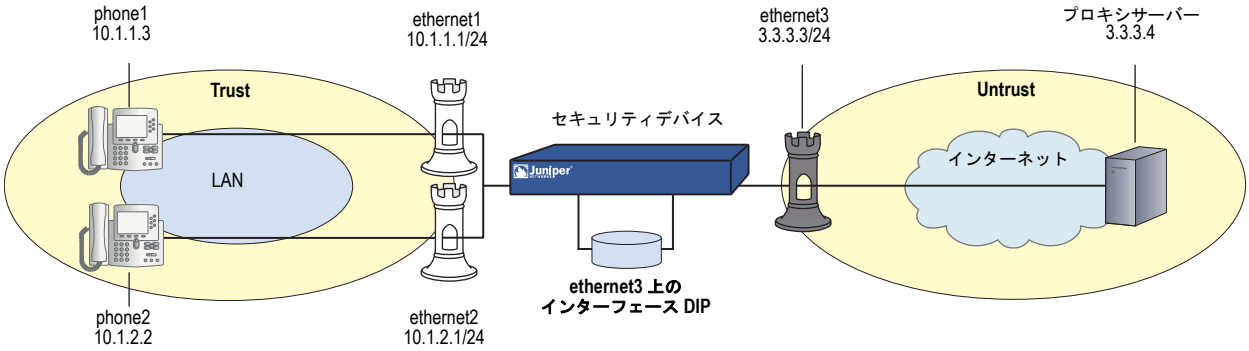
5. **ブロッキング**
   unset zone untrust block

6. **ポリシー**
   set policy from trust to untrust proxy any sip nat src permit
   set policy from untrust to trust any mip(1.1.4.5) sip permit
   save

例 : Trust ゾーン内

この例では、phone1 が Trust ゾーン内の ethernet1 インターフェースにあり、phone2 が Trust ゾーン内の ethernet2 インターフェースにあり、プロキシサーバーが Untrust インターフェース内の ethernet3 インターフェースにあります。Trust ゾーン内の 2 台の電話が互いに通信することを許可するには、ethernet3 インターフェース上に DIP プールを設定してプロキシサーバーとの連絡を許可してから、Trust ゾーンと Untrust ゾーン間の双方向 SIP トラフィックを許可するポリシーを設定します。Trust ゾーンでのブロッキングがデフォルトでオフになっています (定義したカスタムゾーンに同じ)。

図 19: Trust ゾーン内



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface mode: NAT

Network > Interfaces > Edit (ethernet2): 以下を入力して **Apply** をクリックします。

Zone: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.2.1/24
次のように入力してから **OK** をクリックします。
Interface mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 3.3.3.3/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: phone1
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.3/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: phone2
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.2.2/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: proxy
IP Address/Domain Name:
IP/Netmask: (選択), 3.3.3.4/24
Zone: Untrust

3. 受信 NAT での DIP

Network > Interfaces > Edit (ethernet3) > DIP > New: 次のように入力してから **OK** をクリックします。

Incoming NAT: (選択)

4. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), proxy
Service: SIP
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: Enable
(DIP on): None (Use Egress Interface IP)

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address
Address Book Entry: (**選択**) proxy
Destination Address
Address Book Entry: (**選択**) Any
Service: SIP
Action: Permit

> Advanced: 以下を入力して **Return** をクリックすると、拡張オプションが設定されます。

NAT:
Source Translation: (**選択**)
(DIP on): None (Use Egress Interface IP)

CLI

1. **インターフェース**
```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet2 zone trust
set interface ethernet2 ip 10.1.2.1/24
set interface ethernet2 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24
set interface ethernet3 route
```

2. **アドレス**
```
set address trust phone1 10.1.1.3/24
set address trust phone2 10.1.2.2/24
set address untrust proxy 3.3.3.4/24
```

3. **インターフェース DIP**
```
set interface ethernet3 dip interface-ip incoming
```

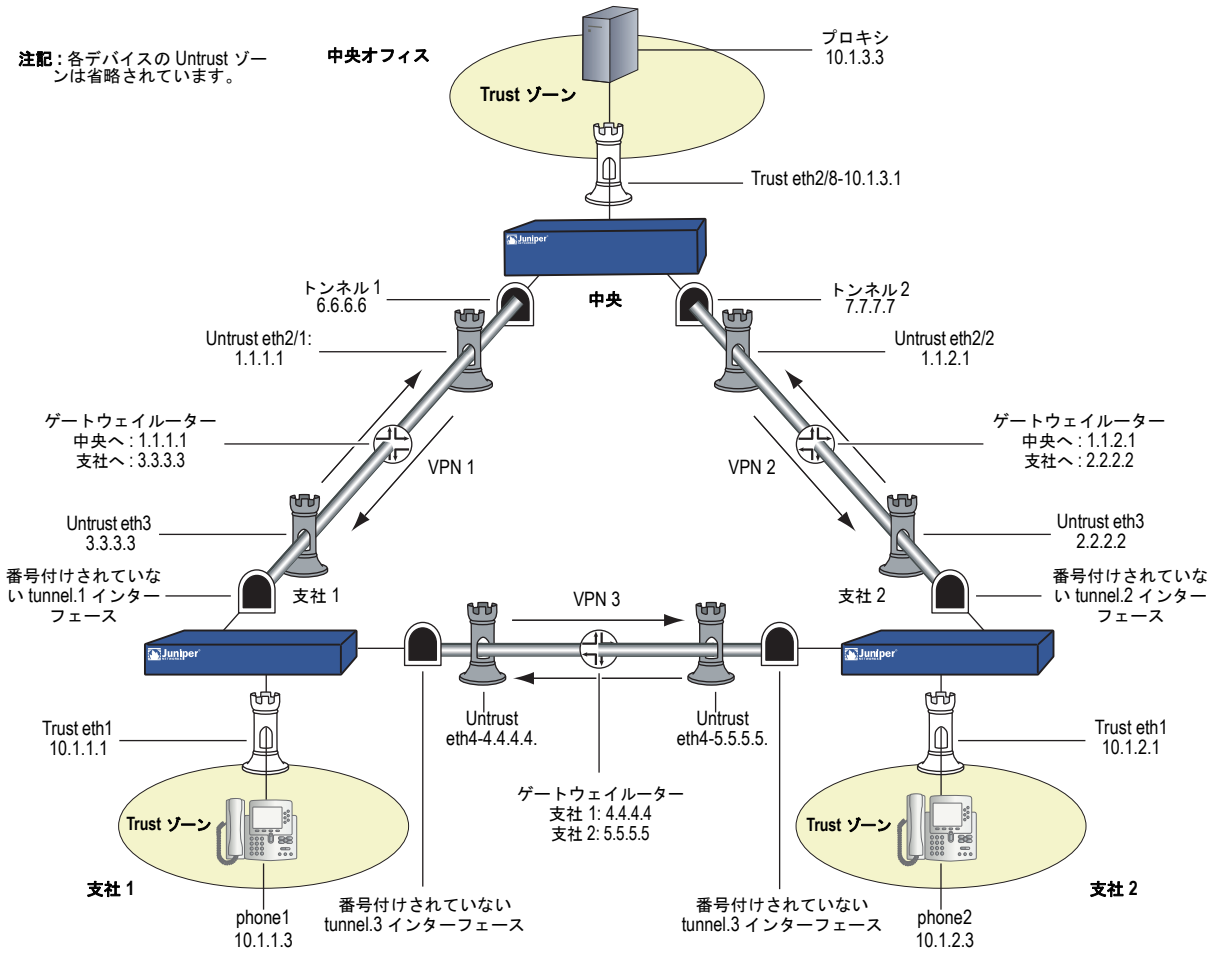
4. **ポリシー**
```
set policy from trust to untrust any proxy sip nat src permit
set policy from untrust to trust proxy dip(ethernet3) sip permit
save
```

例 : フルメッシュ VPN での SIP

この例では、中央オフィスと 2 つの支社がフルメッシュ VPN でリンクされています。各サイトには、1 台のセキュリティデバイスが設置されています。プロキシサーバーが中央オフィスの Trust ゾーンにあり、phone1 が支社 1 の Trust ゾーンにあり、phone2 が支社 2 の Trust ゾーンにあります。デバイスを接続するインターフェースはすべて、それぞれの Untrust ゾーンにあります。各デバイスに他のそれぞれのデバイスと接続するため 2 つのトンネルを設定すると、フルメッシュのネットワークが作成されます。

注 : この例で使用するセキュリティデバイスは、少なくても 3 つの個別構成が可能なインターフェースが使用可能でなければなりません。

図 20: フルメッシュ VPN での SIP



WebUI (中央)

1. **インターフェース**

   Network > Interfaces > Edit (ethernet2/1): 以下を入力して **Apply** をクリックします。

   Zone: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

   Network > Interfaces > Edit (ethernet2/2): 以下を入力して **Apply** をクリックします。

   Zone: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.2.1/24

Network > Interfaces > Edit (ethernet2/8): 以下を入力して **Apply** をクリックします。

Zone: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.3.1/24
次のように入力してから **OK** をクリックします。
Interface mode: ルート

Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 1
Zone (VR): Untrust
IP Address/Netmask: 6.6.6.6/24

Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 2
Zone (VR): Untrust
IP Address/Netmask: 7.7.7.7/24

2. **アドレス**

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: Proxy
IPv4/Netmask: 10.1.3.3/32
Zone: Trust

3. **VPN**

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: to-branch-1
Security Level: Standard
IPvc4/v6 Address/Hostname: 3.3.3.3
Preshare Key: netscreen
Outgoing Interface: ethernet2/1

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn-branch-1

Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Bind to: (選択) Tunnel Interface, tunnel.1

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: to-branch-2
Security Level: Standard
IPvc4/v6 Address/Hostname: 2.2.2.2
Preshare Key: netscreen
Outgoing Interface: ethernet2/2

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn-branch-2

Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Bind to: (選択) Tunnel Interface, tunnel.2

4. ルーティング

Network > Routing > Destination > New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
Interface (選択): tunnel.1

Network > Routing > Destination > New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.2.0/24
Interface (選択): tunnel.2

5. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address (選択) Address Book Entry: Proxy
Destination Address (選択) address Book Entry: Any-IPv4
Service: SIP
Action: Permit

Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

Source Address (選択) Address Book Entry: Any-IPv4
Destination Address (選択) Address Book Entry: Proxy
Service: SIP
Action: Permit

CLI (中央)

1. インターフェース

```
set interface ethernet2/1 zone untrust
set interface ethernet2/1 ip 1.1.1.1/24
set interface ethernet2/2 zone untrust
set interface ethernet2/2 ip 1.1.2.1/24
set interface ethernet2/8 zone trust
set interface ethernet2/8 ip 10.1.3.1/24
set interface ethernet2/8 route
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 6.6.6.6/24
set interface tunnel.2 zone untrust
set interface tunnel.2 ip 7.7.7.7/24
```

2. アドレス

```
set address trust proxy 10.1.3.3/32
```

3. **VPN**

```
set ike gateway to-branch-1 address 3.3.3.3 main outgoing-interface ethernet2/1
    preshare netscreen sec-level standard
set ike gateway to-branch-2 address 2.2.2.2 main outgoing-interface ethernet2/2
    preshare netscreen sec-level standard
set vpn vpn_branch-1 gateway to-branch-1 no-reply tunnel idletime 0 sec-level
    standard
set vpn vpn-branch-1 id 1 bind interface tunnel.1
set vpn vpn-branch-2 gateway to-branch-2 no-reply tunnel idletime 0 sec-level
    standard
set vpn vpn-branch-2 id 2 bind interface tunnel.2
```

4. **ルーティング**

```
set route 10.1.2.0/24 interface tunnel.2
set route 10.1.1.0/24 interface tunnel.1
```

5. **ポリシー**

```
set policy from untrust to trust any proxy sip permit
set policy from trust to untrust proxy any sip permit
save
```

WebUI (支社 1)

1. **インターフェース**

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24
Interface mode: NAT

Network > Interfaces > Edit (ethernet3): 以下を入力して **Apply** をクリックします。

Zone: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 3.3.3.3/24

Network > Interfaces > Edit (ethernet4): 以下を入力して **Apply** をクリックします。

Zone: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 4.4.4.4/24

Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 2
Zone (VR): Untrust
Unnumbered (選択) Interface: ethernet3

Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 3
Zone (VR): Untrust
Unnumbered (選択) Interface: ethernet4

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: phone1
IPv4/Netmask: 10.1.1.3/32
Zone: V1-Trust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: to-central
Security Level: Standard
IPvc4/v6 Address/Hostname: 1.1.2.1
Preshare Key: netscreen
Outgoing Interface: ethernet3

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn-central

Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Bind to (選択): Tunnel Interface, tunnel.1

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: to-ns50
Security Level: Standard
IPvc4/v6 Address/Hostname: 5.5.5.5
Preshare Key: netscreen
Outgoing Interface: ethernet4

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn-ns50

Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Bind to (選択): Tunnel Interface, tunnel.3

4. ルーティング

Network > Routing > Destination > New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.2.0/24
Interface (選択): tunnel.3

Network > Routing > Destination > New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.3.0/24
Interface (選択): tunnel.1

5. **ポリシー**

Policies > (From: Trust, To: Untrust) > New: 次のように入力してから **OK** をクリックします。

Source Address (選択) Address Book Entry: phone2
Destination Address (選択) Address Book Entry: Any-IPv4
Service: SIP
Action: Permit

Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

Source Address (選択) Address Book Entry: Any-IPv4
Destination Address (選択) Address Book Entry: phone2
Service: SIP
Action: Permit

CLI (支社 1)

1. **インターフェース**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 route
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24
set interface ethernet4 zone untrust
set interface ethernet4 ip 4.4.4.4/24
set interface tunnel.2 zone untrust
set interface tunnel.2 ip unnumbered interface ethernet3
set interface tunnel.3 zone untrust
set interface tunnel.3 ip unnumbered interface ethernet4
```

2. **アドレス**

```
set address trust phone1 10.1.1.3/32
```

3. **VPN**

```
set ike gateway to-central address 1.1.1.1 main outgoing-interface ethernet3
    preshare netscreen sec-level standard
set ike gateway to-ns50 address 5.5.5.5 main outgoing-interface ethernet4
    preshare netscreen sec-level standard
set vpn vpncentral gateway to-central no-replay tunnel idletime 0 sec-level standard
set vpn vpncentral bind interface tunnel.1
set vpn vpn-ns50 gateway to-ns50 no-replay tunnel idletime 0 sec-level standard
set vpn vpn-ns50 bind interface tunnel.3
```

4. **ルート**

```
set route 10.1.2.0/24 interface tunnel.3
set route 10.1.3.0/24 interface tunnel.1
```

5. **ポリシー**

```
set policy from trust to untrust phone1 any sip permit
set policy from untrust to trust any phone1 sip permit
save
```

WebUI (支社 2)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.2.1/24
次のように入力してから **OK** をクリックします。
Interface mode: NAT

Network > Interfaces > Edit (ethernet3): 以下を入力して **Apply** をクリックします。

Zone: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > Edit (ethernet4): 以下を入力して **Apply** をクリックします。

Zone: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 4.4.4.4/24

Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 2
Zone (VR): Untrust
Unnumbered (選択) Interface: ethernet3

Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 3
Zone (VR): Untrust
Unnumbered (選択) Interface: ethernet4

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: phone2
IPv4/Netmask: 10.1.2.3/32
Zone: Trust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: to-central
Security Level: Standard
IPvc4/v6 Address/Hostname: 1.1.2.1
Preshare Key: netscreen
Outgoing Interface: ethernet3

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn-central

Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Bind to (選択): Tunnel Interface, tunnel.2

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: to-ns50
Security Level: Standard
IPvc4/v6 Address/Hostname: 4.4.4.4
Preshare Key: netscreen
Outgoing Interface: ethernet4

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn-ns50

Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Bind to (選択): Tunnel Interface, tunnel.3

4. **ルーティング**

Network > Routing > Destination > New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.3.0/24
Interface (選択): tunnel.2

Network > Routing > Destination > New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
Interface (選択): tunnel.3

5. **ポリシー**

Policies > (From: Trust, To: Untrust) New 次のように入力してから **OK** をクリックします。

Source Address (選択) Address Book Entry: phone2
Destination Address (選択) Address Book Entry: Any-IPv4
Service: SIP
Action: Permit

Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

Source Address (選択) Address Book Entry: Any-IPv4
Destination Address (選択) Address Book Entry: phone2
Service: SIP
Action: Permit

CLI (支社 2)

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.2.1/24
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 2.2.2.2/24
   set interface ethernet4 zone untrust
   set interface ethernet4 ip 4.4.4.4/24
   set interface tunnel.2 zone untrust
   set interface tunnel.2 ip unnumbered interface ethernet3
   set interface tunnel.3 zone untrust
   set interface tunnel.3 ip unnumbered interface ethernet4

2. **アドレス**
   set address trust phone2 10.1.2.3/32

3. **VPN**
   set ike gateway to-central address 1.1.2.1 Main outgoing-interface ethernet3
   preshare netscreen sec-level standard
   set ike gateway to-ns50 address 4.4.4.4 Main outgoing-interface ethernet4
   preshare netscreen sec-level standard
   set vpn vpncentral gateway to-central no-replay tunnel idletime 0 sec-level standard
   set vpn vpncentral id 4 bind interface tunnel.2
   set vpn vpn-ns50 gateway to-ns50 no-replay tunnel idletime 0 sec-level standard
   set vpn vpn-ns50 id 5 bind interface tunnel.3

4. **ルート**
   set route 10.1.3.0/24 interface tunnel.2
   set route 10.1.1.0/24 interface tunnel.3

5. **ポリシー**
   set policy from trust to untrust phone2 any sip permit
   set policy from untrust to trust any phone2 sip permit
   save

VoIP サービスの帯域幅管理

標準的な ScreenOS トラフィックシェーピング機構を使用して VoIP サービスの帯域幅を管理するには、以下の方法が推奨されます。

- VoIP トラフィックの帯域幅を保証する - VoIP の通信品質を保証しながらインターフェース上の他のトラフィックタイプを許可する最も有効な方法は、インターフェース上で想定される VoIP トラフィック量に必要な最小の帯域幅を保証するポリシーを作成して、優先順位キューを最高レベルに設定することです。この方法の利点は、VoIP が追加の帯域幅を使用できることです。さらに、VoIP に保証されていない帯域を VoIP が使用していないときに、他のトラフィックタイプがその帯域幅を使用できることです。

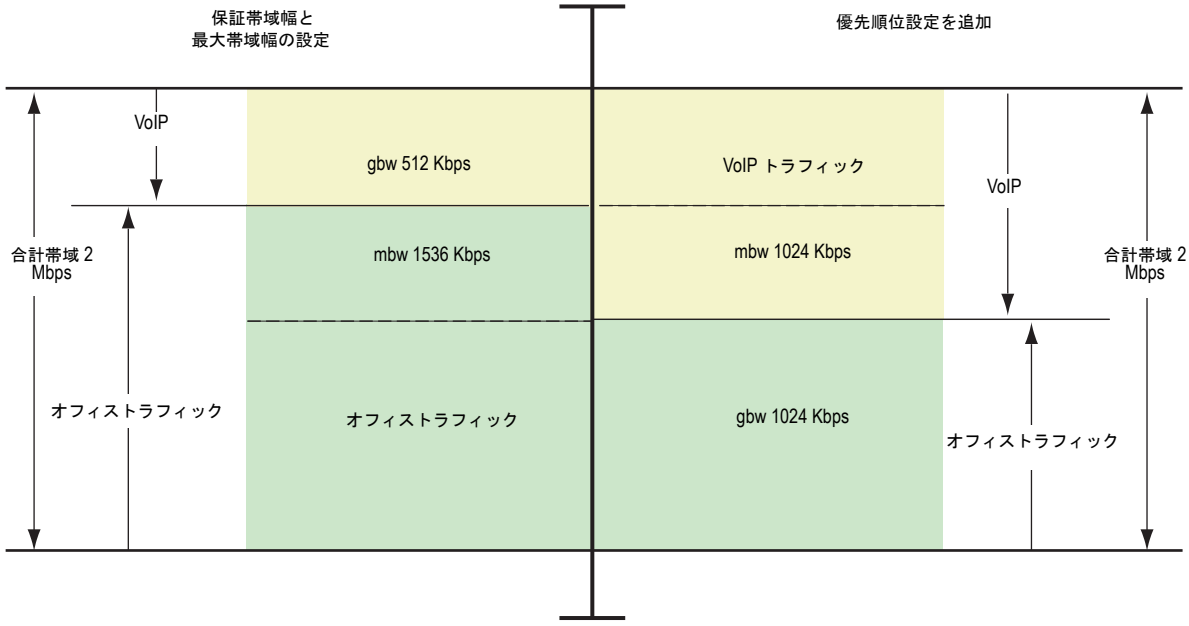
- VoIP 以外のトラフィックの帯域幅を制限する - VoIP 以外のトラフィックについての最大帯域幅を設定すると、残りの帯域を VoIP トラフィックが使用できるようになります。また、VoIP トラフィックの優先順位キューを最高レベルに設定します。この方法の短所は、VoIP 以外のトラフィックは追加の帯域幅を使用できないことです。VoIP トラフィックが使用していないときも使用できません。

- 優先順位キューと DSCP（Differentiated Services Codepoint、差別化されたサービスコードポイント）マーキングの使用 - VoIP トラフィックの帯域幅を保証して、さらに VoIP 以外のトラフィックの帯域幅を制限すると、セキュリティデバイスのスループットを管理することができます。DSCP マーキングを使用すると、設定した優先順位キューのダウンストリームを保持でき、送信元である上流ネットワークデバイスが設定した DSCP 値を受信して維持または変更できます。そのため、通常は LAN または WAN エッジルーターであるネクストホップルーターが、自身の DiffServ ドメインの QoS (通信品質) を強化することができます。VPN 構成では、セキュリティデバイスが IP パケットの外部ヘッダーに印をつけるか（ポリシーでそのように構成されている場合)、または TOS バイトを 0 のままにします。そのため、ネクストホップルーターは暗号化されたトラフィックに正確な QoS を提供することができます。DSCP がポリシー内の優先順位レベルと連携する方法については 175 ページの「トラフィックシェーピング」を参照してください。

65 ページの図 21 は、優先順位レベルを設定することによって、ethernet1 (2 Mbps) インターフェース上の保証帯域幅 (gbw) と最大帯域幅 (mbw) の使用状況に影響を与える様子が示されています。この図では、サポートする VoIP コールが少なくとも 8 つ必要（1 コールにつき 64 Kbps で合計 512 Kbps）であり、時折 最大で 16 コールが必要であると仮定しています。残りの帯域は通常のオフィストラフィック用に保証します。また、オフィストラフィック用で VoIP トラフィックに保障しない帯域の最大値を設定します。これによって、VoIP トラフィックサービスとオフィストラフィックサービスが重複して使用できる帯域が、波線で示されるように 512 Kbps として作成されます。

図 21 の左側は、インターフェース上のオフィストラフィックの帯域使用状況が高く、VoIP トラフィックの帯域使用が低いことを示しています。VoIP トラフィックに必要な帯域幅が急に増えた場合でも、オフィストラフィックサービスより優先順位が高くないと VoIP は帯域幅を取得できません。図 21 の右側における帯域幅の使用状況は、VoIP の優先順位を高くしてオフィストラフィックの優先順位を低くした以外は同じ状況です。帯域と優先順位レベルの構成に関する詳細については、195 ページの「トラフィックシェーピング」を参照してください。

図 21: 優先順位レベルの設定



第 3 章

メディアゲートウェイ制御プロトコルのアプリケーションレイヤーゲートウェイ

本章では、MGCP (メディアゲートウェイ制御プロトコル) ALG (アプリケーションレイヤーゲートウェイ) の概要を示し、実装のファイアウォールセキュリティ機能をリストします。MGCP のアーキテクチャの要約に続いて、一般的なシナリオを例示します。本章のセクションは、以下のようになります。

- 67 ページの「概要」
- 68 ページの「MGCP セキュリティ」
- 69 ページの「MGCP について」
- 74 ページの「例」

概要

MGCP (メディアゲートウェイ制御プロトコル) は、Route モード、透過モード、および NAT (ネットワークアドレス変換) モードのセキュリティデバイス上でサポートされています。MGCP はコールの設定と制御に使うテキストベースのアプリケーションレイヤープロトコルです。MGCP はマスター・スレーブ構成のコール制御アーキテクチャに基づいており、この中でメディアゲートウェイコントローラはコールエージェントを使って、コールコントロールのインテリジェンスを維持し、メディアゲートウェイはコールエージェントの指示を実行します。

MGCP ALG は以下の手順を実行します。

- VoIP シグナリングペイロードの検査を実行します。受信 VoIP シグナリングパケットのペイロードは、関連する RFC と独自の基準に基づいて完全に検査されます。不正パケット攻撃はすべて、ALG がブロックします。
- MGCP シグナリングペイロードの検査を実行します。受信 MGCP シグナリングパケットのペイロードは、RFC 3435 に準拠して完全に検査されます。不正パケット攻撃はすべて、ALG がブロックします。
- ステートフル処理を提供します。対応する VoIP ベースのステートマシンは、構文解析された情報を処理するために呼び出されます。ステート外またはトランザクション外のパケットは特定され、正しく処理されます。

- NAT (ネットワークアドレス変換) を実行します。ペイロードで埋め込まれている IP アドレスとポート情報は、既存のルーティング情報とネットワークトポリジーに基づいて正しく変換され、必要に応じて、変換された IP アドレスとポート番号に置換えられます。

- VoIP トラフィックのピンホールを管理します。VoIP ネットワークをセキュアに維持するために、メディアまたはシグナリングに使う IP アドレスとポート情報は ALG によって特定され、必要なピンホールがあれば動的に作成され、コールセットアップ中に閉じられます。

MGCP セキュリティ

MGCP ALG には、次のセキュリティ機能が搭載されています。

- DoS (サービス拒否) 攻撃からの保護 - ALG はUDP パケットレベル、トランザクションレベル、およびコールレベルでステートフルな検査を実行します。RFC 3435 メッセージ形式、トランザクションステート、およびコールステートに一致する MGCP パケットが処理されます。その他すべてのメッセージはドロップされます。

- ゲートウェイとゲートウェイコントローラ間のファイアウォールポリシーの実施 (シグナリングポリシー)。

- ゲートウェイ間のファイアウォールポリシーの実施 (メディアポリシー)。

- ゲートウェイごとの MGCP メッセージフラッド制御。ゲートウェイが正しく機能していなかったり、ハッカーに侵入されている場合でも、VoIP ネットワーク全体が中断されることはありません。ダメージは、ゲートウェイごとのフラッド制御と一緒に、影響を受けたゲートウェイ内に閉じ込められます。

- ゲートウェイごとの MGCP 接続フラッド制御。

- システム障害が発生した場合、コールが（処理中のコールも含めて）スタンバイファイアウォールに切り替えられる際のシームレスなスイッチオーバー / フェールオーバー

MGCP について

MGCP は、コールの設定と制御に使用できるテキストベースのアプリケーションレイヤープロトコルです。プロトコルはマスター・スレーブ構成のコール制御アーキテクチャに基づいています。この中で、メディアゲートウェイコントローラ (コールエージェント) は、コールコントロールのインテリジェンスを維持し、メディアゲートウェイはコールエージェントからの指示を実行します。

MGCP 内のエンティティ

MGCP には 4 つの基本エンティティがあります。

- 69 ページの「端点」
- 69 ページの「接続」
- 69 ページの「コール」
- 70 ページの「コールエージェント」

端点

MG (メディアゲートウェイ) は端点の集まりです。端点は、アナログライン、トランク、または他のアクセスポイントでもかまいません。端点には次のような名前が付けられます。

local-endpoint-name@domain-name

有効な端点 ID には次のようなものが挙げられます。

group1/Trk8@mynetwork.net

group2/Trk1/*@[192.168.10.8] (ワイルドカードを使用)

$@voiptel.net (MG 内の任意の端点)

*@voiptel.net (MG 内のすべての端点)

接続

接続は、コール設定中に MG によって各端点で作成されます。通常の VoIP コールには 2 つの接続があります。複雑なコール (サードパーティコールや会議コールなど) には多くの接続が必要になる場合があります。MGC (メディアゲートウェイコントローラ) は、メディアゲートウェイに接続を作成、変更、削除、監査するように指示できます。

接続は、接続 ID によって特定されます。この ID は、接続の作成要求時に MG によって作成されます。接続 ID は 16 進数の文字列で表示し、32 文字以内で表記します。

コール

コールは、新しいコールの確立時に MGC によって作成されるコール ID によって特定されます。コール ID は 16 進数の文字列で表示し、32 文字以内で表記します。コール ID は MGC 内では一意的です。2 つ以上の接続が同じコールに属する場合は、同じコール ID を持つことができます。

コールエージェント

VoIP ネットワークの信頼性を高めるために、1 つ以上のコールエージェント (メディアゲートウェイコントローラとも呼ぶ) が MGCP でサポートされています。例として、2 つのコールエージェント名を以下に示します。

CallAgent@voipCA.mynetwork.com

voipCA.mynetwork.com

一部のネットワークアドレスは、DNS (ドメイン名システム) で 1 つのドメイン名で関連付けが可能です。DNS クエリ / 応答データの TTL（生存時間）を追跡し、他の代替ネットワークアドレスを使って再伝送を実装すると、MGCP でスイッチオーバーとフェールオーバーを達成できます。

*通知済みエンティティ*の概念は、MGCP では不可欠です。端点の通知済みエンティティは、現在その端点を制御しているコールエージェントです。端点は、すべての MGCP コマンドを通知済みエンティティに送信します。ただし、異なるコールエージェントが MGCP コマンドをこの端点に送信する場合があります。

通知済みエンティティは起動時に用意された値に設定されますが、MGCP メッセージに含まれた *NotifiedEntity* パラメータを使って、コールエージェントが変更することができます。端点の通知済みエンティティが空である、または明確に設定されていない場合、値はデフォルトで、その端点用に最後に正常に受信した非監査 MGCP コマンドのソースアドレスになります。

コマンド

MGCP プロトコルは、端点と接続を制御するために 9 個のコマンドを定義します。すべてのコマンドは、コマンドヘッダーから構成されており、ヘッダーの後に SDP (セッション記述プロトコル) 情報が入っているものもあります。コマンドヘッダーには次の要素が含まれています。

- コマンドライン: コマンドの動詞 + トランザクション ID + 端点 ID + MGCP バージョン
- パラメータ名とその後にパラメータ値が続くゼロ以上のパラメータライン

表 3 は、サポートされている MGCP コマンドを各コマンドの説明、コマンド構文、例を入れてリストしたものです。コマンド構文の完全な詳細については、RFC 2234 を参照してください。

表 3: MGCP コマンド

コマンドの動詞	説明	コマンド構文	例
EPCF	EndpointConfiguration - コールエージェントが、端点のライン側で期待されるコーディングの特徴 (a-law、mu-law) をゲートウェイに通知する場合に使用します。	ReturnCode [PackageList] EndpointConfiguration (EndpointId, [BearerInformation])	EPCF 2012 wxx/T2@mynet.com MGCP 1.0 B: e:mu
CRCX	CreateConnection - コールエージェントが、端点を内部に入れてゲートウェアとの接続を作成するようにゲートウェイに指示する場合に使用します。	ReturnCode, [ConnectionId,] [SpecificEndPointId,] [LocalConnectionDescriptor,] [SecondEndPointId,] [SecondConnectionId,][PackageList] CreateConnection (CallId, EndpointId, [NotifiedEntity,] [LocalConnectionOption,] Mode, [{RemoteConnectionDescriptor | SecondEndpointId},] [encapsulated RQNT,] [encapsulated EPCF])	CRCX 1205 aaln/1@gw-25.att.net MGCP 1.0 C: A3C47F21456789F0 L: p:10, a:PCMU M: sendrecv X: 0123456789AD R: L/hd S: L/rg v = 0 o = - 25678 753849 IN IP4 128.96.41.1 s = - c = IN IP4 128.96.41.1 t = 0 0 m = audio 3456 RTP/AVP 0
MDCX	ModifyConnection - コールエージェントが、既存の接続用のパラメータを変更するようにゲートウェイに指示する場合に使用します。	ReturnCode, [LocalConnectionDescriptor,] [PackageList] ModifyConnection (CallId, EndpointId, ConnectionId, [NotifiedEntity,] [LocalConnectionOption,] [Mode,] [RemoteConnectionDescriptor,] [encapsulated RQNT,] [encapsulated EPCF])	MDCX 1210 aaln/1@rgw-25.att.net MGCP 1.0 C: A3C47F21456789F0 I: FDE234C8 M: recvonly X: 0123456789AE R: L/hu S: G/rt v = 0 o = - 4723891 7428910 IN IP4 128.96.63.25 s = - c = IN IP4 128.96.63.25 t = 0 0 m = audio 3456 RTP/AVP 0
DLCX	DeleteConnection - コールエージェントが、既存の接続を削除するようにゲートウェイに指示する場合に使用します。 ゲートウェアが持続できない接続を解除する場合にも使用できます。	ReturnCode, ConnectionParameters, [PackageList] DeleteConnection (CallId, EndpointId, ConnectionId, [NotifiedEntity,] [encapsulated RQNT,] [encapsulated EPCF])	例 1: MGC -> MG DLCX 9210 aaln/1@rgw-25.att.net MGCP 1.0 C: A3C47F21456789F0 I: FDE234C8 例 2: MG -> MGC DLCX 9310 aaln/1@rgw-25.att.net MGCP 1.0 C: A3C47F21456789F0 I: FDE234C8 E: 900 — ハードウェアエラー P: PS = 1245, OS = 62345, PR = 780, OR = 45123, PL = 10, JI = 27, LA = 48

コマンドの動詞	説明	コマンド構文	例
RQNT	NotificationRequest コマンドは、コールエージェントが特定の端点の指定イベントまたはシグナルを監視するよう MG に指示する場合に使用します。	ReturnCode, [PackageList] NotificationRequest[(EndpointId, [NotifiedEntity,] [RequestedEvents,] RequestIdentifier, [DigitMap,] [SignalRequests,] [QuarantineHandling,] [DetectEvents,] [encapsulated EPCF])	RQNT 1205 aaln/1@rgw-25.att.net MGCP 1.0 N: ca-new@callagent-ca.att.net X: 0123456789AA R: L/hd (A, E(S(L/dl),R(L/oc,L/hu,D/[0-9#*T](D)))) D: (0T|00T|xx|91xxxxxxxxxx|9011x.T) S: T: G/ft
NTFY	Notify - ゲートウェイが、要求イベントまたはシグナルの発生時間をコールエージェントに通知する場合に使用します。	ReturnCode, [PackageList] Notify (EndpointID, [NotifiedEntity,] RequestIdentifier, ObservedEvents)	NTFY 2002 aaln/1@rgw-25.att.net MGCP 1.0 N: ca@ca1.att.net:5678 X: 0123456789AC O: L/hd,D/9,D/1,D/2,D/0,D/1,D/8,D/2,D/9,D/4, D/2,D/6,D/6
AUEP	AuditEndpoint - コールエージェントが、端点のステータスを監視する場合に使用します。	ReturnCode, EndPointIdList, | { [RequestedEvents,] [QuarantineHandling,] [DigitMap,] [SignalRequests,] [RequestedIdentifier,] [NotifiedEntity,] [ConnectionIdentifier,] [DetectEvents,] [ObservedEvents,] [EventStats,] [BearerInformation,] [BearerMethod,] [RestartDelay,] [ReasonCode,] [MaxMGCPDatagram,] [Capabilities]} [PackageList] AuditEndpoint (EndpointId, [RequestedInfo])	例 1: AUEP 1201 aaln/1@rgw-25.att.net MGCP 1.0 F: A, R,D,S,X,N,I,T,O 例 2: AUEP 1200 *@rgw-25.att.net MGCP 1.0
AUCX	AuditConnection - コールエージェントが、接続に使用するパラメータを収集する場合に使います。	ReturnCode, [CallId,] [NotifiedEntity,] [LocalConnectionOptions,] [Mode,] [RemoteConnectionDescriptor,] [LocalConnectionDescriptor,] [ConnectionParameters,] [PackageList] AuditConnection (EndpointId, ConnectionId, RequestedInfo)	AUCX 3003 aaln/1@rgw-25.att.net MGCP 1.0 I: 32F345E2 F: C,N,L,M,LC,P
RSIP	RestartInProgress - ゲートウェイが、1 つ以上の端点が使用されていない、または再使用されていることをコールエージェントに通知する場合に使用します。	ReturnCode, [NotifiedEntity,] [PackageList] RestartInProgress (EndpointId, RestartMethod, [RestartDelay,] [ReasonCode])	RSIP 5200 aaln/1@rg2-25.att.net MGCP 1.0 RM: graceful RD: 300

応答コード

コールエージェントまたはゲートウェイによって送信される各コマンドは、正常に送信されるされないに関係なく、応答コードが必要です。応答コードは応答メッセージのヘッダーにあり、ヘッダーの後にセッション記述情報を加えることもできます。

応答ヘッダーは応答ラインから構成されており、その後にはゼロ以上のパラメータラインが続きます。各ラインにはパラメータ名の文字が含まれており、その後には値が続きます。応答ヘッダーは 3 桁の応答コード、トランザクション ID、およびオプションとしてその後に続くコメントから構成されています。次の応答メッセージの応答ヘッダーは、応答コード 200 (正常に完了)、その後に ID 1204、およびコメント OK を示したものです。

```
200 1204 OK
I: FDE234C8

v=0
o=- 25678 753849 IN IP4 128.96.41.1
s=-
c=IN IP4 128.96.41.1
t=0 0
m=audio 3456 RTP/AVP 96
a=rtpmap:96 G726-32/8000
```

応答コードの範囲は次のように定義されます。

- 000 - 099: 応答が確認されたことを示します。
- 100 - 199: 一時的な応答を示します。
- 200 - 299: 正常に完了したことを示します (最終応答)。
- 400 - 499: 一時エラーを示します (最終応答)。
- 500 - 599: 永続的なエラーを示します (最終応答)。

応答コードの詳細については、RFC 3661 を参照してください。

コマンドへの応答は、現在通知されたエンティティでなく、コマンドのソースアドレスに送信されます。メディアゲートウェイは、さまざまなネットワークアドレスから同時に MGCP コマンドを受信し、対応するネットワークアドレスに応答を送信することができます。ただし、MGCP コマンドはすべて、現在通知したエンティティに送信されます。

例

このセクションには、以下の構成例があります。

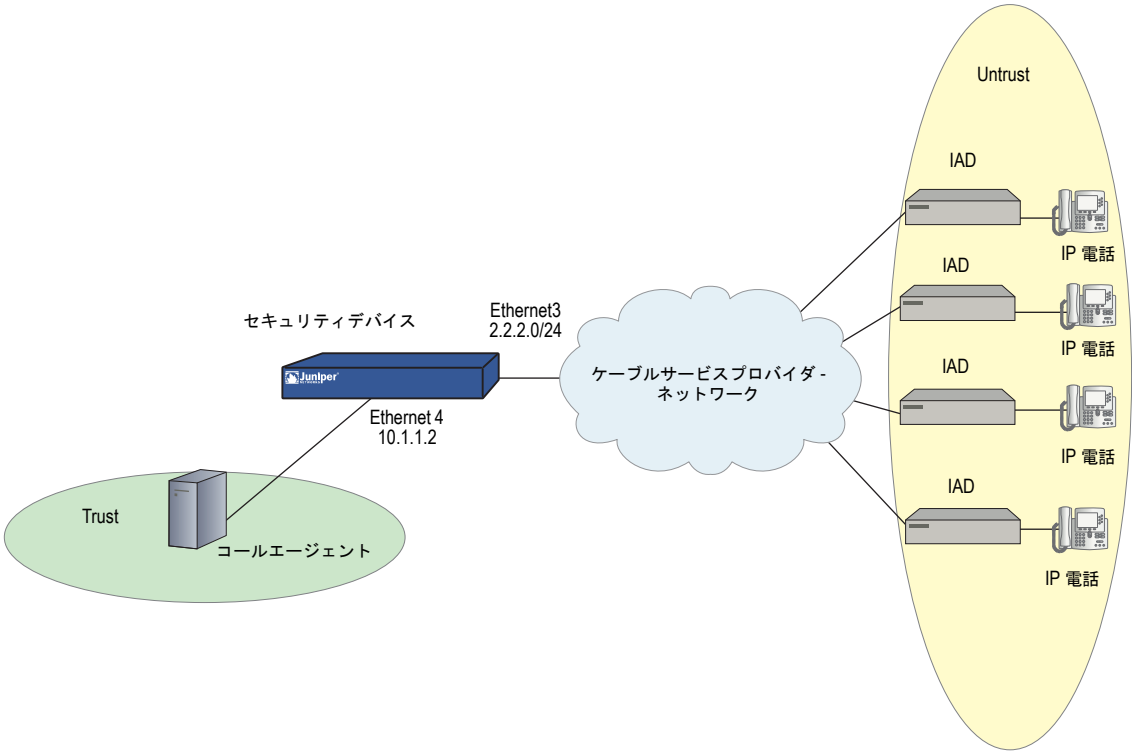
- 74 ページの「加入者の自宅におけるメディアゲートウェイ - ISP でのコールエージェント」
- 76 ページの「ISP ホストサービス」

加入者の自宅におけるメディアゲートウェイ - ISP でのコールエージェント

この例 (図 22 を参照) では、居住ケーブルサービスプロバイダでセキュリティデバイスを設定し、住宅加入者のネットワーク用に MGCP をサポートします。セキュリティデバイスとコールエージェントは、ケーブルサービスプロバイダの構内にあります。IAD (総合アクセスデバイス) またはセットトップボックスは、各加入者の自宅でゲートウェイとしての役割を果たし、各 IAD は異なる住居を示します。コールエージェントは trust_ca zone、住宅用のお客様は res_cust zone にあります。

ゾーン (お客様用には untrust_subscriber、サービスプロバイダ用には trust_ca) を作成した後は、アドレスとポリシーを設定します。ゲートウェイが異なるゾーンに存在するためにメディアトラフィックのポリシーが必要になることはよくありますが、この例では両方のゲートウェイが同じサブネットにあります。ゲートウェイ間の RTP トラフィックはファイアウォールを通過しないため、メディア用のポリシーは必要ありません。

図 22: 加入者の自宅におけるメディアゲートウェイ



WebUI

1. **ゾーン**

   Network > Zones > New: 次のように入力してから **OK** をクリックします。

   Zone Name: untrust_subscriber

   Network > Zones > New: 次のように入力してから **OK** をクリックします。

   Zone Name: trust_ca

2. **アドレス**

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: SubscriberSubNet
   Comment: 加入者のネットワーク
   IP Address/Domain Name:
   IP/Netmask: (選択), 2.2.2.0/24
   Zone: untrust-subscriber

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: call_agent1
   Comment: No.1 コールエージェント
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.101/32
   Zone: trust_ca

3. **インターフェース**

   Network > Interfaces > Edit (ethernet3): 以下を入力して **Apply** をクリックします。

   Zone Name: untrust_subscriber
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 2.2.2.0/24
   次のように入力してから **OK** をクリックします。
   Interface mode: Route

   Network > Interfaces > Edit (ethernet4): 以下を入力して **Apply** をクリックします。

   Zone Name: trust_ca
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.101/32
   次のように入力してから **OK** をクリックします。
   Interface mode: Route

4. **ポリシー**

   Policies > (From: trust-ca, To: untrust_subscriber) New: 次のように入力してから **OK** をクリックします。

   Name: Pol-CA-To-Subscribers
   Source Address
   Address Book Entry: (選択), call_agent1
   Destination Address
   Address Book Entry: (選択), SubscriberSubNet
   Service: MGCP-UA
   Action: Permit

Policies > (From: untrust_subscriber, To: trust-ca) New: 次のように入力してから **OK** をクリックします。

Name: Pol-Subscribers-To-CA
Source Address
Address Book Entry: (選択), SubscriberSubNet
Destination Address
Address Book Entry: (選択), call_agent1
Service: MGCP-CA
Action: Permit

CLI

1. **ゾーン**
set zone name untrust_subscriber
set zone name trust_ca

2. **アドレス**
set address untrust_subscriber SubscriberSubNet 2.2.2.0 255.255.255.0 “Our subscribers' network”
set address trust_ca call_agent1 10.1.1.101 255.255.255.255 “Our No. 1 call agent”

3. **インターフェース**
set interface ethernet3 zone untrust_subscriber “Our subscribers’ network”
set interface ethernet3 ip 2.2.2.0/24
set interface ethernet3 route

set interface ethernet4 zone trust_ca “Our No. 1 call agent”
set interface ethernet4 ip 10.1.1.2/24
set interface ethernet2 route

4. **ポリシー**
set policy name Pol-CA-TO-Subscribers from trust_ca to untrust_subscriber call_agent1 SubscriberSubNet mgcp-ua permit
set policy name Pol-Subscribers-To-CA from untrust_subscriber to trust_ca SubscriberSubNet call_agent1 mgcp-ca permit

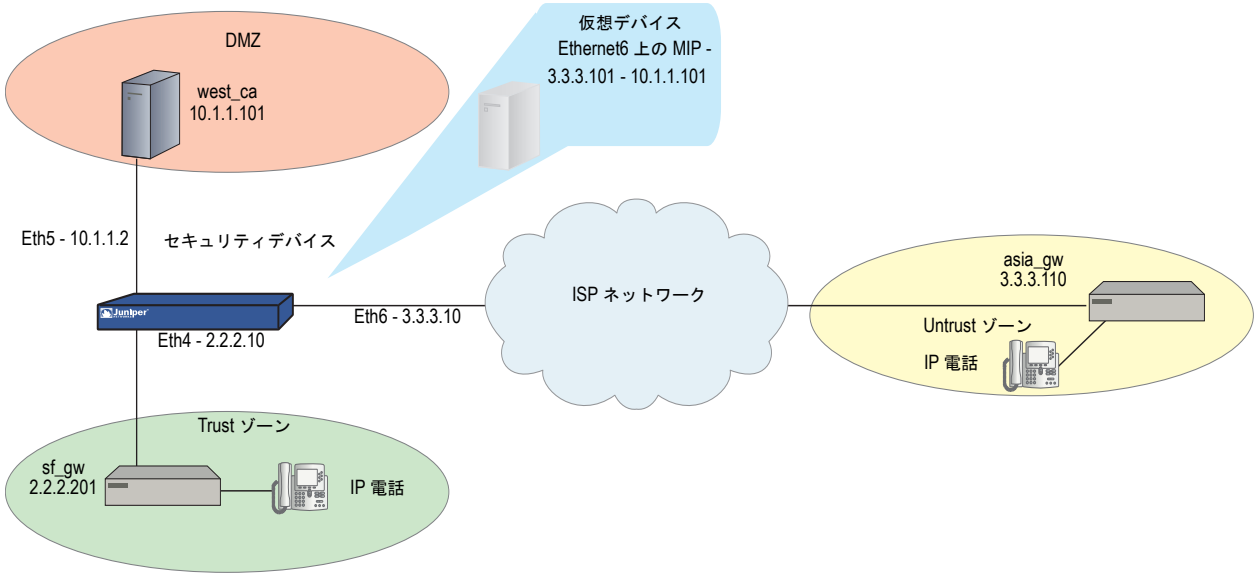
ISP ホストサービス

この例 (図 23 を参照) では、アメリカ西海岸にある ISP はアジアとサンフランシスコのお客様に MGCP サービスを提供します。アジアのお客様は Untrust ゾーンにあり、ゲートウェイ : asia_gw（3.3.3.110）でサポートされます。サンフランシスコのお客様は Trust ゾーンにあり、ゲートウェイ : sf_gw（2.2.2.201）でサポートされます。コールエージェント : west_ca（10.1.1.101）は、DMZ にあります。

ゲートウェイとコールエージェントのアドレスを設定した後は、インターフェースを設定します。その際に、信頼できる ethernet4 と ethernet5 を Route モードにすると、コール設定後にメディアを直接ストリームできます。DMZ 内のコールエージェントの IP アドレスが露出されないようにするには、MIP を ethernet6 に配置します。つまり、コールエージェントの IP アドレス（10.1.1.101）を、ethernet6 インターフェース上のアドレスプールの IP アドレスにマップします。この場合、アドレスは 3.3.3.101 です。3.3.3.101.

最後に、ポリシーを作成します。DMZ のコールエージェントと Untrusted ゾーンのゲートウェイ間で MGCP シグナリングを行うには、各方向に対してコールエージェントを保護する MIP を参照しているポリシーを 1 つ作成します。さらにもう 1 組のポリシーを作成して、コールエージェントと Trust ゾーンのゲートウェイの間でもシグナリングを可能にします。Trusted と Untrusted ゾーンのゲートウェイ間で双方向で通信できるようにするには、1 つのポリシーで十分です。

図 23: ISP ホストサービス



WebUI

1. **アドレス**

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: sf_gw
   Comment: gateway in asia
   IP Address/Domain Name:
   IP/Netmask: (選択), 2.2.2.201/32
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: asia_gw
   Comment: gateway in sf
   IP Address/Domain Name:
   IP/Netmask: (選択), 3.3.3.110/32
   Zone: Untrust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: west_ca
   Comment: ca in west coast
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.101/32
   Zone: DMZ

2. **インターフェース**
   Network > Interfaces > Edit (ethernet4): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 2.2.2.10/24
   次のように入力してから **OK** をクリックします。
   Interface mode: Route

   Network > Interfaces > Edit (ethernet5): 以下を入力して **Apply** をクリックします。

   Zone Name: DMZ
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.2/24
   次のように入力してから **OK** をクリックします。
   Interface mode: Route

   Network > Interfaces > Edit (ethernet6): 以下を入力して **Apply** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 3.3.3.10/24
   次のように入力してから **OK** をクリックします。
   Interface mode: NAT

3. **MIP**
   Network > Interfaces > Edit (ethernet6) > MIP > New: 次のように入力してから **OK** をクリックします。

   Mapped IP: 3.3.3.101
   Netmask: 255.255.255.255
   Host IP Address: 10.1.1.101
   Host Virtual Router Name: trust-vr

4. **ポリシー**
   Policies > (From: DMZ To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address
   　　Address Book Entry: (選択), west_ca
   Destination Address
   　　Address Book Entry: (選択), asia_gw
   Service: MGCP-UA
   Action: Permit

   Policies > (From: Untrust To: DMZ) New: 次のように入力してから **OK** をクリックします。

   Source Address
   　　Address Book Entry: (選択), asia_gw
   Destination Address
   　　Address Book Entry: (選択), west_ca
   Service: MGCP-CA
   Action: Permit

Policies > (From: Trust To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address
Address Book Entry: (選択), sf_gw
Destination Address
Address Book Entry: (選択), west_ca
Service: MGCP-CA
Action: Permit

Policies > (From: DMZ To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address
Address Book Entry: (選択), west_ca
Destination Address
Address Book Entry: (選択), sf_gw
Service: MGCP-UA
Action: Permit

Policies > (From: Trust To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address
Address Book Entry: (選択), sf_gw
Destination Address
Address Book Entry: (選択), asia_gw
Service: MGCP-UA
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: (選択)
DIP on: None (Use Egress Interface IP)

CLI

1. **アドレス**
set address trust sf_gw 2.2.2.201/32 “gateway in s.f.”
set address untrust asia_gw 3.3.3.110/32 “gateway in asia”
set address dmz west_ca 10.1.1.101/32 “ca in west coast”

2. **インターフェース**
set interface ethernet4 ip 2.2.2.10/24
set interface ethernet2 route
set interface ethernet4 zone trust

set interface ethernet5 ip 10.1.1.2/24
set interface ethernet5 route
set interface ethernet5 zone dmz

set interface ethernet6 ip 3.3.3.10/24
set interface ethernet6 zone untrust

3. **マップ IP アドレス**
set interface ethernet6 mip 3.3.3.101 host 10.1.1.101 netmask 255.255.255.255 vrouter trust-vr

4. **ポリシー**

```
set policy from dmz to untrust west_ca asia_gw mgcp-ua permit
set policy from untrust to dmz asia_gw mip(3.3.3.101) mgcp-ca permit

set policy from trust to dmz sf_gw west_ca mgcp-ca permit
set policy from dmz to trust west_ca sf_gw mgcp-ua permit

set policy from trust to untrust sf_gw asia_gw mgcp-ua nat src permit
```

第 4 章

スキニィクライアント制御プロトコルのアプリケーションレイヤーゲートウェイ

本章では、SCCP（スキニィクライアント制御プロトコル）ALG（アプリケーションレイヤーゲートウェイ）の概要を示し、実装のファイアウォールセキュリティ機能をリストします。SCCP のアーキテクチャの要約に続いて、一般的なシナリオを例示します。本章のセクションは、以下のようになります。

- 81 ページの「概要」
- 82 ページの「SCCP セキュリティ」
- 88 ページの「例」

概要

SCCP（スキニィクライアント制御プロトコル）は、ルートモード、透過モード、NAT（ネットワークアドレス変換）モードのセキュリティデバイスによってサポートされます。SCCP はバイナリベースのアプリケーションレイヤープロトコルで、VoIP（音声 IP 化プロトコル）コールの設定と制御に使用されます。SCCP アーキテクチャでは、コールマネージャとして知られる Cisco H.323 プロキシがほとんどの処理を行います。エンドステーションとも呼ばれる IP 電話は、スキニィクライアントを実行し、ポート 2000 の TCP 経由でプライマリの（ある場合はセカンダリも）コールマネージャに接続して、同プライマリコールマネージャに登録します。この接続は、スキニィクライアントが送受信するコールを確立するのに使用されます。

SCCP ALG は、次をサポートします。

- あるスキニィクライアントから、コールマネージャを介して、別のスキニィクライアントへ向かうコールのフロー
- シームレスなフェールオーバー - プライマリで障害が発生している間、すべてのコールをスタンバイのファイアウォールへ切り替えます。
- VoIP シグナリングパケットペイロードの監視 - 関連する RFC と独自の基準に基づき、受信 VoIP シグナリングパケットのペイロードを完全に監視します。不正パケット攻撃はすべて、ALG がブロックします。
- SCCP シグナリングパケットペイロードの監視 - RFC 3435 に基づき、受信 SCCP シグナリングパケットのペイロードを完全に監視します。不正なパケット攻撃はどれも、ALG がブロックします。

- パケット状態処理 - 対応する VoIP ベースの状態マシンを起動し、解析された情報を処理します。ステート外またはトランザクション外のパケットは特定され、正しく処理されます。
- NAT（ネットワークアドレス変換） - 既存のルーティング情報とネットワークトポロジ、さらに必要に応じて変換済みの IP アドレスとポートナンバーに基づき、ペイロードに組み込まれている IP アドレスとポート情報を変換します。
- VoIP トラフィックのピンホールの作成と管理 - メディアまたはシグナリングに使用される IP アドレスとポートナンバーを識別し、メディアが安全にストリームできるようにピンホールを動的に開き（閉じ）ます。

SCCP セキュリティ

SCCP ALG には、次のセキュリティ機能が搭載されています。

- DoS (サービス拒否) 攻撃の防御 ALG は、UDP パケットレベル、トランザクションレベル、コールレベルでパケットの状態を監視します。SCCP メッセージ形式、トランザクション状態、コール状態に一致するパケットが処理されます。その他すべてのメッセージはドロップされます。
- Cisco IP とコールマネージャとの間（クラスタ内）でファイアウォールポリシーを実施
- コールマネージャ間（クラスタ間）でファイアウォールポリシーを実施
- コールマネージャフラッド制御障害が発生している接続先クライアントまたは欠陥のあるデバイスによる大量の新規コールでフラッド状態になることからコールマネージャを保護します。
- ゲートウェイ間のファイアウォールポリシーの実施 (メディアポリシー)。
- ゲートウェイごとの SCCP 接続フラッド制御
- システム障害が発生した場合、コールが（処理中のコールも含めて）スタンバイファイアウォールに切り替えられる際のシームレスなスイッチオーバー / フェールオーバー

SCCP について

以降のセクションでは、SCCP について概要を説明し、その機能について示します。

- 83 ページの「SCCP のコンポーネント」
- 84 ページの「SCCP トランザクション」
- 87 ページの「SCCP メッセージ」

SCCP のコンポーネント

以下に、SCCP VoIP アーキテクチャの基本コンポーネントを示します。

- SCCP クライアント
- コールマネージャ
- クラスタ

SCCP クライアント

SCCP クライアントはエンドステーションとも呼ばれる IP 電話上で動作し、SCCP を使ってシグナリングを実行したり電話をかけたりします。スキニィクライアントが電話をかける際には、まず最初にプライマリコールマネージャに（セカンダリが使用可能であればそれにも）登録する必要があります。クライアントとコールマネージャとの接続は ポート 2000 の TCP で行われます。この接続は、クライアントから、およびクライアントへのコールの確立に使用されます。メディアの伝送は RTP、UDP、IP で行われます。

コールマネージャ

コールマネージャは Cisco H.323 サーバーであり、SCCP VoIP ネットワークのすべてのデバイスと通信の全体を制御します。コールマネージャは、SCCP グループ、数の範囲、ルートプランを定義、監視、および制御する機能を持ち、ネットワーク上のデバイスの初期化、アクセス許可、デバイスの登録を行い、また、アドレス、電話番号、番号形式を格納している冗長データベースを提供します。さらに、呼ばれた側のデバイスまたはそれらのエージェントとの接続を開始し、音声通話が伝送される論理セッションを確立します。

クラスタ

クラスタは、複数の SCCP クライアントと 1 つのコールマネージャからなる集合です。クラスタ内のコールマネージャは、クラスタに存在するすべての SCCP クライアントを把握しています。1 つのクラスタに、バックアップ用を含めて 2 個以上のコールマネージャが存在できます。コールマネージャの動作は、次に示す各クラスタの条件によって異なります。

- クラスタ内。コールマネージャが各 SCCP クライアントを把握しており、コールはクラスタ内の SCCP クライアント間で行われます。
- クラスタ間。コールマネージャが相手のコールマネージャと H.323 を使って通信し、コールを設定する必要があります。
- クラスタ間のコール。アクセス許可の制御とアドレス解決にゲートキーパーが使用されます。

  コールマネージャの動作は、SCCP クライアントと PSTN（パブリックスイッチドテレフォンネットワーク）電話との間のコール、SCCP クライアントと H323 を使用する別の管理ドメインの電話との間のコールによっても異なります。

SCCP トランザクション

SCCP トランザクションは、SCCP コールが進捗するために必要となる処理です。SCCP トランザクションには、次が含まれます。

- クライアントの初期化
- クライアント登録
- コールの設定
- メディアの設定

クライアントの初期化

初期化するために SCCP クライアントが取得しなければならない情報があります。それは、コールマネージャの IP アドレス、ご自身の IP アドレス、および IP ゲートウェイと DNS サーバーの情報です。初期化処理は、ローカル LAN 上で行われます。SCCP クライアントは DHCP（動的ホスト構成プロトコル）要求を送信することによって、IP アドレス、DNS サーバーアドレス、TFTP サーバーの名前とアドレスを取得します。TFTP サーバー名は、次に示す構成ファイルをダウンロードするのに必要です。sep*macaddr*.cnf.TFTP 名が与えられない場合、クライアントは IP 電話のデフォルトのファイル名を使用します。次にクライアントは、TFTP サーバーから構成ファイル .cnf (xml) をダウンロードします。CNF ファイルには、プライマリとセカンダリ Cisco コールマネージャの IP アドレスがあります。この情報を使って、クライアントはコールマネージャに接続して登録します。

クライアント登録

SCCP クライアントは、初期化処理を終了後、既知のデフォルトポート 2000 の TCP 接続でコールマネージャに登録します。クライアント自身の IP アドレス、電話の MAC アドレス、プロトコルやバージョンなどの他の情報をコールマネージャに渡します。登録が済むまでは、クライアントはコールを開始または受信することができません。キープアライブメッセージは、セキュリティデバイスのポリシーが許可する場合にこの TCP 接続を開いたままの状態に保ち、クライアントが任意の時間にコールの開始または受信ができるようにします。

表 4 に、SCCP メッセージをリストし、セキュリティデバイスに影響するメッセージを示します。

表 4: SCCP 登録メッセージ

クライアント側	コールマネージャ側	セキュリティデバイスに影響するもの
RegisterMessage		✓
IPortMessage		✓
	RegisterAckMessage	✓
	CapabilitiesRequest	
CapabilitiesResMessage		
ButtonTemplateReqMessage		
	ButtonTemplateResMessage	
SoftKeyTemplateReqMessage		
	SoftKeyTemplateResMessage	
LineStatReqMessage		✓
	LineStatMessage	✓

コールの設定

SCCP を使った IP 電話間のコール設定は、いつもコールマネージャが処理します。コール設定のためのメッセージはコールマネージャに送信され、コールマネージャはコール状態に適したメッセージを返します。コールの設定が成功し、セキュリティデバイスのポリシーによってコールが許可されると、コールマネージャはメディア設定メッセージをクライアントに送信します。

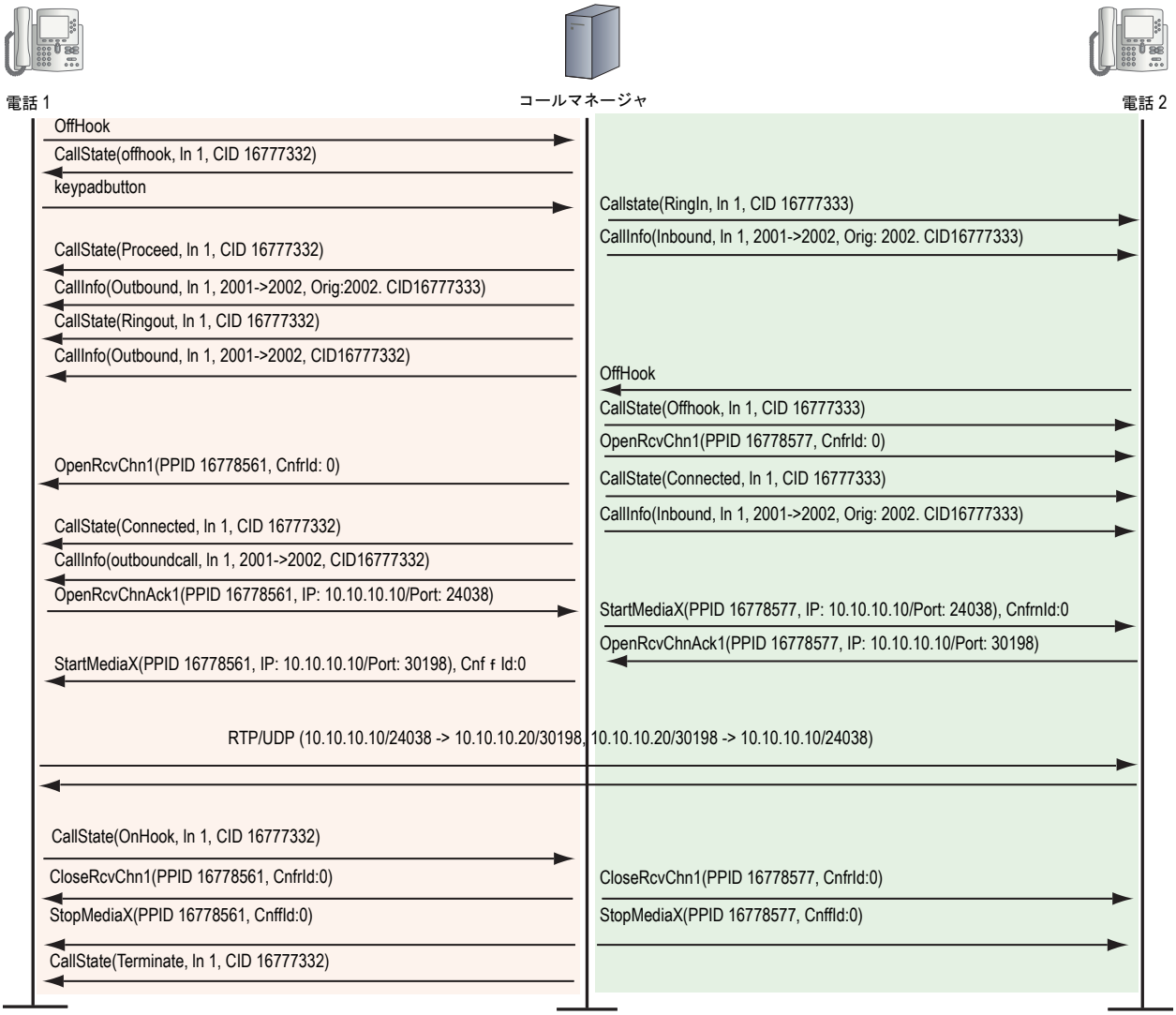
メディアの設定

コールマネージャは、呼び出された側の IP アドレスとポートナンバーを呼び出し側に送信します。さらに呼び出し側のメディア IP アドレスとポートナンバーを呼び出された側に送信します。メディアの設定が終了後、メディアはクライアント間で直接伝送されます。コールが終了すると、コールマネージャに通知され、メディアストリームが終了します。この処理中、コールマネージャがコール設定機能をクライアントに譲ることはありません。メディアは、RTP/UDP/IP 接続で直接クライアント間でやり取りされます。

SCCP 制御メッセージと RTP フロー

図 24 に、*電話 1* と *電話 2* の間の単一コールの設定とティアダウンに使用される SCCP 制御メッセージを示します。*電話 1* でコールを開始する OffHook メッセージ、およびコールの終了を通知する OnHook メッセージを除いて、コールのすべての局面がコールマネージャによって制御されます。

図 24: コールの設定とティアダウン



SCCP メッセージ

表 5, 表 6, 表 7、および表 8 にセキュリティデバイスで許可される 4 間隔の SCCP コールメッセージ ID をリストします。

表 5: ステーションからコールマネージャへのメッセージ

メッセージ	範囲
#define STATION_REGISTER_MESSAGE	0x00000001
#define STATION_IP_PORT_MESSAGE	0x00000002
#define STATION_ALARM_MESSAGE	0x00000020
#define STATION_OPEN_RECEIVE_CHANNEL_ACK	0x00000022

表 6: コールマネージャからステーションへのメッセージ

メッセージ	範囲
#define STATION_START_MEDIA_TRANSMISSION	0x00000001
#define STATION_STOP_MEDIA_TRANSMISSION	0x00000002
#define STATION_CALL_INFO_MESSAGE	0x00000020
#define STATION_OPEN_RECEIVE_CHANNEL_ACK	0x00000022
#define STATION_CLOSE_RECEIVE_CHANNEL	0x00000106

表 7: コールマネージャ 4.0 のメッセージとポストスキニィ 6.2

メッセージ	範囲
#define STATION_REGISTER_TOKEN_REQ_MESSAGE	0x00000029
#define STATION_MEDIA_TRANSMISSION_FAILURE	0x0000002A
#define STATION_OPEN_MULTIMEDIA_RECEIVE_CHANNEL_ACK	0x00000031

表 8: コールマネージャからステーションへ

メッセージ	範囲
#define STATION_OPEN_MULTIMEDIA_RECEIVE_CHANNEL	0x00000131
#define STATION_START_MULTIMEDIA_TRANSMISSION	0x00000132
#define STATION_STOP_MULTIMEDIA_TRANSMISSION	0x00000133
#define STATION_CLOSE_MULTIMEDIA_RECEIVE_CHANNEL	0x00000136

例

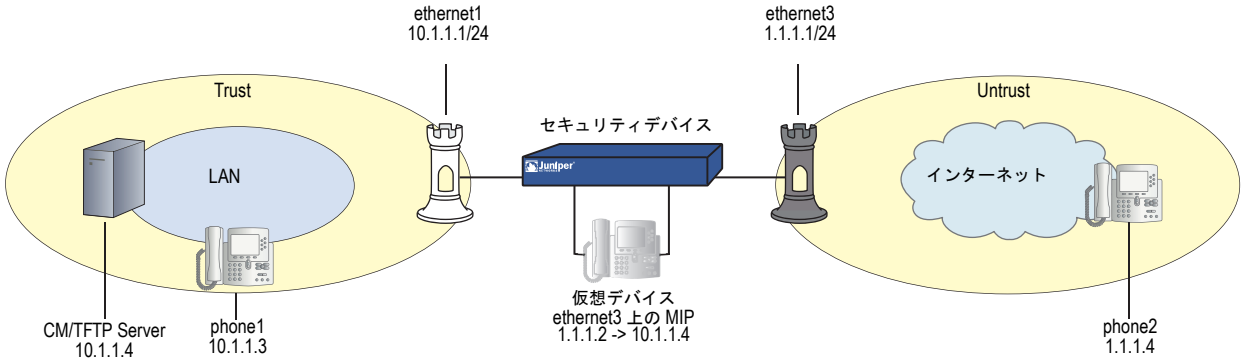
このセクションには、以下のサンプル例があります。

- 88 ページの「例 : Trust ゾーンのコールマネージャ /TFTP サーバー」
- 90 ページの「例 : Untrust ゾーン内のコールマネージャ /TFTP サーバー」
- 92 ページの「例 : 3 ゾーン、DMZ 内のコールマネージャ /TFTP サーバー」
- 96 ページの「例 : ゾーン内、Trust ゾーンのコールマネージャ /TFTP サーバー」
- 99 ページの「例 : ゾーン内、Untrust ゾーンのコールマネージャ /TFTP サーバー」
- 102 ページの「例 : フルメッシュ VPN での SCCP」

例 : Trust ゾーンのコールマネージャ /TFTP サーバー

この例では、phone1 と コールマネージャ /TFTP サーバーが Trust（プライベート）ゾーン内の ethernet1 インターフェースにあり、phone2 が Untrust ゾーン内の ethernet3 インターフェースにあります。コールマネージャ /TFTP サーバー用 MIP を ethernet3 インターフェースに配置します。これによって、phone2 は、起動時に TFTP サーバーに接続してコールマネージャの IP アドレスを取得できます。（TFTP サーバーの構成ファイル（sep <mac_addr>.cnf）にあるコールマネージャの IP アドレスをコールマネージャの MIP IP アドレスに変更することをお勧めします。）次に、SCCP トラフィックの Untrust から Trust ゾーンへの通過を許すポリシーの作成と、ポリシーの MIP 参照を作成します。また、phone1 の Trust ゾーンから Untrust ゾーンへの呼び出しを許可するポリシーも作成します。

図 25: プライベート ゾーン内のコールマネージャ /TFTP サーバー



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 次のように入力してから **OK** をクリックします。

   Zone: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24

次のように入力してから **OK** をクリックします。
Interface mode: Route

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone: Untrust
IP Address/Netmask: 1.1.1.1/24
Interface mode: Route

2. **アドレス**

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: phone1
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.1.1.3/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: phone2
IP Address/Domain Name:
IP/Netmask: (**選択**), 1.1.1.4/24
Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: CM-TFTP_Server
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.1.1.4/24
Zone: Trust

3. **MIP**

Network > Interfaces > Edit (loopback.3) > MIP > New: 次のように入力してから **OK** をクリックします。

Mapped IP: 1.1.1.2
Netmask: 255.255.255.255
Host IP Address: 10.1.1.4
Host Virtual Router Name: trust-vr

4. **ポリシー**

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), any
Destination Address:
Address Book Entry: (**選択**), phone2
Source Translation: Enable
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: (**選択**)
(DIP on): None (Use Egress Interface IP)

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), phone2
Destination Address:
Address Book Entry: (**選択**), MIP(1.1.1.2)
Source Translation: Enable
Action: Permit

CLI

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 route
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24
   set interface ethernet3 route

2. **アドレス**
   set address trust phone1 10.1.1.3/24
   set address untrust phone2 1.1.1.4/24
   set address trust cm-tftp_server 10.1.1.4/24

3. **MIP**
   set interface ethernet3 mip 1.1.1.2 host 10.1.1.4

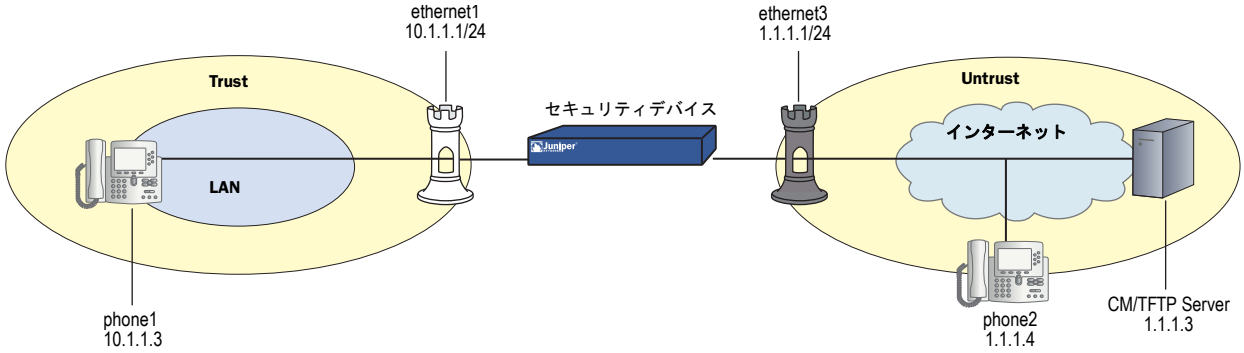
4. **ポリシー**
   set policy from trust to untrust any phone2 s c c p nat src permit
   set policy from untrust to trust phone2 mip(1.1.1.2) sccp permit
   save

注 : この構成例で示すように、キーワード any を使う代わりにサービスを明示的に指定すると安全性が高まります。

例 : Untrust ゾーン内のコールマネージャ /TFTP サーバー

この例では、phone1 が Trust ゾーン内の ethernet1 インターフェースにあり、phone2 とコールマネージャ /TFTP サーバーが Untrust ゾーン内の ethernet3 インターフェースにあります。インターフェースとアドレスの設定が終了したら、Trust から Untrust ゾーンへのポリシーを作成します。これによって、phone1 が Untrust ゾーンのコールマネージャ/TFTP サーバーに登録できることになります。

図 26: Untrust ゾーン内のコールマネージャ /TFTP サーバー



WebUI

1. **インターフェース**

   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface mode: Route

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24
   Interface mode: Route

2. **アドレス**

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: phone1
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.3/24
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: phone2
   IP Address/Domain Name:
   IP/Netmask: (選択), 1.1.1.4/24
   Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: CM/TFTP Server
IP Address/Domain Name:
IP/Netmask: (**選択**), 1.1.1.3/24
Zone: Untrust

3. **ポリシー**

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address
Address Book Entry: (**選択**), phone1
Destination Address
Address Book Entry: (**選択**), any
Source Translation: Enable
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: (**選択**)
(DIP on): None (Use Egress Interface IP)

CLI

1. **インターフェース**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 route
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
```

2. **アドレス**

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address untrust cm-tftp_server 1.1.1.3/24
```

3. **ポリシー**

```
set policy from trust to untrust phone1 any sccp nat src permit
save
```

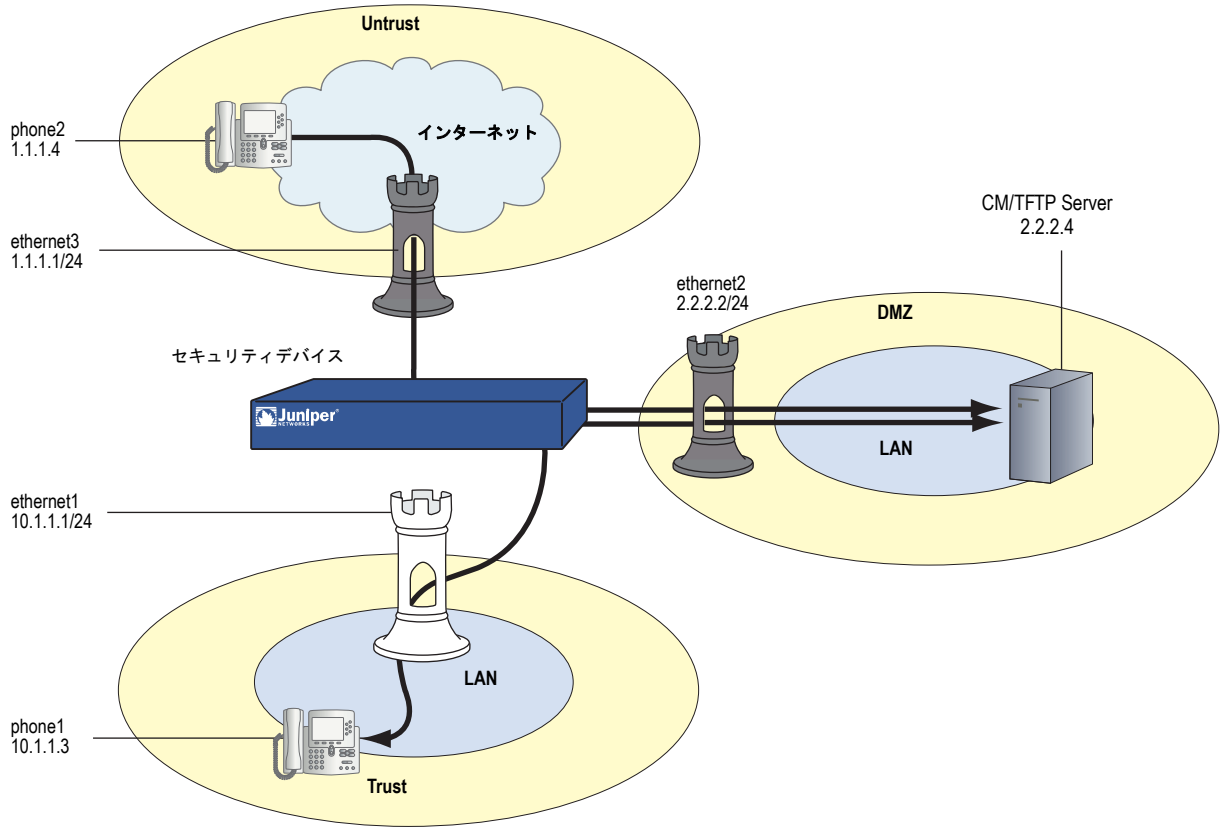
注 : この構成例で示すように、キーワード any を使う代わりにサービスを明示的に指定すると安全性が高まります。

例 : 3 ゾーン、DMZ 内のコールマネージャ /TFTP サーバー

この例では、phone1 が Trust ゾーン内の ethernet1 インターフェースにあり、phone2 が Untrust ゾーン内の ethernet3 インターフェースにあり、コールマネージャ /TFTP サーバーが DMZ 内の ethernet2 インターフェースにあります。シグナリングには、phone1 がコールマネージャ /TFTP サーバーと通信できるように Trust ゾーンから DMZ へのポリシーを作成し、phone2 がコールマネージャ /TFTP サーバーと通信できるように Untrust ゾーンから DMZ へのポリシーを作成します。メディアの伝送には、phone1 と phone2 が直接通信できるように

Trust ゾーンから Untrust ゾーンへのポリシーを作成します。図 27 の矢印は SCCP シグナリングトラフィックの流れを示しています。この場合、Untrust ゾーン内の phone2 が Trust ゾーン内の phone1 を呼び出しています。セッションの開始後、メディアは phone1 と phone2 の間で直接やり取りされます。

図 27: DMZ 内のコールマネージャ /TFTP サーバー



WebUI

1. **インターフェース**

   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface mode: NAT

   Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

   Zone Name: DMZ
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

2. **アドレス**

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: phone1
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.3/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: phone2
IP Address/Domain Name:
IP/Netmask: (選択), 1.1.1.4/24
Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: CM-TFTP_Server
IP Address/Domain Name:
IP/Netmask: (選択), 2.2.2.4/24
Zone: DMZ

3. **ポリシー**

Policies > (From: Trust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), phone1
Destination Address:
Address Book Entry: (選択), CM-TFTP_Server
Source Translation: Enable
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: Enable
(DIP on): None (Use Egress Interface IP)

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), phone2
Destination Address:
Address Book Entry: (選択), CM-TFTP_Server
Source Translation: Enable
Action: Permit

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), phone1
Destination Address:
Address Book Entry: (選択), phone2
Source Translation: Enable
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: Enable
(DIP on): None (Use Egress Interface IP)

CLI

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 route
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
set interface ethernet2 zone dmz
set interface ethernet2 ip 2.2.2.2/24
set interface ethernet2 route
```

2. アドレス

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address dmz cm-tftp_server 2.2.2.4
```

3. ポリシー

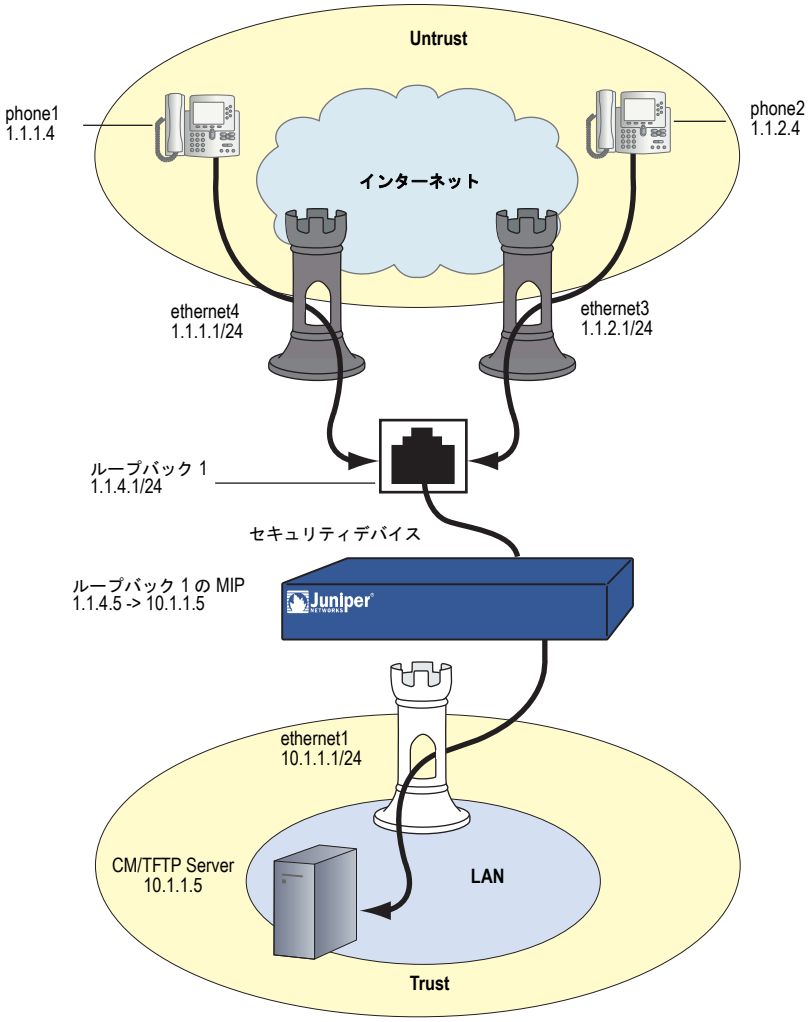
```
set policy from trust to dmz phone1 cm-tftp_server sccp nat src permit
set policy from untrust to dmz phone2 cm-tftp_server sccp permit
set policy from trust to untrust phone1 phone2 sccp nat src permit
save
```

注 : この構成例で示すように、キーワード any を使う代わりにサービスを明示的に指定すると安全性が高まります。

例：ゾーン内、Trust ゾーンのコールマネージャ /TFTP サーバー

この例では、phone1 が Untrust ゾーン内の ethernet4 インターフェースにあり、phone2 が Untrust ゾーン内 ethernet3 インターフェースのサブネット内にあり、コールマネージャ /TFTP サーバーが Trust ゾーン内の ethernet1 インターフェースにあります。Untrust ゾーンにある 2 台の電話間でゾーン内 SCCP トラフィックを許可するには、ループバックインターフェースを作成して、ethernet3 と ethernet4 インターフェースをループバックグループに追加してから、コールマネージャ /TFTP サーバーの IP アドレスのループバックインターフェース上に MIP を配置します。ループバックインターフェースを作成すると、Trust ゾーン内のコールマネージャ /TFTP サーバーに単一の MIP のみを使用することができます。（ループバックインターフェースを使用する詳細については、**8**-71 ページの「MIP とループバックインターフェース」を参照してください。）最後に、ゾーン内でのブロッキングはデフォルトでオンになっているため、Untrust ゾーンのブロッキングを設定解除してゾーン内の通信を許可します。

図 28: ゾーン内、Trust ゾーンのコールマネージャ /TFTP サーバー



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24

   次のように入力してから **OK** をクリックします。

   Interface mode: NAT

   Network > Interfaces > Edit (ethernet4): 次のように入力してから **OK** をクリックします。

   Zone: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.2.1/24

   Network > Interfaces > New Loopback IF: 次のように入力してから **OK** をクリックします。

   Interface Name: loopback.1
   Zone: Untrust (trust-vr)
   IP Address/Netmask: 1.1.4.1/24

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: CM-TFTP_Server
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.5/32
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: phone1
   IP Address/Domain Name:
   IP/Netmask: (選択), 1.1.1.4/32
   Zone: Untrust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: phone2
   IP Address/Domain Name:
   IP/Netmask: (選択), 1.1.2.4/32
   Zone: Untrust

3. **ループバックグループ**
   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   As member of loopback group: (**選択**), loopback.1
   Zone Name: Untrust

   Network > Interfaces > Edit (ethernet4): 次のように入力してから **OK** をクリックします。

   As member of loopback group: (**選択**), loopback.1
   Zone Name: Untrust

4. **MIP**
   Network > Interfaces > Edit (loopback.1) > MIP > New: 次のように入力してから **OK** をクリックします。

   Mapped IP: 1.1.4.5
   Netmask: 255.255.255.255
   Host IP Address: 10.1.1.5
   Host Virtual Router Name: trust-vr

5. **ブロッキング**
   Network > Zones > Edit (Untrust): 次のように入力してから **OK** をクリックします。

   Block Intra-Zone Traffic: (**クリヤ**)

6. **ポリシー**
   Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), CM-TFTP_Server
   Destination Address:
   Address Book Entry: (**選択**), Any
   Source Translation: Enable
   Action: Permit

   > Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

   NAT:
   Source Translation: Enable
   (DIP on): None (Use Egress Interface IP)

   Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), Any
   Destination Address:
   Address Book Entry: (**選択**), MIP(1.1.4.5)
   Source Translation: Enable
   Action: Permit

CLI

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 route
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.2.1/24
   set interface ethernet3 route
   set interface ethernet4 zone untrust
   set interface ethernet2 ip 1.1.1.1/24
   set interface ethernet2 route
   set interface loopback.1 zone untrust
   set interface loopback.1 ip 1.1.4.1/24
   set interface loopback.1 route

2. **アドレス**
   set address trust cm-tftp_server 10.1.1.5/32
   set address untrust phone1 1.1.1.4/32
   set address untrust phone2 1.1.2.4/32

3. **ループバックグループ**
   set interface ethernet3 loopback-group loopback.1
   set interface ethernet4 loopback-group loopback.1

4. **MIP**
   set interface loopback.1 mip 1.1.4.5 host 10.1.1.5

5. **ブロッキング**
   unset zone untrust block

6. **ポリシー**
   set policy from trust to untrust cm/tftp_server any sccp nat src permit
   set policy from untrust to trust any mip(1.1.4.5) sccp permit
   save

注 : この例では、Untrust ゾーンのブロッキングを設定解除してゾーン内通信を許可しますが、次のようにポリシーを作成しても同じ効果を得ることができます。

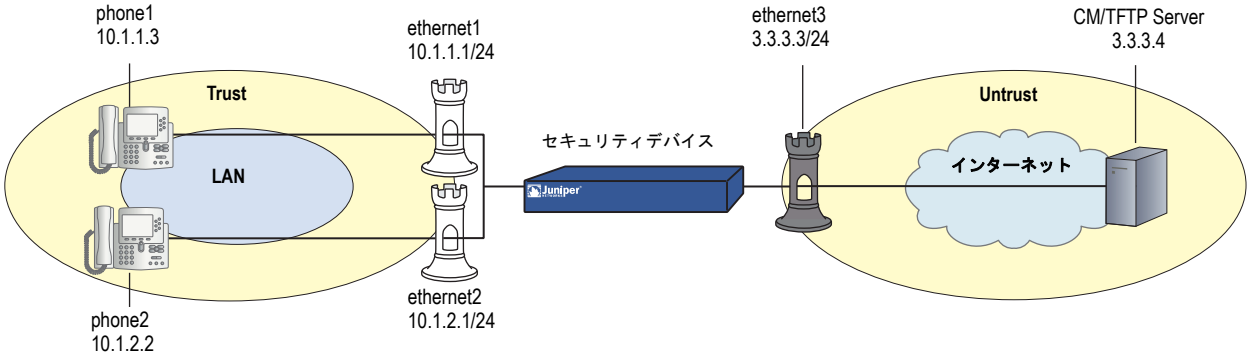
```
set policy from untrust to untrust any any sccp permit
```

この構成例で示すように、キーワード any を使う代わりにサービスを明示的に指定すると安全性が高まります。

例 : ゾーン内、Untrust ゾーンのコールマネージャ /TFTP サーバー

この例では、phone1 が Trust ゾーン内の ethernet1 インターフェースにあり、phone2 が Trust ゾーン内の サブネットの ethernet2 インターフェースにあり、コールマネージャ /TFTP サーバーが Untrust インターフェース内の ethernet3 インターフェースにあります。インターフェースとアドレスを設定後、Trust ゾーンから Untrust ゾーンへのポリシーを作成して phone1 と phone2 が Untrust ゾーン内のコールマネージャ /TFTP サーバーに登録できるようにします。Trust ゾーンでのブロッキングはデフォルトでオフになっています（ユーザー定義のカスタムゾーンと同じ）。しかし安全性をさらに強固にするために、オプションでブロッキングをオフにし、Trust から Trust へのポリシーを作成することも可能です。これによって、SCCP サービスを指定することができ、phone1 と phone2 へのゾーン内コールを制限することができます。

図 29: ゾーン内、Trust ゾーンのコールマネージャ /TFTP サーバー



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように入力してから **OK** をクリックします。
   Interface mode: Route

   Network > Interfaces > Edit (ethernet2): 以下を入力して **Apply** をクリックします。

   Zone: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.2.1/24
   次のように入力してから **OK** をクリックします。
   Interface mode: Route

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 3.3.3.3/24

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: phone1
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.3/24
   Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: phone2
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.1.2.2/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: CM/TFTP Server
IP Address/Domain Name:
IP/Netmask: (**選択**), 3.3.3.4/24
Zone: Untrust

3. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), CM/TFTP Server
Source Translation: Enable
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: Enable
(DIP on): None (Use Egress Interface IP)

CLI

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet2 zone trust
set interface ethernet2 ip 10.1.2.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24
set interface ethernet3 route
```

2. アドレス

```
set address trust phone1 10.1.1.3/24
set address trust phone2 10.1.2.2/24
set address untrust cm-tftp_server 3.3.3.4/24
```

3. ポリシー

```
set policy from trust to untrust any cm-tftp_server sccp nat src permit
save
```

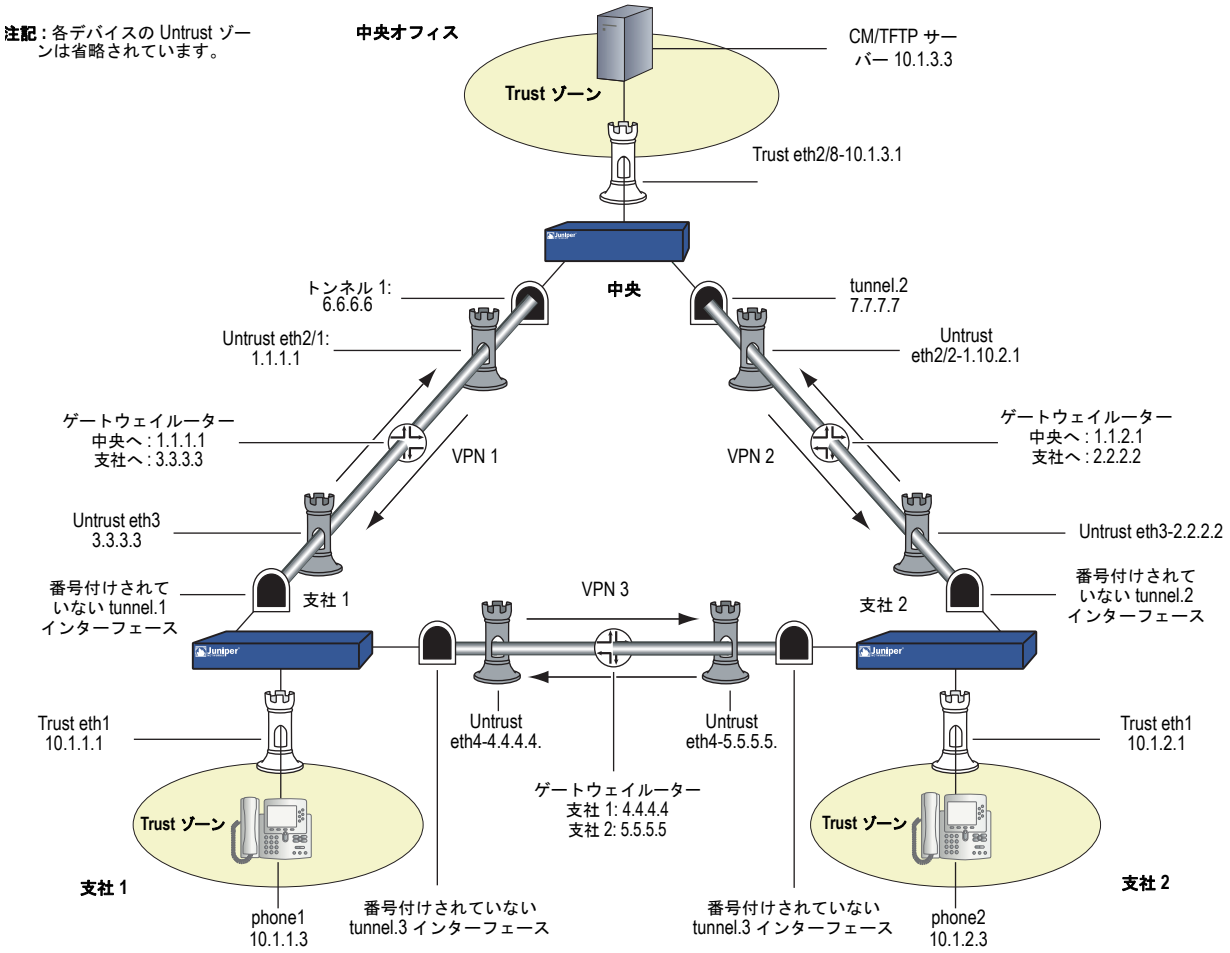
注 : この構成例で示すように、キーワード any を使う代わりにサービスを明示的に指定すると安全性が高まります。

例 : フルメッシュ VPN での SCCP

この例では、中央オフィスと 2 つの支社がフルメッシュ VPN でリンクされています。各サイトには、1 台のセキュリティデバイスが設置されています。コールマネージャ /TFTP サーバーが中央オフィスの Trust ゾーンにあり、phone1 が支社 1 の Trust ゾーンにあり、phone2 が支社 2 の Trust ゾーンにあります。デバイスを接続するインターフェースはすべて、それぞれの Untrust ゾーンにあります。各デバイスに他のそれぞれのデバイスと接続するため 2 つのトンネルを設定すると、フルメッシュのネットワークが作成されます。

注 : この例で使用するセキュリティデバイスは、少なくても 3 つの個別構成が可能なインターフェースが使用可能でなければなりません。

図 30: フルメッシュ VPN での SCCP



注 : この構成例で示すように、キーワード any を使う代わりにサービスを明示的に指定すると安全性が高まります。

WebUI (中央)

1. インターフェース

Network > Interfaces > Edit (ethernet2/1): 以下を入力して **Apply** をクリックします。

Zone: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Edit (ethernet2/2): 以下を入力して **Apply** をクリックします。

Zone: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.2.1/24

Network > Interfaces > Edit (ethernet2/8): 以下を入力して **Apply** をクリックします。

Zone: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.3.1/24
次のように入力してから **OK** をクリックします。
Interface mode: Route

Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 1
Zone (VR): Untrust
IP Address/Netmask: 6.6.6.6/24

Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 2
Zone (VR): Untrust
IP Address/Netmask: 7.7.7.7/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: CM/TFTP Server
IPv4/Netmask: 10.1.3.3/32
Zone: Trust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: to-branch-1
Security Level: Standard
IPvc4/v6 Address/Hostname: 3.3.3.3
Preshare Key: netscreen
Outgoing Interface: ethernet2/1

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn-branch-1

Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Bind to: (選択) Tunnel Interface, tunnel.1

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: to-branch-2
Security Level: Standard
IPvc4/v6 Address/Hostname: 2.2.2.2
Preshare Key: netscreen
Outgoing Interface: ethernet2/2

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn-branch-2

Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Bind to: (選択) Tunnel Interface, tunnel.2

4. **ルーティング**

Network > Routing > Destination > New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
Interface (選択): tunnel.1

Network > Routing > Destination > New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.2.0/24
Interface (選択): tunnel.2

5. **ポリシー**

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address (選択) Address Book Entry: CM/TFTP Server
Destination Address (選択) Address Book Entry: Any-IPv4
Source Translation: Enable
Action: Permit

Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

Source Address (選択) Address Book Entry: Any-IPv4
Destination Address (選択) Address Book Entry: CM/TFTP Server
Source Translation: Enable
Action: Permit

CLI (中央)

1. **インターフェース**

```
set interface ethernet2/1 zone untrust
set interface ethernet2/1 ip 1.1.1.1/24
set interface ethernet2/2 zone untrust
set interface ethernet2/2 ip 1.1.2.1/24
set interface ethernet2/8 zone trust
set interface ethernet2/8 ip 10.1.3.1/24
set interface ethernet2/8 route
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 6.6.6.6/24
set interface tunnel.2 zone untrust
set interface tunnel.2 ip 7.7.7.7/24
```

2. **アドレス**

```
set address trust cm-tftp_server 10.1.3.3/32
```

3. **VPN**

```
set ike gateway to-branch-1 address 3.3.3.3 main outgoing-interface ethernet2/1
    preshare netscreen sec-level standard
set ike gateway to-branch-2 address 2.2.2.2 main outgoing-interface ethernet2/2
    preshare netscreen sec-level standard
set vpn vpn_branch-1 gateway to-branch-1 no-reply tunnel idletime 0 sec-level
    standard
set vpn vpn-branch-1 id 1 bind interface tunnel.1
set vpn vpn-branch-2 gateway to-branch-2 no-reply tunnel idletime 0 sec-level
    standard
set vpn vpn-branch-2 id 2 bind interface tunnel.2
```

4. ***ルーティング***

```
set route 10.1.2.0/24 interface tunnel.2
set route 10.1.1.0/24 interface tunnel.1
```

5. **ポリシー**

```
set policy from trust to untrust cm-tftp_server any sccp permit
set policy from untrust to trust any cm-tftp_server sccp permit
save
```

WebUI (支社 1)

1. **インターフェース**

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24
Interface mode: Route

Network > Interfaces > Edit (ethernet3): 以下を入力して **Apply** をクリックします。

Zone: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 3.3.3.3/24

Network > Interfaces > Edit (ethernet4): 以下を入力して **Apply** をクリックします。

Zone: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 4.4.4.4/24

Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 2
Zone (VR): Untrust
Unnumbered (選択) Interface: ethernet3

Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 3
Zone (VR): Untrust
Unnumbered (選択) Interface: ethernet4

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: phone1
IPv4/Netmask: 10.1.1.3/32
Zone: V1-Trust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: to-central
Security Level: Standard
IPvc4/v6 Address/Hostname: 1.1.2.1
Preshare Key: netscreen
Outgoing Interface: ethernet3

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn-central

Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Bind to (選択): Tunnel Interface, tunnel.1

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: to-ns50
Security Level: Standard
IPvc4/v6 Address/Hostname: 5.5.5.5
Preshare Key: netscreen
Outgoing Interface: ethernet4

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn-ns50

Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Bind to (選択): Tunnel Interface, tunnel.3

4. ルーティング

Network > Routing > Destination > New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.2.0/24
Interface (選択): tunnel.3

Network > Routing > Destination > New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.3.0/24
Interface (選択): tunnel.1

5. ポリシー

Policies > (From: Trust, To: Untrust) > New: 次のように入力してから **OK** をクリックします。

Source Address (選択) Address Book Entry: phone2
Destination Address (選択) Address Book Entry: Any-IPv4
Source Translation: Enable
Action: Permit

Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

Source Address (選択) Address Book Entry: Any-IPv4
Destination Address (選択) Address Book Entry: phone2
Source Translation: Enable
Action: Permit

CLI (支社 1)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 route
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24
set interface ethernet4 zone untrust
set interface ethernet4 ip 4.4.4.4/24
set interface tunnel.2 zone untrust
set interface tunnel.2 ip unnumbered interface ethernet3
set interface tunnel.3 zone untrust
set interface tunnel.3 ip unnumbered interface ethernet4
```

2. アドレス

```
set address trust phone1 10.1.1.3/32
```

3. VPN

```
set ike gateway to-central address 1.1.1.1 main outgoing-interface ethernet3
    preshare netscreen sec-level standard
set ike gateway to-ns50 address 5.5.5.5 main outgoing-interface ethernet4
    preshare netscreen sec-level standard
set vpn vpncentral gateway to-central no-replay tunnel idletime 0 sec-level standard
set vpn vpncentral bind interface tunnel.1
```

set vpn vpn-ns50 gateway to-ns50 no-replay tunnel idletime 0 sec-level standard
set vpn vpn-ns50 bind interface tunnel.3

4. **ルート**
set route 10.1.2.0/24 interface tunnel.3
set route 10.1.3.0/24 interface tunnel.1

5. **ポリシー**
set policy from trust to untrust phone1 any sccp permit
set policy from untrust to trust any phone1 sccp permit
save

WebUI (支社 2)

1. **インターフェース**
Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.2.1/24
次のように入力してから **OK** をクリックします。
Interface mode: Route

Network > Interfaces > Edit (ethernet3): 以下を入力して **Apply** をクリックします。

Zone: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > Edit (ethernet4): 以下を入力して **Apply** をクリックします。

Zone: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 4.4.4.4/24

Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 2
Zone (VR): Untrust
Unnumbered (選択) Interface: ethernet3

Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: 3
Zone (VR): Untrust
Unnumbered (選択) Interface: ethernet4

2. **アドレス**
Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: phone2
IPv4/Netmask: 10.1.2.3/32
Zone: Trust

3. **VPN**

   VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

   Gateway Name: to-central
   Security Level: Standard
   IPvc4/v6 Address/Hostname: 1.1.2.1
   Preshare Key: netscreen
   Outgoing Interface: ethernet3

   VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

   VPN Name: vpn-central

   Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

   Bind to (選択): Tunnel Interface, tunnel.2

   VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

   Gateway Name: to-ns50
   Security Level: Standard
   IPvc4/v6 Address/Hostname: 4.4.4.4
   Preshare Key: netscreen
   Outgoing Interface: ethernet4

   VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

   VPN Name: vpn-ns50

   Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

   Bind to (選択): Tunnel Interface, tunnel.3

4. **ルーティング**

   Network > Routing > Destination > New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 10.1.3.0/24
   Interface (選択): tunnel.2

   Network > Routing > Destination > New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 10.1.1.0/24
   Interface (選択): tunnel.3

5. **ポリシー**

   Policies > (From: Trust, To: Untrust) New 次のように入力してから **OK** をクリックします。

   Source Address (選択) Address Book Entry: phone2
   Destination Address (選択) Address Book Entry: Any-IPv4
   Source Translation: Enable
   Action: Permit

Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

Source Address (選択) Address Book Entry: Any-IPv4
Destination Address (選択) Address Book Entry: phone2
Source Translation: Enable
Action: Permit

CLI (支社 2)

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.2.1/24
   set interface ethernet1 route
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 2.2.2.2/24
   set interface ethernet4 zone untrust
   set interface ethernet4 ip 4.4.4.4/24
   set interface tunnel.2 zone untrust
   set interface tunnel.2 ip unnumbered interface ethernet3
   set interface tunnel.3 zone untrust
   set interface tunnel.3 ip unnumbered interface ethernet4

2. **アドレス**
   set address trust phone1 10.1.2.3/32

3. **VPN**
   set ike gateway to-central address 1.1.1.1 Main outgoing-interface ethernet3
   preshare netscreen sec-level standard
   set ike gateway to-ns50 address 4.4.4.4 Main outgoing-interface ethernet4
   preshare netscreen sec-level standard
   set vpn vpncentral gateway to-central no-replay tunnel idletime 0 sec-level standard
   set vpn vpncentral id 4 bind interface tunnel.2
   set vpn vpn-ns50 gateway to-ns50 no-replay tunnel idletime 0 sec-level standard
   set vpn vpn-ns50 id 5 bind interface tunnel.3

4. **ルート**
   set route 10.1.3.0/24 interface tunnel.1
   set route 10.1.2.0/24 interface tunnel.3

5. **ポリシー**
   set policy from trust to untrust phone2 any sccp permit
   set policy from untrust to trust any phone2 sccp permit
   save

索引

A

ALG....17
- SIP....13
- SIP NAT....23

S

SDP....17–19

SIP
- ALG....17, 20
- RTCP....19
- RTP....19
- SDP....17–19
- 応答コード....16
- シグナリング....17
- 接続情報....18
- 定義....13
- ピンホール....17
- マルチメディアセッション....13
- メッセージ....14
- メディア通知....18
- 要求メソッド....14

SIP NAT
- DIP プールを使用....36
- DMZ 内のプロキシ....45
- Trust ゾーン内....52
- Untrust ゾーン内....48, 96
- VPN、フルメッシュの使用....54, 102
- インターフェース DIP を使用....33
- コール設定....23, 29
- 受信 DIP を使用....32
- 受信、MIP で....36, 38
- 定義....23
- パブリックゾーン内のプロキシ....43
- プライベートゾーン内のプロキシ....40, 88

SIP タイムアウト
- シグナリング無活動....21, 22
- セッション無活動....21
- 無活動....21
- メディア無活動....21, 22

お

音声 IP 化
- 帯域幅管理....63

け

ゲートキーパーデバイス....1

さ

サービスブック、サービスグループ (WebUI)....65

ひ

ピンホール....19

ま

マルチメディアセッション、SIP....13

概念と用例
ScreenOS リファレンス ガイド

第 7 部 :
ルーティング

リリース 6.0.0、改訂 02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

品番 : 530-017773-01-JP, 改訂 02

Copyright Notice

Copyright © 2007 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

目次

本編について xi

ドキュメントの規則 xii
Web ユーザーインターフェースの規則 xii
コマンドラインインターフェースの規則 xii
ネーミング規則および文字タイプ xiii
説明図の規則 xiv
技術ドキュメントおよびテクニカルサポート xv

第 1 章 静的ルーティング 1

概要 1
静的ルートのしくみ 2
静的ルートを構成するとき 3
静的ルートの構成 5
静的ルートの設定 5
トンネルインターフェースに静的ルートを設定する 9
ゲートウェイトラッキングを使用可能にする 10
Null インターフェースへトラフィックを転送する 11
他のルーティングテーブルのルートルックアップを防ぐ 11
トンネルトラフィックが非トンネルインターフェース上に送信されることを防ぐ 11
ルートの要約により生じたループを防ぐ 12
永続アクティブルート 12
等価コストマルチパスのルーティング優先度の変更 13

第 2 章 ルーティング 15

概要 16
仮想ルータールーティングテーブル 17
宛先ベースのルーティングテーブル 18
ソースベースのルーティングテーブル 19
ソースのインターフェースベースのルーティングテーブル 22
仮想ルーターの作成と変更 24
仮想ルーターの設定変更 24
仮想ルーター ID を割り当てる 25
仮想ルーター間でトラフィックを転送する 26
2 つの仮想ルーターの設定 26
仮想ルーターの作成と削除 28
カスタム仮想ルーターを作成する 28
カスタム仮想ルーターを削除する 29
仮想ルーターと仮想システム 29
Vsys 上に仮想ルーターを作成する 30
仮想ルーター間の共有ルート 31
ルーティングテーブルの最大ルート情報数 32

ルーティング機能および例 32
ルートの選択 32
ルートの優先度値を設定する 33
ルートのメトリック 34
デフォルトのルートルックアップ順序の変更 34
複数の仮想ルーターにおけるルートルックアップ 36
等価コストマルチパスルーティングの構成 38
ルート情報の再配布 40
ルートマップの設定 40
ルートのフィルタリング 42
アクセスリストの構成 43
ルート情報を OSPF に再配布 43
仮想ルーター間でルート情報をエクスポート / インポート 45
エクスポート規則を設定する 45
自動エクスポートを設定する 46

第 3 章 オープンショーテストパスファースト (OSPF) 49

概要 50
エリア 50
ルーターの分類 51
Hello プロトコル 51
ネットワークタイプ 52
ブロードキャストネットワーク 52
ポイントツーポイントネットワーク 52
ポイントツーマルチポイントネットワーク 52
接続状態の通知 53
OSPF の基本設定 53
OSPF ルーティングインスタンスの作成と削除 54
OSPF インスタンスを作成する 54
OSPF インスタンスを削除する 55
OSPF エリアの作成および削除 55
OSPF エリアを作成する 56
OSPF エリアの削除 56
OSPF エリアにインターフェースを割り当て 57
エリアにインターフェースを割り当てる 57
エリア範囲の設定 57
インターフェース上で OSPF を稼動 58
インターフェース上で OSPF を稼動 58
インターフェース上の OSPF を停止する 58
設定内容の確認 59
ルーティングプロトコルへのルート情報の再配布 60
再配布されたルート情報の要約 61
再配布されたルート情報の要約 61
OSPF に関する大域パラメータ 62
デフォルトルートの通知 63
仮想リンク 63
仮想リンクの作成 64
仮想リンクの自動作成 65
インターフェースごとの OSPF パラメータ 66
セキュリティ構成 68
接続デバイスを認証する 68
クリアテキストパスワードを設定する 68
MD5 パスワードを設定する 68
OSPF 隣接ノードリストの設定 69

セキュリティ構成（続き）
デフォルトルートを拒否する 70
フラッディングの回避 70
Hello しきい値を構成する 70
LSA しきい値を構成する 71
フラッディングを省略する設定 71
トンネルインターフェースについて、要求回路を作成する 71
ポイントツーマルチポイントトンネルインターフェース 72
OSPF リンクタイプの設定 73
Route-deny 機能の無効化 73
ポイントツーマルチポイントネットワークの作成 73

第 4 章 ルーティング情報プロトコル (RIP) 77

概要 78
RIP の基本設定 79
RIP インスタンスの作成と削除 80
RIP インスタンスの作成 80
RIP インスタンスの削除 80
RIP をインターフェースで使用可能・不可にする 81
インターフェース上の RIP を有効にする 81
インターフェース上の RIP を停止する 81
ルートの再配布 81
RIP 情報の表示 83
RIP データベースの表示 83
RIP 詳細の表示 84
RIP 隣接情報の表示 85
特定のインターフェースの RIP 詳細の表示 86
RIP に関する大域パラメータ 87
デフォルトルートの通知 88
RIP インターフェースパラメータの構成 89
セキュリティ構成 90
パスワードを設定して隣接ノードを認証する 90
Trusted 隣接ノードを構成する 91
デフォルトルートを拒否する 92
フラッディングの回避 92
アップデートしきい値を構成する 93
トンネルインターフェース上で RIP を稼動させる 93
オプションの RIP 構成 94
RIP バージョンの構成 94
プレフィックスサマリを使用不可・可能にする 96
プレフィックスサマリを有効にする 96
プレフィックスサマリを使用不可にする 97
代替ルートを設定する 97
トンネルインターフェースの要求回路 99
静的隣接ノードの構成 100
ポイントツーマルチポイントトンネルインターフェースの構成 100

第 5 章 境界ゲートウェイプロトコル 107

概要 108
BGP メッセージのタイプ 108
パス属性 109
外部および内部 BGP 109

基本的な BGP 構成 110
BGP インスタンスを作成して使用可能にする 111
BGP ルーティングインスタンスを作成する 111
BGP インスタンスを削除する 112
BGP をインターフェースで使用可能・不可にする 112
BGP をインターフェースで使用可能にする 112
BGP をインターフェースで使用不可にする 112
BGP ピアおよびピアグループの構成 113
BGP ピアを構成する 114
IBGP ピアグループを構成する 114
BGP 構成を確認する 116
セキュリティ構成 117
BGP 近隣ノードを認証する 117
デフォルトルートを拒否する 118
オプションの BGP 構成 118
ルートを BGP へ再配布する 120
AS-Path アクセスリストの構成 120
BGP にルートを追加 121
条件付きルートアドバタイズメント 122
ルートの重みの設定 122
ルート属性の設定 123
Route-Refresh 機能 123
インバウンドルーティングテーブルアップデートの要求 124
アウトバウンドルーティングテーブルアップデートの要求 124
ルートリフレクションを構成する 125
コンフェデレーションの構成 127
BGP コミュニティ 128
ルートの集約 129
異なる AS-Path のルートを集約 129
更新の際、より限定的なルートを除外 130
パス属性を割り当てるルートの選択 131
集約ルートの属性変更 132

第 6 章 ポリシーベースのルーティング 133

ポリシーベースのルーティングの概要 134
拡張アクセスリスト 134
適合グループ 134
アクショングループ 135
ポリシーベースのルーティングを使用するルートルックアップ 136
ポリシーベースのルーティングの構成 136
拡張アクセスリストの構成 137
適合グループの構成 138
アクショングループの構成 139
PBR ポリシーの構成 140
ポリシーベースのルーティングポリシーのバインディング 140
ポリシーベースのルーティングポリシーのインターフェースへのバインディング 140
ポリシーベースのルーティングポリシーのゾーンへのバインディング 140
ポリシーベースのルーティングポリシーの仮想ルーターへのバインディング 141

ポリシーベースのルーティングの出力の表示 141
拡張アクセスリストの表示 141
適合グループの表示 142
アクショングループの表示 142
ポリシーベースのルーティングポリシー構成の表示 143
完全なポリシーベースのルーティング構成の表示 143
高度な PBR の例 144
ルーティング 145
PBR 要素 146
拡張アクセスリスト 147
適合グループ 147
アクショングループ 147
PBR ポリシー 148
インターフェースのバインディング 148
可用性およびスケーラビリティが高い、高度な PBR 148
回復力のある PBR ソリューション 148
スケーラブルな PBR ソリューション 149

第 7 章 マルチキャストルーティング 151

概要 151
マルチキャストアドレス 152
逆方向パス転送 152
セキュリティデバイスによるマルチキャストルーティング 153
マルチキャストルーティングテーブル 153
静的マルチキャストルートの設定 154
アクセスリスト 155
トンネルインターフェース上に一般ルーティングのカプセル化を構成する 155
マルチキャストポリシー 157

第 8 章 IGMP (Internet Group Management Protocol) 159

概要 160
ホスト 161
マルチキャストルーター 161
セキュリティデバイスで稼動する IGMP 162
BGP をインターフェースで使用可能・不可にする 162
あるインターフェース上で IGMP を稼動させる 162
インターフェース上の IGMP を停止する 163
ホストの参加を許可するグループを列挙したアクセスリストの設定 ..163
IGMP の構成 164
IGMP に関する設定事項の確認 166
IGMP 運用パラメータ 167
IGMP プロキシ 168
メンバーシップレポートをソースに転送する手順 169
マルチキャストデータを受信者に送る手順 169
IGMP プロキシの設定 170
インターフェース上で IGMP プロキシを設定する 171
IGMP および IGMP プロキシ設定のマルチキャストポリシー 173
IGMP 用のマルチキャストグループポリシーの作成 173
IGMP プロキシ設定の作成 173
IGMP 送信元プロキシの設定 180

第 9 章　プロトコル独立マルチキャスト　187

概要 188
PIM-SM 190
マルチキャスト配布ツリー 190
代表ルーター 191
集合地点のグループへのマッピング 191
配布ツリーでのトラフィックの転送 192
PIM-SM 194
セキュリティデバイスで PIM-SM を構成する方法 195
VR 上に PIM-SM インスタンスを有効にし、削除します。 195
PIM-SM インスタンスを有効にする 195
PIM-SM インスタンスの削除 196
PIM-SM をインターフェースで使用可能・不可にする 196
インターフェース上の PIM-SM を有効にする 196
インターフェース上の PIM-SM を無効にする 197
マルチキャストグループポリシー 197
Static-RP-BSR メッセージ 197
Join-Prune メッセージ 197
PIM-SM のマルチキャストグループポリシーの定義 198
PIM-SM の基本設定 198
設定内容の確認 203
集合地点の設定 205
静的集合地点の設定 205
Candidate 集合地点の設定 206
セキュリティ検討事項 207
マルチキャストグループの制限 207
マルチキャストソースの制限 208
集合地点の制限 209
PIM-SM インターフェースパラメータ 210
Neighbor Policy を定義する 210
Bootstrap Border を定義する 211
プロキシ集合地点の設定 212
PIM-SM および IGMPv3 221

第 10 章　ICMP ルーター検出プロトコル　223

概要 223
ICMP ルーター検出プロトコルの構成 224
ICMP ルーター検出プロトコルを使用可能にする 224
WebUI からの ICMP ルーター検出プロトコルの構成 224
CLI からの ICMP ルーター検出プロトコルの構成 225
インターフェースの通知 225
アドレスのブロードキャスト 225
最大通知間隔の設定 225
最小通知間隔の設定 225
通知寿命値の設定 226
応答遅延の設定 226
初期通知間隔の設定 226
初期通知パケット数の設定 226
IRDP を使用不可にする 227
IRDP 設定の表示 227

索引 ..... IX-I

本編について

*第 7 部: ルーティング*には、以下の章が含まれます。

- 第 1 章「静的ルーティング」は、ルートテーブルについて説明し、宛先ベースのルーティング、ソースインターフェースベースのルーティングまたはソースベースのルーティングのための静的ルートの構成方法を説明します。
- 第 2 章「ルーティング」は、セキュリティデバイス上の仮想ルーターの構成方法およびプロトコル間または仮想ルーター間のルーティングテーブルエントリの再配布の方法を説明します。
- 第 3 章「オープンショーテストパスファースト (OSPF)」は、Open Shortest Path First (OSPF) の構成方法を説明します。
- 第 4 章「ルーティング情報プロトコル (RIP)」は、ルーティング情報プロトコル 1 (RIP) の構成方法を説明します。
- 第 5 章「境界ゲートウェイプロトコル」は、境界ゲートウェイプロトコル (BGP) の構成方法を説明します。
- 第 6 章「ポリシーベースのルーティング」は、トラフィックをネットワークの特定のパスを通過させる方法について説明します。
- 第 7 章「マルチキャストルーティング」は、マルチキャストルーティングの基本を説明し、この中には静的マルチキャストルートの構成方法も含まれます。
- 第 8 章「IGMP (Internet Group Management Protocol)」は、インターネットグループ管理プロトコル (IGMP) の構成方法を説明します。
- 第 9 章「プロトコル独立マルチキャスト」は、Protocol Independent Multicast - Sparse Mode (PIM-SM) および Protocol Independent Multicast - Source Specific Multicast (PIM-SSM) の構成方法を説明します。
- 第 10 章「ICMP ルーター検出プロトコル」は、ホストとルーターの間の ICMP（インターネット制御メッセージプロトコル）交換をセットアップする方法について説明します。

ドキュメントの規則

このドキュメントは、次のセクションで説明されている規則を使用しています。

- x ページの「Web ユーザーインターフェースの規則」
- x ページの「コマンドラインインターフェースの規則」
- xi ページの「ネーミング規則および文字タイプ」
- xii ページの「説明図の規則」

Web ユーザーインターフェースの規則

WebUI（Web ユーザーインターフェース）では、各作業の操作指示は、操作手順と構成設定値に分かれています。構成設定を入力できる WebUI ページを開くには、画面の左側にあるナビゲーション ツリーのメニュー項目をクリックして、そのページに移動します。先へ進むと、ナビゲーション パスが画面の上部に表示されます。各ページは角括弧で分離されています。

WebUI のパスおよびアドレスを定義するためのパラメータは、以下のとおりです。

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.2.2.5/32
Zone: Untrust

構成設定のオンラインヘルプを開くには、画面の左上にある疑問符（?）をクリックします。

ナビゲーションツリーにも、Help > Config Guide 構成ページがあり、セキュリティポリシーおよび IPSec （インターネットプロトコルセキュリティ）の構成に役立ちます。ドロップダウンメニューからオプションを選択して、そのページの指示に従います。構成設定のオンラインヘルプを開くには、左上にある **?** 文字をクリックします。

コマンドラインインターフェースの規則

次の規則は、例とテキストにおいて、コマンドラインインターフェース（CLI）コマンドの構文を示すために使用されます。

例においては、次のように使用されます。

- 角括弧 [ ] 内にあるものはすべてオプションです。
- 中括弧 { } 内にあるものはすべて必須です。
- 選択肢が複数ある場合、各選択肢はパイプ (|) で区切られています。次に例を示します。

```
set interface { ethernet1 | ethernet2 | ethernet3 } manage
```

- 変数は*斜体*で表示されます。

  set admin user *name1* password *xyz*

テキストにおいては、コマンドは**太字**で、変数は*斜体*で表示されます。

注： キーワード入力時には、単語を間違いなく識別できる数の文字を入力すれば十分です。**set admin user wheezer j12fmt54** というコマンドを入力する際には、**set adm u whee j12fmt54** と入力するだけで十分です。ただし、本編に記載されたコマンドはすべて本来の形式で記載されています。

ネーミング規則および文字タイプ

ScreenOS はオブジェクトの名前 (アドレス、管理ユーザー、認証サーバー、IKE ゲートウェイ、仮想システム、VPN トンネルおよびゾーンなど、ScreenOS 構成に定義されているもの) に関して、次の規則に従います。

- 名前文字列に 1 つまたは複数のスペースが含まれる場合、文字列全体を二重引用符で囲む必要があります。例 :

  set address trust “local LAN” 10.1.1.0/24

- 二重引用符で囲まれた文字列の先頭または末尾のスペースを取り除きます。たとえば、**「 local LAN 」**は**「local LAN」**となります。

- 連続した複数のスペースは、一つのスペースとして扱われます。

- CLI キーワードの多くはケースセンシティブではありませんが、名前文字列はケースセンシティブです。たとえば、**「local LAN」**は**「local lan」**とは異なります。

ScreenOS は、次の文字タイプをサポートします。

- 1 バイト文字セット (SBCS) およびマルチバイト文字セット (MBCS)。SBCS の例に、ASCII、欧州言語、およびヘブライ語があります。2 バイト文字セット (DBCS) とも呼ばれる MBCS の例に、中国語、韓国語、および日本語があります。

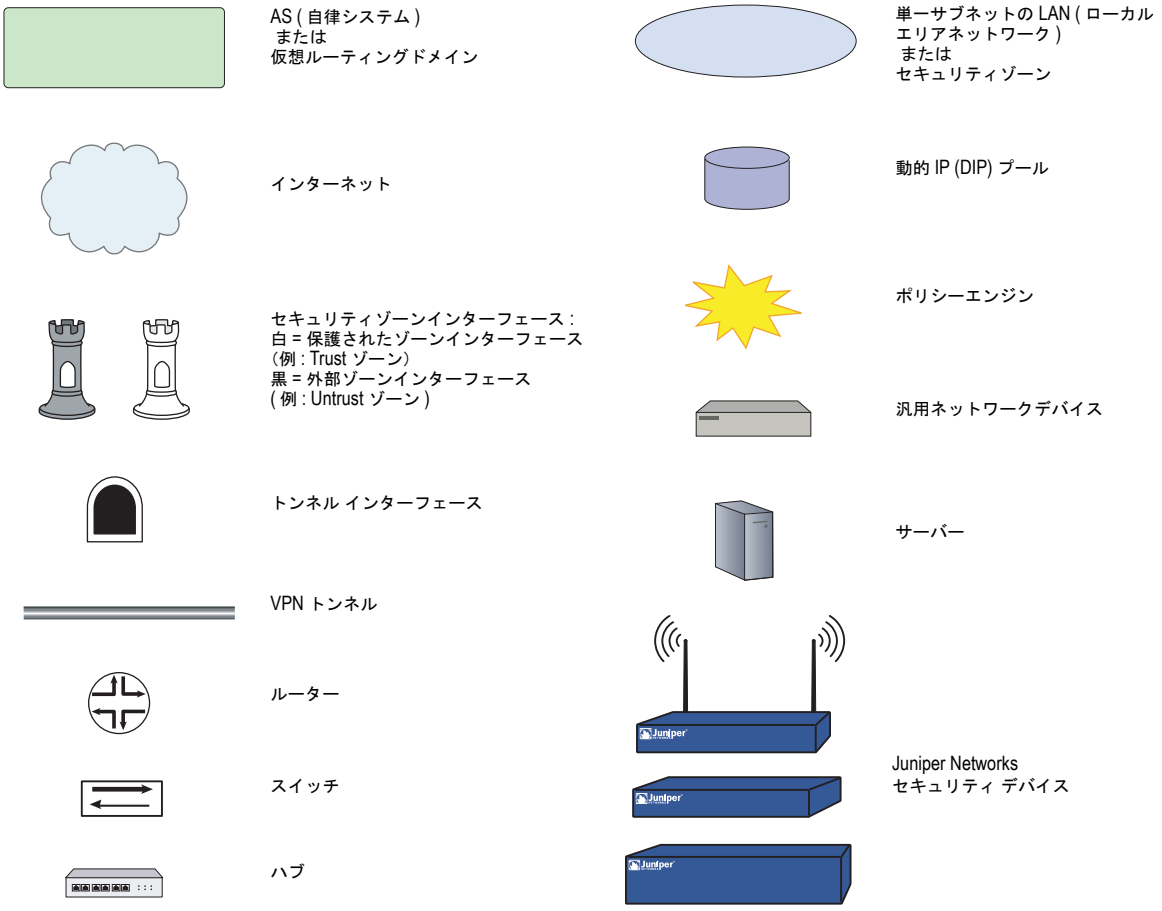
- ASCII 文字の 32（16 進数の 0x20）から 255（0xff)。ただし二重引用符 (“) は、スペースを含む名前文字列の先頭と末尾を示す特殊な意味をもつため、例外とします。

注： コンソール接続では、SBCS のみがサポートされます。ご利用のブラウザがサポートする文字セットに応じて、WebUI は SBCS および MBCS の両方をサポートします。

説明図の規則

次の図は、本編を通して説明図に使用されている画像の基本的なものです。

図 1: 説明図の画像



技術ドキュメントおよびテクニカルサポート

Juniper Networks 製品のいずれかの技術ドキュメントを入手するには、www.juniper.net/techpubs/ をご覧になってください。

テクニカルサポートについては、http://www.juniper.net/customers/support/ にある Case Manager を使って事例サポートを開くか、1-888-314-JTAC (米国内) か 1-408-745-9500 (その他の国) までお問い合わせください。

本書に間違いや欠落があった場合は、techpubs-comments@juniper.net までお知らせください。

第 1 章
静的ルーティング

この章では静的ルーティングについて、いつそしてどのように静的ルートを設定するかを説明します。本章のセクションは、以下のようになります。

- 1 ページの「概要」
  - 2 ページの「静的ルートのしくみ」
  - 3 ページの「静的ルートを構成するとき」
  - 5 ページの「静的ルートの構成」
  - 10 ページの「ゲートウェイトラッキングを使用可能にする」
- 11 ページの「Null インターフェースへトラフィックを転送する」
  - 11 ページの「他のルーティングテーブルのルートルックアップを防ぐ」
  - 11 ページの「トンネルトラフィックが非トンネルインターフェース上に送信されることを防ぐ」
  - 12 ページの「ルートの要約により生じたループを防ぐ」
- 12 ページの「永続アクティブルート」
- 13 ページの「等価コストマルチパスのルーティング優先度の変更」

概要

静的ルートは手動で構成した IP ネットワークアドレスのマッピングで、ルーターなどのレイヤー 3 転送デバイスに定義する、次のホップ宛先（他のルーター）の設定を含みます。

他のネットワークとの接続点が少ないネットワークの場合、または内部ネットワーク接続が比較的一定している場合、動的ルーティングを設定するより、静的ルートを定義する方が効率的です。ScreenOS は、明示的に削除されるまで静的ルートを保持します。ただし、必要な場合、静的ルートを動的ルーティング情報で上書きすることができます。

ScreenOS ルーティングテーブルで静的ルートを表示できます。ロードバランスを強制的に行うには、等価コストマルチパス (ECMP) を設定します。アクティブゲートウェイだけを使用するには、ゲートウェイトラッキングを設定します。

最低 1 つの*デフォルトルート*（ネットワークアドレス）を null ルートに設定します。デフォルトルートとは、ルーティングテーブルで定義された以外のネットワークを宛先とするパケットのキャッチオールエントリです。

静的ルートのしくみ

ホストがパケットを異なるネットワーク上の他のホストに送信する場合、各パケットヘッダーは宛先ホストのアドレスを含みます。ルーターがパケットを受信する場合、宛先アドレスをルーティングテーブルに含まれるすべてのアドレスと比較します。ルーターは、宛先アドレスに対して最も固有なルートをルーティングテーブルから選択して、選択したルートエントリから、次のホップを判別してパケットを転送します。

注： 最も固有なルートは、ルーティングテーブルの各エントリに対して、宛先アドレスおよびネットワークマスクのビットワイズ論理 AND を最初に実行することで判別されます。たとえば、サブネットマスクが 255.255.255.0 の IP アドレス 10.1.1.1 のビットワイズ論理 AND は 10.1.1.0 になります。サブネットマスクで最高値が 1 に設定されているルートが、最も固有なルート (「最長マッチングルート」とも言います) です。

図 2 は静的ルーティングを使用するネットワークの例およびサンプル IP パケットを示します。この例ではネットワーク A のホスト 1 はネットワーク C のホスト 2 に到達しようとしています。送信するパケットは、次のデータをヘッダーに含みます。

- ソース IP アドレス
- 宛先 IP アドレス
- ペイロード（メッセージ）

図 2: 静的ルーティングの例

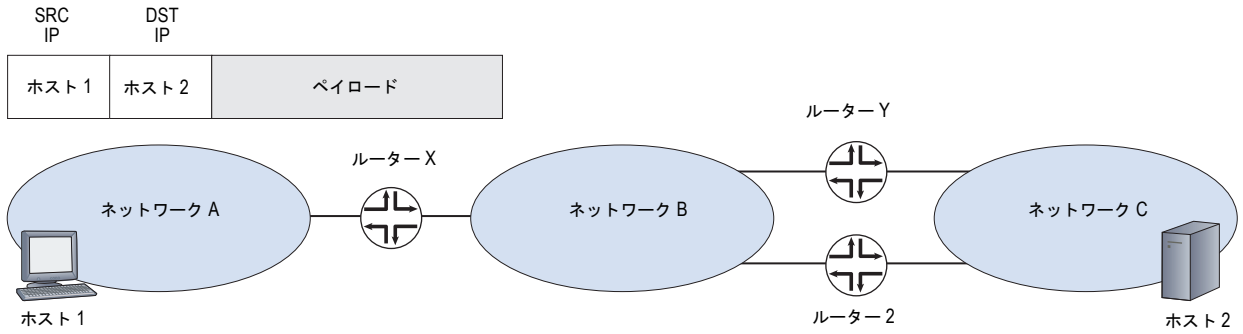


表 1 は各ルーターのルーティングテーブルの概要です。

表 1: ルーター X 、Y および Z のルーティングテーブルサマリ

ルーター X		ルーター Y		ルーター Z	
ネットワーク	ゲートウェイ	ネットワーク	ゲートウェイ	ネットワーク	ゲートウェイ
ネット A	Connected	ネット A	ルーター X	ネット A	ルーター X
ネット B	Connected	ネット B	Connected	ネット B	Connected
ネット C	ルーター Y	ネット C	Connected	ネット C	Connected

表 1 では、ゲートウェイ (次のホップ) がルーター Y であるネットワーク C 用に構成された静的ルートをルーター X は有します。ルーター X がネットワーク C のホスト 2 行きのパケットを受信する場合、パケットの宛先アドレスをルーティングテーブルと比較し、テーブルの最後のルートエントリが宛先アドレスに対して最も固有なルートであることを認めます。最後のルート入力は、ネットワーク C 向けのトラフィックをデリバリのためにルーター Y に送信するように指定します。ルーター Y はパケットを受信します。またネットワーク C が直接接続されると判断しているので、そのネットワークに接続されているインターフェースを通してパケットを送信します。

ルーター Y が故障、あるいはルーター Y とネットワーク C 間のリンクが利用不可能である場合、パケットはホスト 2 に到達することができません。ルーター Z を通してネットワーク C 用に別のルートがありますが、そのルートはルーター X で静的に構成されていないのでルーター X は代替ルートを識別しません。

静的ルートを構成するとき

動的ルーティングプロトコルを使用するときでも、最低複数の静的ルートを定義する必要があります。以下に挙げるような条件に対して静的ルートを定義する必要があります。

- 静的ルートを定義して、デフォルトルート (0.0.0.0/0) を仮想ルーターのルーティングテーブルに追加する必要があります。たとえば、同じセキュリティデバイス上で 2 つの仮想ルーターを使用する場合、trust-vr ルーティングテーブルには、untrust-vr を次のホップとして指定するデフォルトルートを含めることができます。これにより、trust-vr ルーティングテーブルにない宛先のトラフィックを untrust-vr に送ることができます。また、デフォルトルートを untrust-vr で定義して、untrust-vr ルーティングテーブルにない宛先のトラフィックを特定のルーター IP アドレスに送ることもできます。
- ネットワークがセキュリティデバイスに直接接続されていないが、VR 内のインターフェースからルーターを介してアクセスできる場合、そのルーターの IP アドレスでネットワークの静的ルートを定義する必要があります。例えば、Untrust ゾーンインターフェースは異なるインターネットサービスプロバイダ (ISP) に接続している 2 つのサブネット上に存在することがあります。特定の ISP にトラフィックを転送するために、どのルーターを使用するか定義する必要があります。
- 同じセキュリティデバイスで 2 つの仮想ルーターを使用しているときに、受信トラフィックが trust-vr インターフェースに接続されているネットワークに送られる untrust-vr インターフェースに送られる場合、次のホップとして trust-vr が指定されている宛先ネットワークの untrust-vr ルーティングテーブルで静的エントリを定義する必要がありますこの場合、trust-vr のルート情報を untrust-vr にエキスポートすると、静的ルート設定する必要がありません。

- デバイスが透過モードの場合、そのデバイス自体 (ファイアウォールを通過するユーザートラフィックに対して) からリモート宛先に送られる管理トラフィックを導く静的ルートを定義する必要があります。たとえば、リモート管理者のアドレスに syslog、SNMP、WebTrends メッセージを導く静的ルートを定義する必要があります。また、認証要求を RADIUS 、SecurID 、LDAP サーバーに導くルートを定義する必要があります。そして URL は Websense サーバーにチェックします。

注 : セキュリティデバイスが透過モードの場合、宛先がデバイスと同じサブネット上であっても、デバイスからの管理トラフィックのために静的ルートを定義する必要があります。

- アウトバウンド仮想プライベートネットワーク (VPN) トラフィックでは、宛先に 1 つ以上の出力インターフェースがある場合、希望するインターフェース経由で外部ルーターにアウトバウンドトラフィックを導くため、ルートを設定する必要があります。

- trust-vr のセキュリティゾーンのインターフェースが NAT の場合、また untrust-vr ルーティングドメインのソースから受信トラフィックを受信するためにそのインターフェース上にマップ IP (MIP) あるいは仮想 IP (VIP) を構成した場合、ゲートウェイとして trust-vr にポイントする untrust-vr の MIP あるいは VIP へのルートを作成してください。

- デフォルトでは、セキュリティデバイスは宛先 IP アドレスを元に、パケットを転送する最適ルートを見つけます。また、仮想ルーター上のソースベースまたはソースのインターフェースベースのルーティングテーブルを有効にすることも可能です。ソースベースのルーティングテーブルと、ソースのインターフェースベースのルーティングテーブルのどちらにも、仮想ルーター上で構成する静的ルートがあります。

静的ルートの構成

静的ルートを構成するには、以下を定義する必要があります。

- ルートが所属している仮想ルーター (VR)
- 宛先ネットワークの IP アドレスおよびネットマスク。
- ルートの次のホップ。これは、セキュリティデバイスの別の仮想ルーター、またはゲートウェイ (ルーター)IP アドレスです。別の仮想ルーターを指定する場合、宛先ネットワークのエントリがその仮想ルーターのルーティングテーブルにあることを確認してください。
- ルート指定されたトラフィックが送信されるときに通過するインターフェース。インターフェースは、物理インターフェースなどの任意の ScreenOS サポートインターフェース (たとえば ethernet1/2)、またはトンネルインターフェースです。特定のアプリケーションには、Null インターフェースを指定することもできます。11 ページの「Null インターフェースへトラフィックを転送する」を参照してください。

オプションとして、次の要素を定義することもできます。

- ルートメトリックは、同じ宛先ネットワークに複数のルートがあり、それらの優先度が同じときにアクティブルートを選択する場合に使用されます。静的ルートのデフォルトメトリックは 1 です。
- ルートタグは、ルーター再配布時のフィルタとして使用できる値です。たとえば、指定したタグ値を含むルートだけを仮想ルーターにインポートするよう選択できます。
- ルートの優先度値。デフォルトでは、静的ルートはすべて同じ優先度値が仮想ルーターに設定されています。
- 転送インターフェースがダウンしているか、または IP アドレスがインターフェースから削除されても、ルートがアクティブなままかどうか。

このセクションには、以下の例があります。

- 5 ページの「静的ルートの設定」
- 9 ページの「トンネルインターフェースに静的ルートを設定する」

静的ルートの設定

7 ページの図 3 では、ネットワークアドレス変換 (NAT) モードに Trust ゾーンインターフェースがあるセキュリティデバイスがマルチレベルネットワークを保護しています。ローカルとリモート管理の両方があります (NetScreen-Security Manager 経由)。セキュリティデバイスは SNMP トラップと syslog レポートをローカル管理者に送信し (Trust ゾーンのネットワーク上で位置しています)、NetScreen-Security Manager レポートをリモート 管理者に送信します (Untrust ゾーンのネットワーク上に位置しています)。デバイスは非武装地帯 (DMZ) ゾーンの SecurID サーバーを使用してユーザーを認証し、Trust ゾーンの Websense サーバーを使用してウェブフィルタリングを実行します。

注： この例を完了するには、次のゾーンをバインドする必要があります。ethernet1 を Trust ゾーンに、ethernet2 を DMZ ゾーンに、そして ethernet3 を Untrust ゾーンにバインドします。インターフェース IP アドレスは、それぞれ 10.1.1.1/24 、2.2.10.1/24 、2.2.2.1/24 となります。

trust-vr と untrust-vr ルーティングテーブルは、次の宛先のルート情報が必要です。

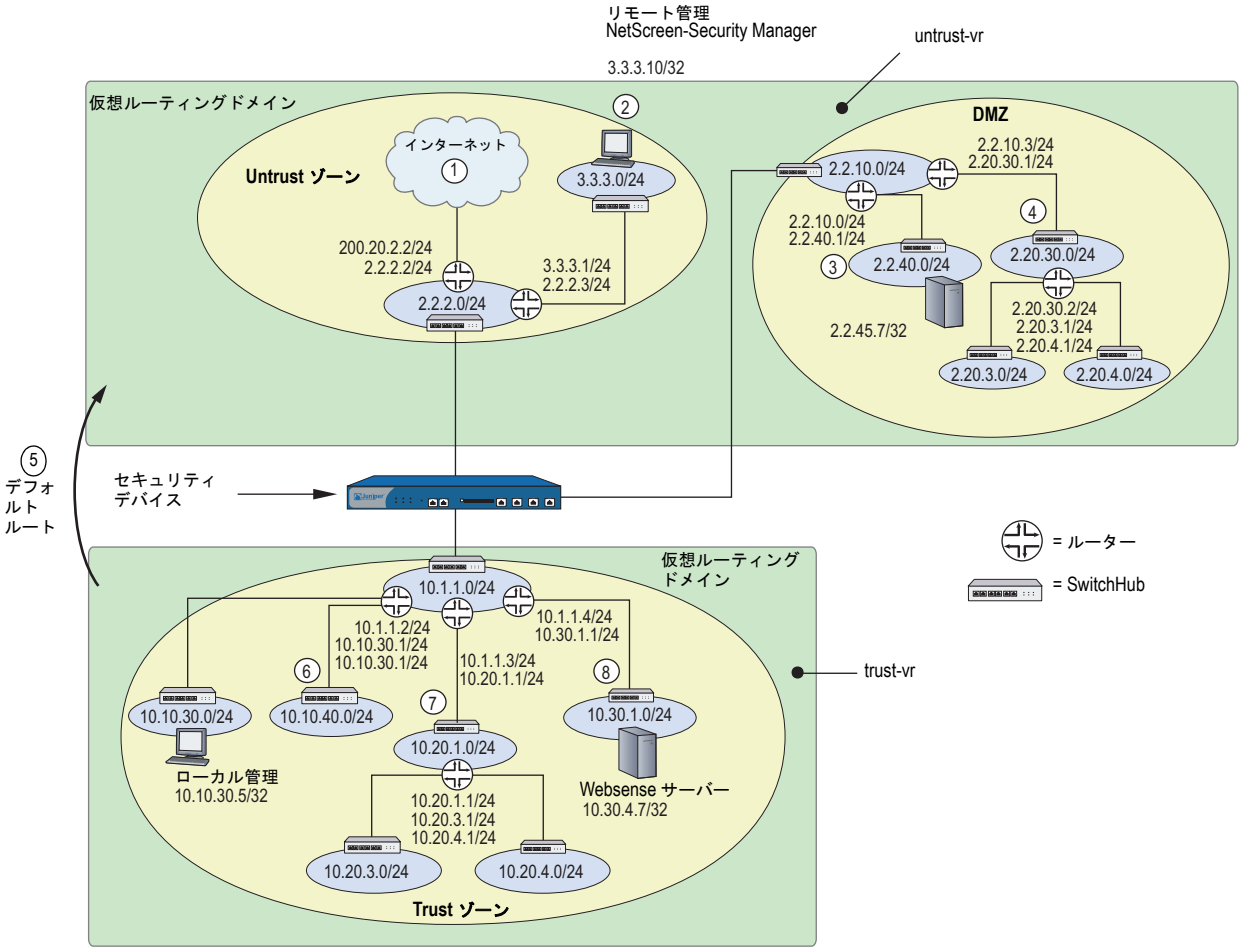
untrust-vr

1. インターネットのデフォルトゲートウェイ (VR のデフォルトルート)
2. サブネット 3.3.3.0/24 内のリモート管理者
3. DMZ ゾーン内のサブネット 2.2.40.0/24
4. DMZ ゾーン内のサブネット 2.20.0.0/16

trust-vr

5. trust-vr ルーティングテーブルにないすべてのアドレスの untrust-vr (VR のデフォルトルート)
6. Trust ゾーン内のサブネット 10.10.0.0/16
7. Trust ゾーン内のサブネット 10.20.0.0/16
8. Trust ゾーン内のサブネット 10.30.1.0/24

図 3: 静的ルート構成



WebUI

1. **untrust-vr**

   Network > Routing > Destination > untrust-vr New: 以下を入力して untrust デフォルトゲートウェイを作成し、**OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選択)
   Interface: ethernet3
   Gateway IP Address: 2.2.2.2

   Network > Routing > Destination > untrust-vr New: 以下を入力して、セキュリティデバイスによって生成されたシステムレポートをリモート管理に導いて、**OK** をクリックします。

   Network Address/Netmask: 3.3.3.0/24
   Gateway: (選択)
   Interface: ethernet3
   Gateway IP Address: 2.2.2.3

Network > Routing > Destination > untrust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 2.2.40.0/24
Gateway: (**選択**)
Interface: ethernet2
Gateway IP Address: 2.2.10.2

Network > Routing > Destination > untrust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 2.20.0.0/16
Gateway: (**選択**)
Interface: ethernet2
Gateway IP Address: 2.2.10.3

2. trust-vr

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Next Hop Virtual Router Name: (**選択**); untrust-vr

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.10.0.0/16
Gateway: (**選択**)
Interface: ethernet1
Gateway IP Address: 10.1.1.2

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.20.0.0/16
Gateway: (**選択**)
Interface: ethernet1
Gateway IP Address: 10.1.1.3

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.30.1.0/24
Gateway: (**選択**)
Interface: ethernet1
Gateway IP Address: 10.1.1.4

注 : 入力を削除するには、**Remove** をクリックしてください。メッセージが表示され、削除を確認するよう指示します。**OK** をクリックしてアクションを続行するか、**Cancel** をクリックしてアクションを中止してください。

CLI

1. **untrust-vr**

   set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.2
   set vrouter untrust-vr route 3.3.3.0/24 interface ethernet3 gateway 2.2.2.3
   set vrouter untrust-vr route 2.2.40.0/24 interface ethernet2 gateway 2.2.10.2
   set vrouter untrust-vr route 2.20.0.0/16 interface ethernet2 gateway 2.2.10.3

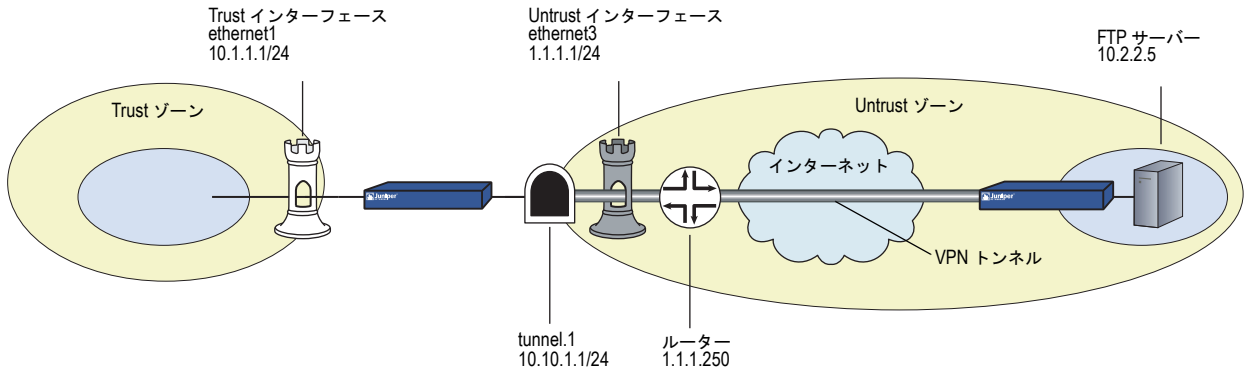
2. **trust-vr**

   set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
   set vrouter trust-vr route 10.10.0.0/16 interface ethernet1 gateway 10.1.1.2
   set vrouter trust-vr route 10.20.0.0/16 interface ethernet1 gateway 10.1.1.3
   set vrouter trust-vr route 10.30.1.0/24 interface ethernet1 gateway 10.1.1.4
   save

トンネルインターフェースに静的ルートを設定する

図 4 では、trusted ホストは trusted インターフェースではなく、別のサブネットに存在します。File Transfer Protocol (FTP) サーバーは、VPN トンネル経由で内向きのトラフィックを受信します。トンネルインターフェースを終了して、サーバーのあるサブネットに通じる内部ルーターへトラフィックを導くルートを設定してください。

図 4: トンネルインターフェースの静的ルート



WebUI

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.2.2.5/32
Gateway: (**選択**)
Interface: tunnel.1
Gateway IP Address: 0.0.0.0

注： **tunnel.1** を Interface ドロップダウンリストに表示するには、まず tunnel.1 インターフェースを作成してください。

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

CLI

```
set vrouter trust-vr route 10.2.2.5/32 interface tunnel.1
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
save
```

ゲートウェイトラッキングを使用可能にする

セキュリティデバイスはゲートウェイに対してインターフェースと独立した静的ルートを設定することができ、これにより到達性のトラッキングができます。デフォルトでは、静的ルートはトラッキングされません。しかしながら、ゲートウェイルートに対しては、到達性をトラッキングするようにセキュリティデバイスを構成することができます。デバイスは、各ゲートウェイの到達性により、トラッキングされたルートをアクティブまたは非アクティブとして記録します。例えば、ゲートウェイに到達できない場合、セキュリティデバイスはルートを非アクティブに設定します。ゲートウェイが再度アクティブになると、ルートはアクティブに戻ります。

ゲートウェイトラッキングができる静的ルートを追加するには、仮想ルーター (VR) レベルとゲートウェイアドレスにて、ルートを明示的に設定する必要があります。インターフェースには IP アドレスを設定しません。

このコマンドを使用して、プリフィックス 1.1.1.0 、長さ 2. の IP アドレス 1.1.1.254 に対して、ゲートウェイがトラッキングできる静的ルートを追加できます。ゲートウェイ IP アドレスを入力してゲートウェイトラッキングを設定しますが、このときインターフェースは設定しません。

WebUI

Network > Routing > Destination: **New** をクリックして、次を入力します。

IPv4/Netmask: 1.1.1.0/24
Gateway: (**選択**)
Gateway IP Address: 1.1.1.254

CLI

```
set vrouter trust route 1.1.1.0/24 gateway 1.1.1.254
unset vrouter trust route 1.1.1.0/24 gateway 1.1.1.254
save
```

Null インターフェースへトラフィックを転送する

Null インターフェースの静的ルートを、出力インターフェースとして構成することができます。Null インターフェースは常にアクティブとみなされるため、Null インターフェースを宛先とするトラフィックはドロップされます。Null インターフェースへのルートを*切り札*とするには、他のルートより高いメトリックを定義します。Null インターフェースにトラフィックを転送する静的ルートを使用する 3 つの目的は以下の通りです。

- 他のルーティングテーブルのルートルックアップを防ぐ
- 非トンネルインターフェースで送信されるトンネルトラフィックを防ぐ
- トラフィックループを防ぐ

他のルーティングテーブルのルートルックアップを防ぐ

ソースのインターフェースベースのルーティングが有効になっている場合、セキュリティデバイスはデフォルトで、ソースのインターフェースベースのルーティングテーブルのルートルックアップを実行します。(ソースのインターフェースベースのルーティングの構成については、22 ページの「ソースのインターフェースベースのルーティングテーブル」 . を参照してください) ソースのインターフェースベースのルーティングテーブルにルートがなく、ソースベースのルーティングが有効になっている場合、セキュリティデバイスはソースベースのルーティングテーブルのルートルックアップを実行します。ソースベースのルーティングテーブルにルートがない場合、セキュリティデバイスは宛先ベースのルーティングテーブルのルックアップを実行します。ソースベースのルーティングテーブルでも、宛先ベースのルーティングテーブルでもルートルックアップを行わないようにするには、デフォルトのルートを、Null インターフェースのソースのインターフェースベースのルーティングテーブルに、出力インターフェースとして作成します。ルートに一致するソースのインターフェースベースのルートが他に存在しない場合にのみ、このルートが使われるように、他のルートよりも高いメトリックを使用してください。

トンネルトラフィックが非トンネルインターフェース上に送信されることを防ぐ

出力トンネルインターフェースの静的ルートや動的ルートを使って、指定した宛先へのトラフィックを暗号化することができます。トンネルインターフェースが非アクティブになると、インターフェースに定義されているルートはすべて非アクティブになります。非トンネルインターフェースに別のルートがあれば、トラフィックは暗号化せずに送信されます。暗号化されるトラフィックを非トンネルインターフェースで送信されないようにするには、Null インターフェースのトンネルトラフィックと同じ宛先への静的ルートを、出力インターフェースとして定義します。このルートにトンネルインターフェースのルートよりも高いメトリックを定義すると、ルートはトンネルインターフェースのルートが利用できない場合にのみアクティブとなります。トンネルインターフェースが非アクティブになると、Null インターフェースのルートがアクティブになり、トンネルの宛先へのトラフィックはドロップされます。

ルートの要約により生じたループを防ぐ

セキュリティデバイスがルート情報の要約を通知すると、デバイスはルーティングテーブルにないプレフィックスのトラフィックを受信できます。そして、そのデフォルトのルートに基づいたトラフィックを転送します。次に、受信ルーターは、ルート情報の要約の通知を受けて、トラフィックをセキュリティデバイスに返送します。このようなループを防ぐには、Null インターフェースのある要約したルート情報のプレフィックスに対する静的ルートを、出力インターフェースとして定義し、さらに高いルートメトリックを定義します。セキュリティデバイスがルート情報の要約の通知にあるプレフィックスのトラフィックを受信しても、それがルーティングテーブルにない場合、そのトラフィックはドロップされます。

この例では、前の例で設定した、ネットワーク 2.1.1.0/24 を要約したルートに対する NULL インターフェースを設定します。ネットワーク 2.1.1.0/24 の中には、2.1.1.2、2.1.1.3、2.1.1.4 の各ホストがあります。2.1.1.10 宛のパケットはこの要約ルートの範囲に入ります。セキュリティデバイスはこのようなパケットも受け入れますが、転送先が見つからないため送信元に送り返し、ループが生じてしまいます。これを回避するため、このルートに NULL インターフェースを設定します。このとき、高めの優先度やメトリックを設定することが重要です。

WebUI

Network > Routing > Destination > trust-vr New: 以下を入力し **OK** をクリックします。

Network Address/Netmask: 2.1.1.0/24
Gateway: (**選択**)
Interface: Null
Gateway IP Address: 0.0.0.0
Preference: 255
Metric: 65535

CLI

```
set vrouter trust-vr route 2.1.1.0/24 interface null preference 255 metric 65535
save
```

永続アクティブルート

特定の状況では、ルートに関連する物理インターフェースがダウンしたり、割り当てられた IP アドレスがなくても、ルーティングテーブルのステータスをアクティブなままにすることがあります。たとえば、XAuth サーバーは、サーバーにトラフィックを送信するたびに、セキュリティデバイス上のインターフェースに IP アドレスを割り当てることができます。インターフェース上で IP アドレスが割り当てられていない場合でも、XAuth サーバーへのルートは常にアクティブとなり、XAuth サーバーへのトラフィックがドロップされないようにしておく必要があります。

また、IP トラッキングが構成されるインターフェース全体でルートをアクティブにしておくことも便利です。IP トラッキングを構成すると、セキュリティデバイスでは、ターゲット IP アドレスが元のインターフェースから宛先不明になった場合、別のインターフェースから出力トラフィックを再ルーティングできます。セキュリティデバイスは、別のインターフェースへのトラフィックを再ルーティングしますが、ターゲットが再び到達可能になるかどうかを判断するために、元のインターフェースで ping 要求を送信できなければなりません。

等価コストマルチパスのルーティング優先度の変更

等価コストマルチパス (ECMP) の静的ルートのルーティング優先度を変更することもできます。詳細は 38 ページの「等価コストマルチパスルーティングの構成」を参照してください。

第 2 章

ルーティング

この章はルーティングおよび仮想ルーター (VR) 管理を説明します。本章のセクションは、以下のようになります。

- 16 ページの「概要」
- 17 ページの「仮想ルータールーティングテーブル」
  - 18 ページの「宛先ベースのルーティングテーブル」
  - 19 ページの「ソースベースのルーティングテーブル」
  - 22 ページの「ソースのインターフェースベースのルーティングテーブル」
- 24 ページの「仮想ルーターの作成と変更」
  - 24 ページの「仮想ルーターの設定変更」
  - 25 ページの「仮想ルーター ID を割り当てる」
  - 26 ページの「仮想ルーター間でトラフィックを転送する」
  - 26 ページの「2 つの仮想ルーターの設定」
  - 28 ページの「仮想ルーターの作成と削除」
  - 29 ページの「仮想ルーターと仮想システム」
  - 32 ページの「ルーティングテーブルの最大ルート情報数」
- 32 ページの「ルーティング機能および例」
  - 32 ページの「ルートの選択」
  - 38 ページの「等価コストマルチパスルーティングの構成」
  - 40 ページの「ルート情報の再配布」
  - 45 ページの「仮想ルーター間でルート情報をエクスポート / インポート」

概要

ルーティングとは、最終的な宛先に向けてネットワーク間でパケットを転送するプロセスのことです。ルーターはあるネットワークが他のネットワークに接触する箇所に存在するデバイスで、これらのネットワーク間でトラフィックを導きます。

デフォルトでは、セキュリティデバイスはルート操作モードに入り、Layer-3 ルーターとして作動します。しかしながら、セキュリティデバイスを設定して、Layer-2 スイッチとして透過モードで作動させることもできます。

注： どちらの操作モードにおいても、いくつかのルートは手動で設定する必要があります。

Juniper Networks セキュリティデバイスは、ルーティングを仮想ルーター (VR) と呼ばれるプロセスを通して行います。セキュリティデバイスは、ルーティング構成要素を 2 つ以上の VR に分け、それぞれの VR はルーティングテーブル、ルーティング論理および関連したセキュリティゾーンで、既知のネットワークリストを維持しています。単一の VR は次の 1 つ以上をサポートできます。

- 静的または手動で構成されたルート
- 動的ルート（動的ルーティングプロトコルが学習したものなど）
- マルチキャストルート（ホストマシンのグループへのルートなど）

セキュリティデバイスには、2 つの定義済み VR があります。

- trust-vr: デフォルトでは、すべての定義済みセキュリティゾーンおよび任意のユーザ定義ゾーンが含まれます。
- untrust-vr: デフォルトでは、セキュリティゾーンは含まれません。

trust-vr や untrust-vr 仮想ルーターを削除することはできません。仮想ルーターは複数あっても構いませんが、デフォルトの仮想ルーターは *trust-vr* です。VR テーブルでは、アスタリスク（*）は、trust-vr がコマンドラインインターフェース（CLI）のデフォルトの仮想ルーターであることを表しています。VR テーブルは、**get vrouter** CLI コマンドを使って参照することができます。他の仮想ルーター内にゾーンとインターフェースを構成するには、untrust-vr などの名前で仮想ルーターを指定してください。NHTB の詳細については、**2**-25 ページの「ゾーン」を参照してください。

セキュリティデバイスによっては、追加のカスタム仮想ルーターを作成できます。ルーティング情報を複数の VR に分け、他のドメインが見えるルーティング情報の量を管理することができます。たとえば、企業ネットワーク「内部」のセキュリティゾーン全体のルーティング情報は、定義済み仮想ルーター trust-vr で維持し、一方企業ネットワーク「外部」については、他の定義済み仮想ルーター untrust-vr で維持する、といった運用が考えられます。内部のネットワークルーティング情報を、社外からの信用できないソースからの情報と別にすることができます。というのは、1 つの VR のルーティングテーブルの詳細は、他方には見えないからです。

仮想ルータールーティングテーブル

セキュリティデバイスでは、各 VR はそれ自体のルーティングテーブルを保持しています。ルーティングテーブルは既知のネットワークの最新リストおよびそれに到達するための指示です。セキュリティデバイスの受信パケットを処理する場合、ルーティングテーブルルックアップを実行して、宛先アドレスまでの適切なインターフェースを探します。

それぞれのルートテーブルエントリは、トラフィックを転送する宛先ネットワークを識別します。宛先ネットワークは IP ネットワーク、サブネットワーク、スーパーネットまたはホストでありえます。それぞれのルーティングテーブルエントリーはユニキャスト（ 1 つのホストマシンを参照する 1 つの IP アドレスに送信されたパケット）またはマルチキャスト（複数のホストマシンを参照する 1 つの IP アドレスに送信されたパケット）でありえます。

ルーティングテーブルエントリには、以下のソースのものを使用できます。

- 直接接続しているネットワーク (宛先ネットワークはルートモードでインターフェースに割り当てる IP アドレスです)
- 動的ルーティングプロトコル。オープンショーテストパスファースト (OSPF) 、境界ゲートウェイプロトコル (BGP) またはルーティング情報プロトコル (RIP) などがあります。
- インポートされたルートの形をとった、他のルーターや仮想ルーター
- 静的に構成されたルート
- ホストルート

注 : ルートモードでインターフェースに IP アドレスを設定する場合、ルーティングテーブルはインターフェースを行き来するトラフィックのために隣接するサブネットに自動的に接続ルートを作成します。

VR は 3 つのタイプのルーティングテーブルをサポートします。

- 宛先ベースのルーティングテーブルを使用すると、セキュリティデバイスは受信データパケットの宛先 IP アドレスに基づいたルートルックアップを実行します。デフォルトでは、セキュリティデバイスは宛先 IP アドレスだけを元に、パケットを転送する最適ルートを見つけます。
- ソースベースのルーティングテーブルを使用すると、セキュリティデバイスは受信データパケットのソース IP アドレスに基づいたルートルックアップを実行します。ソースベースのルーティングテーブルにエントリを追加するには、NetScreen デバイスがルートルックアップを実行するよう指定したソースアドレスの静的ルートを構成しなければなりません。このルーティングテーブルは、デフォルトでは使用不可に設定されています。19 ページの「ソースベースのルーティングテーブル」を参照してください。
- ソースのインターフェースベースのルーティングテーブルを使用すると、セキュリティデバイスは、データパケットがデバイスに到着するインターフェースに基づいたルートルックアップを実行します。ソースのインターフェースベースのルーティングテーブルにエントリを追加するには、仮想

ルーターがルートルックアップを実行するよう指定したインターフェースの静的ルートを構成しなければなりません。このルーティングテーブルは、デフォルトでは使用不可に設定されています。22 ページの「ソースのインターフェースベースのルーティングテーブル」を参照してください。

宛先ベースのルーティングテーブル

仮想ルーターには常に、宛先ベースのルーティングテーブルが入っています。また、仮想ルーター上のソースベースまたはソースのインターフェースベースのルーティングテーブル、あるいはその両方を有効にすることも可能です。ScreenOS の宛先ベースのルーティングテーブルの例は、以下のとおりです。

```
device-> get route

IPv4 Dest-Routes for <untrust-vr> (0 entries)
--------------------------------------------------------------------------------
H: Host C: Connected S: Static A: Auto-Exported
I: Imported R: RIP P: Permanent D: Auto-Discovered
iB: IBGP eB: EBGP O: OSPF E1: OSPF external type 1
E2: OSPF external type 2

IPv4 Dest-Routes for <trust-vr> (11 entries)
--------------------------------------------------------------------------------
   ID          IP-Prefix      Interface         Gateway   P Pref    Mtr     Vsys
--------------------------------------------------------------------------------
*   8          0.0.0.0/0         eth1/1     10.100.37.1   S   20      1     Root
*   7        1.1.1.1/32          eth1/2         0.0.0.0   H    0      0     Root
*   3     192.168.1.1/32            mgt         0.0.0.0   H    0      0     Root
*   2     192.168.1.0/24            mgt         0.0.0.0   C    0      0     Root
*   4     10.100.37.0/24         eth1/1         0.0.0.0   C    0      0     Root
*   5   10.100.37.170/32         eth1/1         0.0.0.0   H    0      0     Root
*   6        1.1.1.0/24          eth1/2         0.0.0.0   C    0      0     Root
*   9       11.3.3.0/24            agg1         0.0.0.0   C    0      0     Root
*  10       11.3.3.0/32            agg1         0.0.0.0   H    0      0     Root
*  11        3.3.3.0/24           tun.1         0.0.0.0   C    0      0     Root
*  12        3.3.3.0/32           tun.1         0.0.0.0   H    0      0     Root
```

各宛先ネットワークについて、ルーティングテーブルには次の情報が含まれます。

- 宛先ネットワークのトラフィックが転送されるセキュリティデバイスのインターフェース。
- 次のホップは、セキュリティデバイスの別の仮想ルーター、またはゲートウェイ IP アドレスです (通常はルーターアドレスです)。
- ルート元のプロトコルルーティングテーブルのプロトコル列は、ルートのタイプを示しています。
  - Connected network (C)
  - Static (S)
  - Auto-exported (A)
  - Imported (I)
  - 動的ルーティングプロトコル。RIP (R) 、オープンショーテストパスファーストまたは OSPF (O) 、OSPF 外部タイプ 1 またはタイプ 2 （それ

ぞれ E1 または E2 ）、内部または外部境界ゲイトウェイプロトコル（それぞれ iB または eB ）

- Permanent (P)
- Host (H)

  32 ビットマスクのホストルートエントリは、それぞれのインターフェースを IP アドレスで構成すると表示されます。ホストルートはルートテーブルでは必ずアクティブで、ルートルックアップは必ず成功します。ホストルートは自動的に構成された変更（インターフェース IP アドレス削除など）で更新され、絶対に再配布されたり、エクスポートされたりしません。ホストルートにより、トラフィックが迷う可能性がなくなり、処理能力を節約します。

- *優先度*は、同じ宛先ネットワークに複数のルートがあるときに使用するルートを選択する場合に使用されます。この値は、プロトコルまたはルート元で判別されます。優先度値が低いルートほど、優先してアクティブルートとして選択されます。

  各プロトコルまたはルート元の優先度値は、仮想ルーターごとに変更できます。詳細は 32 ページの「ルートの選択」を参照してください。

- *メトリック*は、同じ宛先ネットワークに複数のルートがあり、それらの優先度が同じときに使用するルートを選択する場合に使用できます。接続ルートのメトリック値は常に 0 です。静的ルートのデフォルトメトリック値は 1 ですが、静的ルートを定義するときに別の値を指定できます。

- このルートが属する仮想システム (vsys)。仮想ルーターについての詳細については、29 ページの「仮想ルーターと仮想システム」を参照してください。この例では、untrust-vr テーブルヘッダーの下にエントリがなく、trust-vr テーブルヘッダーの下に 11 のエントリがあります。

通常、ルーティングテーブルには、*デフォルトルート* (ネットワークアドレス 0.0.0.0/0) があります。これは、ルーティングテーブルで定義されている以外のネットワークに送られるパケットに対するキャッチオールエントリです。

宛先ベースのルーティングテーブルの例については、5 ページの「静的ルートの構成」を参照してください。

ソースベースのルーティングテーブル

セキュリティデバイスがトラフィックの転送先を判断する基準として、データパケットの宛先 IP アドレスでなく、ソース IP アドレスを使うよう設定することができます。これにより、ある特定のサブネットに属するユーザーからのトラフィックについてのみ、転送するパスを別のサブネットからの場合とは区別する、といった使い方が可能です。仮想ルーターでソースベースのルーティングが有効になると、セキュリティデバイスは、ソースベースのルーティングテーブルにあるパケットのソース IP アドレスでルーティングテーブルのルックアップを実行します。ソースベースのルーティングテーブルの中にソース IP アドレスのルートがない場合、セキュリティデバイスは宛先ベースのルーティングテーブルのルートルックアップに、パケットの宛先 IP アドレスを使用します。

ソースベースのルートは、特定の仮想ルーターに対して、静的ルートとして定義します。ソースベースのルートは、構成した VR に適用されますが、ソースベースのルートに対しては、他の VR を次ホップとして指定できます。しかしながら、ソースベースのルートを別の仮想ルーターやルーティングプロトコルに再配布することもできません。

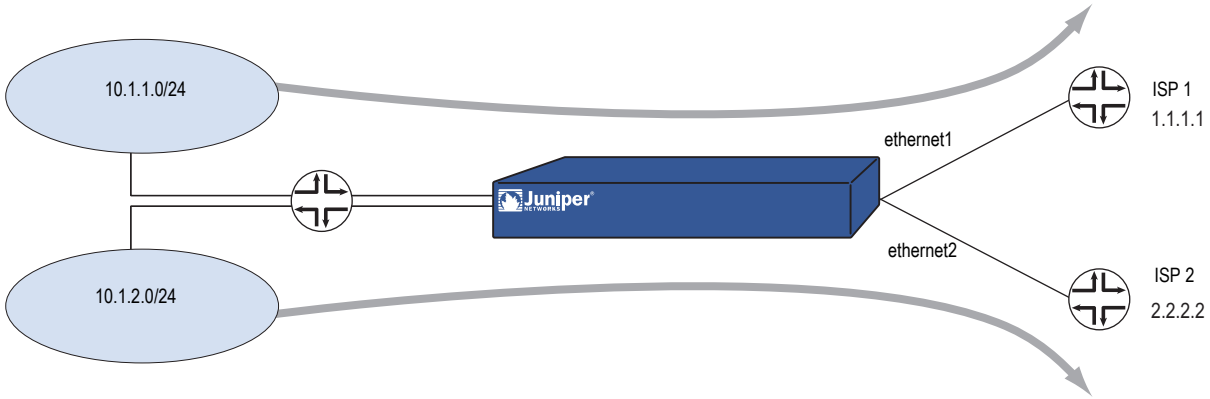
この機能が使えるようにする手順を以下に示します。

1. この情報を指定して、1 つ以上のソースベースのルートを作成してください。
   - ソースベースのルーティングを適用する仮想ルーター名。
   - ソース IP アドレス。ソースベースのルーティングテーブルにはこのアドレスが登録され、セキュリティデバイスはこれに対してルーティングテーブルルックアップを実行します。
   - パケットを転送する外向きインターフェース名。
   - ソースベースルート次のホップ点 (**set interface** *interface* **gateway** *ip_addr* というCLI コマンドで、インターフェースのデフォルトゲートウェイが設定済みであれば、指定は不要です。このデフォルトゲートウェイを、次のホップ点と看做します。**set vrouter** *vrouter* **route source** *ip_addr/netmask* **vrouter** *next-hop_vrouter* で、他の VR をソースベースルートの次ホップに指定することもできます)
   - ソースベースルートのメトリック。(同一のプレフィックスのソースベースルートが複数ある場合、ルートルックアップにはメトリック値が最小のルートのみが採用され、他のルートには「使用しない」旨の印をつけます。)
2. 当該仮想ルーターについて、ソースベースのルーティングを有効にします。セキュリティデバイスは、ソースベースのルーティングテーブルのルートルックアップに、パケットのソース IP を使用します。これで見つからなければ、宛先 IP アドレスがルーティングテーブルルックアップに使用されます。

図 5 では、サブネット 10.1.1.0/24 に属するユーザーからのトラフィックは ISP 1 に転送し、10.1.2.0/24 からの場合は ISP 2 に転送するよう設定します。デフォルト trust-vr 仮想ルーターのルーティングテーブルに以下の 2 つのルート情報を追加し、ソースベースのルーティングを有効にします。

- サブネット 10.1.1.0/24、転送インターフェース ethernet3、次のホップ点は ISP 1 のルーター (1.1.1.1)
- サブネット 10.1.2.0/24、転送インターフェース ethernet4、次のホップ点は ISP 2 のルーター (2.2.2.2)

図 5: ソースベースのルーティング例



WebUI

Network > Routing > Source Routing > New (trust-vr): 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0 255.255.255.0
Interface: ethernet3 (選択)
Gateway IP Address: 1.1.1.1

Network > Routing > Source Routing > New (trust-vr): 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.2.0 255.255.255.0
Interface: ethernet4 (選択)
Gateway IP Address: 2.2.2.2

注 : WebUI 画面で設定する場合、デフォルトの優先度値およびメトリックの初期値は 1 となっています。

Network > Routing > Virtual Routers > Edit (trust-vr): **Enable Source Based Routing** を選択し、**OK** をクリックします。

CLI

```
set vrouter trust-vr route source 10.1.1.0/24 interface ethernet3 gateway 1.1.1.1
    metric 1
set vrouter trust-vr route source 10.1.2.0/24 interface ethernet4 gateway 2.2.2.2
    metric 1
set vrouter trust-vr source-routing enable
save
```

ソースのインターフェースベースのルーティングテーブル

ソースのインターフェースベースのルーティング (SIBR) を使用すると、セキュリティデバイスは、ソースインターフェース (データパケットがセキュリティデバイスに到着するインターフェース) に基づいたトラフィックを転送します。仮想ルーターで SIBR が有効になると、セキュリティデバイスは SIBR ルーティングテーブルでルートルックアップを実行します。ソースインターフェースの SIBR ルーティングテーブル内にルートエントリが見つからない場合、セキュリティデバイスは、ソースベースのルーティングテーブル (仮想ルーターでソースベースのルーティングが有効な場合) または先ベースのルーティングテーブルでルートルックアップを実行します。

ソースのインターフェースベースのルートは、指定されたソースインターフェースの静的ルートとして定義します。ソースのインターフェースベースのルートは、構成した VR に適用されますが、ソースのインターフェースベースのルートに対しては、他の VR を次ホップとして指定することもできます。しかしながら、ソースのインターフェースベースのルートを別の仮想ルーターにエクスポートしたり、ルーティングプロトコルに再配布することはできません。

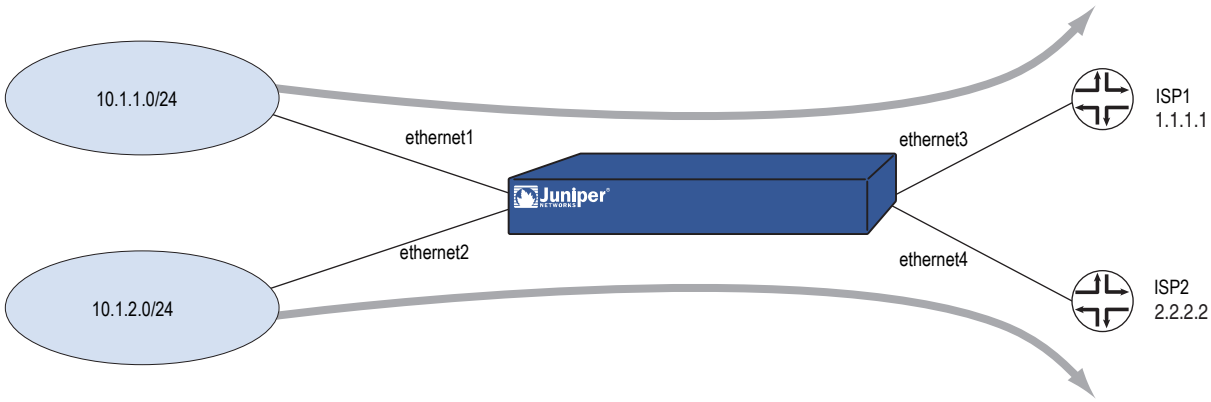
この機能が使えるようにする手順を以下に示します。

1. 以下の情報を指定して、1 つ以上のソースのインターフェースベースのルートを作成してください。
   - このルートを適用する仮想ルーター名。
   - セキュリティデバイスが SIBR テーブルにおいてルックアップを行う、ソースインターフェース。(インターフェースはルーティングテーブルのエントリとして表示されます。)
   - ルートの IP アドレスおよびネットマスクのプレフィックス。
   - パケットを転送する外向きインターフェース名。
   - ソースのインターフェースベースルートの次ホップ点。(**set interface** *interface* **gateway** *ip_addr* という CLI コマンドで、インターフェースのデフォルトゲイトウェイが既に指定してある場合、指定は不要です。インターフェースのデフォルトゲートウェイを、次のホップ点と看做します。**set vrouter** *vrouter* **route source** *ip_addr/netmask* **vrouter** *next-hop_vrouter* で、他の VR をソースベースルートの次ホップに指定することもできます)
   - ソースのインターフェースベースルートのメトリック。(同一のプレフィックスのソースのインターフェースベースルートが複数ある場合、ルートルックアップにはメトリック値が最小のルートのみが採用され、他のルートには「使用しない」旨の印をつけます。)
2. SIBR に対して VR を有効にします。セキュリティデバイスは、SIBR テーブルのルートルックアップに、パケットのソースインターフェースを使用します。

図 6 では、サブネット 10.1.1.0/24 に属するユーザーからのトラフィックは、ethernet1 インターフェースのセキュリティデバイスに到着して ISP 1 に転送され、10.1.2.0/24 からの場合は、ethernet2 インターフェースのセキュリティデバイスに到着して ISP 2 に転送されます。デフォルト trust-vr 仮想ルーターのルーティングテーブルに以下の 2 つのエントリを構成し、SIBR を有効にします。

- サブネット 10.1.1.0/24、ソースインターフェース ethernet1、転送インターフェース ethernet3、次のホップ点は ISP 1 のルーター 1.1.1.1
- サブネット 10.1.2.0/24、ソースインターフェース ethernet2、転送インターフェース ethernet4、次のホップ点は ISP 2 のルーター 2.2.2.2

図 6: ソースのインターフェースベースのルーティング (SIBR) の例



WebUI

Network > Routing > Source Interface Routing > New (ethernet1): 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0 255.255.255.0
Interface: ethernet3 (選択)
Gateway IP Address: 1.1.1.1

Network > Routing > Source Interface Routing > New (ethernet2): 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.2.0 255.255.255.0
Interface: ethernet4 (選択)
Gateway IP Address: 2.2.2.2

注 : WebUI 画面で設定する場合、デフォルトの優先度値およびメトリックの初期値は 1 となっています。

Network > Routing > Virtual Routers > Edit (trust-vr): **Enable Source Interface Based Routing** を選択し、**OK** をクリックします。

CLI

```
set vrouter trust-vr route source in-interface ethernet1 10.1.1.0/24 interface
    ethernet3 gateway 1.1.1.1 metric 1
set vrouter trust-vr route source in-interface ethernet2 10.1.2.0/24 interface
    ethernet4 gateway 2.2.2.2 metric 1
set vrouter trust-vr sibr-routing enable
save
```

仮想ルーターの作成と変更

このセクションでは、既存の仮想ルーター (VR) の変更および変更および、カスタム VR の作成および削除に関するさまざまな例および手順があります。

仮想ルーターの設定変更

定義済み仮想ルーター、カスタム仮想ルーターの設定変更は、WebUI 画面からでも CLI を使っても可能です。たとえば trust-vr 仮想ルーターを修正する手順は以下のようになります。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit

CLI

set vrouter trust-vr

仮想ルーターに関して修正できるパラメータは以下のとおりです。

- 仮想ルーター ID （ 32 ページの「ルーティングテーブルの最大ルート情報数」を参照)。
- ルーティングテーブルの許容最大エントリ数。
- プロトコルに応じたルートの優先度値 (33 ページの「ルートの優先度値を設定する」を参照)
- 仮想ルーターがトラフィックを転送する基準としてデータパケットのソース IP アドレスを用いること (デフォルトでは、データパケットの宛先 IP アドレスが基準。19 ページの「ソースベースのルーティングテーブル」を参照してください。)
- ルートモードで設定したインターフェースに対して、untrust-vr に自動エクスポートする機能の ON/OFF (trust-vr のみ)。
- 他の仮想ルーターを次のホップ点とするようなデフォルトルートの追加 (trust-vr のみ)。
- 動的ルーティング MIB 用の SNMP トラップをプライベートと設定すること (デフォルトルートレベル仮想ルーターのみ)。
- 動作していないインターフェース上のルートでも、通知できるようにする (デフォルトでは、アクティブインターフェース上で定義されたアクティブルートのみが他のプロトコルへの再配布や、他の仮想ルーターへのエクスポートの対象となります)。
- インターフェースどうしのサブネットが重複していても、仮想ルーターでは無視してよいとすること (デフォルトでは、同一の仮想ルーターに属するインターフェースどうしでは、重複を禁止)。
- 仮想ルーターが、NetScreen 冗長性プロトコル (NSRP) ピア上の仮想ルーターと、設定を同期できるようにすること

仮想ルーター ID を割り当てる

動的ルーティングプロトコルでは、ルーティングデバイスどうしが情報を交換できるようにするため、それぞれに一*意的な*識別番号を割り当てる必要があります。この識別子は、IP アドレスのようなドット区切り 10 進記法で表しても、単に整数値として表しても構いません。仮想ルーター ID (VR ID) を設定することなく動的ルーティングプロトコルを有効にした場合、ScreenOS は自動的に、当該仮想ルーター上で稼動しているインターフェースのうち最も大きな IP アドレスを、仮想ルーター ID として割り当てます。

デフォルトでは、セキュリティデバイスはすべて、VLAN1 インターフェースに IP アドレス 192.168.1.1 が割り当てられています。したがって、セキュリティデバイス上の動的ルーティングプロトコルを使用可能にする前にルーター ID を指定しないと、自動的に割り当てられるルーター ID はすべてこの 192.168.1.1 になってしまいます。すると、ルーティングが正常に働かなくなる恐れがあります。同一のルーティングドメイン内に、同一のルーター ID のセキュリティ仮想ルーターが複数存在することになるからです。これを避けるためにも、ネットワーク内で一意的な仮想ルーター ID を、明示的に割り当てるよう推奨します。ループバックインターフェースが NetScreen 冗長性プロトコル (NSRP) クラスターの仮想セキュリティインターフェース (VSI) でなければ、ループバックインターフェースアドレスを仮想ルーター ID としても構いません (NSRP クラスターの設定について詳しくは、*第 11 部 : 高可用性* を参照。)

ここでは trust-vr のルーター ID として、0.0.0.10 を割り当てます。

注 : WebUI 画面から設定する場合、ルーター ID はドット区切り 10 進記法で入力しなければなりません。CLI の場合は、ドット区切り 10 進記法で 0.0.0.10 と指定しても、単に 10 と入力しても構いません。後者の場合、0.0.0.10 と変換されます。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit: 次のように入力してから **OK** をクリックします。

Virtual Router ID: Custom (**選択**)
テキストボックスに 0.0.0.10 を入力します。

CLI

```
set vrouter trust-vr router-id 10
save
```

注 : 仮想ルーターで動的ルーティングプロトコルを有効にしてからでは、ルーター ID の割り当てや変更はできません。変更する場合は、あらかじめ仮想ルーターの動的ルーティングプロトコルを無効にしておいてください。その具体的な手順については、この巻の該当する章を参照してください。

仮想ルーター間でトラフィックを転送する

セキュリティ上に 2 つの VR が存在する場合、ある VR のゾーンからのトラフィックは、他方の VR のゾーンに自動的に転送*されません*。これはそのトラフィックを許可するポリシーがある場合もそうです。VR 間をトラフィックが通る場合、次の手順の 1 つを行う必要があります。

- 一方の仮想ルーターに、もう一方の仮想ルーターが次のホップ点となるよう、静的ルートを設定する方法。これが仮想ルーターのデフォルトルートであっても構いません。たとえば trust-vr のデフォルトルートを、untrust-vr が次のホップ点になるように設定することも考えられます。外向きパケットの宛先が trust-vr のルーティングテーブルに載っていなければ、そのまま untrust-vr に転送することになります静的ルートの構成の詳細については、5 ページの「静的ルートの構成」を参照してください。

- ルート情報を、ある仮想ルーターから別の仮想ルーターにエクスポートする方法。エクスポート / インポートの操作は、ルートごとに個別に行えます。また、trust-vr から untrust-vr に、ルート情報をすべてエクスポートすることも可能です。これにより、untrust-vr が受け取ったパケットはそのまま、trust-vr 側の宛先に転送されることになります。詳細については、45 ページの「仮想ルーター間でルート情報をエクスポート / インポート」を参照してください。

2 つの仮想ルーターの設定

セキュリティデバイス内に複数の VR が存在する場合、それぞれの VR は個別のルーティングテーブルを維持します。デフォルトでは、定義済みおよびユーザー定義のセキュリティゾーンは、trust-vr にバインドされています。すなわち、このようなセキュリティゾーンにバインドされているインターフェースはすべて、trust-vr にも属しているということです。このセクションでは、セキュリティゾーン (およびそのインターフェース) を、untrust-vr 仮想ルーターにバインドする手順を解説します。

セキュリティゾーンは、1 つの仮想ルーターにしかバインドできません。また、複数のセキュリティゾーンを同一の仮想ルーターにバインドできるのは、ゾーンどうしでアドレスが重複しない場合に限ります。すなわち、各ゾーンのインターフェースをすべてルーとモードでしなければならない、ということです。ゾーンを仮想ルーターにバインドすれば、そのゾーンのインターフェースはすべて、当該仮想ルーターに属することになります。セキュリティゾーンをバインドする仮想ルーターを変更することはできますが、その場合、あらかじめインターフェースをすべて削除しておかなければなりません (インターフェースとセキュリティゾーンのバインドおよびその解除については **2**-35 ページの「インターフェース」を参照)。

セキュリティゾーンを untrust-vr 仮想ルーターにバインドする手順の概要は、以下のようになります。

1. untrust-vr にバインドしようとするゾーンから、インターフェースをすべて削除します。インターフェースが残ったままでは、ゾーンと仮想ルーターとのバインド関係を変更することはできません。インターフェースに IP アドレスを割り当てている場合は、あらかじめ削除しておいてください。

2. ゾーンを untrust-vr 仮想ルーターに割り当てます。

3. インターフェースを元どおりゾーンに割り当て直します。

この例では、Untrust セキュリティゾーンがデフォルトで trust-vr にバインドされ、さらに、インターフェース ethernet3 がこの Untrust セキュリティゾーンにバインドされている状態だとします (ほかにバインドされたインターフェースはありません)。ethernet3 の IP アドレス / ネットマスクを 0.0.0.0 に変更しておいてから、Untrust セキュリティゾーンを untrust-vr にバインドし直します。

WebUI

1. **Untrust ゾーンにバインドされたインターフェースを解除**
   Network > Interfaces(ethernet3) > Edit: 次のように入力してから **OK** をクリックします。

   Zone Name: Null
   IP Address/Netmask: 0.0.0.0/0

2. **Untrust ゾーンを untrust-vr にバインド**
   Network > Zones (untrust) > Edit: Virtual Router Name ドロップダウンリストで **untrust-vr** を選択し、**OK** をクリックします。

3. **インターフェースを Untrust ゾーンにバインド**
   Network > Interfaces(ethernet3) > Edit: Zone Name ドロップダウンリストで **Untrust** を選択してから **OK** をクリックします。

CLI

1. **Untrust ゾーンにバインドされたインターフェースを解除**
   unset interface ethernet3 ip
   unset interface ethernet3 zone

2. **Untrust ゾーンを untrust-vr にバインド**
   set zone untrust vrouter untrust-vr

3. **インターフェースを Untrust ゾーンにバインド**
   set interface eth3 zone untrust
   save

次のアウトプット例では **get zone** コマンドによりデフォルトインターフェース、ゾーンおよび VR バインドが表示されています。デフォルトでは Untrust ゾーンが trust-vr にバインドされています。

```
device-> get zone
Vsys ルートに合計 12 のゾーン。7 つの構成可能ポリシーゾーン
------------------------------------------------------------
ID Name         Type    Attr    VR          Default-IF   VSYS
 0 Null         Null    Shared untrust-vr   null         Root
 1 Untrust      Sec(L3) Shared trust-vr     ethernet3    Root
 2 Trust        Sec(L3)        trust-vr     ethernet1    Root
 3 DMZ          Sec(L3)        trust-vr     ethernet2    Root
 4 Self         Func           trust-vr     self         Root
 5 MGT          Func           trust-vr     vlan1        Root
 6 HA           Func           trust-vr     null         Root
10 Global       Sec(L3)        trust-vr     null         Root
11 V1-Untrust   Sec(L2)        trust-vr     v1-untrust   Root
12 V1-Trust     Sec(L2)        trust-vr     v1-trust     Root
13 V1-DMZ       Sec(L2)        trust-vr     v1-dmz       Root
16 Untrust-Tun Tun             trust-vr     null         Root
------------------------------------------------------------
```

untrust-vr に対して、ゾーンバインドを変更することができます。**get zone** コマンドを実行すると、変更したインターフェース、ゾーンおよび VR バインド（この場合、untrust ゾーンは untrust-vr にバインドされています）が表示されます。

```
device-> get zone
Vsys ルートに合計 12 のゾーン。7 つの構成可能ポリシーゾーン
------------------------------------------------------------------
ID Name          Type    Attr    VR          Default-IF   VSYS
 0 Null          Null    Shared untrust-vr   null         Root
 1 Untrust       Sec(L3) Shared untrust-vr   ethernet3    Root
 2 Trust         Sec(L3)        trust-vr     ethernet1    Root
 3 DMZ           Sec(L3)        trust-vr     ethernet2    Root
 4 Self          Func           trust-vr     self         Root
 5 MGT           Func           trust-vr     vlan1        Root
 6 HA            Func           trust-vr     null         Root
10 Global        Sec(L3)        trust-vr     null         Root
11 V1-Untrust    Sec(L2)        trust-vr     v1-untrust   Root
12 V1-Trust      Sec(L2)        trust-vr     v1-trust     Root
13 V1-DMZ        Sec(L2)        trust-vr     v1-dmz       Root
16 Untrust-Tun Tun              trust-vr     null         Root
------------------------------------------------------------------
```

仮想ルーターの作成と削除

さえきゅうりティデバイスの機種によっては、定義済みの 2 つの仮想ルーターに加え、カスタム仮想ルーターを作成することができます。ユーザー定義の仮想ルーターについては、仮想ルーター ID、ルーティングテーブルに登録できる最大ルート情報数、特定のプロトコルに応じた優先度値など、さまざまな事項を自由に設定できます。

注： カスタム仮想ルーターを作成できない機種もあります。また、カスタム仮想ルーターの作成にはソフトウェアライセンスキーが必要です。

カスタム仮想ルーターを作成する

この例では、trust2-vr と呼ばれるカスタム仮想ルーターを作成し、trust2-vr から untrust-vr に、自動的にルート情報をエクスポートするよう設定します。

WebUI

Network > Routing > Virtual Routers > New: 次のように入力してから **OK** をクリックします。

Virtual Router Name: trust2-vr
Auto Export Route to Untrust-VR: (**選択**)

CLI

```
set vrouter name trust2-vr
set vrouter trust2-vr auto-route-export
save
```

カスタム仮想ルーターを削除する

ここでは、trust2-vr という既存のユーザー定義の仮想ルーターを削除します。

WebUI

Network > Routing > Virtual Routers: trust2-vr に対応する **Remove** をクリックします。

削除の確認プロンプトが表示されるので、**OK** をクリックします。

CLI

```
unset vrouter trust2-vr
```

vrouter unset, are you sure? y/[n] という削除の確認プロンプトが表示されるので、**Y** を入力します。

```
save
```

注 : 定義済み仮想ルーターである untrust-vr、trust-vr は削除できませんが、ユーザー定義の仮想ルーターはどれでも削除できます。ユーザー定義仮想ルーターの名前や ID を変更したい場合は、いったん削除してから新しい名前または VR ID で作成し直してください。

仮想ルーターと仮想システム

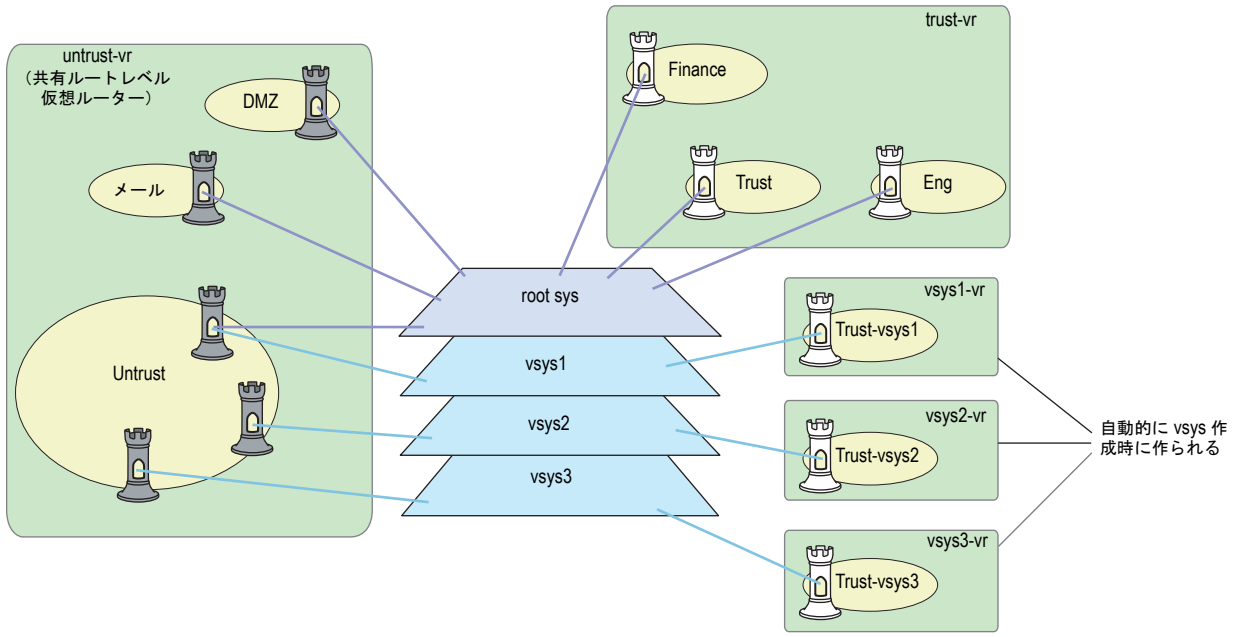
仮想システムに対応したシステム上にルートレベル管理者が作成した vsys は、初めから以下の仮想ルーターが使えるようになっています。

- ルートレベル仮想ルーターのうち、共有可と定義されているもの。untrust-vr は共有仮想ルーターであり、どの vsys からも使えます。ほかのルートレベル仮想ルーターも、共有可と設定することができます。
- vsys レベル仮想ルーター。vsys を作成すると自動的に vsys レベル仮想ルーターも作られます。これは Trust-*vsysname* ゾーンのルーティングテーブルを管理しています。仮想ルーター名は、デフォルトでは *vsysname*-vr ですが、別に定義することもできます。これを他の vsys と共有することはできません。

注 : Juniper Networks セキュリティシステム (NetScreen-500, NetScreen-5200, NetScreen-5400) だけがをサポートします。また、vsys オブジェクトの作成にはソフトウェアライセンスキーが必要です。

カスタム仮想ルーターは vsys ごとにいくつでも定義できます。仮想システムの詳細は、*第 10 部 : 仮想 システム* を参照してください。図 7 では、3 つの vsys のそれぞれに、仮想ルーターが 2 つずつあります。すなわち、*vsysname*-vr という vsys レベル仮想ルーターと、untrust-vr です。

図 7: Vsys 内の仮想ルーター



Vsys 上に仮想ルーターを作成する

この例では、my-vsys1 という仮想システム上に、カスタム仮想ルーター vr-1a を定義します。仮想ルーター ID は 10.1.1.9 とします。

WebUI

Vsys > Configure > Enter (my-vsys1) > Network > Routing > Virtual Routers > New: 以下を入力して **Apply** をクリックします。

Virtual Router Name: vr-1a
Virtual Router ID: Custom (選択)
テキストボックスに **10.1.1.9** と入力

CLI

```
set vsys my-vsys1
(my-vsys1) set vrouter name vr-1a
(my-vsys1/vr-1a) set router-id 10.1.1.9
(my-vsys1/vr-1a) exit
(my-vsys1) exit
```

次のプロンプトが現れたら **Y** と入力。

```
Configuration modified, save? [y]/n
```

vsys 作成時に作られた vsys レベル仮想ルーターは、この vsys のデフォルト仮想ルーターでもあります。これをカスタム仮想ルーターに変更することもできます。たとえば、先に作成したカスタム仮想ルーター vr-1a を仮想システム my-vsys1 のデフォルト仮想ルーターにする手順は、以下のとおりです。

WebUI

Vsys > Configure > Enter (my-vsys1) > Network > Routing > Virtual Routers > Edit (vr-1a): **Make This Vrouter Default-Vrouter for the System** を選んで、**Apply** をクリック。

CLI

```
set vsys my-vsys1
(my-vsys1) set vrouter vr-1a
(my-vsys1/vr-1a) set default-vrouter
(my-vsys1/vr-1a) exit
(my-vsys1) exit
```

次のプロンプトが現れたら **Y** と入力。

```
Configuration modified, save? [y]/n
```

デフォルトでは、定義済みのセキュリティゾーン Trust-*vsysname* に、vsys 作成時に作られた vsys レベル仮想ルーターがバインドされています。しかし、定義済みのセキュリティゾーン Trust-*vsysname* やユーザー定義の vsys レベルセキュリティゾーンには、この vsys で使えるものならばどの仮想ルーターをバインドしても構いません。

デフォルトでは、untrust-vr はすべての vsys 間で共有されています。vsys レベル仮想ルーターは共有不可ですが、ルートレベル仮想ルーターならば、vsys 間で共有するよう定義できます。したがって、vsys レベル仮想ルーターに、共有ルートレベル仮想ルーターが次のホップ点となるようなルート（経路）を定義できるのです。また、vsys レベル仮想ルーターと共有ルートレベル仮想ルーターとの間で、ルート（経路）情報を再配布するよう定義することも可能です。

仮想ルーター間の共有ルート

この例では、ルートレベル仮想ルーター my-router のルートテーブルに、4.0.0.0/8 ネットワークに関するエントリが載っているとします。ルートレベル仮想ルーター my-router を vsys 間で共有するよう設定すれば、vsys レベル仮想ルーターに、my-router を次のホップ点とする、4.0.0.0/8 宛のルートを定義することができます。この例では、仮想システムを my-vsys1、vsys レベル仮想ルーターを my-vsys1-vr とします。

WebUI

Network > Routing > Virtual Routers > New: 次のように入力してから **OK** をクリックします。

```
Virtual Router Name: my-router
Shared and accessible by other vsys: ( 選択 )
```

Vsys > Configure > Enter (my-vsys1) > Network > Routing > Routing Entries > New (my-vsys1-vr): 次のように入力してから **OK** をクリックします。

```
Network Address/Netmask: 40.0.0.0 255.0.0.0
Next Hop Virtual Router Name: ( 選択 ) my-router
```

CLI

```
set vrouter name my-router sharable
set vsys my-vsys1
(my-vsys1) set vrouter my-vsys1-vr route 40.0.0.0/8 vrouter my-router
(my-vsys1) exit
```

次のプロンプトが現れたら **Y** と入力。

```
Configuration modified, save? [y]/n
```

ルーティングテーブルの最大ルート情報数

各仮想ルーターには、システム全体で確保されたプールから、ルーティングテーブル用に必要な容量が割り当てられます。ルーティングテーブルに登録できる最大ルート情報数は、セキュリティデバイスの機種と、そのデバイス上に設定されている仮想ルーターの個数によって決まります。しかしこれとは別に、ある仮想ルーターに割り当てる最大数を制限することも可能です。これにより、ある特定の仮想ルーターがシステム全体の資源を消費し尽くしてしまうことを、回避することができます。

注： Juniper Networks セキュリティデバイスの、機種別の最大ルート情報数については、該当する機種のデータシートを参照してください。

この例では、trust-vr 用のルーティングテーブルに登録できる最大ルート情報数を 20 と設定します。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr): 次のように入力してから **OK** をクリックします。

Maximum Route Entry:
Set Limit at: (**選択**), 20

CLI

```
set vrouter trust-vr max-routes 20
save
```

ルーティング機能および例

ネットワークに必要な仮想ルーターを構成したら、どのルーティング機能を使うか決めます。これらの機能は、ルーティング動作およびルーティングテーブルデータに影響を与えます。そして、静的ルーティングおよび動的ルーティングプロトコルに適用されます。

本セクションは、以下のようになります。

- 32 ページの「ルートの選択」
- 38 ページの「等価コストマルチパスルーティングの構成」
- 40 ページの「ルート情報の再配布」
- 45 ページの「仮想ルーター間でルート情報をエクスポート / インポート」

ルートの選択

ルーティングテーブルには、同一のプレフィックス (IP アドレスおよびネットマスク) 宛のルートが、複数登録されることもあります。同じ宛先のルートが複数ある場合は、各ルーターの優先度値を比較します。優先度値が最小のルートを採用します。これも同じ場合はメトリック値を比較し、やはり最小のルートを採用します。

注： 優先度値が*同一*でメトリック値が*同一*な同じ宛先への複数のルートがある場合、いずれかのルートを任意に選びます。あるルートが採用されやすいとか、予測できるということはありません。

ルートの優先度値を設定する

ルートの優先度とは、トラフィックがその宛先に到達する最適パスを判定する際、当該ルートに対して加える「重み」のことです。ルーティングテーブルにルート情報をインポートあるいは追加する際、仮想ルーターはルートの優先度値を設定します。この値は、ルートの学習に使われたプロトコルによって決まります。この値が小さい (0 に近い) 方が、大きい (0 から離れている) 値よりも優先度は高いものとして扱います。

仮想ルーターでは、プロトコルに従ってルートの優先度値を設定します。表 2 には、それぞれのプロトコルのデフォルト優先度値がリストされています。

表 2: デフォルトルート優先度値

プロトコル	デフォルトの優先度値
Connected	0
Static	20
Auto-Exported	30
EBGP	40
OSPF	60
RIP	100
Imported	140
OSPF External Type 2	200
IBGP	250

優先度値を調整して、あるパスを優先的に使うようにすることも可能です。

この例では、untrust-vr のルートテーブルに「直接接続」ルートを追加する際に設定する優先度値として、4 を指定します。

注 : あるプロトコル (たとえば OSPF Type 1) に対する優先度値を変更すれば、ルーティングテーブルを表示すると新しい値に変わっているはずです。しかし実際には、ルート情報が再収集されるまで、すなわち、動的ルーティングプロトコルによりいったんルート情報が無効になり、その後再び有効になるまでは、元の優先度値のままです。静的ルートの場合は、いったん削除して再び追加した段階で、新しい優先度値が反映されます。

優先度を変更したために既存のルートが影響されることはありません。既存のルートに変更を適用するには、いったんルートを削除してから、もう一度追加することが必要です。動的ルートの場合は、いったんプロトコルを使用不可にしてからもう一度使用可能にするか、またはデバイスを再起動することが必要です。

「直接接続」とは、ルーターのあるインターフェースに、宛先ネットワークの該当する IP アドレスが割り当てられている状態のことです。

WebUI

Network > Routing > Virtual Routers > Edit (untrust-vr): 次のように入力してから **OK** をクリックします。

Route Preference:
Connected: 4

CLI

```
set vrouter untrust-vr preference connected 4
save
```

ルートのメトリック

ルートのメトリック値は、パケットが特定の宛先に到達するための、最適パスを判定するために使います。同一の宛先に到達するルートが複数ある場合、ルーターはメトリック値を比較して、どちらのルートを採用するか判断します。すなわち、同一の宛先ネットワークに到達でき、優先度値も同じであれば、メトリック値が最小のルートを採用するのです。

ルートのメトリックは、次の要素のすべてまたはその組み合わせに基づいています。

- 宛先に到達するために、パケットが行き来するルーターの数
- パスの相対的スピードおよび帯域幅
- パスを構成するリンクのコスト ($)
- その他の要素

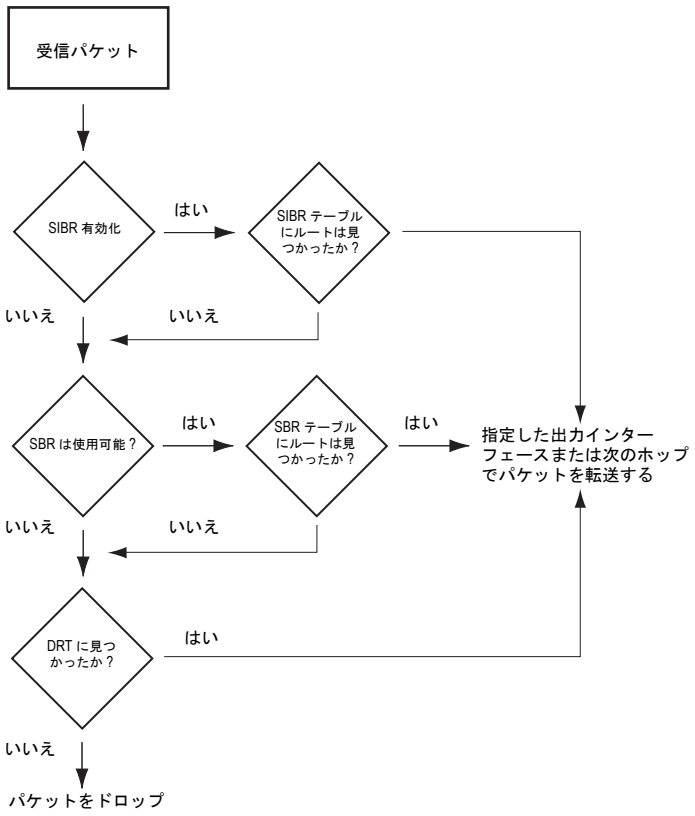
動的に学習されるルートについては、その起点となる接続ルーターがメトリック値を決めます。接続されたルートのデフォルトのメトリックは必ず 0 です。静的ルートのデフォルトのメトリックは 1 です。

デフォルトのルートルックアップ順序の変更

仮想ルーターでソースベースのルーティングとソースのインターフェースベースのルーティングの両方を有効にすると、ルーティングテーブルと受信パケットを指定された順番にチェックすることにより、ルートルックアップを実行します。このセクションでは、デフォルトのルートルックアップの順序および各ルートテーブルの優先度値の設定による順序の変更方法について説明します。

受信パケットが既存のセッションと一致しない場合は、セキュリティデバイスは先頭パケットの処理を行い、ルートルックアップを行います。図 8 はデフォルトのルートルックアップ順序を示します。

図 8: デフォルトのルートルックアップの順序



1. 仮想ルーターでソースのインターフェースベースルーティングが有効な場合、まずルートエントリがパケットの到着するインターフェースと一致するか、ソースのインターフェースベースルーティングテーブルをチェックします。ソースのインターフェースベースルーティングテーブル内にソースインターフェースのルートエントリが見つかると、セキュリティデバイスはマッチングルートエントリで指定したパケットを転送します。ソースのインターフェースベースルーティングテーブル内にソース IP アドレスのルートエントリが見つからない場合、セキュリティデバイスは、仮想ルーターでソースベースのルーティングが有効かどうかをチェックします。

2. 仮想ルーターでソースベースルーティングが有効な場合、ルートエントリがパケットの到着するインターフェースと一致するか、ソースベースルーティングテーブルをチェックします。ソース IP アドレスに一致したルートエントリが見つかると、セキュリティデバイスはエントリで指定したパケットを転送します。ソースベースルーティングテーブル内にソース IP アドレスのルートエントリが見つからない場合、セキュリティデバイスは、宛先ベースのルーティングテーブルをチェックします。

3. このチェックは、宛先ベースのルーティングテーブルで、ルートエントリがパケットの宛先 IP アドレスと一致するかどうかを見ます。宛先 IP アドレスに一致したルートエントリが見つかると、セキュリティデバイスはエントリで指定したパケットを転送します。完全にマッチングルートエントリが見つからなくても、仮想ルーターに設定したデフォルトのルートがある場合は、デバイスはデフォルトのルートで指定したパケットを転送します。宛先 IP アドレスにマッチングルートエントリが見つからず、デフォルトのルートもない場合、パケットはドロップされます。

ルートのチェックの順序は、各ルーティングテーブルに割り当てられた優先度値によって決まります。最も優先度値の高いルーティングテーブルが最初にチェックされ、低いものほど後になります。デフォルトでは、ソースのインターフェースベースルーティングテーブルが最も優先度値の高い (3) となっており、次が優先度値 (2) のソースベースルーティングテーブル、そして宛先ベースのルーティングテーブルは最も優先度値の低い (1) となっています。

ユーザは新しい優先度値を割り当てて、仮想ルーターにおけるルートルックアップの順序を変更することができます。デバイスは、優先度値の高い順にルーティングテーブルをチェックするということを念頭に置いてください。

以下の例では、trust-vr における SIBR およびソースベースのルーティングの両方を有効にします。ルートルックアップを次の順序で実行するものとします。最初にソースベースルーティング、SIBR 、そして宛先ベースのルーティングを実行します。このルートルックアップの順序を設定するには、ソースベースのルーティングの優先度値を SIBR より高く設定しなければなりません。この例では、ソースベースのルーティングに優先度値 4 を割り当てることにします。

WebUI

Network > Routing > Virtual Router > Edit (trust-vr): 次のように入力してから **OK** をクリックします。

Route Lookup Preference (1-255): (**選択**)
For Source Based Routing: 4
Enable Source Based Routing: (**選択**)
Enable Source Interface Based Routing: (**選択**)

CLI

```
set vrouter trust-vr sibr-routing enable
set vrouter trust-vr source-routing enable
set vrouter trust-vr route-lookup preference source-routing 4
save
```

複数の仮想ルーターにおけるルートルックアップ

次のホップ点として、別の仮想ルーターを宛先ベースのルートエントリに指定することができますが、ソースベースまたはソースのインターフェースベースのルートエントリに対しては指定できません。例えば、宛先ベースのルーティングテーブルのデフォルトルートは、次ホップ点として untrust-vr を指定することができます、すると untrust-vr エントリは DMZ などのほかの仮想ルーターを指定できます。デバイスは最高 3 つの仮想ルーターをチェックします。ある仮想ルーターのルートルックアップが、別の仮想ルーターに影響するため、セキュリティデバイスは常に宛先ベースのルートテーブルで 2 度目のルートルックアップを実行します。

以下の例では、trust-vr および untrust-vr ルーティングテーブルの両方のソースベースのルーティングを有効にしています。trust-vr には、次のルーティングエントリがあります。

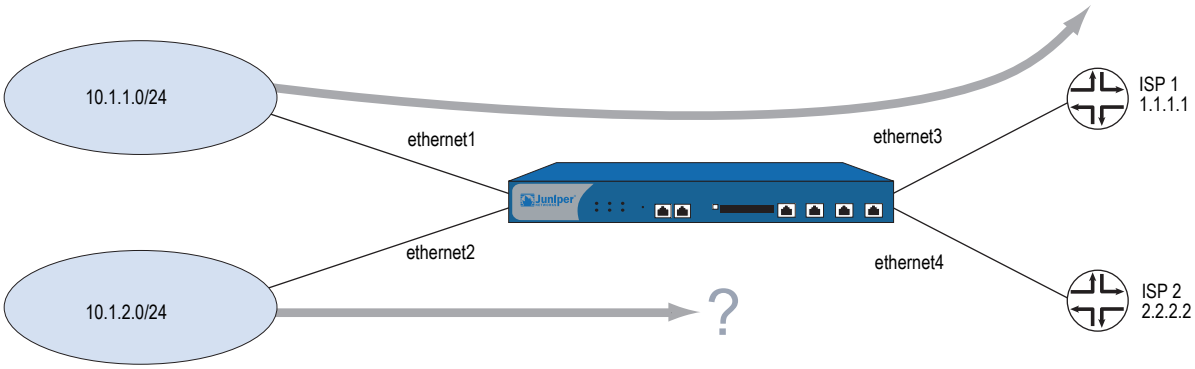
- サブネット 10.1.1.0/24 のソースベースのルーティングエントリ、転送インターフェース ethernet3、次のホップ点のルーター 1.1.1.1
- 次のホップ点 untrust-vr のデフォルトルート

untrust-vr には、次のルーティングエントリがあります。

- サブネット 10.1.2.0/24 のソースベースのルーティングエントリ、転送インターフェース ethernet4、次のホップ点のルーター 2.2.2.2
- 転送インターフェース ethernet3 および次のホップ点のルーター 1.1.1.1 のデフォルトルート

図 9 では、サブネット 10.1.2.0/24 からのトラフィックが、ethernet3 から 1.1.1.1 のルーターに必ず転送されます。

図 9: 複数の仮想ルーターでのルートルックアップ



trust-vr のソースベースルーティングテーブルには、次のエントリがあります。

```
  ID          IP-Prefix      Interface         Gateway   P Pref    Mtr     Vsys
*  1        10.1.1.0/24           eth3       2.2.2.250   S   20      1     Root
```

untrust-vr の宛先ベースルーティングテーブルには、次のエントリがあります。

```
  ID          IP-Prefix      Interface         Gateway   P Pref    Mtr     Vsys
*  1        0.0.0.0/24            n/a      untrust-vr   S   20      0     Root
```

サブネット 10.1.2.0/24 からのトラフィックは、ethernet2 のセキュリティデバイスに到着します。一致するソースベースのルートエントリがないため、セキュリティデバイスは宛先ベースのルーティングテーブルでルートルックアップを実行します。宛先ベースのルーティングテーブルのデフォルトルートは、次のホップ点として untrust-vr を指定します。

次に、セキュリティデバイスは次のエントリを探すために、untrust-vr のソースベースルーティングテーブルをチェックしません。

```
  ID          IP-Prefix      Interface         Gateway   P Pref    Mtr     Vsys
*  1        10.1.2.0/24           eth4       2.2.2.250   S   20      1     Root
```

そのかわり、セキュリティデバイスは宛先ベースルーティングテーブルをチェックし、次のエントリを探します。

```
  ID          IP-Prefix      Interface          Gateway   P Pref    Mtr     Vsys
*  1         0.0.0.0/24           eth3        1.1.1.150   S   20      0     Root
```

untrust-vr では、untrust-vr のソースベースのルーティングテーブルにトラフィックに一致するエントリがあるにもかかわらず、セキュリティデバイスは宛先ベースのルーティングテーブルでのみルートルックアップを実行します。宛先ベースのルーティングテーブルにある一致したルート (デフォルトのルート) は、ethernet3 インターフェースにトラフィックを転送します。

等価コストマルチパスルーティングの構成

Juniper Networks セキュリティデバイスは、セッション単位の等価コストマルチパス (ECMP) ルーティングをサポートしています。コストの等価なルートは、優先度値とメトリック値が同じです。セキュリティデバイスはセッションとルートを関連付けると、さらに優れたルートを学習するか、現在のルートが使用できなくなるまで、このルートを使用します。このルートには、同一ゾーンにある出力インターフェースが必要です。

注 : 出力インターフェースが同一ゾーンになく、リターンパケット予期しないゾーンに行くと、セッションが一致せず、トラフィックが通過しないおそれがあります。

注 : ECMP が使用可能で、出力インターフェースが異なり、かつ NAT モードである場合、複数のセッションを作成する HTTP などのアプリケーションは正常に動作しなくなります。1 つのセッションを作成する Telnet や SSH などのアプリケーションは、正常に動作します。

ECMP は同じ宛先への 2 つから 4 つのルート間のロードバランスをサポートするか、または 2 つ以上の宛先で使用する帯域幅の効率を向上させます。ECMP を有効にすると、セキュリティデバイスはルーティングプロトコル経由で、静的に定義したルートか、同じ宛先への動的な複数のルートを使用します。等価コストルートは、回転（ラウンドロビン）方式で割り当てます。

ECMP が有効でない場合は、最初に学習したルートか、定義済みのルートを利用します。現在アクティブなルートがアクティブでなくなるまで、等価コストの他のルートは使用されません。

注 : ECMP の使用中に、隣接する 2 つのセキュリティデバイスがあり、パケットが消失したりロードバランスが不適切な場合は、隣接デバイスのアドレス解決プロトコル (ARP) の構成をチェックして、**arp always-on-dest** 機能が無効 (デフォルト) になっていることを確認してください。ARP 関連コマンドの詳細は **2**-76 ページの「ダウン状態のインターフェースとトラフィックフロー」をご覧ください。

例えば、trust-vr 宛先ベースのルーティングテーブルにある、次の 2 つのルートについて考えてみます。

```
   ID         IP-Prefix      Interface         Gateway   P Pref    Mtr     Vsys

*   8         0.0.0.0/0      ethernet3       1.1.1.250   C    0      1     Root
    9         0.0.0.0/0      ethernet2       2.2.2.250   S   20      1     Root
```

この例では、2 つの異なる ISP に接続する 2 つのデフォルトルートがあり、目的は両方のデフォルトルートを ECMP で使用することです。

2 つのルートのメトリック値は同じですが、1 つ目のルートは接続されています (優先度値 0 の C)。1 つ目のルートは DHCP または PPP 経由で確立し、デフォルトルートは手動構成で確立しました。2 つ目のルートは手動構成した静的ルートです (自動優先度値 20 の S)。ECMP を無効にすると、セキュリティデバイスは ethernet3 で接続したルートにすべてのトラフィックを転送します。

両方のルートのロードバランスを取るには、**set vrouter** *trust-vr* **preference static 0** コマンドを入力してから ECMP を有効にすることによって、静的ルートのルート優先度値を 0 に変更して、接続したルートに一致させます。ECMP が有効な場合、セキュリティデバイスは 2 つの ECMP ルートを変更して、トラフィックのロードバランスを取ります。以下の画面表示は、更新されたルーティングテーブルを示しています。

```
  ID         IP-Prefix      Interface         Gateway   P Pref    Mtr     Vsys

*  8         0.0.0.0/0      ethernet3       1.1.1.250    C   0      1     Root
*  9         0.0.0.0/0      ethernet2       2.2.2.250    S   0      1     Root
```

ECMP を有効にして、ルーティングテーブルに等価コストのマッチングルートが 1 つ以上見つかると、デバイスは各ルートルックアップに別の等価コストルートを選択します。上記のルートでは、ethernet3 と ethernet2 の間で変更して、ネットワーク 0.0.0.0/0 にトラフィックを転送しています。

等価コストルートが 2 つ以上ある場合、最大構成数まで順番 (ラウンドロビン方式) に並んだルートから選択して、各ルートルックアップに別々の ECMP ルートを選択できるようにします。

ECMP はデフォルトで無効になっています (ルートの最大数 = 1)。ECMP ルーティングを有効にするには、仮想ルーターごとに等価コストルートの最大数を指定しなければなりません。ルート数は最大 4 つまで指定できます。ルートの最大数を指定すると、それ以上のルートを学習してもルートは追加も変更もされません。

次の例では ECMP のルートの最大数を 2 に設定します。同一のゾーンおよびルーティングテーブルに、等価コストのルートが 3 つまたは 4 つ存在する可能性がありますが、セキュリティアドバイスは構成したルート数内でのみ変更します。この場合は、指定した 2 つの ECMP パスでのみ転送します。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr): 次のように入力してから **OK** をクリックします。

Maximum ECMP Routes:
Set Limit at: (**選択**), 2

CLI

```
set vrouter trust-vr max-ecmp-routes 2
save
```

ルート情報の再配布

仮想ルーターのルーティングテーブルに蓄積されたルート情報には、動的ルーティングプロトコルにより収集されたもののほか、静的ルートや直接接続ルートにより収集されたものがあります。通常、動的ルーティングプロトコル (OSPF、RIP、BGP など) は、以下の条件に合致するルートのみを、隣接ノードやピアに広告するようになっています。

- ルーティングテーブル上でアクティブになっていること。
- 動的ルーティングプロトコルにより学習されたルート情報であること。

注 : OSPF、RIP、BGP では、このプロトコルが有効になっている ScreenOS インターフェースに直接接続されたルートも通告します。

他のプロトコルにより学習されたルート情報 (静的ルートを含む) も通告するようにしたい合は、ソースプロトコルから通告に使うプロトコルに、当該ルート情報を*再配布*する必要があります。

あるルーティングプロトコルにより学習されたルート情報 (静的に構成されたルートを含む) は、同一の仮想ルーターに属する他のルーティングプロトコルに再配布できます。すると、受信する側のルーティングプロトコルを使って、再配布されたルート情報を通告することができます。ルート情報をインポートする場合、既知のルートなどの情報をプロトコルに合わせて変換するのは、インポートする側のドメインの役割です。たとえば、相互に接続されている一方のルーティングドメインが OSPF、もう一方が BGP を使っている場合、OSPF ドメインでは、BGP ドメインからルート情報をすべてインポートしなければ、BGP ドメイン内のデバイスへの到達方法を OSPF 隣接ノードに通知することができません。

ルート情報をプロトコル間で再配布する際、システム管理者またはネットワーク管理者が定義した*再配布規則*を参照します。仮想ルーターのルーティングテーブルにルート情報が追加されると、再配布規則を 1 つずつ順に調べて、再配布するかどうか判定します。ルート情報が削除された場合も同様にして、仮想ルーター内の他のプロトコルのルーティングテーブルから削除するかどうか判定します。ここで、再配布規則は、追加・削除されたルート情報に対してすべて適用されることに注意してください。適用順序は不定ですし、「最初に条件に合致したものを適用」するということもありません。

注 : 再配布規則は、プロトコルの 2 つ組に対して 1 つしか定義できません。

セキュリティデバイスに*ルートマップ*を設定して、どのルート情報のどの属性を再配布するか、指定することができます。

ルートマップの設定

*ルートマップ*は一連の文から成り、これをルート情報に対して順に適用します。文には条件部があり、これをルート情報と比較するようになっています。すなわち、指定されたルートマップのステートメントの条件部を、合致が見つかるまで番号順にルート情報と比較し、文指定のアクションが適用されます。条件に合致した場合の処理として、ルートマップステートメントを使った転送を許可する、あるいは拒否することができます。またルートマップのステートメントでは、合

致したルートの属性値の一部を変更することもできます。ルートマップの末尾には「すべて拒否」という文があるものと看做します。したがって、どの条件文にも合致しなかった場合、そのルートは破棄されることになります。表 3 はルートマップ合致条件およびその詳細を示しています。

表 3: ルートマップ合致条件

条件	説明
BGP AS Path	指定された AS パスアクセスリストに合致。42 ページの「ルートのフィルタリング」を参照してください。
BGP Community	指定されたコミュニティリストに合致。42 ページの「ルートのフィルタリング」を参照してください。
OSPF route type	OSPF internal、external type 1、external type 2 に合致。
Interface	指定されたインターフェースに合致。
IP address	指定されたアクセスリストに合致。42 ページの「ルートのフィルタリング」を参照してください。
Metric	指定されたメトリック値に合致。
Next-hop	指定されたアクセスリストに合致。42 ページの「ルートのフィルタリング」. を参照してください。
Tag	指定されたルートタグ値または IP アドレスに合致。

条件ごとに、これに合致したルートを許可するか拒否するか指定できます。許可する場合はさらに、ルートの属性値を設定することもできます。表 4 にはそれぞれのルートマップの属性および説明があります。

表 4: ルートマップの属性

属性の設定	説明
BGP AS Path	指定された AS パスアクセスリストを、マッチングルートのパスリスト属性の先頭に追加。
BGP Community	指定されたコミュニティリストを、マッチングルートのコミュニティ属性として設定。
BGP local preference	指定された値を、マッチングルートの local-pref 属性として設定。
BGP Weight	マッチングルートの重みとして設定。
Offset metric	指定された値の分、マッチングルートのメトリック値を増やします。これにより、優先度の低いパスでメトリック値が大きくなります。RIP ルートでは、通知されたルート (route-map out) または学習したルート (route-map in) の両方を増やすことができます。他のルートでは、別の仮想ルーターにエクスポートされるルートを増やすことができます。
OSPF metric type	マッチングルートの OSPF メトリックタイプとして、external type 1 または external type 2 のいずれかを設定。
Metric	指定された値を、マッチングルートのメトリックとして設定。
Next-hop of route	マッチングルートの次のホップ点を、指定された IP アドレスに設定。
Preserve metric	別の仮想ルーターにエクスポートされるマッチングルートのメトリックを保持。
Preserve preference	別の仮想ルーターにエクスポートされるマッチングルートの優先度値を保持。
Tag	マッチングルートのタグとして、指定されたタグ値または IP アドレスを設定。

ルートのフィルタリング

ルートのフィルタリング機能を使うと、どのルート情報を仮想ルーターに許可するか、どのルートをピアに広告するか、どのルート情報を他のプロトコルに再配布するか、といったコントロールができます。フィルターを適用できるのは、ルーティングピアから送られてくるルート情報や、セキュリティ仮想ルーターからピアルーターに送出するルート情報です。実際に適用できるしくみとしては、以下のようなものがあります。

- アクセスリストの設定方法については買Aクセスリストの構成iを参照してください。

- BGP AS パスアクセスリスト - AS パス属性とは、ルート情報の広告に際して経由した自律システム (AS、Autonomous System) のリストで、ルート情報の一部を成すものです。AS パスアクセスリストは、特定の AS を表す正規表現を列挙したものです。ルートが行き来した AS に基づいて、AS パスアクセスリストを使ってルートをフィルターできます。AS パスアクセスリストの設定方法については 120 ページの「AS-Path アクセスリストの構成」を参照してください。

- BGP コミュニティリスト - BGP ルートが属するコミュニティの識別子を列挙したもの。ルートに属するコミュニティを基準として、ルート情報を選別することができます。BGP コミュニティリストの設定方法については 128 ページの「BGP コミュニティ」を参照してください。

アクセスリストの構成

アクセスリストは一連のステートメントから成り、これをルート情報と比較するようになっています。各文には、ネットワークプレフィックスの IP アドレス / ネットマスクと、転送を許可するか拒否するかの区別が指定されています。たとえばアクセスリストの文は、サブネット 1.1.1.0/24 宛のルートを許可することができます。あるいは同じアクセスリストの文は、サブネット 2.2.2.0/24 宛のルートは拒否することもできます。条件に合致したルートは、そのステートメントに従って許可または拒否されることになります。

アクセスリストでは、文の順序に重要な意味があります。ルート情報は、リスト上の先頭の文から順に比較され、合致した時点で終了します。合致した場合、それ以降のステートメントと比較されることはありません。したがって、より限定的な条件の文を先に置くようにするとよいでしょう。たとえば、「サブネット 1.1.1.1/30 宛のルートを拒否する」旨の文は、「サブネット 1.1.1.0/24 宛のルートを許可する」旨の文よりも前に置くことになります。

アクセスリストを使用して、マルチキャストトラフィックのフローを制御することもできます。詳細については、155 ページの「アクセスリスト」を参照してください。

ここでは trust-vr 上にアクセスリストを作成します。アクセスリストに、以下のよう特性があります。

- Identifier (識別番号): 2 (アクセスリストの設定時には、アクセスリスト識別子を指定する必要があります)
- Forwarding Status: permit
- IP Address/Netmask Filtering: 1.1.1.1/24
- Sequence Number: 10 (これがアクセスリスト中の何番目の文に当たるかを表す番号)

WebUI

Network > Routing > Virtual Routers > Access List: > New (trust-vr): 次のように入力してから **OK** をクリックします。

Access List ID: 2
Sequence No.: 10
IP/Netmask: 1.1.1.1/24
Action: Permit

CLI

```
set vrouter trust-vr access-list 2 permit ip 1.1.1.1/24 10
save
```

ルート情報を OSPF に再配布

この例では、自律システム 65000 を経由する BGP ルート情報を、OSPF 用に再配布します。まず AS パスアクセスリストを設定して、AS 65000 を経由するルートを許可するようにします (AS パスアクセスリストの設定については 120 ページの「AS-Path アクセスリストの構成」を参照)。次に、AS パスアクセスリスト中のルートに合致するよう、ルートマップ "rtmap1" を設定します。最後に OSPF 側で、ルートマップ "rtmap1" を使用した再配布規則を設定します。再配布元は BGP とします。

WebUI

1. **BGP AS パスアクセスリスト**
   Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > AS Path: 次のように入力してから **Add** をクリックします。

   AS Path Access List ID: 1
   Permit: (選択)
   AS Path String: _65000_

2. **ルートマップ**
   Network > Routing > Virtual Routers > Route Map > New (trust-vr): 次のように入力してから **OK** をクリックします。

   Map Name: rtmap1
   Sequence No.: 10
   Action: Permit (選択)
   Match Properties:
   AS Path: (選択), 1

3. **再配布規則**
   Network > Routing > Virtual Router > Edit (trust-vr) > Edit OSPF Instance > Redistributable Rules: 次のように選んでから **Add** をクリックします。

   Route Map: rtmap1
   Protocol: BGP

CLI

1. **BGP AS パスアクセスリスト**
   set vrouter trust-vr protocol bgp as-path-access-list 1 permit _65000_

2. **ルートマップ**
   set vrouter trust-vr
   device(trust-vr)-> set route-map name rtmap1 permit 10
   device(trust-vr/rtmap1-10)-> set match as-path 1
   device(trust-vr/rtmap1-10)-> exit
   device(trust-vr)-> exit

3. **再配布規則**
   set vrouter trust-vr protocol ospf redistribute route-map rtmap1 protocol bgp
   save

仮想ルーター間でルート情報をエクスポート / インポート

セキュリティデバイス上に仮想ルーターを 2 つ設定した場合、一方の仮想ルーターで学習したルート情報を、もう一方でも利用できるようにすることが可能です。そのためには、一方の仮想ルーターに、もう一方へのエクスポートを許可するような*エクスポート規則*を設定する必要があります。ルート情報をエクスポートすれば、他の仮想ルーターでもネットワーク情報を参照できるようになります。エクスポート先仮想ルーターでも、*インポート規則*を設定して、どのようなルート情報をインポートするかコントロールできます。インポート規則がない場合は、エクスポートされたルート情報をすべて受理します。

仮想ルーター間でルート情報をエクスポート / インポートする手順は以下のようになります。

1. エクスポート側仮想ルーターにエクスポート規則を定義。
2. (必要な場合のみ) インポート側仮想ルーターにインポート規則を定義。必須ではありませんが、どのようなルート情報をインポートするか細かくコントロールしたい場合は、インポート規則を定義するとよいでしょう。

セキュリティデバイスでエクスポート / インポート規則を設定する場合、以下の事項を指定する必要があります。

- エクスポート先仮想ルーター (エクスポート規則の場合)、インポート元仮想ルーター (インポート規則の場合)
- エクスポート / インポートするルート情報のプロトコル
- エクスポート / インポートするルート情報
- (必要な場合のみ) エクスポート / インポート時に、ルート情報に追加する属性、修正する属性

設定手順は再配布規則の場合と同様です。*ルートマップ*を設定して、どのルートのどの属性をエクスポート / インポートするかを指定します。

trust-vr から untrust-vr に、ルートテーブルの中身をすべて、自動的にエクスポートする設定もできます。また、ユーザー定義仮想ルーターから他の仮想ルーターに、自動的にエクスポートする設定も可能です。ただし、NAT モードのインターフェースに直接接続されているネットワーク内のルートは、エクスポートできません。

エクスポート規則を設定する

ここでは、仮想ルーター trust-vr から untrust-vr ルーティングドメインに、1.1.1.1/24 ネットワーク宛の OSPF ルート情報をエクスポートします。まず、ネットワークプレフィックス 1.1.1.1/24 のアクセスリストを作成します。ルートマップ "rtmap1" ではこれを使って、1.1.1.1/24 宛のルートに合致する条件を選別します。次に、trust-vr から untrust-vr に OSPF ルート情報をエクスポートする、エクスポート規則を作成します。

WebUI

trust-vr

1. **アクセスリスト**
   Network > Routing > Virtual Routers > Access List: > New (trust-vr): 次のように入力してから **OK** をクリックします。

   Access List ID: 2
   Sequence No.: 10
   IP/Netmask: 1.1.1.1/24
   Action: Permit

2. **ルートマップ**
   Network > Routing > Virtual Routers > Route Map > New (trust-vr): 次のように入力してから **OK** をクリックします。

   Map Name: rtmap1
   Sequence No.: 10
   Action: Permit (選択)
   Match Properties:
   Access List: (選択), 2

3. **エクスポート規則**
   Network > Routing > Virtual Routers > Export Rules > New (trust-vr): 次のように入力してから **OK** をクリックします。

   Destination Virtual Router: untrust-vr
   Route Map: rtmap1
   Protocol: OSPF

CLI

trust-vr

1. **アクセスリスト**
   ```
   set vrouter trust-vr
   device(trust-vr)-> set access-list 2 permit ip 1.1.1.1/24 10
   ```

2. **ルートマップ**
   ```
   device(trust-vr)-> set route-map name rtmap1 permit 10
   device(trust-vr/rtmap1-10)-> set match ip 2
   device(trust-vr/rtmap1-10)-> exit
   ```

3. **エクスポート規則**
   ```
   device(trust-vr)-> set export-to vrouter untrust-vr route-map rtmap1 protocol
       ospf
   device(trust-vr)-> exit
   save
   ```

自動エクスポートを設定する

trust-vr から untrust-vr に、ルートテーブルの中身をすべて、自動的にエクスポートする設定もできます。



注意 : この機能はすべての trust ルートを untrusted ネットワークで表示し、trust-vr と untrust-vr 間の分離を優先します。

untrust-vr 側にインポート規則を設定すれば、インポート規則に合致したルート情報のみインポートすることができるのです。ここでは、trust-vr がルート情報をすべて自動的に untrust-vr にエクスポートするように設定し、untrust-vr 側では内部 OSPF ルートのみインポートするよう、インポート規則で設定します。

WebUI

trust-vr

Network > Routing > Virtual Router > Edit (trust-vr): **Auto Export Route to Untrust-VR** を選択し、**OK** をクリックします。

untrust-vr

Network > Routing > Virtual Router > Route Map (untrust-vr) > New: 次のように入力してから **OK** をクリックします。

Map Name: from-ospf-trust
Sequence No.: 10
Action: Permit (選択)
Route Type: internal-ospf (選択)

CLI

trust-vr

```
set vrouter trust-vr auto-route-export
```

untrust-vr

```
set vrouter untrust-vr
device(untrust-vr)-> set route-map name from-ospf-trust permit 10
device(untrust-vr/from-ospf-trust-10)-> set match route-type internal-ospf
device(untrust-vr/from-ospf-trust-10)-> exit
device(untrust-vr)-> set import-from vrouter trust-vr route-map from-ospf-trust
    protocol ospf
device(untrust-vr)-> exit
save
```

第 3 章

オープンショーテストパスファースト (OSPF)

この章では、セキュリティデバイスに組み込まれたルーティングプロトコルである Open Shortest Path First (OSPF) ついて説明します。本章のセクションは、以下のようになります。

- 50 ページの「概要」
  - 50 ページの「エリア」
  - 51 ページの「ルーターの分類」
  - 51 ページの「Hello プロトコル」
  - 52 ページの「ネットワークタイプ」
  - 53 ページの「接続状態の通知」
- 53 ページの「OSPF の基本設定」
  - 54 ページの「OSPF ルーティングインスタンスの作成と削除」
  - 55 ページの「OSPF エリアの作成および削除」
  - 57 ページの「OSPF エリアにインターフェースを割り当て」
  - 58 ページの「インターフェース上で OSPF を稼動」
  - 59 ページの「設定内容の確認」
- 60 ページの「ルーティングプロトコルへのルート情報の再配布」
- 61 ページの「再配布されたルート情報の要約」
- 62 ページの「OSPF に関する大域パラメータ」
  - 63 ページの「デフォルトルートの通知」
  - 63 ページの「仮想リンク」
- 66 ページの「インターフェースごとの OSPF パラメータ」

- 68 ページの「セキュリティ構成」
  - 68 ページの「接続デバイスを認証する」
  - 69 ページの「OSPF 隣接ノードリストの設定」
  - 70 ページの「デフォルトルートを拒否する」
  - 70 ページの「フラッディングの回避」
- 71 ページの「トンネルインターフェースについて、要求回路を作成する」
- 72 ページの「ポイントツーマルチポイントトンネルインターフェース」
  - 73 ページの「OSPF リンクタイプの設定」
  - 73 ページの「Route-deny 機能の無効化」
  - 73 ページの「ポイントツーマルチポイントネットワークの作成」

概要

オープン最短パスファースト (OSPF) はインテリアゲートウェイプロトコル (IGP) の一つで、自律システム (AS) 内のルーティング処理を行います。OSPF が動作するルーターは、定期的に*接続状態の通知* (LSA) をフラッドさせることにより、使用可能なインターフェース、接続ノードへの到達可能性などといった状態情報を AS 全体に配布します。

各 OSPF ルーターは、隣接するルーターの LSA を使用し、*接続状態データベース*を最新の状態に保ちます。接続状態データベースは、周辺ネットワークのトポロジーや状態に関する情報の管理に使います。AS 内での定期的な LSA の交換によって、AS のすべてのルーターが同一の接続状態のデータベースを維持します。

OSPF は接続状態データベースを使って、AS 内のネットワークに到達する最適パスを見つけます。そのために、AS 内の各ネットワークに到達する最短パスをグラフとして表現した、*最短パスツリー*を生成します。接続状態データベースはどのルーターも同じですが、最短パスツリーはそれぞれ異なります。各ルーターが、自分自身をルート (最上位) とするツリーを生成するからです。

エリア

デフォルトでは、ルーターはすべて、エリア 0 (通常 エリア 0.0.0.0 と表記) という同じ「バックボーン」エリアに属しているものとして扱われます。しかし大規模に分散されたネットワークは、複数のエリアに分割するのが普通です。ネットワークの拡大に伴い接続状態データベースも大きくなるので、これを分割して扱うことにより、拡張性を改善しようとしているのです。

エリアに分割すると、ネットワーク上を行き来するルーティング情報の量を減らすことができます。各ルーターは、属するエリア内の接続状態データベースを管理するだけでよくなるからです。エリア外のネットワークやルーターに関する接続状態情報は管理しません。複数のエリアに接続されたルーターは、そのエリアごとに接続状態データベースを管理します。仮想リンクを作成するとき以外は、エリアは直接エリア 0 に接続する必要があります。仮想リンクについて詳しくは 63 ページを参照してください。

AS 外部通知は、他の自律システム内の宛先に到達するルートを記述したもので、AS 全体に流布されます。ある条件を満たす OSPF エリアは、*スタブエリア* (行き止まりエリア) と設定することができます。AS 外部通知は、スタブエリアには流れません。OSPF で使われるエリアには、以下の 2 種類があります。

- **スタブエリア** - バックボーンエリアから要約ルート情報を受け取るが、OSPF 以外のソース (BGP など) を使って収集したルート情報を、他のエリアからの LSA (接続状態の通知) として受け取ることはないエリアです。さらに、要約ルート情報をまったく受け取らない場合は、*完全スタブエリア*と看做します。

- **準スタブエリア (NSSA)** - 通常のスタブエリアと同様、当該エリア外から、OSPF 以外のソースから収集されたルートを受け取ることはありません。しかし、エリア内で収集した外部ルート情報を受け取り、他のエリアに通知することはできます。

ルーターの分類

OSPF によるルーティングに関与するルーターは、機能やネットワーク上の位置により、以下のように分類できます。

- **内部ルーター** - インターフェースがすべて同じエリアに属するルーター。

- **バックボーンルーター** - バックボーンエリアにインターフェースを持つルーター。

- **エリア境界ルーター** - 複数のエリアに接続しているルーター (ABR) 。バックボーン以外のエリアに関するルート情報を要約し、バックボーンエリアに流す働きがあります。セキュリティデバイスの場合、OSPF を稼動させると、バックボーンエリアは最初から作成された状態になっています。仮想ルーターでもう 1 つエリアを作成すると、当該デバイスは ABR として機能するようになります。

- **ASBR (AS 境界ルーター)** - OSPF エリアが別の AS と隣接している場合に、AS 間を接続するルーター。外部 AS のルーティング情報を AS 全体に通知する役割があります。

Hello プロトコル

2 つのルーターのインターフェースが同じサブネット上にある場合、この 2 つは *接続関係* にあるといいます。Hello プロトコルには、この関係を確立、維持する働きがあります。2 つのルーターが双方向で通信できるようになった場合は、*隣接関係* (adjacency) を確立したといいます。隣接関係を確立していなければ、互いにルーティング情報を交換することはできません。

ネットワーク上にルーターが複数ある場合、そのうちの 1 つを*代表ルーター* (DR) 、もう 1 つを*バックアップ代表ルーター* (BDR) とする必要があります。DR には、ネットワーク上にある OSPF 対応ルーターを列挙した LSA を、ネットワーク全体に流布させる役割があります。ネットワーク上の他のルーターと隣接関係を確立できるのは DR だけです。言い替えると、ネットワーク上の他のルーターにルーティング情報を通知できるのは、DR に限るということです。BDR は、DR に障害があった場合に、代表ルーターとしての役割を果たします。

ネットワークタイプ

Juniper Networks セキュリティデバイスは次のような OSPF ネットワークタイプに対応しています。

- ブロードキャストネットワーク
- ポイントツーポイントネットワーク
- ポイントツーマルチポイントネットワーク

ブロードキャストネットワーク

*ブロードキャストネットワーク*とは、多くのルーターが接続されたネットワークで、物理的に 1 つのメッセージをブロードキャスト (同報) の形で各ルーターに送ることができるものをいいます。ブロードキャストネットワーク内にある 2 つのルーターは、相互に通信できるという前提になっています。イーサネットはその一例です。

ブロードキャストネットワークでは、OSPF ルーターは動的に接続ルーターを検出するため、マルチキャストアドレス 224.0.0.5 に Hello パケットを送信します。また、DR や BDR を選ぶためにも Hello プロトコルを使います。

*非ブロードキャストネットワーク*とは、多くのルーターが接続されていても、メッセージをブロードジャスト (同報) することはできないもののことです。この場合、OSPF プロトコルパケットをマルチキャストアドレス宛に送ることはできないので、各接続ルーターに個別に送信します。Juniper Networks セキュリティデバイスでは、非ブロードキャストネットワーク上で OSPF を動かすことはできません。

ポイントツーポイントネットワーク

*ポイントツーポイントネットワーク*では、通常、WAN (ワイドエリアネットワーク) 上の 2 つのルーターが直接つながっています。たとえば IPSec VPN トンネル経由で 2 台のセキュリティデバイスを接続するネットワークがこれに当たります。この場合、OSPF ルーターはマルチキャストアドレス 224.0.0.5 に Hello パケットを送信して、動的に接続ルーターを検出します。

ポイントツーマルチポイントネットワーク

*ポイントツーマルチポイント*ネットワークとは、非ブロードキャストネットワークであって、OSPF がルーター間接続をポイントツーポイントリンクとして扱うもののことです。代表ルーターや LSA フラッディングを選ぶことはできません。この場合、ルーターは直接通信できる隣接ノードすべてに Hello パケットを送信します。

注 : セキュリティデバイスで OSPF ポイントツーマルチポイントの設定ができるのは、トンネルインターフェースに限ります。また、通常のネットワーク運営のためには route-deny を無効にしなければなりません。物理 Ethernet インターフェースをポイントツーマルチポイント接続用に設定することはできません。詳細については、72 ページの「ポイントツーマルチポイントトンネルインターフェース」を参照してください。

接続状態の通知

それぞれの OSPF ルーターは、ルーターのローカル状態情報を定義する LSA を送信します。さらにそのルーターの OSPF 機能により、ルーターが送信できる他のタイプの LSA があります。表 5 は流布されている LSA のタイプおよびその内容を示しています。

表 5: LSA のタイプおよび内容の概要

LSA のタイプ	送信元	流布させる範囲	LSA で送信する情報
ルーター LSA	すべての OSPF ルーター	エリア	エリア内のすべてのルーターインターフェースの状態を通知。
ネットワーク LSA	ブロードキャストネットワーク、NBMA (非ブロードキャストマルチアクセス) ネットワークの代表ルーター	エリア	ネットワークに接続されたすべてのルーターのリスト。
要約 LSA	エリア境界ルーター	エリア	AS 内の他のエリア宛のルートを通知。これにはさらに 2 つのタイプがあります。 ■ タイプ 3 要約 LSA はネットワーク宛のルートを通知。 ■ タイプ 4 要約 LSA は AS 境界ルーター宛のルートを通知。
AS 外部	AS 境界ルーター	AS (自律システム)	他の AS にあるネットワークへのルート。これがデフォルトルート (0.0.0.0/0) であることもあります。

OSPF の基本設定

セキュリティデバイスでは、仮想ルーターごとに OSPF の設定をするようになっています。仮想ルーター (VR) が複数あれば、それぞれ独立に OSPF を稼動させることができます。

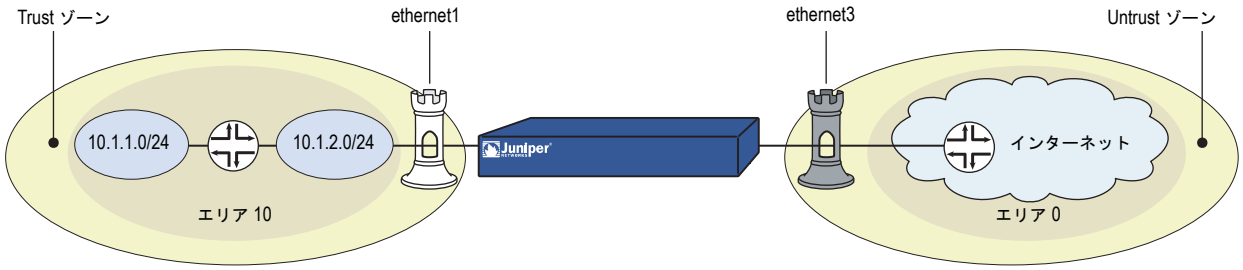
注 : 動的ルーティングプロトコルをセキュリティデバイス上で構成する前に、VR ID を第 2 章 , 「ルーティング」の説明にしたがって割り当てる必要があります。

ここでは、セキュリティデバイスの VR 上で OSPF の設定をする基本的な手順を説明します。

1. VR 上に OSPF ルーティングインスタンスを作成し、有効にします。このとき、自動的に OSPF バックボーンエリア (エリア ID は 0.0.0.0) も生成されます。これは削除できません。
2. (必要な場合のみ) OSPF インターフェースをすべてバックボーンエリアに接続するのでなければ、OSPF エリアを定義し、エリア ID を割り当てておきます。たとえばセキュリティデバイスを ABR として使う場合には、バックボーンエリアに加え、新しい OSPF エリアを生成する必要があります。通常のエリアのほか、スタブエリア、準スタブエリアとして設定することも可能です。
3. 各 OSPF エリアにインターフェースを割り当てます。OSPF エリア (バックボーンエリアも含む) にインターフェースが自動的に割り当てられるわけではないので、明示的に割り当ててください。
4. 各インターフェースについて OSPF を有効にします。
5. OSPF が正常に設定され、稼動していることを確かめます。

この例では、セキュリティデバイスを ABR として扱い、ethernet3 経由でエリア 0、ethernet1 経由でエリア 10 に接続します。図 10 を参照してください。

図 10: OSPF 構成例



必要に応じ以下のような OSPF パラメータも設定できます。

- 仮想リンクなど OSPF プロトコル用の大域パラメータで、VR ごとに設定するもの (62 ページの「OSPF に関する大域パラメータ」を参照)。
- 認証などに関する OSPF プロトコル用のインターフェースパラメータで、インターフェースごとに設定するもの (66 ページの「インターフェースごとの OSPF パラメータ」を参照)。
- セキュリティ関連の OSPF パラメータで、VR ごとまたはインターフェースごとに設定するもの (68 ページの「セキュリティ構成」を参照)。

OSPF ルーティングインスタンスの作成と削除

OSPF ルーティングインスタンスを、セキュリティデバイス上のある特定の VR 上に作成し、有効にします。OSPF ルーティングインスタンスを削除するには、OSPF インスタンスを無効にし、それから削除します。このとき、自動的に OSPF バックボーンエリアも生成されます。この作業が終わると、OSPF が有効になっている VR 上の各インターフェースと、パケットをやり取りできるようになります。

OSPF インスタンスを作成する

次の例では、最初に 0.0.0.10 を trust-vr のルーター ID として割り当てます。次に trust-vr 上に OSPF ルーティングインスタンスを作成します (仮想ルーターやその設定方法については , 15 ページの「ルーティング」を参照してください。)

WebUI

1. **ルーター ID**
   Network > Routing > Virtual Router (trust-vr) > Edit: 次のように入力してから **OK** をクリックします。

   Virtual Router ID: Custom (選択)
   テキストボックスに 0.0.0.10 を入力します。

2. **OSPF ルーティングインスタンス**
   Network > Routing > Virtual Router (trust-vr) > Edit > Create OSPF Instance: **OSPF Enabled** を選択し、**OK** をクリックします。

CLI

1. **ルーター ID**
   set vrouter trust-vr router-id 10
2. **OSPF ルーティングインスタンス**
   set vrouter trust-vr protocol ospf
   set vrouter trust-vr protocol ospf enable
   save

注 : CLI で設定する場合、OSPF ルーティングインスタンスをまず作成しておき、次にこれを有効にします。コマンドが 2 つに分かれているのはそのためです。

OSPF インスタンスを削除する

ここでは trust-vr 上に作成した OSPF ルーティングインスタンスを無効にします。trust-vr 上の、OSPF が有効になっているすべてのインターフェースに対し、OSPF パケットの送信および処理を停止します。

WebUI

Network > Routing > Virtual Routers (trust-vr) > Edit > Edit OSPF Instance: **OSPF Enabled** を選択解除し、**OK** をクリックします。

Network > Routing > Virtual Router (trust-vr) > Edit > Delete OSPF Instance を実行。確認プロンプトが現れるので **OK** をクリックします。

CLI

unset vrouter trust-vr protocol ospf
deleting OSPF instance, are you sure? y/[n]
save

注 : CLI において、OSPF インスタンスの削除を確認します。

OSPF エリアの作成および削除

エリアに分割すると、ネットワーク上を行き来するルーティング情報の量を減らすことができます。各ルーターは、属するエリア内の接続状態データベースを管理するだけでよくなるからです。エリア外のネットワークやルーターに関する接続状態情報は管理しません。

エリアはすべて、エリア 0 に接続する必要があります。これは仮想ルーター上で OSPF ルーティングインスタンスを設定すると作成されます。これ以外に作成した OSPF エリアについては、スタブエリアあるいは準スタブエリアと定義することもできます。エリアタイプについて詳しくは 50 ページの「エリア」を参照してください。

表 6 はエリアパラメータとその説明、そしてそれぞれのデフォルト値を示します。

表 6: OSPF エリアパラメータおよびデフォルト値

エリアパラメータ	説明	デフォルト値
デフォルトルート通知のメトリック値	(スタブエリア、準スタブエリアのみ) デフォルトルート通知のメトリック値	1
デフォルトルート通知のメトリックタイプ	(準スタブエリアのみ) デフォルトルートの外部メトリックタイプ 1 または 2 を指定	1
要約なし	(スタブエリア、準スタブエリアのみ) 要約 LSA をこのエリアに通知*しない*旨の指定	要約 LSA はこのエリアに通知される
範囲	(すべてのエリア) 要約 LSA を通知する IP アドレスの範囲と、通知するか否かの区別	—

OSPF エリアを作成する

ここでは OSPF エリアを作成し、エリア ID として 10 を割り当てます。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit OSPF Instance > Area: 次のように入力してから **OK** をクリックします。

Area ID: 10
Type: normal (**選択**)
Action: Add

CLI

```
set vrouter trust-vr protocol ospf area 10
save
```

OSPF エリアの削除

OSPF エリアを削除する前に、仮想ルーターの OSPF 処理を無効にします。次の例では、OSPF 処理を停止し、次に ID エリアが 10 の OSPF エリアを削除します。

WebUI

Network > Routing > Virtual Routers (trust-vr) > Edit > Edit OSPF Instance: **OSPF Enabled** を選択解除し、**OK** をクリックします。

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit OSPF Instance > Area: **Remove** をクリックします。

CLI

```
unset vrouter trust-vr protocol ospf enable
unset vrouter trust-vr protocol ospf area 0.0.0.10
save
```

OSPF エリアにインターフェースを割り当て

作成したエリアにはインターフェースを割り当てることができます。WebUI 画面から実行するか、**set interface** という CLI コマンドを使います。

エリアにインターフェースを割り当てる

この例では、インターフェースとして、OSPF area 10 に ethernet1、OSPF area 0 に ethernet3 を割り当てます。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit OSPF Instance > Area > Configure (Area 10): **Add** ボタンで、インターフェース ethernet1 を、Available Interface(s) 列から Selected Interfaces 列に移動。**OK** をクリックする。

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit OSPF Instance > Area > Configure (Area 0): **Add** ボタンで、インターフェース ethernet3 を、Available Interface(s) 列から Selected Interfaces 列に移動。**OK** をクリックする。

CLI

```
set interface ethernet1 protocol ospf area 10
set interface ethernet3 protocol ospf area 0
save
```

エリア範囲の設定

デフォルトでは、ABR はあるエリアから別のエリアに送るルート情報を集約しません。エリア範囲を設定すると、エリアに属するサブネットのグループを単一のネットワークアドレスに集約し、1 件の要約 LSA で他のエリアに通知するようになります。さらに、これを LSA で通知するか否かも指定できます。

次の例では、area 10 のアドレス範囲を以下のように定義します。

- 10.1.1.0/24: 通知する
- 10.1.2.0/24: 通知しない

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit OSPF Instance > Area > Configure (0.0.0.10): Area Range セクションに以下を入力し **Add** をクリックします。

IP/Netmask: 10.1.1.0/24
Type: (選択) Advertise

Area Range セクションに以下を入力し **Add** をクリックします。

IP/Netmask: 10.1.2.0/24
Type: (選択) No Advertise

CLI

```
set vrouter trust-vr protocol ospf area 10 range 10.1.1.0/24 advertise
set vrouter trust-vr protocol ospf area 10 range 10.1.2.0/24 no-advertise
save
```

インターフェース上で OSPF を稼動

デフォルトでは、仮想ルーター (VR) のどのインターフェースでも OSPF は無効になっています。したがって、エリアにインターフェースを割り当てた後、明示的に OSPF を有効にする必要があります。OSPF を無効にすると、当該インターフェースを介して OSPF がパケットを送受信することはなくなりますが、設定パラメータはそのまま保存されています。

注： VR 上で OSPF ルーティングインターフェースを無効にする (55 ページの「OSPF インスタンスを削除する」を参照) と、OSPF が有効になっている他のインターフェースに対し、OSPF パケットを送信することはなくなります。

インターフェース上で OSPF を稼動

この例では、先に area 10、area 0 にそれぞれ割り当てた、インターフェース ethernet1 および ethernet3 上の OSPF ルーティングインスタンスを有効にします。

WebUI

Network > Interfaces > Edit (ethernet1) > OSPF: **Enable Protocol OSPF** を選択して **Apply** をクリックします。

Network > Interfaces > Edit (ethernet3) > OSPF: **Enable Protocol OSPF** を選択して **Apply** をクリックします。

CLI

```
set interface ethernet1 protocol ospf enable
set interface ethernet3 protocol ospf enable
save
```

インターフェース上の OSPF を停止する

ここではインターフェース ethernet1 上の OSPF ルーティングインスタンスのみを無効にします。OSPF を有効にしてある trust-vr 仮想ルーター (VR) 上のこれ以外のインターフェースについては、OSPF パケットの送信や処理が停止することはありません。

WebUI

Network > Interfaces > Edit (ethernet1) > OSPF: **Enable Protocol OSPF** をオフにして **Apply** をクリックします。

CLI

```
unset interface ethernet1 protocol ospf enable
save
```

注： VR 上で OSPF ルーティングインスタンスを無効にすると、OSPF が有効になっている他のすべてのインターフェースに対し、OSPF パケットを送信・処理することはなくなります（ 55 ページの「OSPF インスタンスを削除する」を参照)。

設定内容の確認

trust-vr の設定内容は次の CLI コマンドで確認できます。

```
device-> get vrouter trust-vr protocol ospf config
VR: trust-vr RouterId: 10.1.1.250
----------------------------------
set protocol ospf
set enable
set area 0.0.0.10 range 10.1.1.0 255.255.255.0 advertise
set area 0.0.0.10 range 10.1.2.0 255.255.255.0 no-advertise
set interface ethernet1 protocol ospf area 0.0.0.10
set interface ethernet1 protocol ospf enable
set interface ethernet3 protocol ospf area 0.0.0.0
set interface ethernet3 protocol ospf enable
```

OSPF が仮想ルーター上で稼動していることは、**get vrouter trust-vr protocol ospf** というコマンドで確認できます。

```
device-> get vrouter trust-vr protocol ospf
VR: trust-vr RouterId: 10.1.1.250
----------------------------------
OSPF enabled
Supports only single TOS(TOS0) route
Internal Router
Automatic vlink creation is disabled
Numbers of areas is 2
Number of external LSA(s) is 0
SPF Suspend Count is 10 nodes
Hold time between SPFs is 3 second(s)
Advertising default-route lsa is OFF
Default-route discovered by ospf will be added to the routing table
RFC 1583 compatibility is disabled.
Hello packet flooding protection is not enabled
LSA flooding protection is not enabled
Area 0.0.0.0
        Total number of interfaces is 1, Active number of interfaces is 1
        SPF algorithm executed 2 times
        Number of LSA(s) is 1
Area 0.0.0.10
        Total number of interfaces is 1, Active number of interfaces is 1
        SPF algorithm executed 2 times
        Number of LSA(s) is 0
```

ハイライトになっている部分は、OSPF が稼動していることを表し、アクティブな OSPF や各 OSPF エリアのアクティブなインターフェースを確認する内容になっています。

注 : デフォルト値を使用せずに、常にルーター ID を明確に割り当てることをお薦めします。ルーター ID の設定については、15 ページの「ルーティング」を参照してください。

OSPF がインターフェース上で稼動していることを確認し、インターフェースの状態を調べることができます。**get vrouter trust-vr protocol ospf interface** という コマンドを実行してください。

```
device-> get vrouter trust-vr protocol ospf interface
VR: trust-vr RouterId: 10.1.1.250
---------------------------------
Interface   IpAddr        NetMask       AreaId        Status   State
-------------------------------------------------------------------------------
ethernet3   2.2.2.2       255.255.255.0 0.0.0.0       enabled Designated Router
ethernet1   10.1.1.1      255.255.255.0 0.0.0.10      enabled Up
```

仮想ルーターが代表ルーター (DR) やバックアップ代表ルーター (BDR) として選ばれる、優先度を設定できます。上の例では、State 列が各仮想ルーターの優先度を表します。

セキュリティデバイス上の OSPF ルーティングインスタンスが、OSPF 隣接ノードと隣接関係を確立した旨は、**get vrouter trust-vr protocol ospf neighbor** というコマンドで確認できます。

```
device-> get vrouter trust-vr protocol ospf neighbor
VR: trust-vr RouterId: 10.1.1.250
---------------------------------
                Neighbor(s) on interface ethernet3 (Area 0.0.0.0)
IpAddr/If Index RouterId        Priority State    Options
-------------------------------------------------------------------------------
2.2.2.2        2.2.2.250              1 Full     E
Neighbor(s) on interface ethernet1 (Area 0.0.0.10)
IpAddr/If Index RouterId        Priority State    Options
-------------------------------------------------------------------------------
10.1.1.1       10.1.1.252             1 Full     E
```

上の例の State 列に Full と書いてあれば、隣接ノードと完全に隣接関係が確立していることを表します。

ルーティングプロトコルへのルート情報の再配布

ルート再配布とは、ルーティングプロトコル間のルート情報の交換のことです。たとえば以下のようなルート情報を、同一の仮想ルーターにある OSPF ルーティングインスタンスに再配布することができます。

- BGP や RIP から得たルート
- 直接接続されたルート
- インポートされたルート
- 静的に構成されたルート

ルート再配布を構成するときは、まず再配布されるルートにフィルタをかけるルートマップを指定する必要があります。ルート再配布のためのルートマップ作成の詳細は、第 2 章 ,「ルーティング」を参照してください。

この例では、BGP ルーティングドメインから、現在稼動している OSPF ルーティングドメインに、ルート情報を再配布します。CLI コマンド、WebUI 画面のどちらも、add-bgp というルートマップが作成済みであると想定しています。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit OSPF Instance > Redistributable Rules: 次のように入力してから **Add** をクリックします。

Route Map: add-bgp
Protocol: BGP

CLI

```
set vrouter trust-vr protocol ospf redistribute route-map add-bgp protocol bgp
save
```

再配布されたルート情報の要約

数千単位のネットワークアドレスが含まれる大規模ネットワークでは、一部のルーターに、ルート情報が過度に集中することがあります。他のプロトコルで収集した一連のルート情報を、現在稼動している OSPF ルーティングインスタンスに再配布した後、これを要約ネットワークルート情報としてまとめることができます。いくつものルートがあっても 1 つと認識されるので、検索処理が簡潔になります。

大規模で複雑なネットワークで、ルート情報を要約して扱うようにすると、トポロジーが変化しても他のルーターには影響を与えずに済む、という利点もあります。たとえばあるドメインのあるリンクが断続的に障害と復旧を繰り返すと、ルーティングテーブルがその都度変化してしまいますが、この場合でも要約されたルート情報は変化しないので、ドメイン外のルーターには影響が及ばないのです。

バックボーンルーターのルーティングテーブルで管理するルート情報数が少なくて済むほか、要約ネットワークを停止あるいは再起動した場合でも、LSA を他のエリアに送る必要がありません。エリア内、エリア外のルートのどちらでも、要約することができます。

要約したルートにより、ループが発生する場合もあります。ループを防ぐには、NULL インターフェースへのルートを設定します。要約されたルートを作成する例に続いて、NULL インターフェースを設定する例を以下に示します。

再配布されたルート情報の要約

この例では、BGP ルートを現在稼動している OSPF ルーティングインスタンスに再配布します。次に、インポートされたルート情報を、ネットワークアドレス 2.1.1.0/24 に要約します。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit OSPF Instance > Redistributable Rules: 次のように入力してから **Add** をクリックします。

Route Map: add-bgp
Protocol: BGP

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit OSPF Instance > Summary Import: 次のように入力してから **Add** をクリックします。

IP/Netmask: 2.1.1.0/24

CLI

```
set vrouter trust-vr protocol ospf redistribute route-map add-bgp protocol bgp
set vrouter trust-vr protocol ospf summary-import ip 2.1.1.0/24
save
```

OSPF に関する大域パラメータ

この節では、仮想ルーター (VR) ごとに設定できる OSPF の大域パラメータについて解説します。VR に対して OSPF パラメータを設定すると、OSPF を有効にしたすべてのインターフェースの動作に反映されます。大域パラメータの設定は、CLI の OSPF ルーティングプロトコルコンテキストから実行するほか、WebUI 画面からも変更できます。

表 7 OSPF パラメータとそのデフォルト値を説明します。

表 7: OSPF 大域パラメータおよびデフォルト値

OSPF 大域パラメータ	説明	デフォルト値
Advertise default route	VR ルートテーブルに登録された、アクティブなデフォルトルート (0.0.0.0/0) を、すべての OSPF エリアに通知するか否か。さらに、メトリック値を指定する、あるいはルート本来のメトリック値を保存するよう指定することもできます。メトリックタイプ (ASE type 1 または type 2) も指定できます。また、デフォルトルートを常に通知するよう指定することもできます。	デフォルトルートは通知しない。
Reject default route	OSPF で収集したデフォルトルート情報を、ルートテーブルに登録しない旨の指定。	OSPF で収集したデフォルトルート情報はルートテーブルに登録する。
Automatic virtual link	OSPF バックボーンに到達できない場合、VR が自動的に仮想リンクを生成する機能の有効 / 無効。	無効
Maximum hello packets	VR が Hello 間隔の間に受け取れる OSPF Hello パケットの最大数。	10
Maximum LSA packets	VR が所定の時間内（秒）に受け取れる OSPF LSA パケットの最大数。	初期値なし。
RFC 1583 compatibility	OSPF ルーティングインスタンスが、OSPF の旧版である RFC 1583 に準拠して動作するよう指定。	RFC 2328 に規定された OSPF version 2 に準拠して動作。
Equal cost multipath routing (ECMP)	コストが等しいパスが複数ある宛先について、負荷分散させるパスの最大数 (1 〜 4)。38 ページの「等価コストマルチパスルーティングの構成」を参照してください。	無効 (1) 。
Virtual link configuration	仮想リンク用の OSPF エリアやルーター ID を設定。必要に応じ、仮想リンクの認証方法、Hello パケットの間隔、再送信間隔、送信遅延、接続デッド間隔なども設定できます。	仮想リンクの構成なし。

デフォルトルートの通知

デフォルトルート 0.0.0.0/0 は、ルーティングテーブルのどの宛先ネットワークにも合致しますが、よりプレフィックスが合致するルート情報があればそちらが優先します。

この例では、現行 OSPF ルーティングインスタンスのデフォルトルートを通知します。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit OSPF Instance: **Advertising Default Route Enable** を選択し **OK** をクリックします。

注 : WebUI 画面で設定する場合、62 を手動で入力し、デフォルトではメトリック値がメトリックタイプが ASE タイプ 1 となっています。

CLI

```
set vrouter trust-vr protocol ospf advertise-default-route metric 1 metric-type 1
save
```

仮想リンク

すべてのエリアは直接バックボーンに接続しますが、時として物理的にバックボーンに接続できない、新しいエリアを作成する必要があります。仮想リンクはこのような場合に使います。これは、他のエリアを通ってバックボーンに接続される、論理的なパスのことです。

仮想リンクは、その両端のルーターに設定しなければなりません。セキュリティデバイスに仮想リンクを設定する場合、次のようなパラメータが必要です。

- 仮想リンクが通過する OSPF エリアの ID。バックボーンエリアやスタブエリアを通過する仮想リンクは作成できません。
- 仮想リンクの反対側の端にあるルーターの ID。

表 8 は仮想リンクのオプションのパラメータを示します。

表 8: 仮想リンクのオプションのパラメータ

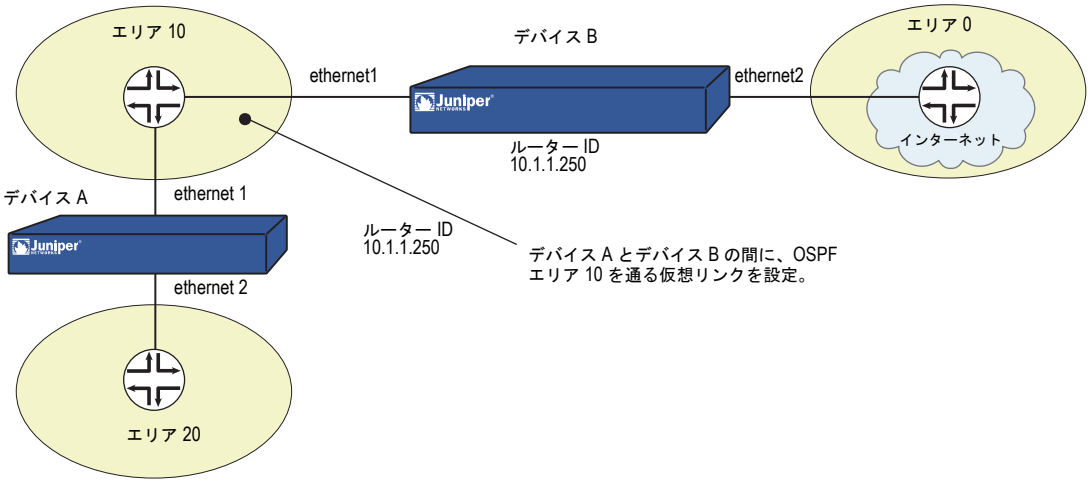
仮想リンクに関するパラメータ	説明	デフォルト値
Authentication	認証方法として、クリアテキストパスワード、MD5 認証のいずれかを指定。	認証なし
Dead interval	OSPF 接続ノードから応答がない場合に、これが稼動していないと判断するまでの時間 (秒単位)。	40 秒
Hello interval	OSPF Hello パケットを送出する間隔 (秒単位)。	10 秒
Retransmit interval	接続ノードが LSA に応答しない場合に、インターフェースが LSA を再送するまでの時間 (秒単位)。	5 秒
Transmit delay	インターフェースを介して接続状態更新パケットを送信する間隔 (秒単位)。	1 秒

仮想リンクの作成

この例では、OSPF エリア 10 を通って、デバイス A (ルーター ID は 10.10.1.250) からデバイス -B (ルーター ID は 10.1.1.250) に到る仮想リンクを作成します。(ルーター ID の設定方法については 15 ページの「ルーティング」を参照。) 仮想リンクの送信遅延 (Transit delay) の値は 10 秒とします。各セキュリティデバイスについて、仮想リンクの反対側にあるルーターの ID を指定する必要があります。

図 11 は仮想リンクのネットワーク設定例を示します。

図 11: 仮想リンクの作成



注 : OSPF は各デバイスの両インターフェースに対して有効にしなければなりません。また、仮想リンクをアクティブにする前に、A、B 両デバイスのインターフェース上で OSPF が稼動していることを確認してください。

WebUI (デバイス A)

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit OSPF Instance > Virtual Link: 次のように入力してから **Add** をクリックします。

Area ID: 10 (**選択**)
Router ID: 10.1.1.250

> Configure: 送信遅延フィールドに **10** と入力し、**OK** をクリックします。

CLI (デバイス A)

```
set vrouter trust-vr protocol ospf vlink area-id 10 router-id 10.1.1.250
set vrouter trust-vr protocol ospf vlink area-id 10 router-id 10.1.1.250 transit-delay
    10
save
```

注 : CLI で設定する場合、仮想リンクを作成しておいてから、必要に応じてパラメータを設定することになります。上のコマンド例で、作成と設定の 2 つに分かれているのはそのためです。

WebUI (デバイス B)

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit OSPF Instance > Virtual Link: 次のように入力してから **Add** をクリックします。

Area ID: 10
Router ID: 10.10.1.250

> Configure: 送信遅延フィールドに **10** と入力し、**OK** をクリックします。

CLI (デバイス B)

```
set vrouter trust-vr protocol ospf vlink area-id 10 router-id 10.10.1.250
set vrouter trust-vr protocol ospf vlink area-id 10 router-id 10.10.1.250
    transit-delay 10
save
```

仮想リンクの自動作成

仮想ルーター (VR) に指示して、ネットワークバックボーンに到達できないインスタンスへの仮想リンクを自動的に作成することができます。こうしておけば、手動で個別に仮想リンクを作成する必要がありません。仮想リンクを自動作成するよう設定する例を示します。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit OSPF Instance: **Automatically Generate Virtual Links** を選択し、**OK** をクリックします。

CLI

```
set vrouter trust-vr protocol ospf auto-vlink
save
```

インターフェースごとの OSPF パラメータ

このセクションでは、インターフェースごとに設定できる OSPF パラメータについて説明します。これは当該インターフェース上の動作にのみ影響を及ぼします。パラメータの設定は、**interface** という CLI コマンドを使うか、または WebUI 画面から行います。

表 9 に、OSPF パラメータ（オプション）とそのデフォルト値を説明します。

表 9: OSPF インターフェースパラメータ（オプション）およびデフォルト値

OSPF インターフェースパラメータ	説明	デフォルト値
Authentication	このインターフェースを使う OSPF 通信の認証方法として、クリアテキストパスワード、MD5 認証のいずれかを指定。パスワードとして、前者の場合最大 8 字、後者の場合最大 16 字の文字列を指定します。さらに MD5 の場合は、キー文字列を設定する必要があります。	認証なし
Cost	インターフェースのメトリックを指定。インターフェースのコストは、そこにつながるリンクの帯域幅によって決まります。帯域幅が大きいほどコスト値が小さくなり、優先度は上がります。	100 MB 以上のリンクに対しては 1 10 MB ならば 10 1MB ならば 100
Dead interval	OSPF 接続ノードから応答がない場合に、これが稼動していないと判断するまでの時間 (秒単位)。	40 秒
Hello interval	OSPF Hello パケットを送出する間隔 (秒単位)。	10 秒
Link type	トンネルインターフェースをポイントツーポイントリンクまたはポイントツーマルチポイントリンクとして指定。72 ページの「ポイントツーマルチポイントトンネルインターフェース」を参照してください。	イーサネットはブロードキャストインターフェースとして扱う。 OSPF エリアにバインドされたトンネルインターフェースは、デフォルトではポイントツーポイントインターフェース。
Neighbor list	隣接関係を確立しうる OSPF 接続ノードが属するサブネットを、アクセスリストの形で指定。	なし (インターフェース上のすべての接続ノードと隣接関係を確立)。
Passive interface	インターフェースの IP アドレスを、外部ルートではなく OSPF ルートとして OSPF ドメインに通知するが、このインターフェース自身が OSPF パケットを送受信することはないと設定。同じインターフェース上で BGP も稼動させる場合に有用です。	OSPF を有効にしたインターフェースは、OSPF パケットを送受信する。
Priority	仮想ルーターを DR (代表ルーター) または BDR (バックアップ代表ルーター) として扱うための優先度を指定。優先度が高いほど、DR や BDR になる可能性は高くなりますが、保証されるわけではありません。	1
Retransmit interval	接続ノードが LSA に応答しない場合に、インターフェースが LSA を再送するまでの時間 (秒単位)。	5 秒

OSPF インターフェースパラメータ	説明	デフォルト値
Transit delay	このインターフェースを介して接続状態更新パケットを送信する間隔 (秒単位)。	1 秒
Demand circuit	(トンネルインターフェースのみ) トンネルインターフェースを RFC 1793 で定義されたデマンド回線として設定。71 ページの「トンネルインターフェースについて、要求回路を作成する」を参照。	無効
Reduce flooding	デマンド回線上の LSA フラッディングを軽減する指定。	無効
Ignore MTU	OSPF データベースネゴシエーション中に、maximum transmission unit (MTU) 値がローカルインターフェースとリモートインターフェースで一致しないことを検出しても無視する設定。ローカル側の MTU 値が リモート側よりも小さい場合にのみ有効にしてください。	無効

注 : 隣接関係を確立するためには、すべての OSPF ルーターについて、hello、dead、retransmit interval の値が同じでなければなりません。

この例では、ethernet1 インターフェースに次のような OSPF パラメータを設定します。

- OSPF Hello メッセージの送出間隔 (Hello interval) を 15 秒に増加。
- OSPF 再送信間隔 (Retransmit interval) を 7 秒に増加。
- 接続状態更新パケットの送信間隔 (Transit delay) を 2 秒に増加。

WebUI

Network > Interfaces > Edit (ethernet1) > OSPF: 以下を入力して **Apply** をクリックします。

Hello Interval: 15
Retransmit Interval: 7
Transit Delay: 2

CLI

```
set interface ethernet1 protocol ospf hello-interval 15
set interface ethernet1 protocol ospf retransmit-interval 7
set interface ethernet1 protocol ospf transit-delay 2
save
```

セキュリティ構成

この節では、OSPF ルーティングドメインに起こりうるセキュリティ上の問題と、攻撃の防御方法について説明します。

注： OSPF の安全性を確保するためには、OSPF ドメイン内のルーターをすべて、同じセキュリティレベルに設定しなければなりません。そうでないと、最も安全性の低い OSPF ルーターが原因となって、OSPF ルーティングドメイン全体が危険にさらされる恐れがあります。

接続デバイスを認証する

LSA は暗号化されておらず、どんなプロトコルアナライザーでも OSPF パケットを分析できるので、OSPF ルーターのなりすまし (spoofing) 攻撃は容易です。これを回避する方法としては、OSPF 接続ノードの認証が最善です。

OSPF には、接続ノードから受け取った OSPF パケットの確認手段として、単純なパスワード認証と MD5 認証の 2 つがあります。認証に失敗した OSPF パケットはすべて破棄することになります。デフォルトでは、どの OSPF インターフェースも認証は無効になっています。

MD5 認証のためには、送信側および受信側の OSPF ルーターが、同じキーを共有している必要があります。同一のセキュリティデバイスに複数の MD5 キーを登録することもできます。キーはそれぞれ、キー識別子と組になっています。MD5 キーが複数ある場合、接続ルーターとの通信を認証するために使うキーは、キー識別子で指定します。したがって、MD5 キーを定期的に変更しても、パケットを失う危険はほとんどありません。

クリアテキストパスワードを設定する

ここでは、OSPF ルーターのインターフェース ethernet1 に対し、12345678 というクリアテキストパスワードを設定します。

WebUI

Network > Interfaces > Edit (ethernet1) > OSPF: 以下を入力して **Apply** をクリックします。

Password: (選択), 12345678

CLI

```
set interface ethernet1 protocol ospf authentication password 12345678
save
```

MD5 パスワードを設定する

この例では、インターフェース ethernet1 に対して MD5 キーを 2 つ設定しておき、そのうち一方をアクティブキーに選択します。それぞれの MD5 キーは最長 16 文字です。キー ID 番号は 0 から 255 にします。デフォルトのキー ID は 0 なので、最初に設定した MD5 はキー ID を指定する必要がありません。

WebUI

Network > Interfaces > Edit (ethernet1) > OSPF: 以下を入力して **Apply** をクリックします。

Authentication:
MD5 Keys: (選択)
1234567890123456
9876543210987654
Key ID: 1
Preferred: (選択)

CLI

```
set interface ethernet1 protocol ospf authentication md5 1234567890123456
set interface ethernet1 protocol ospf authentication md5 9876543210987654
    key-id 1
set interface ethernet1 protocol ospf authentication md5 active-md5-key-id 1
save
```

OSPF 隣接ノードリストの設定

マルチアクセス環境にすると、ルーターなどのデバイスが、比較的容易にネットワークに接続できてしまします。そのため、信頼性に劣るデバイスが接続されると、安定性や性能に問題が生じる可能性があります。

ScreenOS 仮想ルーター (VR) の OSPF ルーティングインスタンスは、デフォルトのままであれば、OSPF を有効にしたインターフェースを介して通信できるすべての接続ノードと、隣接関係を確立しようとします。これを制限して、所定のサブネットに属する当該 OSPF 接続ノードだけが隣接関係を確立するようにすることができます。指定したサブネットにあるホストやルーターだけが OSPF ルーティングインスタンスと隣接関係を確立できるようになります。このサブネットの指定は、VR ごとに、アクセスリストを定義する形で行います。

ここではまず、サブネット 10.10.10.130/27 上のホストのみを許可する、アクセスリストを設定します。次に、OSPF 隣接関係を確立するノードを、このアクセスリストの範囲に制限します。

WebUI

Network > Routing > Virtual Router (trust-vr) > Access List > New: 次のように入力してから **OK** をクリックします。

Access List ID: 4
Sequence No.: 10
IP/Netmask: 10.10.10.130/27
Action: Permit (選択)

Network > Interfaces > Edit (ethernet1) > OSPF: 以下を入力して **Apply** をクリックします。

Neighbor List: 4

CLI

```
set vrouter trust-vr access-list 4
set vrouter trust-vr access-list 4 permit ip 10.10.10.130/27 10
set interface ethernet1 protocol ospf neighbor-list 4
save
```

デフォルトルートを拒否する

Route Detour Attack では、あるルーターがデフォルトルート (0.0.0.0/0) をルーティングドメインに挿入してパケットをそのルーターに迂回させます。このルーターはパケットを破棄することでサービスの崩壊を招いたり、パケットを転送する前に内部の機密情報を得ることができます。Juniper Networks セキュリティデバイスのデフォルトでは、OSPF により収集したデフォルトルート情報をすべて受け入れ、ルーティングテーブルに登録するようになっています。

ここでは OSPF によりデフォルトルートの情報を収集しないよう設定します。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit OSPF Instance: **Do Not Add Default-route Learned in OSPF** チェックボックスを選択して **OK** をクリックします。

CLI

```
set vrouter trust-vr protocol ospf reject-default-route
save
```

フラッディングの回避

ルーターが正しく設定されていなかったり、攻撃を受けたりした場合、OSPF Hello パケットや LSA を接続ノードに大量に送りつけて (フラッディング、洪水) しまうことがあります。各ルーターは、ネットワーク上の他のルーターから LSA を受け取って、ルーティングテーブルのパス情報を最新の状態に保っています。LSA フラッド保護機能により、仮想ルーター (VR) に入る LSA の数を制限することができます。過剰な LSA を受け取った VR はフラッディング状態に陥り、正常に機能しなくなります。LSA フラッディング攻撃とは、短時間にルーターが過大な LSA を生成し、他の OSPF ルーターの CPU を SPF アルゴリズムの実行に消費させ、本来のサービスを妨害するというものです。

ScreenOS の VR に、Hello パケット間隔当たりの最大パケット数、所定の時間内に OSPF インターフェースが受け取れる最大 LSA 数を設定できます。この数以上のパケットは破棄されます。デフォルトでは、Hello パケット間隔当たりの最大パケット数は 10 になっています (Hello パケット間隔の初期値は 10 秒です)。最大 LSA 数の初期値はないので、そのままであれば、LSA をすべて受理します。

Hello しきい値を構成する

ここでは Hello パケット間隔当たりのしきい値を 20 パケットと設定します。Hello パケット間隔は OSPF インターフェースごとに設定できますが、ここではデフォルトである 10 秒のままにしておきます。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit OSPF Instance: 次のように入力してから **OK** をクリックします。

Prevent Hello Packet Flooding Attack: On
Max Hello Packet: 20

CLI

```
set vrouter trust-vr protocol ospf hello-threshold 20
save
```

LSA しきい値を構成する

この例では、OSPF LSA フラッディング攻撃を回避するため、そのしきい値を 10 秒当たり 20 パケットに制限します。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit OSPF Instance: 次のように入力してから **OK** をクリックします。

LSA Packet Threshold Time: 20
Maximum LSAs: 10

CLI

```
set vrouter trust-vr protocol ospf lsa-threshold 20 10
save
```

フラッディングを省略する設定

シリアル、トンネルまたは Asynchronous Digital Subscriber Line (ADSL) インターフェースなどのポイントツーポイントインターフェース、または Ethernet のブロードキャストインターフェースにおいて、フラッディング省略機能で LSA フラッディングを抑止することができます。次の例では、tunnel.1 インターフェースについて、定期的な LSA フラッディングを省略します。Hello パケットの送信は影響を受けません。

WebUI

Network > Interfaces > Edit (tunnel.1) > OSPF: 以下を入力して **Apply** をクリックします。

Reduce flooding: (**選択**)

CLI

```
set interface tunnel.1 protocol ospf reduce-flooding
save
```

トンネルインターフェースについて、要求回路を作成する

OSPF 要求回路とは、RFC 1793 に定義されているもので、接続時間や使い方によってそのコストが変化するようなネットワークセグメントです。要求回路上では、OSPF により生成されたトラフィックは、ネットワークトポロジーの変更にのみ制限する必要があります。Juniper Networks セキュリティデバイスでは、シリアル、トンネルまたは ADSL Asynchronous Digital Subscriber Line (ADSL) インターフェースなどのポイントツーポイントインターフェースのみが要求回路になります。正常動作には、トンネルの両端を要求回路として手動で構成します。

トンネルインターフェースを要求回路として設定すると、セキュリティデバイスは OSPF Hello パケットの送信や定期的な LSA 更新のフラッディングを省略して、オーバーヘッドを減らすようになります。もちろん、省略するのは、OSPF 隣接ノードの状態が Full になって (Hello パケットが合致し、ルーターやネットワーク LSA がすべての隣接ノードの状態を反映して) からのことです。LSA の中身が変わった場合はフラッディングを実行します。

次の例では tunnel.1 インターフェースを要求回路として設定します。

注： リモートピアのトンネルインターフェースをデマンド回線として設定する必要があります。しかしリモートピア側では、LSA フラッディングを省略するよう設定する必要はありません。

WebUI

Network > Interfaces > Edit > OSPF: 以下を入力して **Apply** をクリックします。

Demand Circuit: (**選択**)

CLI

```
set interface tunnel.1 protocol ospf demand-circuit
save
```

ポイントツーマルチポイントトンネルインターフェース

セキュリティデバイスでトンネルインターフェースを OSPF エリアにバインドすると、特に指定しなくても、ポイントツーポイント OSPF トンネルが作成されます。ポイントツーポイントトンネルインターフェースは、リモート側の OSPF ルーター 1 台とのみ隣接関係を結びます。ローカルトンネルインターフェースが複数のトンネルにバインドされている場合は、これをポイントツーマルチポイントインターフェースとして設定し、route-deny 機能は*無効*にしなければなりません。

注： トンネルインターフェースは、OSPF を有効にする前にポイントツーマルチポイントインターフェースとして設定する必要があります。ポイントツーマルチポイントインターフェースにすると、要求回路として設定することはできません (71 ページの「トンネルインターフェースについて、要求回路を作成する」を参照。) ただし LSA フラッディングを省略する設定は可能です。

複数のトンネルをトンネルインターフェースにバインドする例は 5-281 ページの「自動ルートおよび NHTB テーブル エントリのバインディング」を参照してください。次のセクションでは以下の例が示されています。

- リンクタイプの設定（73 ページの「OSPF リンクタイプの設定」を参照）
- Route-deny 機能の設定（73 ページの「Route-deny 機能の無効化」を参照）
- ポイントツーマルチポイントトンネルインターフェースのネットワークの構成（73 ページの「ポイントツーマルチポイントネットワークの作成」を参照）

OSPF リンクタイプの設定

複数のトンネルを介して OSPF 隣接ノードを接続する場合、リンクタイプをポイントツーマルチポイント (p2mp) に設定する必要があります。

次の例では、ネットワークの運用に合わせて、tunnel.1 のリンクタイプをポイントツーマルチポイント (p2mp) に設定します。

WebUI

Network > Interface > Edit > OSPF: Link Type ラジオボタンから **Point-to-Multipoint** を選択します。

CLI

```
set interface tunnel.1 protocol ospf link-type p2mp
save
```

Route-deny 機能の無効化

明示的に禁止する設定をしない限り、セキュリティデバイスは同じインターフェース上でパケット送信と受信の両方ができるようになっています。ポイントツーマルチポイントで運用する場合は、このような動作が望ましいでしょう。同じインターフェースで送受信できるようにするためには、route-deny 機能による制限を無効にする必要があります。この例では、CLI を使って、ポイントツーマルチポイントトンネルインターフェース tunnel.1 の route-deny 制限を無効にします。

WebUI

注 : Route-deny 機能の設定には CLI を使う必要があります。

CLI

```
unset interface tunnel.1 route-deny
save
```

ポイントツーマルチポイントネットワークの作成

図 12 は、中央オフィス (CO) をサンフランシスコに、リモートサイトをシカゴ、ロサンゼルス、モントリオール、ニューヨークに持つ中規模企業のネットワークです。各オフィスには、1 台のセキュリティデバイスが設置されています。

以下の項目は、CO のセキュリティデバイスに特に必要な設定条件です。

1. 仮想ルーターは、OSPF インスタンスが稼働するよう設定し、OSPF を有効にします。さらに、tunnel.1 インターフェースを設定します。

2. VPN を 4 つ設定し、tunnel.1 インターフェースにバインドします。

以下の項目は、リモートサイトのセキュリティデバイスに特に必要な設定条件です。

1. 仮想ルーターは、OSPF インスタンスが稼働するよう設定し、OSPF を有効にします。さらに、tunnel.1 インターフェースを設定します。

2. VPN を設定し、tunnel.1 インターフェースにバインドします。

各デバイスが隣接関係を成すために、タイマー値を一致させておく必要があります。図 12 は説明したネットワークシナリオを示します。

図 12: ポイントツーマルチポイントネットワーク例

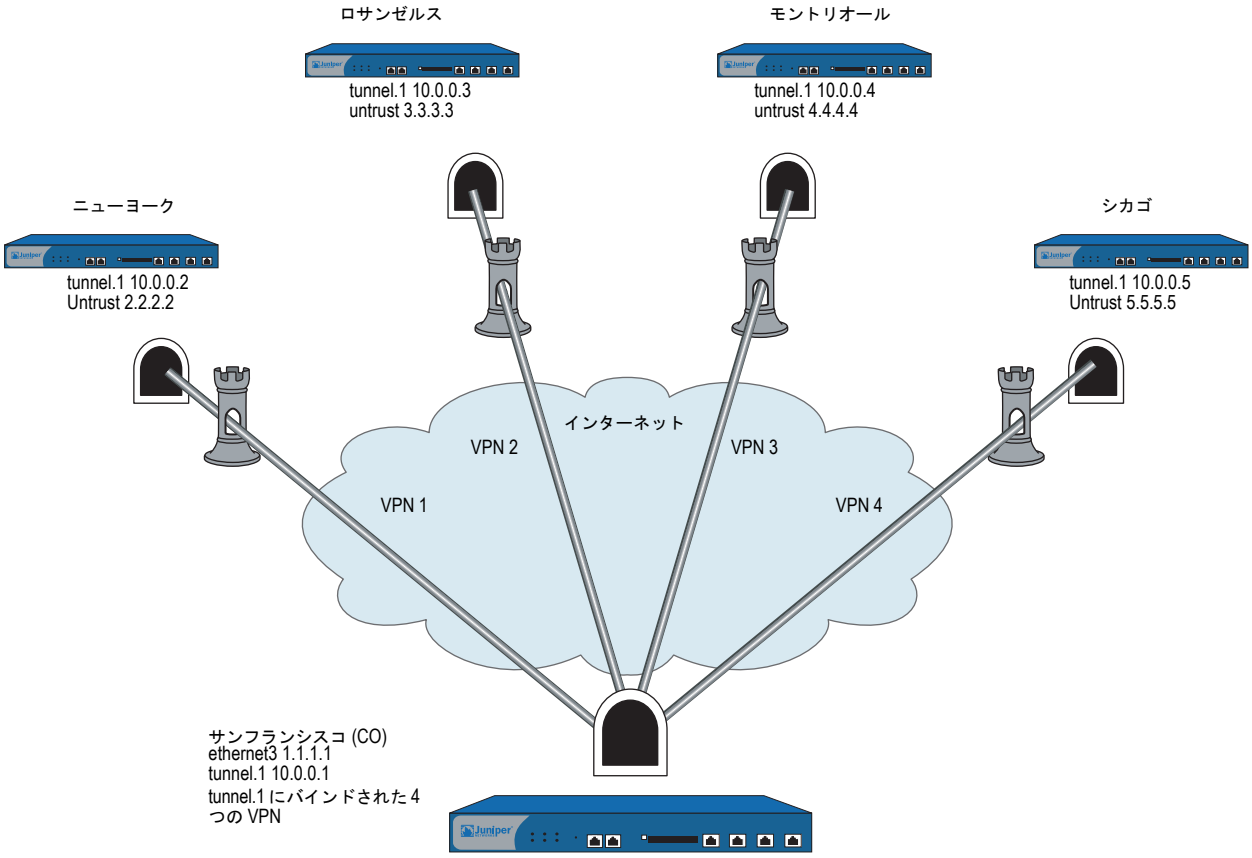


図 12 では、サンフランシスコのセキュリティデバイスから 4 つの VPN が出ており、ニューヨーク、ロサンゼルス、モントリオール、シカゴのリモートオフィスに放射状に伸びています。

この例では、CO のセキュリティデバイスに以下の項目を設定しています。

1. セキュリティゾーンおよびインターフェース
2. VPN
3. ルートと OSPF

ネットワークの設定を終了するには、4 つの各リモートオフィスのデバイスに以下の設定を行います。

1. インターフェースおよび OSPF
2. VPN
3. ポリシー

注： WebUI 手順は、例が長すぎないようにするため、省略されています。CLI については完全な例を示します。具体的なパラメータ値については、CLI の例を参照してください。

WebUI (中央オフィスのデバイス)

1. **セキュリティゾーンおよびインターフェース**
   Network > Interfaces > **New Tunnel IF** をクリック して、構成ページに進む。

   Network > Interfaces > IP アドレスおよびゾーンを編集 (Ethernet3) および構成。

   Network > Interface > Edit (for tunnel.1) > OSPF: Link Type ラジオボタンから **Point-to-Multipoint** を選択します。

2. **VPN**
   VPNs > AutoKey Advanced > Gateway

3. **ルートと OSPF**
   Network > Routing > Virtual Routers > 仮想ルーターの **Edit** をクリックして、OSPF パラメータを構成。

CLI (中央オフィスのデバイス)

1. **セキュリティゾーンおよびインターフェース**
```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.10.10.1/24
```

2. **VPN**
```
set ike gateway gw1 address 2.2.2.2 main outgoing-interface ethernet3 preshare
    ospfp2mp proposal pre-g2-3des-sha
set ike gateway gw2 address 3.3.3.3 main outgoing-interface ethernet3 preshare
    ospfp2mp proposal pre-g2-3des-sha
set ike gateway gw3 address 4.4.4.4 main outgoing-interface ethernet3 preshare
    ospfp2mp proposal pre-g2-3des-sha
set ike gateway gw4 address 5.5.5.5 main outgoing-interface ethernet3 preshare
    ospfp2mp proposal pre-g2-3des-sha
set vpn vpn1 gateway gw1 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn1 monitor rekey
set vpn1 id 1 bind interface tunnel.1
set vpn vpn2 gateway gw2 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn2 monitor rekey
set vpn2 id 2 bind interface tunnel.1
set vpn vpn3 gateway gw3 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn3 monitor rekey
set vpn3 id 3 bind interface tunnel.1
set vpn vpn4 gateway gw4 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn4 monitor rekey
set vpn4 id 4 bind interface tunnel.1
```

3. **ルートと OSPF**
```
set vrouter trust router-id 10
set vrouter trust protocol ospf
set vrouter trust protocol ospf enable
set interface tunnel.1 protocol ospf area 0
set interface tunnel.1 protocol ospf enable
set interface tunnel.1 protocol ospf link-type p2mp
unset interface tunnel.1 route-deny
save
```

注： デフォルト状態では、route-deny は無効になっています。しかし、これを有効にしていたとすると、ポイントツーマルチポイントトンネルインターフェースで運用する際には無効に設定し直す必要があります。

この手順に従って、リモートオフィスのセキュリティデバイスの設定を行います。Juniper Networks セキュリティデバイスは LSA を受けて近隣ノードを認識します。

Figure 12 on page 74 に示したようなネットワーク構成で運用するためには、リモート側の各デバイスについて以下の設定をした上で、それぞれの IP アドレス、ゲートウェイ名、VPN 名を変更し、必要に応じてポリシーを設定することになります。リモートサイトごとに、trust および untrust ゾーンは異なります。

注： WebUI 手順は、例が長すぎないようにするため、省略されています。CLI については完全な例を示します。具体的なパラメータ値については、CLI の例を参照してください。

WebUI (リモートオフィスのデバイス)

1. **インターフェースおよび OSPF**
   Network > Interfaces > **New Tunnel IF をクリックして**、構成ページに進む。
2. **VPN**
   VPNs > AutoKey Advanced > Gateway
3. **ポリシー**
   ポリシー (All zones から All zones) > New をクリック。

CLI (リモートオフィスのデバイス)

1. **インターフェースおよび OSPF**
```
set vrouter trust protocol ospf
set vrouter trust protocol ospf enable
set interface untrust ip 2.2.2.2/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.0.0.2/24
set interface tunnel.1 protocol ospf area 0
set interface tunnel.1 protocol ospf enable
```
2. **VPN**
```
set ike gateway gw1 address 1.1.1.1/24 main outgoing-interface untrust preshare
    ospfp2mp proposal pre-g2-3des-sha
set vpn vpn1 gateway gw1 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn1 monitor rekey
set vpn vpn1 id 1 bind interface tunnel.1
```
3. **ポリシー (必要に応じて設定)**
```
set policy id 1 from trust to untrust any any any permit
set policy id 2 from untrust to trust any any any permit
save
```

変更後の設定内容は、**get vrouter** *vrouter* **protocol ospf config** というコマンドで参照できます。

第 4 章

ルーティング情報プロトコル (RIP)

この章では、Juniper Networks セキュリティデバイスに組み込まれたルーティングプロトコルであるルーティング情報プロトコル (RIP) version 2 について説明します。本章のセクションは、以下のようになります。

- 78 ページの「概要」
- 79 ページの「RIP の基本設定」
  - 80 ページの「RIP インスタンスの作成と削除」
  - 81 ページの「RIP をインターフェースで使用可能・不可にする」
  - 81 ページの「ルートの再配布」
- 83 ページの「RIP 情報の表示」
  - 83 ページの「RIP データベースの表示」
  - 84 ページの「RIP 詳細の表示」
  - 85 ページの「RIP 隣接情報の表示」
  - 86 ページの「特定のインターフェースの RIP 詳細の表示」
- 87 ページの「RIP に関する大域パラメータ」
- 88 ページの「デフォルトルートの通知」
- 89 ページの「RIP インターフェースパラメータの構成」
- 90 ページの「セキュリティ構成」
  - 90 ページの「パスワードを設定して隣接ノードを認証する」
  - 91 ページの「Trusted 隣接ノードを構成する」
  - 92 ページの「デフォルトルートを拒否する」
  - 92 ページの「フラッディングの回避」

- 94 ページの「オプションの RIP 構成」
  - 94 ページの「RIP バージョンの構成」
  - 96 ページの「プレフィックスサマリを使用不可・可能にする」
  - 97 ページの「代替ルートを設定する」
  - 99 ページの「トンネルインターフェースの要求回路」
  - 100 ページの「静的隣接ノードの構成」
- 100 ページの「ポイントツーマルチポイントトンネルインターフェースの構成」

概要

ルーティング情報プロトコル (RIP) はインテリアゲートウェイプロトコル (IGP) の一つで、距離ベクトルプロトコルにより、中規模の AS (自律システム) 内のルーティング処理を行います。ScreenOS は RFC 2453 で定義された RIP version 2 (RIPv2) に対応しています。RIPv2 の認証機構は簡単なパスワード (プレインテキスト) によるもののみですが、ScreenOS の実装では、RFC 2082 で定義されている MD5 認証拡張も使えるようになっています。

注 : RIP は番号付けされていないトンネルインターフェースではサポート*されていません*。RIP プロトコルを使用するインターフェースは番号付けする必要があります。番号付けされていないインターフェースを RIP を使って構成・実行しようとすると、予測できないルーティング障害が起きることがあります。

RIP は企業 LAN のような、小規模で同種のノードから成るネットワークで、ルート情報を管理します。RIP ネットワークでは、最大 15 ホップまでのパスを扱えます。メトリック値 16 は、無効あるいは到達不可であることを表します。RIP ネットワークの最大ホップ数である 15 を超えるので、「無限大」とも呼ばれています。

その一方、大規模ネットワークには向いていませんし、遅延、信頼性、負荷などをリアルタイムに測定しながらルートを選択するような処理にも対応できません。RIP は、(VPN でよく使われる) ポイントツーポイントネットワーク、ブロードキャスト / マルチキャスト Ethernet ネットワークのどちらにも対応しています。RIP は、構成要求回路の有無にかかわらず、トンネルインターフェースのポイントツーマルチポイント接続をサポートしています。要求回路の詳細については、99 ページの「トンネルインターフェースの要求回路」を参照してください。

RIP は、完全なルーティングテーブルを含んだメッセージを、接続ルーターすべてに宛てて 30 秒ごとに送信します。通常、マルチキャストとしてアドレス 224.0.0.9 に向けて、RIP ポートから送信します。

RIP ルーティングデータベースには、RIP ルーティングインスタンス経由で到達できる宛先ごとに、1 つのエントリがあります。次のようなルート情報が記録されています。

- 宛先の IPv4 アドレス。RIP はネットワークとホストを区別しません。
- 宛先へのルート上にある最初のルーター (次のホップ点) の IP アドレス。

- 最初のルーターに到達するためのネットワークインターフェース。
- 宛先までの距離 (あるいはコスト) を表すメトリック値。ほとんどの RIP 実装では、各ネットワークのメトリック値をすべて 1 として処理します。
- データベース中の当該ルート情報を最後に更新してからの経過時間。

RIP の基本設定

セキュリティデバイス上に仮想ルーターベースで RIP を作成します。システムに仮想ルーター (VR) が複数あれば、VR ごとにバージョン 1 または 2 のインスタンスを設定し、いくつもの RIP を稼動させることができます。デフォルトでは、RIP バージョン 2 をサポートしています。

注 : 動的ルーティングプロトコルをセキュリティデバイス上で構成する前に、VR ID を 15 ページの「ルーティング」の説明にしたがって割り当てる必要があります。

ここではセキュリティデバイスで RIP を設定する基本的な手順を説明します。

1. 仮想ルーターに RIP ルーティングインスタンスを作成します。
2. RIP インスタンスを有効にします。
3. 他の RIP ルーターに接続するインターフェースについて、RIP を有効にします。
4. 他のルーティングプロトコル (OSPF、BGP、静的ルートなど) で収集したルート情報を、RIP インスタンスに再配布します。

以下、この手順にそって、具体的な操作方法を説明します。CLI を使う方法と、WebUI 画面から操作する方法があります。

さらに、以下のような RIP パラメータも設定できます。

- RIP の仮想ルーターごとに設定する大域パラメータ。タイマー、信頼できる RIP 隣接ノードなど (87 ページの「RIP に関する大域パラメータ」を参照)。
- インターフェースごとに設定するパラメータ。隣接ノードの認証方法など (89 ページの「RIP インターフェースパラメータの構成」を参照)。
- セキュリティ関連の RIP パラメータ。仮想ルーターごとに設定するものと、インターフェースごとに設定するものがあります (90 ページの「セキュリティ構成」を参照)。

RIP インスタンスの作成と削除

セキュリティデバイス上の特定の仮想ルーター (VR) に RIP ルーティングインスタンスを作成して使用可能にします。この作業が終わると、RIP が有効になっている VR 上の各インターフェースと、パケットをやり取りできるようになります。

VR から RIP ルーティングインスタンスを削除すると、VR に属するインターフェースすべてについて、RIP 設定情報が削除されます。

仮想ルーターやその設定方法については 15 ページの「ルーティング」を参照。

RIP インスタンスの作成

trust-vr に RIP ルーティングインスタンスを作成してから、RIP を有効にします。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit: **Virtual Router ID** を入力して **Create RIP Instance** を選びます。

Enable RIP を選択して **OK** をクリックします。

CLI

1. **ルーター ID**
   set vrouter trust-vr router-id 10
2. **RIP ルーティングインスタンス**
   set vrouter trust-vr protocol rip
   set vrouter trust-vr protocol rip enable
   save

注 : CLI からの RIP インスタンスの作成は、2 つの手順から成るプロセスです。RIP インスタンスを作成してから、RIP を有効にします。

RIP インスタンスの削除

ここでは trust-vr 上に作成した RIP ルーティングインスタンスを無効にします。trust-vr の RIP が有効になっているインターフェースに対し、RIP パケットの送信・処理を停止します。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIP Instance: Enable RIP をオフにして **OK** をクリックします。

Network > Routing > Virtual Router (trust-vr) > Edit > Delete RIP Instance を実行。確認プロンプトが現れるので **OK** をクリックします。

CLI

unset vrouter trust-vr protocol rip enable
unset vrouter trust-vr protocol rip
save

RIP をインターフェースで使用可能・不可にする

デフォルトでは、VR のどのインターフェースでも RIP は無効になっているため、稼動させようとするインターフェースごとに、明示的に有効にする必要があります。あるインターフェースについて RIP を無効にすると、そこでは RIP パケットの送受信を行わないようになります。ただし設定パラメータはそのまま保存されます。

注 : VR 上で RIP ルーティングインターフェースを無効にする (80 ページの「RIP インスタンスの削除」を参照) と、RIP が有効になっている他のインターフェースに対し、RIP パケットを送信することはなくなります。

インターフェース上の RIP を有効にする

ここでは Trust インターフェース上で RIP を稼動させます。

WebUI

Network > Interface > Edit (Trust) > RIP: プロトコル RIP の **Enable** を選択し、**Apply** をクリックします。

CLI

```
set interface trust protocol rip enable
save
```

インターフェース上の RIP を停止する

ここでは Trust インターフェース上の RIP を停止します。RIP の構成を完全に停止するには、2 行目の CLI コマンドを入力してから保存してください。

WebUI

Network > Interface (Trust) > RIP: プロトコル RIP の **Enable** を選択し、**Apply** をクリックします。

CLI

```
unset interface trust protocol rip enable
unset interface trust protocol rip
save
```

ルートの再配布

ルート再配布とは、ルーティングプロトコル間のルート情報の交換のことです。たとえば以下のようなルート情報を、同一の仮想ルーターにある RIP ルーティングインスタンスに再配布することができます。

- BGP により学習したルート情報
- OSPF により学習したルート情報
- 直接接続されたルート
- インポートされたルート
- 静的に構成されたルート

ルート情報再配布の設定に当たっては、再配布するルートを分別するためのルートマップを指定する必要があります。ルートマップの作成について詳しくは、15 ページの「ルーティング」、を参照してください

他のプロトコルから RIP にインポートしたルートの、デフォルトのメトリック値は 10 です。これは変更できます (87 ページの「RIP に関する大域パラメータ」を参照)。

この例では、サブネットワーク 20.1.0.0/16 内の静的ルートを、仮想ルーター trust-vr に属する RIP 隣接ノードに再配布します。そのために、サブネット 20.1.0.0/16 に属するアドレスを許可するアクセスリストを作成します。次に、このアクセスリストに一致するアドレスを許可するよう、ルートマップを設定します。最後に、このルートマップを使って、静的ルートを RIP ルーティングインスタンスに再配布するよう指定します。

WebUI

Network > Routing > Virtual Router (trust-vr) > Access List > New: 次のように入力してから **OK** をクリックします。

Access List ID: 20
Sequence No.: 1
IP/Netmask: 20.1.0.0/16
Action: Permit (選択)

Network > Routing > Virtual Router (trust-vr) > Route Map > New: 次のように入力してから **OK** をクリックします。

Map Name: rtmap1
Sequence No.: 1
Action: Permit (選択)
Match Properties:
Access List: (選択), 20 (選択)

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIP Instance > Redistributable Rules: 次のように入力してから **Add** をクリックします。

Route Map: rtmap1 (選択)
Protocol: Static (選択)

CLI

```
set vrouter trust-vr access-list 20 permit ip 20.1.0.0/16 1
set vrouter trust-vr route-map name rtmap1 permit 1
set vrouter trust-vr route-map rtmap1 1 match ip 20
set vrouter trust-vr protocol rip redistribute route-map rtmap1 protocol static
save
```

RIP 情報の表示

RIP パラメータを変更すると、RIP の詳細について以下の項目を参照できます。

- データベース。ルーティング情報を表示します。
- プロトコル。仮想ルーターの RIP とインターフェースの詳細を表示します。
- 隣接ノード

RIP データベースの表示

RIP ルーティング情報は、CLI から確認することができます。RIP データベースの全エントリの一覧を表示するか、1 エントリを表示するかを選択できます。

この例では、RIP データベースの詳細情報を表示します。参照する仮想ルーターの IP アドレスとマスクを追加することにより、データベースの全エントリを参照するか、または 1 つのデータベースエントリのみを参照するかを選択することができます。

この例では、trust-vr を指定して、プレフィックスと IP アドレス 10.10.10.0/24 を追加することにより、1 つのテーブルエントリのみを参照します。

WebUI

注 : RIP データベースを表示するには、CLI を使用してください。

CLI

```
get vrouter trust-vr protocol rip database prefix 10.10.10.0/24
save
```

次の CLI コマンドを入力すると、RIP データベースエントリが表示されます。

```
device-> get vrouter trust-vr protocol rip database 10.10.10.0/24
VR: trust-vr
------------------------------------------------------------------------------
Total database entry: 3
Flags: Added in Multipath - M, RIP - R, Redistributed - I,
       Default (advertised) - D, Permanent - P, Summary - S,
       Unreachable - U, Hold - H
DBID Prefix         Nexthop    Ifp  Cost Flags Source
   7 10.10.10.0/24  20.20.20.1 eth1    2    MR 20.20.20.1
------------------------------------------------------------------------------
```

RIP データベースには以下のフィールドがあります。

- DBID: エントリのデータベース識別子
- Prefix: IP アドレスおよびプレフィックス
- Nexthop: 次のホップ点のアドレス (ルーター)
- Ifp: 接続の種類 (ethernet または tunnel)
- ソースからの距離を示すために割り当てたコストメトリック値

Flag には、以下のいずれか 1 つ以上が当てはまります。multipath (M)、RIP (R)、Redistributed (I)、Advertised default (D)、Permanent (P)、Summary (S)、Unreachable (U)、または Hold (H)。

この例では、データベース識別子は 7、IP アドレスおよびプレフィックスは 10.10.10.0/24、次のホップ点は 20.20.20.1 となっています。また、コスト 2 のイーサネット接続です。フラグは M と R で、このルートがマルチパスで RIP が稼働していることを示しています。

RIP 詳細の表示

RIP 構成がネットワークのニーズに合っているかを確認するために、RIP の詳細を表示することができます。表示出力をインターフェースの要約テーブルのみに制限するには、CLI コマンドに *interface* を追加します。

RIP の全情報を表示して、構成をチェックしたり保存されている変更内容がアクティブかどうかを確認することができます。

WebUI

注： RIP の詳細を表示するには、CLI を使用してください。

CLI

get vrouter trust-vr protocol rip

このコマンドは、次に似た出力を生成します。

```
device-> get vrouter trust-vr protocol rip
VR: trust-vr
------------------------------------------------------------------------------
State: enabled
Version: 2
Default metric for routes redistributed into RIP: 10
Maximum neighbors per Interface: 16
Not validating neighbor in same subnet: disabled
RIP update transmission not scheduled
Maximum number of Alternate routes per prefix: 2
Advertising default route: disabled
Default routes learnt by RIP will not be accepted
Incoming routes filter and offset-metric: not configured
Outgoing routes filter and offset-metric: not configured
Update packet threshold is not configured
Total number of RIP interfaces created on vr(trust-vr): 1
Update| Invalid|   Flush| DC Retransmit| DC Poll| Hold Down (Timers in seconds)
------------------------------------------------------------------------------
    30|     180|     120|       5|      40|90
Flags: Split Horizon - S, Split Horizon with Poison Reverse - P, Passive - I
       Demand Circuit - D
Interface   IP-Prefix    Admin       State    Flags   NbrCnt Metric Ver-Rx/Tx
------------------------------------------------------------------------------
tun.1       122.1.2.114/8 enabled    disabled       SD        1      1  v1v2/v1v
```

RIP の設定、パケットの詳細、RIP のタイマー情報、インターフェース表の概要を表示することができます。

RIP 隣接情報の表示

仮想ルーターの RIP 隣接情報の詳細を表示することができます。表示する隣接情報の IP アドレスを追加することにより、全隣接情報の一覧または特定の隣接情報のエントリのみを取得できます。これらの統計から、ルートのステータスをチェックしたり、隣接ルーターとセキュリティデバイス間の接続を確認することができます。

次の例では、trust-vr の RIP 隣接情報を表示します。

WebUI

注 : RIP 隣接情報を表示するには、CLI を使用してください。

CLI

get vrouter trust-vr protocol rip neighbors

このコマンドは、次に似た出力を生成します。

```
device-> get vrouter trust-vr protocol rip neighbors
VR: trust-vr
-------------------------------------------------------------------------------
Flags: Static - S, Demand Circuit - T, NHTB - N, Down - D, Up - U, Poll - P,
       Demand Circuit Init - I
Neighbors on interface tunnel.1
-------------------------------------------------------------------------------
IpAddress       Version  Age          Expires      BadPackets BadRoutes Flags
-------------------------------------------------------------------------------
10.10.10.1      v2       -            -                     0         0 TSD
```

IP アドレスや RIP のバージョンだけでなく、以下の RIP 隣接情報も参照することができます。

- エントリのエージ
- 有効期限
- 不良パケット数
- 不良ルート数
- Flags: static (S)、demand circuit (T)、NHTB (N)、down (D)、up (U)、poll (P)、demand circuit init (I)

特定のインターフェースの RIP 詳細の表示

全インターフェースの RIP の全関連情報や隣接ノードの詳細の要約を表示することができます。オプションで、特定の隣接情報の IP アドレスを追加して、出力を制限することもできます。

以下の例では、IP アドレス 10.10.10.2 にある隣接インターフェース tunnel.1 についての情報を見ることができます。

WebUI

注： RIP インターフェースの詳細を表示するには、CLI を使用してください。

CLI

get interface tunnel.1 protocol rip neighbor 10.10.10.2

このコマンドは、次に似た出力を生成します。

```
device-> get interface tunnel.1 protocol rip
VR: trust-vr
-------------------------------------------------------------------------------
Interface: tunnel.1, IP: 10.10.10.2/8, RIP: enabled, Router: enabled
Receive version v1v2, Send Version v1v2
State: Down, Passive: No
Metric: 1, Split Horizon: enabled, Poison Reverse: disabled
Demand Circuit: configured
Incoming routes filter and offset-metric: not configured
Outgoing routes filter and offset-metric: not configured
Authentication: none
Current neighbor count: 1
Update not scheduled
Transmit Updates: 0 (0 triggered), Receive Updates: 0
Update packets dropped because flooding: 0
Bad packets: 0, Bad routes: 0
Flags: Static - S, Demand Circuit - T, NHTB - N, Down - D, Up - U, Poll - P
Neighbors on interface tunnel.1
-------------------------------------------------------------------------------
IpAddress       Version  Age          Expires      BadPackets BadRoutes Flags
-------------------------------------------------------------------------------
10.10.10.1      -        -            -                     0         0 TSD
```

この情報の概要では、現在の不良パケット数や不良ルート数、RIP による接続のオーバーヘッド、認証設定を表示することができます。

RIP に関する大域パラメータ

この節では、VR ごとに設定できる RIP の大域パラメータについて解説します。VR に対して RIP パラメータを設定すると、RIP を有効にしたすべてのインターフェースの動作に反映されます。大域パラメータの設定は、CLI の RIP ルーティングプロトコルコンテキストから実行するほか、WebUI 画面からも変更できます。

表 10 に、RIP 大域パラメータとそのデフォルト値を説明します。

表 10: RIP 大域パラメータおよびデフォルト値

RIP に関する大域パラメータ	説明	デフォルト値
Default metric	OSPF や BGP など、他のプロトコルから RIP にインポートしたルートの、デフォルトメトリック値。	10
Update timer	隣接ノードに RIP ルート情報の更新通知を送る間隔 (秒単位)。	30 秒
Maximum packets per update	1 回の更新通知で受信する最大パケット数。	制限なし
Invalid timer	隣接ノードからの通知がなくなってから、ルート情報を無効と看做すまでの時間 (秒単位)。	180 秒
Flush timer	ルート情報が無効になってから、実際に削除するまでの時間 (秒単位)。	120 秒
Maximum neighbors	RIP 隣接ノードの最大数。	プラットフォームにより異なる
Trusted neighbors	RIP 隣接ノードを定義したアクセスリストを指定。この指定がない場合は、マルチキャストまたはブロードキャストにより、当該インターフェース上の隣接ノードを検出します。91 ページの「Trusted 隣接ノードを構成する」を参照してください。	隣接ノードはすべて信頼できると看做す。
Allow neighbors on different subnets	他のサブネットに属する RIP 隣接ノードも許可する旨の指定。	無効
Advertise default route	デフォルトルート (0.0.0.0/0) を通知するか否かを指定。	無効
Reject default routes	他のプロトコルで収集したデフォルトルート情報を拒否する旨の指定。92 ページの「デフォルトルートを拒否する」を参照してください。	無効
Incoming route map	RIP で収集したルート情報を分別するためのフィルタを指定。	なし
Outgoing route map	RIP で通知するルートを分別するためのフィルタ。	なし
Maximum alternate routes	RIP ルートデータベースに追加可能な同一プレフィックスの最大 RIP ルート数を指定。97 ページの「代替ルートを設定する」を参照してください。	0
Summarize advertised routes	サマリの範囲内にある全ルートに対応するサマリルートの通知を指定。96 ページの「プレフィックスサマリを使用不可・可能にする」を参照してください。	なし
RIP protocol version	仮想ルーターが使用している RIP のバージョンを指定。インターフェースごとにバージョンを個別指定することができます。94 ページの「RIP バージョンの構成」を参照してください。	バージョン 2
Hold-timer	ルートテーブルへのルートフラップを禁止。最小値 (update timer の値の 3 倍) から最大値 (update timer と hold timer の和。ただし、flush timer の値を超えてはならない) の間で指定できます。	90 秒

RIP に関する大域パラメータ	説明	デフォルト値
Retransmit timer	要求回路から出される応答の再送信の間隔を指定。retransmit timer を設定することにより、ネットワークのニーズに合った再試行回数を割り当てることができます。	5 秒 再試行 10 回
Poll-timer	隣接ルーターが起動しているかを確認するため、要求回路のリモート隣接ルーターをチェック。poll timer を分単位で構成することにより、ネットワークのニーズに合った再試行回数を割り当てることができます。再試行回数が 0 の場合、永久にポーリングを行います。	180 秒 再試行 0 回

デフォルトルートの通知

RIP 設定を変更して、デフォルトルート (非 RIP ルート) の通知を含むようにし、特定の VR ルーティングテーブルにあるデフォルトルートに関連しているメトリックを変更することができます。

デフォルトでは、デフォルトルート (0.0.0.0/0) は RIP 隣接ノードに通知しないようになっています。次のコマンドは、仮想ルーター trust-vr 上の RIP 隣接ノードに対し、デフォルトルートのメトリック値が 5 であると通知します (メトリック値を指定してください)。このデフォルトルートは、ルーティングテーブルに登録されているものと想定します。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIP Instance: 次のように入力してから **OK** をクリックします。

Advertising Default Route: (**選択**)
Metric: 5

CLI

```
set vrouter trust-vr protocol rip advertise-def-route metric number 5
save
```

注 : RIP ルーティングプロトコルのコンテキストで設定できる大域パラメータについて詳しくは、*ScreenOS CLI Reference Guide: IPv4 Command Descriptions* を参照してください。

RIP インターフェースパラメータの構成

この節では、インターフェースごとに設定できる RIP パラメータについて説明します。これは当該インターフェース上の動作にのみ影響を及ぼします。パラメータの設定は、**interface** という CLI コマンドを使うか、または WebUI 画面から行います。

表 11 に、RIP インターフェースパラメータとそのデフォルト値を説明します。

表 11: RIP インターフェースパラメータおよびデフォルト値

RIP インターフェースパラメータ	説明	デフォルト値
Split-horizon	スプリットホライズン (split-horizon) コントロールをするか否かを指定（あるインターフェースから受信したルート情報を、同一のインターフェースに対しては通知しないよう制限する機能です）。さらにポイズンリバース (poison-reverse) 機能を有効にすることもできます。この場合、インターフェースから収集したルートを、メトリック値が 16 の状態にして、同一のインターフェースに送信するようになります。	Split-horizon は有効。ポイズンリバースは無効。
RIP metric	インターフェースの RIP メトリックを指定。	1
Authentication	認証方法として、クリアテキストパスワード、MD5 認証のいずれかを指定。90 ページの「パスワードを設定して隣接ノードを認証する」を参照してください。	認証なし
Passive mode	インターフェースが RIP パケットの受信のみを行い、送信はしないよう設定。	No
Incoming route map	RIP で収集したルート情報を分別するためのフィルタを指定。	なし
Outgoing route map	RIP で通知するルートを分別するためのフィルタ。	なし
RIP version for sending or receiving updates	インターフェースの更新の受信や送信の RIP プロトコルのバージョンを指定。送信用インターフェースと受信用インターフェースのバージョンは同じである必要はありません。94 ページの「RIP バージョンの構成」を参照してください。	仮想ルーター用に設定したバージョン。
Route summarization	インターフェースのルート要約を有効にするかどうかを指定。96 ページの「プレフィックスサマリを使用不可・可能にする」を参照してください。	無効
Demand-circuit	指定したトンネルインターフェースの要求回路を指定。変更された場合にのみ、セキュリティデバイスは更新メッセージを送信します。99 ページの「トンネルインターフェースの要求回路」を参照してください。	なし
Static neighbor IP	手動で割り当てた RIP の隣接ノードの IP アドレスを指定。	なし

内向きおよび外向きのルートマップは、仮想ルーターごとあるいはインターフェースごとに定義できます。両方の定義がある場合は、当該インターフェースに対して定義したルートマップの方を優先します。したがって、たとえば内向きルートマップを仮想ルーターに対して定義し、あるインターフェースに対してはさらに別の内向きルートマップを定義した場合、当該インターフェースに関しては、後者のルートマップを使うことになります。詳細については、40 ページの「ルートマップの設定」を参照してください。

この例では、trust インターフェースに次のような RIP パラメータを設定します。

- MD5 認証の設定。キーは 1234567898765432、キー ID は 215 とします。
- スプリットホライズンを有効にし、ポイズンリバースも行うようにします。

WebUI

Network > Interfaces > Edit (Trust) > RIP: 次のように入力してから **OK** をクリックします。

Authentication: MD5 (**選択**)
Key: 1234567898765432
Key ID: 215
Split Horizon: Enabled with poison reverse (**選択**)

CLI

```
set interface trust protocol rip authentication md5 1234567898765432 key-id
    215
set interface trust protocol rip split-horizon poison-reverse
save
```

セキュリティ構成

この節では、RIP ルーティングドメインに起こりうるセキュリティ上の問題と、攻撃の防御方法について説明します。

注 : RIP の安全性を確保するためには、RIP ドメイン内のルーターをすべて、同一のセキュリティレベルに設定しなければなりません。そうでないと、最も安全性の低い RIP ルーターが原因となって、RIP ルーティングドメイン全体が危険にさらされる恐れがあります。

パスワードを設定して隣接ノードを認証する

RIP パケットは暗号化されておらず、どんなプロトコルアナライザーでも RIP パケットを分析できるので、RIP ルーターのなりすまし (spoofing) 攻撃は容易です。これを回避する方法としては、RIP 隣接ノードの認証が最善です。

RIP には、隣接ノードから受け取った RIP パケットの確認手段として、単純なパスワード認証と MD5 認証の 2 つがあります。認証に失敗した RIP パケットはすべて破棄することになります。デフォルトでは、どの RIP インターフェースも認証は無効になっています。

MD5 認証のためには、送信側および受信側の RIP ルーターが、同一のキーを共有している必要があります。同一のセキュリティデバイスに複数の MD5 キーを登録することもできます。キーはそれぞれ、キー識別子と組になっています。MD5 キーが複数ある場合、接続ルーターとの通信を認証するために使うキーは、キー識別子で指定します。したがって、MD5 キーを定期的に変更しても、パケットを失う危険はほとんどありません。

この例では、インターフェース ethernet1 に対して MD5 キーを 2 つ設定しておき、そのうち一方をアクティブキーに選択します。デフォルトではキー識別子が 0 となっているので、最初に設定した MD5 キーに対してはキー識別子を指定する必要はありません。

WebUI

Network > Interfaces > Edit (ethernet1) > RIP: 以下を入力して **Apply** をクリックします。

MD5 Keys: (選択)
1234567890123456 (1 つめのフィールド)
9876543210987654 (2 つめのフィールド)
Key ID: 1
Preferred: (選択)

CLI

```
set interface ethernet1 protocol rip authentication md5 1234567890123456
set interface ethernet1 protocol rip authentication md5 9876543210987654
    key-id 1
set interface ethernet1 protocol rip authentication md5 active-md5-key-id 1
save
```

Trusted 隣接ノードを構成する

マルチアクセス環境にすると、ルーターなどのデバイスが、比較的容易にネットワークに接続できてしまします。そのため、接続されたデバイスが信頼性に欠ける場合、安定性や性能に問題が生じる可能性があります。これを回避するため、所定のノードだけが RIP 隣接ノードになれるよう、アクセスリストを定義して制限することができます。デフォルトでは、仮想ルーターと同一のサブネットに属するデバイスだけが、RIP 隣接ノードになれるよう制限しています。

ここでは、仮想ルーター trust-vr で稼動する RIP ルーティングインスタンスに対して、次のような大域パラメータを設定します。

- RIP 隣接ノードの最大数を 1 とします。
- 信頼できる隣接ノード IP アドレス 10.1.1.1 をアクセスリストで指定します。

WebUI

Network > Routing > Virtual Router (trust-vr) > Access List > New: 次のように入力してから **OK** をクリックします。

Access List ID: 10
Sequence No.: 1
IP/Netmask: 10.1.1.1/32
Action: Permit (選択)

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIP Instance: 次のように入力してから **OK** をクリックします。

Trusted Neighbors: (選択), 10
Maximum Neighbors: 1

CLI

```
set vrouter trust-vr
device(trust-vr)-> set access-list 10 permit ip 10.1.1.1/32 1
device(trust-vr)-> set protocol rip
device(trust-vr/rip)-> set max-neighbor-count 1
device(trust-vr/rip)-> set trusted-neighbors 10
device(trust-vr/rip)-> exit
device(trust-vr)-> exit
save
```

デフォルトルートを拒否する

Route Detour Attack では、あるルーターがデフォルトルート (0.0.0.0/0) をルーティングドメインに挿入してパケットをそのルーターに迂回させます。このルーターはパケットを破棄することでサービスの崩壊を招いたり、パケットを転送する前に内部の機密情報を得ることができます。Juniper Networks セキュリティデバイスのデフォルトでは、RIP により収集したデフォルトルート情報をすべて受け入れ、ルーティングテーブルに登録するようになっています。

次の例では、仮想ルーター trust-vr 上で稼動する RIP ルーティングインスタンスに対し、デフォルトルートの情報を RIP で収集しないよう設定します。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIP Instance: 次のように入力してから **OK** をクリックします。

Reject Default Route Learnt by RIP: (**選択**)

CLI

```
set vrouter trust-vr protocol rip reject-default-route
save
```

フラッディングの回避

ルーターが正しく設定されていなかったり、攻撃を受けたりした場合、RIP 更新パケットを隣接ノードに大量に送りつけて、フラッディング（洪水) してしまうことがあります。仮想ルーターに対して、更新間隔内に RIP インターフェース上で受け取る更新パケットの最大数を制限することにより、これを回避できます。この数以上のパケットは破棄されます。このしきい値を設定していない場合は、更新パケットをすべて受理します。

隣接ノードに大きなルーティングテーブルがある場合は、このしきい値の選び方にも注意してください。フラッシュアップデートのために、一時的に大量の更新パケットが送られる可能性があります。そうすると、しきい値を超えたパケットは破棄され、有効なルート情報も取得できなくなってしまいます。

アップデートしきい値を構成する

ここではあるインターフェースで RIP が受け取る更新パケットの最大数を 4 と設定します。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIP Instance: 次のように入力してから **OK** をクリックします。

Maximum Number Packets per Update Time: (選択), 4

CLI

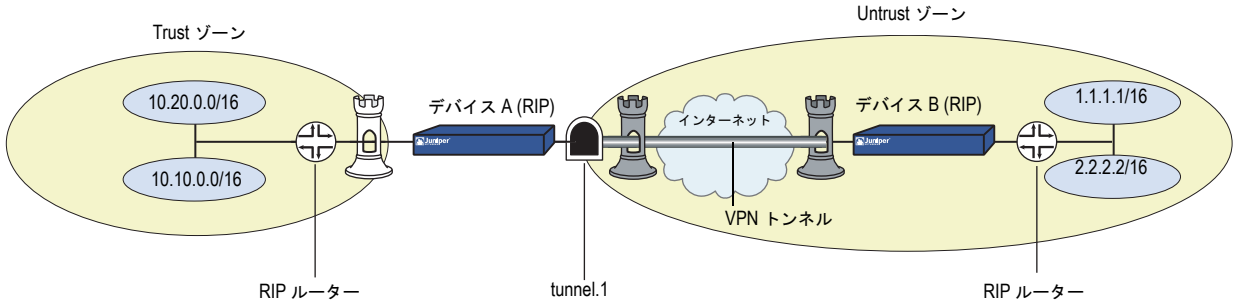
```
set vrouter trust-vr protocol rip threshold-update 4
save
```

トンネルインターフェース上で RIP を稼動させる

この例では、Device-A デバイスの仮想ルーター Trust-VR に、RIP ルーティングインスタンスを作成し、稼動させます。VPN トンネルインターフェースと Trust ゾーンインターフェースの両方について、RIP を有効にします。サブネット 10.10.0.0/16 内のルートだけを、Device-B 上の RIP 隣接ノードに通知します。そのためにまず、サブネット 10.10.0.0/16 に属するアドレスのみを許可するアクセスリストを作ります。次に、ルートマップ *abcd* を指定して、このアクセスリストに合致するルートのみを許可するようにします。最後に、このルートマップを使って、RIP 隣接ノードに通知するルートを分別します。

図 13 は説明したネットワークシナリオを示します。

図 13: RIP を使ったトンネルインターフェース



WebUI

Network > Routing > Virtual Router > Edit (trust-vr) > Create RIP Instance: **Enable RIP** を選択して **OK** をクリックします。

Network > Routing > Virtual Router > Access List (trust-vr) > New: 次のように入力してから **OK** をクリックします。

Access List ID: 10
Sequence No.: 10
IP/Netmask: 10.10.0.0/16
Action: Permit

Network > Routing > Virtual Router > Route Map (trust-vr) > New: 次のように入力してから **OK** をクリックします。

Map Name: abcd
Sequence No.: 10
Action: Permit
Match Properties:
Access List: (選択), 10

Network > Routing > Virtual Router > Edit (trust-vr) > Edit RIP Instance: 次のように選択してから **OK** をクリックします

Outgoing Route Map Filter: abcd

Network > Interfaces > Edit (tunnel.1) > RIP: 以下を入力して **Apply** をクリックします。

Enable RIP: (選択)

Network > Interfaces > Edit (trust) > RIP: 以下を入力して **Apply** をクリックします。

Enable RIP: (選択)

CLI

```
set vrouter trust-vr protocol rip
set vrouter trust-vr protocol rip enable
set interface tunnel.1 protocol rip enable
set interface trust protocol rip enable
set vrouter trust-vr access-list 10 permit ip 10.10.0.0/16 10
set vrouter trust-vr route-map name abcd permit 10
set vrouter trust-vr route-map abcd 10 match ip 10
set vrouter trust-vr protocol rip route-map abcd out
save
```

オプションの RIP 構成

このセクションでは、構成可能な RIP 機能について説明します。

RIP バージョンの構成

Juniper Networks セキュリティデバイスでは、仮想ルーターおよび更新の送受信を行う各ルーティング情報プロトコル (RIP) インターフェースに対して、RIP プロトコルのバージョンを設定することができます。RFC 2453 ごとに、仮想ルーターは特定のインターフェース上で稼働している RIP のインスタンスとは異なる RIP のバージョンを実行します。また、RIP インターフェース上で更新を送受信する、別の RIP バージョンも設定できます。

仮想ルーターでは、RIP のバージョン 1 または 2 を設定できますが、デフォルトはバージョン 2 です。RIP インターフェース上での更新の送信には、バージョン 1、バージョン 2、またはバージョン 1 互換モードのいずれかを設定できます (RFC 2453 に記載)。RIP インターフェース上での更新の受信には、RIP バージョン 1、2、またはその両方のいずれかを設定できます。

注 : ただし、バージョン 1 と 2 の両方を同時に使用することは推奨していません。プロトコルのバージョン 1 と 2 の間でネットワークに問題が起きるおそれがあります。

RIP インターフェース上での更新の送受信については、RIP プロトコルのデフォルトのバージョンが仮想ルーターに設定されます。

次の例では、trust-vr 上で RIP プロトコルのバージョンを 1 に設定しています。interface ethernet3 では、更新の送受信両方にバージョン 2 を設定しています。

WebUI

Network > Routing > Virtual Router > Edit (trust-vr) > Edit RIP Instance: バージョンに V1 を選択し、**Apply** をクリックします。

Network > Interfaces > Edit (for ethernet3) > RIP: Sending and Receiving in Update Version に V2 を選択し、**Apply** をクリックします。

CLI

```
set vrouter trust-vr protocol rip version 1
set interface ethernet3 protocol rip receive-version v2
set interface ethernet3 protocol rip send-version v2
save
```

仮想ルーターおよび RIP インターフェースの RIP バージョンを確認するには、**get vrouter trust-vr protocol rip** コマンドを入力します。

```
device-> get vrouter trust-vr protocol rip
VR: trust-vr
---------------------------------
State: enabled
Version: 1
Default metric for routes redistributed into RIP: 10
Maximum neighbors per Interface: 512
Not validating neighbor in same subnet: disabled
Next RIP update scheduled after: 14 sec
Advertising default route: disabled
Default routes learnt by RIP will be accepted
Incoming routes filter and offset-metric: not configured
Outgoing routes filter and offset-metric: not configured
Update packet threshold is not configured
Total number of RIP interfaces created on vr(trust-vr): 1
Update Invalid Flush (Timers in seconds)
-------------------------------------------------------------
    30     180   120
Flags: Split Horizon - S, Split Horizon with Poison Reverse - P, Passive - I
       Demand Circuit - D
Interface   IP-Prefix        Admin      State    Flags   NbrCnt Metric Ver-Rx/Tx
-------------------------------------------------------------------------------
ethernet3   20.20.1.2/24     enabled    enabled  S            0      1   2/2
```

上記の例では、trust-vr 上では RIP バージョン 1 が稼働していますが、更新の送受信の ethernet3 インターフェースではバージョン 2 が稼働しています。

プレフィックスサマリを使用不可・可能にする

RIP が通知するルートプレフィックスの範囲を含むサマリルートを設定することができます。セキュリティデバイスは、サマリの範囲内にあるルートごとに通知するのではなく、その範囲に対応する 1 ルートにのみ通知します。これにより、RIP の更新で送信されるルートエントリの数と、RIP 隣接ノードがルーティングテーブルに保存する必要のあるエントリ数を減らすことができます。デバイスが送信する場所からの RIP インターフェースのルート要約を有効にしてください。別のインターフェース上では要約せず、1 つのインターフェース上でのみ要約して、ルートを送信することもできます。

注： 特定のサマリ範囲の要約を選択的に有効にすることはできません。あるインターフェース上の要約を有効にすると、設定したサマリルートはすべてルーティングの更新に表示されます。

サマリルートを設定すると、オーバーラップする複数のプレフィックスの範囲は指定できません。また、デフォルトルートを含むプレフィックスの範囲も指定できません。オプションで、サマリルートのメトリックを指定することができます。メトリックを指定しない場合は、サマリの範囲内にある全ルートの中で最も大きなメトリックを使用します。

要約したルートにより、ループが発生する場合もあります。ループを防ぐには、NULL インターフェースへのルートを設定します。NULL インターフェースの設定の詳細については、12 ページの「ルートの要約により生じたループを防ぐ」を参照してください。

プレフィックスサマリを有効にする

以下の例では、プレフィックス 10.1.1.0/24 および 10.1.2.0/24 を含むサマリルート 10.1.0.0/16 を設定しています。RIP の更新で ethernet3 がサマリルートを送信できるようにするには、インターフェース上での要約を有効にする必要があります。

WebUI

Network > Routing > Virtual Routers > Edit (for trust-vr) > Edit RIP Instance > Summary IP: 次のように入力してから **Add** をクリックします。

Summary IP: 10.1.0.0
Netmask: 16
Metric: 1

Network > Interface > Edit (for ethernet3) > RIP: **Summarization** を選択して **Apply** をクリックします。

CLI

```
set vrouter trust-vr protocol rip summary-ip 10.1.0.0/16
set interface ethernet3 protocol rip summary-enable
save
```

プレフィックスサマリを使用不可にする

以下の例では、trust-vr 上で ethernet3 のプレフィックスサマリを使用不可にしています。

WebUI

Network > Interfaces > Edit > RIP: **Summarization** を選択解除し、**Apply** をクリックします。

CLI

```
unset vrouter trust-vr protocol rip summary-ip 10.1.0.0/16
unset interface ethernet3 protocol rip summary-enable
save
```

代替ルートを設定する

セキュリティデバイスは、プロトコルが学習したルートの RIP データベースと RIP に再配布されるルートを維持します。デフォルトでは、プレフィックスの中で最良のルートのみをデータベースに維持します。RIP データベースに入れることのできる同一プレフィックスの代替 RIP ルートが 1、2、または 3 つかを指定することができます。RIP データベース内のプレフィックスの代替ルートを使用できるようにすると、別の次のホップ点や RIP ソースを持つ同一プレフィックスへのルートがデータベースに追加されます。これにより、RIP は要求回路と迅速なフェールオーバーに対応します。

注 : 弊社は、要求回路に代替ルートを使用するよう推奨しています。要求回路の詳細については、99 ページの「トンネルインターフェースの要求回路」を参照してください。

プレフィックスの中で RIP データベース内にある最良のルートのみが仮想ルーターのルーティングテーブルに追加され、RIP 更新に通知されます。仮想ルーターのルーティングテーブルから最良のルートを削除すると、RIP はデータベースから 2 番目に良いルートを追加します。既存のルートより良い、新しいルートがデータベースに追加されると、そのルートを使用するようルーティングテーブルを更新し、古いルートの使用を停止します。古いルートをデータベースから削除するかどうかは、設定した代替ルートの制限によります。

RIP データベースは、次の CLI コマンドによって参照することができます。**get vrouter** *vrouter* **protocol rip database**。以下の例では、データベースの代替ルートの数が 0 より大きい値に設定されています。プレフィックス 10.10.70.0/24 のエントリは、コスト 2 と 4 の 2 つがあります。プレフィックスの最良ノート、最もコストの低いルートは仮想ルーターのルーティングテーブル内にあります。

```
device-> get vrouter trust-vr protocol rip database
VR: trust-vr
--------------------------------------------------------------------------------
Total database entry: 14
Flags: Added in Multipath - M, RIP - R, Redistributed - I
       Default (advertised) - D, Permanent - P, Summary - S
       Unreachable - U, Hold - H
DBID   Prefix               Nexthop            Interface  Cost Flags Source
--------------------------------------------------------------------------------
                                        .
                                        .
                                        .
  47   10.10.70.0/24         10.10.90.1         eth4          2 MR    10.10.90.1
  46   10.10.70.0/24         10.10.90.5         eth4          4 R     10.10.90.5
                            .
                            .
```

等価コストマルチパスルーティング (ECMP) が有効になっており (38 ページの「等価コストマルチパスルーティングの構成」を参照)、指定プレフィックスの等価コストの複数のルートがデータベース内にある場合、ルーティングテーブルに ECMP の最大限までルートを追加します。代替ルートの制限によっては、ルートをルーティングテーブルに追加できない場合もあります。ECMP の制限が代替ルート以下の場合、ルーティングテーブルに追加されない RIP ルートは、データベース内に残ります。そして、以前追加されたルートが削除されるか、またはネットワークプレフィックスの「最良」RIP ルートでなくなった場合にのみ、テーブルに追加されます。

例えば、ECMP の制限が 2 で、データベースの代替ルートが 3 の場合、ルーティングテーブルに追加できる、同一コストで同一プレフィックスのルートは、2 つだけです。同一プレフィックス、同一コストのルートがデータベースにあっても構いませんが、仮想ルーターのルーティングテーブルに追加できるのは 2 つだけとなります。

以下の例では、trust-vr のデータベース内のプレフィックスの代替ルート数を 1 に設定しています。これにより、いずれのプレフィックスも、「最良」ルート数および代替ルート数は 1 となります。

WebUI

Network > Routing > Virtual Routers > Edit (for trust-vr) > Edit RIP Instance: Maximum Alternative Route フィールドに **1** と入力して、**Apply** をクリックします。

CLI

```
set vrouter trust-vr protocol rip alt-route 1
save
```

トンネルインターフェースの要求回路

要求回路とは、2 つのトンネルインターフェース間にあるポイントツーポイント接続です。メッセージに関する最小限のネットワークオーバーヘッドが、要求回路の終点間を通過します。RIP の要求回路は、RFC 2091 によってワイドエリアネットワーク (WAN) 用に定義され、Juniper Networks セキュリティデバイス上の VPN トンネルにある大容量の RIP 隣接ノードをサポートします。

要求回路を使用すると、トンネルインターフェースでの RIP パケットの定期的な送信がなくなります。オーバーヘッドをなくすため、セキュリティデバイスは、ルーティングデータベースが変更された場合にのみ RIP 情報を送信します。また、有効な肯定応答を受信するまで、更新情報と要求も送信します。セキュリティデバイスは、静的隣接ノードの設定から RIP 隣接ノードを学習し、VPN トンネルがダウンすると、そのルートを消去します。

要求回路は永続状態にあるため、要求回路から学習したルートは RIP タイマーと同じ時間にはなりません。永続状態にあるルートは、以下の条件で削除することができます。

- 以前アクセス可能だったルートが、受信応答で宛先不明に変わった場合
- 未確認の再送信数が多すぎるために、VPN トンネルか要求回路がダウンした場合

セキュリティデバイスでは、要求回路としてポイントツーポイントまたはポイントツーマルチポイントのトンネルインターフェースを設定することもできます。ポイントツーマルチポイントの route-deny オプションは無効にして (設定している場合)、全ルートがリモートサイトにアクセスできるようにしてください。必須ではありませんが、ポイントツーマルチポイントの split horizon オプションを無効にすることもできます。split horizon を無効にすると、終点同士が学習するようになります。

トンネル状態を学習するには、VPN トンネルで VPN 監視に再入力オプションを設定します。

要求回路と静的隣接ノードを設定すると、ネットワークの必要条件に準拠させる RIP retransmit-timer、poll-timer、hold-down-timer を設定できます。

設定方法の例については、このセクションの後半で説明します。ポイントツーマルチポイントトンネルインターフェースでの要求回路の RIP ネットワーク設定例については、100 ページを参照してください。

以下の例では、要求回路として *tunnel.1* インターフェースを設定し、保存します。

WebUI

Network > Interfaces > Edit > RIP: **Demand Circuit** を選択し、**Apply** をクリックします。

CLI

```
set interface tunnel.1 protocol rip demand-circuit
save
```

要求回路を有効にすると、**get vrouter** *vrouter* **protocol rip database** コマンドを使用して、そのステータスとタイマーをチェックすることができます。表 12 はタイマー設定により影響される、性能問題のトラブルシューティングを列挙します。

表 12: 要求回路 Retransmit タイマーのトラブルシューティング

要求回路のパフォーマンス	提案
Relatively slow	retransmit timer をより高い値に再設定して、再送信回数を減らすことができます。
Loss free	retransmit timer の再試行回数を減らすことができます。
Congested and lossy	retransmit timer の再試行回数を増やして、静的隣接ノードが POLL 状態になる前に応答時間を長くすることができます。

静的隣接ノードの構成

RIP の稼働しているポイントツーマルチポイントインターフェースには、静的隣接ノードが構成されている必要があります。要求回路では、セキュリティデバイスに隣接ノードのアドレスを学習させるには、手動で構成するしかありません。RIP 静的隣接ノードを構成するには、インターフェース名と IP アドレスを入力します。

以下の例では、tunnel.1 インターフェースの IP アドレス 10.10.10.2 における隣接ノードを設定しています。

WebUI

Network > Interfaces > (Edit) RIP: **Static Neighbor IP** ボタンをクリックして、静的隣接ノード IP テーブルに進みます。隣接ノードの IP アドレスを入力して、**Add** をクリックします。

CLI

```
set interface tunnel.1 protocol rip neighbor 10.10.10.2
unset interface tunnel.1 protocol rip neighbor 10.10.10.2
save
```

ポイントツーマルチポイントトンネルインターフェースの構成

RIP バージョン 1 および 2 の番号の付いたトンネルインターフェースでは、ポイントツーマルチポイントがサポートされています。

注意 :RIP は番号付けされていないトンネルインターフェースではサポートされていません。RIP プロトコルを使用するインターフェースは番号付けする必要があります。番号付けされていないインターフェースを RIP を使って構成・実行しようとすると、予測できないルーティング障害が起きることがあります。

要求回路の有無を設定するポイントツーマルチポイントインターフェーストンネルでは、split horizon を無効にして、メッセージが全リモートサイトに到着するようにします。要求回路のないポイントツーマルチポイントトンネルインターフェースでは、split horizon を無効（デフォルト）のままにしておきます。RIP は隣接ノードを動的に学習します。送信メッセージはすべてマルチキャストアドレス 224.0.0.9 に送信され、必要に応じて、全トンネルに再複製されます。

RIP を要求回路でポイントツーマルチポイントトンネルとして設定する場合は、ネットワークはハブアンドスポーク構成で設計してください。

注 : この例では、コマンドラインインターフェースのみ参照します。そしてゾーンやその他に必要な構成手順については触れません。

この例は、中央オフィス (CO) をサンフランシスコに、リモートサイトをシカゴ、ロサンゼルス、モントリオール、ニューヨークに持つ中規模企業のネットワークです。各オフィスには、1 台のセキュリティデバイスが設置されています。102 ページの図 14 を参照してください。

以下の項目は、CO のセキュリティデバイスに特に必要な設定条件です。

1. 仮想ルーターは、RIP インスタンスが稼働するよう設定し、RIP を有効にします。さらに、tunnel.1 インターフェースを設定します。
2. VPN を 4 つ設定し、tunnel.1 インターフェースにバインドします。
3. CO のセキュリティデバイスに RIP 静的隣接ノードを設定します。
4. この例では、デフォルトのタイマーの値は変更しません。

以下の項目は、リモートサイトの Juniper Networks セキュリティデバイスに特に必要な設定条件です。

1. 仮想ルーターは、RIP インスタンスが稼働するよう設定し、RIP を有効にします。さらに、tunnel.1 インターフェースを設定します。
2. VPN を設定し、tunnel.1 インターフェースにバインドします。
3. リモートオフィスのデバイスには、静的隣接ノードを設定しません。最初のマルチキャスト要求で見つかる隣接デバイスは 1 つだけです。

注 : この例では、デフォルトのタイマーの値を変更する必要はありません。

図 14: トンネルインターフェースネットワークでのポイントツーマルチポイント例

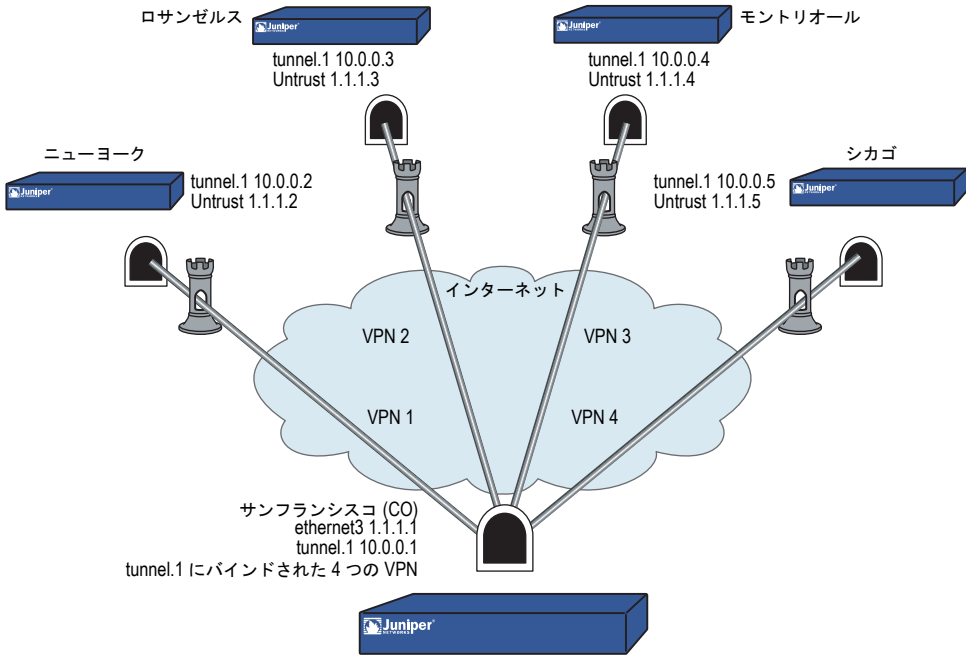


図 14 に示されているネットワーク図では、サンフランシスコのセキュリティデバイスから 4 つの VPN が出ており、ニューヨーク、ロサンゼルス、モントリオール、シカゴのリモートオフィスに放射状に伸びています。

この例では、CO のセキュリティデバイスに以下の項目を設定しています。

1. セキュリティゾーンおよびインターフェース
2. VPN
3. ルートおよび **RIP**
4. 静的隣接ノード
5. 要約ルート

CO にあるデバイスの回路のステータスをチェックするには、VPN の監視を有効にしてください。

ネットワークの設定を終了するには、4 つの各リモートオフィスのデバイスに以下の設定を行います。

1. セキュリティゾーンおよびインターフェース
2. VPN
3. ルートおよび RIP
4. 静的隣接ノード
5. 要約ルート

注 : WebUI 手順は、例が長すぎないようにするため、省略されています。CLI については完全な例を示します。具体的なパラメータ値については、CLI の例を参照してください。

WebUI (中央オフィスのデバイス)

1. セキュリティゾーンおよびインターフェース

Network > Interfaces > **New Tunnel IF** をクリック して、構成ページに進む。

Network > Interfaces > Edit (ethernet3)

2. VPN

VPNs > AutoKey Advanced > Gateway

3. ルートおよび RIP

Network > Routing > Virtual Routers > 仮想ルーターの **Edit** をクリックして次に **Create RIP Instance** をクリックし、仮想ルーターの RIP を使用可能にします。

Network > Interfaces > Edit > **Edit** をクリックし、次に **RIP** をクリックして RIP をインターフェース上で使用可能にします。

4. 静的隣接ノード

Network > Interfaces > Edit > RIP > Static Neighbor IP そして次に **Add Neighbor IP Address.**

5. 要約ルート

Network > Routing > Virtual Router Edit (RIP) > に続いて **Summary IP** をクリックし、サマリ IP アドレスを構成します。

CLI (中央オフィスのデバイス)

1. セキュリティゾーンおよびインターフェース

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.0.0.1/24
```

2. VPN

```
set ike gateway gw1 address 1.1.1.2 main outgoing-interface ethernet3 preshare
    ripdc proposal pre-g2-3des-sha
```

```
set ike gateway gw2 address 1.1.1.3 main outgoing-interface ethernet3 preshare
    ripdc proposal pre-g2-3des-sha
set ike gateway gw3 address 1.1.1.4 main outgoing-interface ethernet3 preshare
    ripdc proposal pre-g2-3des-sha
set ike gateway gw4 address 1.1.1.5 main outgoing-interface ethernet3 preshare
    ripdc proposal pre-g2-3des-sha

set vpn vpn1 gateway gw1 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn1 monitor rekey
set vpn vpn1 bind interface tunnel.1

set vpn vpn2 gateway gw2 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn2 monitor rekey
set vpn vpn2 bind interface tunnel.1

set vpn vpn3 gateway gw3 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn3 monitor rekey
set vpn vpn3 bind interface tunnel.1

set vpn vpn4 gateway gw4 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn4 monitor rekey
set vpn vpn4 bind interface tunnel.1
```

3. **ルートおよび RIP**

```
set vrouter trust protocol rip
set vrouter trust protocol rip enable
set vrouter protocol rip summary-ip 100.10.0.0/16

set interface tunnel.1 protocol rip
set interface tunnel.1 protocol rip enable
set interface tunnel.1 protocol rip demand-circuit
```

4. **静的隣接ノード**

```
set interface tunnel.1 protocol rip neighbor 10.0.0.2
set interface tunnel.1 protocol rip neighbor 10.0.0.3
set interface tunnel.1 protocol rip neighbor 10.0.0.4
set interface tunnel.1 protocol rip neighbor 10.0.0.5
```

5. **要約ルート**

```
set interface tunnel.1 protocol rip summary-enable
save
```

この手順に従って、リモートオフィスのセキュリティデバイスの設定を行います。リモートオフィスの設定では、静的隣接ノードを設定する必要はありません。要求回路の環境では、リモートデバイスにある隣接ノードは 1 つだけで、起動時にマルチキャストメッセージを送信すると、リモートデバイスはこのノードの情報を学習します。

102 ページの図に示した設定を完了するには、各リモートデバイスについてこのセクションの設定を繰り返して行い、ネットワークに合うように IP アドレス、ゲートウェイの名前、VPN の名前を変更してください。リモートサイトごとに、trust および untrust ゾーンは異なります。

注： WebUI 手順は、例が長すぎないようにするため、省略されています。CLI については完全な例を示します。具体的なパラメータ値については、CLI の例を参照してください。

WebUI (リモートオフィスのデバイス)

1. **セキュリティゾーンおよびインターフェース**
   Network > Interfaces > **New Tunnel IF** をクリック して、構成ページに進む。

   Network > Interfaces > Edit (ethernet3)

2. **VPN**
   VPNs > AutoKey Advanced > Gateway

3. **ルートおよび RIP**
   Network > Routing > Virtual Routers > 仮想ルーターの **Edit** をクリックして次に **Create RIP Instance** をクリックし、仮想ルーターの RIP を使用可能にします。

   Network > Interfaces > Edit > **Edit** をクリックし、次に RIP をクリックして RIP をインターフェース上で使用可能にします。

4. **ポリシー (必要に応じて設定)**
   ポリシー (All zones から All zones) > New をクリック。

CLI (リモートオフィスのデバイス)

1. **インターフェースおよびルーティングのプロトコル**
   ```
   set vrouter trust-vr protocol rip
   set vrouter trust-vr protocol rip enable
   set interface untrust ip 1.1.1.1/24
   set interface tunnel.1 zone untrust
   set interface tunnel.1 ip 10.0.0.2/24
   ```

2. **VPN**
   ```
   set ike gateway gw1 address 1.1.1.1/24 main outgoing-interface untrust preshare
       ripdc proposal pre-g2-3des-sha
   set vpn vpn1 gateway gw1 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
   set vpn vpn1 monitor rekey
   set vpn vpn1 id 1 bind interface tunnel.1
   ```

3. **ルートおよび RIP**
   ```
   set interface tunnel.1 protocol rip
   set interface tunnel.1 protocol rip demand-circuit
   set interface tunnel.1 protocol rip enable
   ```

4. **ポリシー (必要に応じて設定)**
   ```
   set policy id 1 from trust to untrust any any any permit
   set policy id 2 from untrust to trust any any any permit
   save
   ```

変更後の設定内容は、**get vrouter** *vrouter* **protocol rip neighbors** コマンドで確認できます。要求回路の隣接ノードは、neighbor table に表示され、この情報は古くならず、また期限切れにもなりません。RIP データベースは、**get vrouter** *vrouter* **protocol rip database** コマンドで確認できます。*permanent* の場合は、要求回路のエントリの横に *P* と表示されます。

第 5 章

境界ゲートウェイプロトコル

本章では、Juniper Networks セキュリティデバイス上の境界ゲートウェイプロトコル (BGP) について説明します。本章のセクションは、以下のようになります。

- 108 ページの「概要」
  - 108 ページの「BGP メッセージのタイプ」
  - 109 ページの「パス属性」
  - 109 ページの「外部および内部 BGP」
- 110 ページの「基本的な BGP 構成」
  - 111 ページの「BGP インスタンスを作成して使用可能にする」
  - 112 ページの「BGP をインターフェースで使用可能・不可にする」
  - 113 ページの「BGP ピアおよびピアグループの構成」
  - 116 ページの「BGP 構成を確認する」
- 117 ページの「セキュリティ構成」
  - 117 ページの「BGP 近隣ノードを認証する」
  - 118 ページの「デフォルトルートを拒否する」
  - 120 ページの「ルートを BGP へ再配布する」
  - 120 ページの「AS-Path アクセスリストの構成」
  - 121 ページの「BGP にルートを追加」
  - 123 ページの「Route-Refresh 機能」
  - 125 ページの「ルートリフレクションを構成する」
  - 127 ページの「コンフェデレーションの構成」
  - 128 ページの「BGP コミュニティ」
  - 129 ページの「ルートの集約」

概要

Border Gateway Protocol (境界ゲートウェイプロトコル) は、ルーティング情報を AS (自律システム) 間で伝えるためのパスベクトルプロトコルです。AS は、同一の管理ドメイン内にあるルーターの一式です。

BGP ルーティング情報には、ネットワークプレフィックス (ルート) が行き来した AS 番号のシーケンスが含まれます。このパス情報はプレフィックスに関連付けられており、ループ防止を可能にし、ルーティングポリシーを施行するために使用されます。ScreenOS は、RFC 1771. に定義されている BGP バージョン 4 (BGP-4) をサポートしています。

2 つの *BGP ピア*が、ルーティング情報を交換するために *BGP セッション*を確立します。BGP ルーターは、別のピアとの BGP セッションに参加できます。BGP ピアは、最初に自分たちの間に TCP 接続を確立して GP セッションを開く必要があります。最初の接続がつくられると、ピアはルーティングテーブルをまるごと交換します。ルーティングテーブルに変更が生じるとき、BGP ルーターは更新メッセージをピアと交換します。BGP ルーターは、セッションがある、すべてのピアのルーティングテーブルの最新バージョンを保持します。BGP ルーターはこれらのピアとセッションを維持し、定期的にキープアライブメッセージをピアに送信して、接続を確認します。

BGP ピアは、自分が積極的に使用しているルートだけをアドバタイズ (通知) します。BGP ピアはルートを近隣ノードに自分の接続デバイスを通知するとき、そのルートの特性を説明するパス属性も含めます。BGP ルーターはパス属性とプレフィックスを比較して、所定の宛先へ向かうのに使用できるあらゆるパスの中から最適なルートを選びます。

BGP メッセージのタイプ

BGP は、次の 4 種類のメッセージタイプを使用してピアと情報をやりとりします。

- **Open** メッセージは、BGP ピアを互いに識別して BGP セッションを開始します。これらのメッセージは、ピアが TCP セッションを確立した後で送信されます。オープンメッセージの交換中、BGP ピアは自分たちのプロトコルバージョン、AS 番号、保持時間、および BGP 識別子を指定します。
- **Update** メッセージは、ピアへのルートを公表し、それまでにアドバタイズ (通知) したルートを取り消します。
- **Notification** メッセージは、エラーを知らせます。BGP セッションは終了し、その TCP セッションは閉じます。

注 : オープンメッセージの交換中、あるピアが、自分がサポートしているプロトコル機能をセキュリティデバイスがサポートしないことを知らせると、セキュリティデバイスは通知メッセージをこのピアに送信しません。

- **Keepalive** メッセージは、BGP セッションを保持するために使用します。セキュリティデバイスはデフォルトで、キープアライブメッセージをピアに 60 秒間隔で送信します。この間隔は設定可能です。

パス属性

BGP パス属性は、ルートの特性を説明するパラメータのセットです。BGP はこれらの属性と説明するルートをペアにし、ある宛先へ向かうのに使用できるすべてのパスを比較して、その宛先に達するのに最適なルートを選び出します。一般に使われる必須パス属性として次のようなものがあります。

- **Origin** は、ルートがどこで得られたかを表し、可能な値は IGP、EGP、Incomplete のいずれかです。
- **AS-Path** には、ルートのアドバタイズメント (通知) 情報が経由した自律システムのリストが含まれます。
- **Next-Hop** は、ルートのトラフィックの送信先となるルーターの IP アドレスです。

必要に応じて、次のパス属性も設定できます。

- **Multi-Exit Discriminator** (MED) は、AS 間に複数のリンクがあるパスのためのメトリックです (MED は一方の AS が設定し、別の AS がパスを選択するために使用します)。
- **Local-Pref** は、BGP ピアに、ルートに対するローカルルーターの優先権を知らせるために使用するメトリックです。
- **Atomic-Aggregate** は BGP ピアに、あるピアから受け取った重複するルートのセットの中から特定の少ないルートをローカルルーターが選んだことを通知します。
- **Aggregator** は、ルートの集約を行った AS やルーターを示します。
- **Communities** は、このルートが属する 1 つ以上のコミュニティを示します。
- **Cluster List** には、ルートが経由してきたリフレクタクラスタのリストが含まれます。

BGP ルーターは、ルートをピアに通知する前にオプションのパス属性の追加や変更を選択できます。

外部および内部 BGP

EBGP (外部 BGP) は、異なる ISP ネットワークが互いに接続するときや企業ネットワークが ISP ネットワークするときのように、自律システム間で使用します。IBGP (内部 BGP) は、企業ネットワーク内のように AS の内部で使用します。IBGP の主要目的は、EBGP から得たルートを AS 内のルーターへ配布することです。IBGP ルーターはその EBGP ピアから得たルートを IBGP ピアへ再通知できますが、IBGP ピアから得たルートを別の IBGP ピアには通知できません。この制限により、ネットワーク内でルートアドバタイズメントにループが生じるのを防いでいますが、IBGP ネットワークが完全メッシュでなければならないことを意味します (つまり、ネットワーク内のすべての BGP ルーターは、ネットワーク内の他のすべてのルーターとセッションを持たなければなりません)。

一部のパス属性は、EBGP または IBGP だけに適用可能です。たとえば、MED 属性は EBGP メッセージだけに使われ、LOCAL-PREF 属性は IBGP メッセージ内だけに存在します。

基本的な BGP 構成

セキュリティデバイスでは、仮想ルーター (VR) ごとに BGP インスタンスの設定をするようになっています。デバイスに複数の VR がある場合、各 VR にインスタンスを 1 つずつ、複数の BGP のインスタンスを使用可能にすることができます。

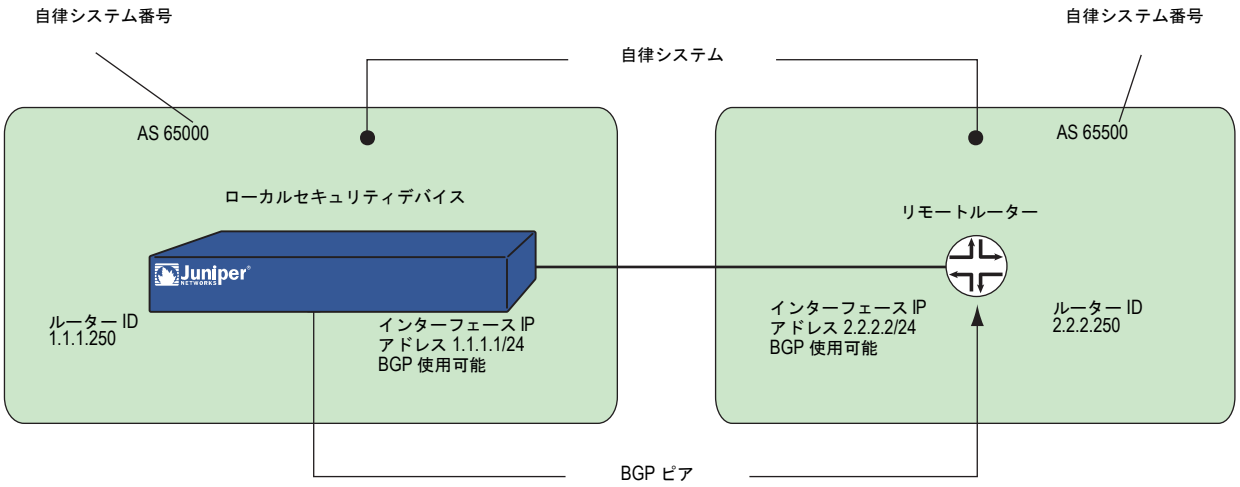
注： 動的ルーティングプロトコルをセキュリティデバイス上で構成する前に、仮想ルーター ID を第 2 章、「ルーティング」の説明にしたがって割り当てる必要があります。

セキュリティデバイス上の VR に BGP の設定をする際は、次の 5 段階で進めます。

1. BGP ルーティングインスタンスを VR 内で作成して使用可能にするために、最初に自律システム番号を BGP インスタンスに割り当て、次にこの BGP インスタンスを使用可能にします。
2. ピアに接続されているインスタンスの BGP を使用可能にします。
3. 各 BGP ピアを使用可能にします。
4. 1 つ以上のリモート BGP ピアを構成します。
5. BGP が正しく構成されて作動していることを確認します。

このセクションは、次の例に対して CLI または WebUI を使用して実行する方法を説明します。図 15 は AS 65000 において、セキュリティデバイスを BGP ピアとして示しています。セキュリティデバイスを構成して、AS 65500 のピアと BGP セッションを確立します。

図 15: BGP 構成例



BGP インスタンスを作成して使用可能にする

セキュリティデバイス上の特定の仮想ルーター (VR) に BGP ルーティングインスタンスを作成して使用可能にします。BGP ルーティングインスタンスを作成するには、最初に VR が存在する自律システム番号を指定する必要があります VR が IBGP ルーターの場合、自律システム番号は ネットワーク内の他の IBGP ルーターと同じにする必要があります。VR の BGP ルーティングインスタンスを使用可能にすると、この BGP ルーティングインスタンスは構成する BGP ピアと接触してセッションを確立可能になります。

注 : 自律システム (AS) 番号は、EBGP ルーティング情報の交換と AS の識別に使用する全体で一意の番号です。AS 番号を割り当てる団体としては、American Registry for Internet Numbers (ARIN)、Réseaux IP Européens (RIPE)、そして Asia Pacific Network Information Center (APNIC) があります。64512 ～ 65535 の番号は民間で使用されるため、インターネットではアドバタイズされません。

BGP ルーティングインスタンスを作成する

次の例では、最初に 0.0.0.10 を trust-vr のルーター ID として割り当てます。次に、AS 65000 のセキュリティデバイスに存在する trust-vr の BGP ルーティングインスタンスを作成して使用可能にします。(仮想ルーターとセキュリティデバイスでの仮想ルーターの構成の詳細は、15 ページの「ルーティング」を参照してください。

WebUI

1. **ルーター ID**
   Network > Routing > Virtual Router (trust-vr) > Edit: 次のように入力してから **OK** をクリックします。

   Virtual Router ID: Custom (**選択**)
   テキストボックスに 0.0.0.10 を入力します。

2. **BGP ルーティングインスタンス**
   Network > Routing > Virtual Routers > Edit (trust-vr) > Create BGP Instance: 次のように入力してから **OK** をクリックします。

   AS Number (**必須**): 65000
   BGP Enabled: (**選択**)

CLI

1. **ルーター ID**
   set vrouter trust-vr router-id 10

2. **BGP ルーティングインスタンス**
   set vrouter trust-vr protocol bgp 65000
   set vrouter trust-vr protocol bgp enable
   save

BGP インスタンスを削除する

この例では、trust-vr の BGP ルーティングインスタンスを使用不可にして削除します。BGP はすべてのピアとのセッションを中止します。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit > Edit BGP Instance: BGP 有効化を選択解除して、**OK** をクリックします。

Network > Routing > Virtual Routers (trust-vr) > Edit: **Delete BGP Instance** を選択し、確認プロンプトで **OK** をクリックします。

CLI

```
unset vrouter trust-vr protocol bgp enable
unset vrouter trust-vr protocol bgp 65000
save
```

BGP をインターフェースで使用可能・不可にする

BGP をピアが存在するインターフェースで使用可能にする必要があります。(デフォルトでは、セキュリティデバイスのインターフェースはいずれのルーティングプロトコルにもバインドされていません。)

BGP をインターフェースで使用可能にする

この例では、BGP をインターフェース ethernet4 で使用可能にします。

WebUI

Network > Interfaces > Edit > BGP: **Protocol BGP enable** を選択して、**OK** をクリックします。

CLI

```
set interface ethernet4 protocol bgp
save
```

BGP をインターフェースで使用不可にする

この例では、BGP をインターフェース *ethernet4* で使用不可にします。BGP を使用可能にした他のインターフェースでは、まだ BGP パケットを送信および処理できるので注意してください。

WebUI

ネットワーク > インターフェース > 構成 (ethernet4): **Protocol BGP enable** を選択解除して、**OK** をクリックします。

CLI

```
unset interface ethernet4 protocol bgp
save
```

BGP ピアおよびピアグループの構成

2 台の BGP デバイスが通信し、ルートを交換する前に、BGP セッションを開始できるように相互を識別する必要があります。BGP ピアの IP アドレスを指定し、セッションを確立して保持するためのパラメータをオプションとして構成する必要があります。ピアは、内部 (IBGP) ピアと外部 (EBGP) ピアのどちらかにできます。EBGP ピアの場合、ピアが存在する自律システムを指定する必要があります。

すべての BGP セッションは、ピアが通知した BGP ピア識別子と AS 番号をチェックすることで認証されます。成功したピアとの接続はログされます。ピア接続に何か異常が発生すると、BGP 通知メッセージがピアへ送信またはピアから受信し、これにより接続は失敗または終了します。

個々のピアアドレスのパラメータを構成できます。またピアを *peer-group* に割り当てることもできます。これにより、ピアグループ全体としてのパラメータを構成可能になります。

注 : ただし、IBGP ピアと EBGP ピアを同じピアグループに割り当てることはできません。

表 13 は、BGP ピアに構成可能なパラメータとデフォルト値を記載しています。「ピア」列の X は個々のピア IP アドレスに構成できるパラメータであることを示し、「ピアグループ」列の X はピアグループに構成できるパラメータであることを示します。

表 13: ピアおよびピアグループパラメータおよびデフォルト値

BGP パラメータ	ピア	ピアグループ	説明	デフォルト値
Advertise default route	X		仮想ルーター内のデフォルトルートを BGP ピアへ通知します。	デフォルトルートは通知されません
EBGP multihop	X	X	ローカル BGP と近隣との間のノード数。	0 (使用不可)
Force connect	X	X	BGP インスタンスは指定したピアとの既存の BGP 接続をドロップして、新しい接続を受け入れます。このパラメータはピア接続のより速い再確立を可能にするため 、停止した後で復帰して BGP ピアを再確立しようとするルーターに接続する場合に便利です。[1]	なし
Hold time	X	X	ピアが停止したと考えられるまでこのピアからのメッセージがなく経過した時間。	180 秒
Keepalive	X	X	キープアライブの送信と送信の間の時間。	保持時間の 1/3
MD5 authentication	X	X	MD-5 認証を構成します。	チェックしたピア識別子と AS 番号のみ
MED	X		MED 属性値を構成します。	0
Next-hop self	X	X	ピアに送信されたルートの場合、Next Hop パス属性はローカル仮想ルーターのインターフェースの IP アドレスに設定されます。	Next Hop 属性は変わりません。
Reflector client	X	X	ローカル BGP がルートリフレクタとして設定された場合、ピアはリフレクタクライアントです。	なし
Reject default route	X		BGP ピアからのデフォルトルート通知を無視します。	ピアからのデフォルトルートはルーティングテーブルへ追加されます。
Retry time	X	X	セッション未遂後の時間で、この時間が経つと BGP セッションが再試行されます。	120 秒

BGP パラメータ	ピア	ピアグループ	説明	デフォルト値
Send community	X	X	コミュニティ属性をピアへ送信します。	コミュニティ属性はピアへ送信されません
Weight	X	X	ローカル BGP とピア間のパスの優先順位。	100

1.**exec neighbor disconnect** コマンドを使用すると、BGP インスタンスに指定したピアとの既存の BGP 接続をドロップさせて新しい接続を受け入れさせることができます。この exec コマンドを実行しても BGP ピアの構成は変わりません。たとえば、この exec コマンドは、ピアに適用されているルートマップの構成を変更する場合に使用できます。

一部のパラメータは、ピアレベルとプロトコルレベルの両方で構成できます (127 ページの「コンフェデレーションの構成」を参照)。たとえば、プロトコルレベルのデフォルト hold-time 値を 180 秒にしながら特定のピアの hold-time 値を 210 秒に構成すると、ピア構成が優先されます。プロトコルレベルとピアレベルで異なる MED 値を設定すると、ピアレベルで設定した MED 値は、これらのピアに通知されたルートにのみ適用されます。

BGP ピアを構成する

次の例では、BGP ピアを構成して使用可能にします。このピアには、次の属性があります。

- IP アドレス 1.1.1.250
- AS 65500 に存在

注 : 構成するそれぞれのピア接続を使用可能にする必要があります。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Neighbors: 次のように入力してから **Add** をクリックします。

AS Number: 65500
Remote IP: 1.1.1.250

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Neighbors > Configure (ここで追加したピアの): **Peer Enabled** を選択し、**OK** をクリックします。

CLI

```
set vrouter trust-vr protocol bgp neighbor 1.1.1.250 remote-as 65500
set vrouter trust-vr protocol bgp neighbor 1.1.1.250 enable
save
```

IBGP ピアグループを構成する

次の例では、**ibgp** という名前で次の IP をもつ IBGP ピアグループを構成します。IP アドレスは 10.1.2.250 と 10.1.3.250 です。ピアグループを定義してしまえば、そのピアグループの全メンバに適用されるパラメータ (MD5 認証など) を構成できます。

注 : 構成するそれぞれのピア接続を使用可能にする必要があります。ピアをピアグループの一部として構成する場合でも、ピア接続を 1 つずつ使用可能にする必要があります。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Peer Group: グループ名に **ibgp** を入力し、**Add** をクリックします。

> 構成 (ibgp): ピア認証フィールドで **verify03** を入力し、**OK** をクリックします。

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Neighbors: 次のように入力してから **Add** をクリックします。

AS Number: 65000
Remote IP: 10.1.2.250
Peer Group: ibgp (**選択する**)

次のように入力してから **Add** をクリックします。

AS Number: 65000
Remote IP: 10.1.3.250
Peer Group: ibgp (**選択する**)

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Neighbors > Configure (10.1.2.250): **Peer Enabled** を選択し、**OK** をクリックします。

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Neighbors > Configure (10.1.3.250): **Peer Enabled** を選択し、**OK** をクリックします。

CLI

```
set vrouter trust-vr protocol bgp neighbor 10.1.2.250 peer-group ibgp
set vrouter trust-vr protocol bgp neighbor peer-group ibgp remote-as 65000
set vrouter trust-vr protocol bgp neighbor peer-group ibgp md5-authentication
    verify03
set vrouter trust-vr protocol bgp neighbor 10.1.2.250 remote-as 65000
set vrouter trust-vr protocol bgp neighbor 10.1.2.250 peer-group ibgp
set vrouter trust-vr protocol bgp neighbor 10.1.3.250 remote-as 65000
set vrouter trust-vr protocol bgp neighbor 10.1.3.250 peer-group ibgp
set vrouter trust-vr protocol bgp neighbor 10.1.2.250 enable
set vrouter trust-vr protocol bgp neighbor 10.1.3.250 enable
save
```

BGP 構成を確認する

WebUI または CLI で設定した内容は、**get vrouter** *vrouter* **protocol bgp config** というコマンドで確認できます。

```
device-> get vrouter trust-vr protocol bgp config
set protocol bgp 65000
set enable
set neighbor peer-group "ibgp"
set neighbor peer-group "ibgp" md5-authentication "cq1tu6gVNU5gvfsO60CsvxVPNnntO
PwY/g=="
set neighbor 10.1.2.250 remote-as 65000
```

アウトプットは続きます。

```
exit
```

仮想ルーター上で BGP が動作していることは、**get vrouter** *vrouter* **protocol bgp** というコマンドで確認できます。

```
device-> get vrouter trust-vr protocol bgp
Admin State:           enable
Local Router ID:       10.1.1.250
Local AS number:       65000
Hold time:             180
Keepalive interval:    60 = 1/3 hold time, default
Local MED is:          0
Always compare MED:    disable
Local preference:      100
Route Flap Damping:    disable
IGP synchronization:   disable
Route reflector:       disable
Cluster ID:            not set (ID = 0)
Confederation based on RFC 1965
Confederation:         disable(confederation ID = 0)
Member AS:             none
Origin default route:  disable
Ignore default route:  disable
```

仮想ルーター (VR) の管理状態やルーター ID など、BGP に特有のパラメータも確認できます。

注： デフォルトを使用せずに、常にルーター ID を明確に割り当てることをお薦めします。ルーター ID の設定については、15 ページの「ルーティング」を参照してください。

BGP ピアまたはピアグループが有効であることを確認し、BGP セッションの状態を調べるには、**get vrouter** *vrouter* **protocol bgp neighbor** というコマンドを実行してください。

```
device-> get vrouter trust-vr protocol bgp neighbor
Peer AS Remote IP   Local IP     Wt Status   State ConnID
  65500 1.1.1.250    0.0.0.0    100 Enabled ACTIVE  up
total 1 BGP peers shown
```

この例では BGP ピアが有効であること、セッションがアクティブであることを確認します。

セッションの状態は、次のいずれかです。

- **Idle** - 接続の最初の状態
- **Connect** - BGP は、正常な TCP トランスポート接続を待っています
- **Active** - BGP はトランスポート接続を起動中です
- **OpenSent** - BGP は、ピアからの OPEN メッセージを待っています
- **OpenConfirm** - BGP は、ピアからの KEEPALIVE メッセージか NOTIFICATION メッセージを待っています
- **Established** - BGP はピアと UPDATE パケットを交換中です

注 : セッション状態が Active と Connect の間で継続的に変わる場合は、ピア間の接続に問題があることを示す場合があります。

セキュリティ構成

このセクションでは、BGP ルーティングドメインで起こりうるセキュリティ問題と、攻撃を防御する方法について説明します。

注 : BGP をより安全にするために、BGP ドメイン内のすべてのルーターを同じセキュリティレベルに構成しなければなりません。でないと、欠陥のある BGP ルーターによって BGP ルーティングドメイン全体が停止してしまう可能性があります。

BGP 近隣ノードを認証する

BGP パケットは暗号化されておらず、ほとんどのプロトコルアナライザーが BGP パケットの脱カプセル化を備えているため、BGP ルーターは容易にスプーフィング可能です。こうした種類の攻撃をかわすには、BGP ピアを認証するのが最もよい方法です。

BGP は、ピアから受信した BGP パケットを確認する MD5 認証を備えています。MD5 認証を行うと、送信側と受信側の両 BGP ルーターが同じ鍵を使用していなければなりません。指定したピアから受信した BGP パケットは、そのピアが認証されなければすべて破棄されます。デフォルトでは、BGP ピアのピア識別子と AS 番号だけがチェックされます。

次の例では、最初に BGP ピアを AS 65500 のリモート IP アドレス 1.1.1.250 を使用して構成します。それから、MD5 認証のピアを鍵 1234567890123456 を使用して構成します。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Neighbors: 次のように入力してから **Add** をクリックします。

AS Number: 65500
Remote IP: 1.1.1.250

> Configure (Remote IP 1.1.1.250): 次のように入力してから **OK** をクリックします。

Peer Authentication: Enable (選択)
MD5 password: 1234567890123456
Peer Enabled: (選択)

CLI

```
set vrouter trust-vr
(trust-vr)-> set protocol bgp
(trust-vr/bgp)-> set neighbor 1.1.1.250 remote-as 65500
(trust-vr/bgp)-> set neighbor 1.1.1.250 md5-authentication 1234567890123456
(trust-vr/bgp)-> set neighbor 1.1.1.250 enable
(trust-vr/bgp)-> exit
(trust-vr)-> exit
save
```

デフォルトルートを拒否する

Route Detour Attack では、あるルーターがデフォルトルート (0.0.0.0/0) をルーティングドメインに挿入してパケットをそのルーターに迂回させます。このルーターはパケットを破棄することでサービスの崩壊を招いたり、パケットを転送する前に内部の機密情報を削除することができます。セキュリティデバイス上では、BGP はデフォルトで BGP ピアから送信されたあらゆるデフォルトルートを受け入れてこのデフォルトルートをルーティングテーブルに追加します。

この例では、trust-vr 内で動作している BGP ルーティングインスタンスが、BGP ピアから送信されたあらゆるデフォルトルートを無視するように構成します。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit > Edit BGP Instance: 次のように入力してから **OK** をクリックします。

Ignore default route from peer: (選択)

CLI

```
set vrouter trust-vr protocol bgp reject-default-route
save
```

オプションの BGP 構成

このセクションでは、仮想ルーター内の BGP ルーティングプロトコルに構成可能なパラメータについて説明します。これらのパラメータは、CLI BGP コンテキストコマンドと WebUI のどちらでも構成できます。このセクションでは、もう少し複雑なパラメータ構成のいくつかについて説明します。表 14 に、BGP パラメータとそのデフォルト値を説明します。

表 14: オプションの BGP パラメータおよびデフォルト値

BGP プロトコルパラメータ	説明	デフォルト値
Advertise default route	仮想ルーター内のデフォルトルートを BGP ピアへ通知します。	デフォルトルートは通知されません
Aggregate	統合ルートを作成します。129 ページの「ルートの集約」を参照してください。	無効
Always compare MED	ルート内の MED 値を比較します。	無効
AS path access list	ルートを許可または拒否する AS パスアクセスリストを作成します。	—
Community list	コミュニティリストを作成します。128 ページの「BGP コミュニティ」を参照してください。	—
AS confederation	コンフェデレーションを作成します。127 ページの「コンフェデレーションの構成」を参照してください。	—
Equal cost multipath routing (ECMP)	等価コスト複数ルートを追加すると負荷分散が可能になります。38 ページの「等価コストマルチパスルーティングの構成」を参照してください。	無効 (デフォルト = 1)
Flap damping	ルートが安定するまでアドバタイズメントを阻止します。	無効
Hold time	ピアが停止したと考えられるまでこのピアからのメッセージがなく経過した時間。	180 秒
Keepalive	キープアライブの送信と送信の間の時間。	保持時間の 1/3
Local preference	LOCAL_PREF メトリックを構成します。	100
MED	MED 属性値を構成します。	0
Network	BGP に静的ネットワークおよびサブネットのエントリを追加します。BGP はこのスタティックルートを BGP ピアすべてにアドバタイズします。121 ページの「BGP にルートを追加」を参照してください。	—
Route redistribution	BGP へルートを別のルーティングプロトコルからインポートします。	—
Reflector	ローカル BGP インスタンスをクライアントへのルートリフレクタとして構成します。125 ページの「ルートリフレクションを構成する」を参照してください。	無効
Reject default route	BGP ピアからのデフォルトルートアドバタイズメントを無視します。	ピアからのデフォルトルートはルーティングテーブルへ追加されます。
Retry time	ピアとの BGP セッション確立の失敗後の時間で、この時間が経つとセッション確立が再試行されます。	12 秒
Synchronization	OSPF や RIP などの IGP との同期化を使用可能にします。	無効

ルートを BGP へ再配布する

ルート再配布とは、ルーティングプロトコル間のルート情報の交換のことです。たとえば以下のようなルート情報を、同一の仮想ルーターにある BGP ルーティングインスタンスに再配布することができます。

- OSPF や RIP から得たルート
- 直接接続されたルート
- インポートされたルート
- 静的に構成されたルート

ルート再配布を構成するときは、まず再配布されるルートにフィルタをかけるルートマップを指定する必要があります。ルート再配布のためのルートマップ作成の詳細は、第 2 章 ,「ルーティング」を参照してください。

次の例では、OSPF ルーティングドメインから始まるルートを現行の BGP ルーティングドメインへと再配布します。CLI と WebUI のどちらの例でも、すでに add-ospf というルートマップが作成されていることを前提としています。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Redist.Rules: 次のように入力してから **Add** をクリックします。

Route Map: add-ospf
Protocol: OSPF

CLI

```
set vrouter trust-vr protocol bgp redistribute route-map add-ospf protocol ospf
save
```

AS-Path アクセスリストの構成

AS-path 属性は、ルートが行き来した AS のリストが含まれます。BGP は、ルートが AS を通過するときローカル AS 番号を AS-path 属性の先頭に付けます。*AS-path アクセスリスト*を使用して、ルートを AS-path 情報に基づいてフィルタリングできます。AS-path アクセスリストは、AS-path 情報を定義する正規表現のセットで構成され、AS-path 情報に一致するルートを許可するか拒否するかが示されています。たとえば、AS-path アクセスリストを使用して、特定の AS を通過したルートや特定の AS で開始したルートにフィルタをかけることができます。

正規表現は、AS-path 属性の中の特定パターンの検索を定義する方法です。特殊記号と特殊文字を正規表現の作成で使用できます。たとえば、AS 65000 を通過したルートに一致させるには、正規表現の **_65000_** を使用します (アンダースコアは 65000 の前後のあらゆる文字に一致します)。65000$ の正規表現を使用すると AS 65000 から発生したルートが一致します (ドル記号は AS-path 属性の終わりに一致し、ルートが発生した AS になります)。

次の例では、AS 65000 を通ったルートを許可するが AS 65000 で開始したルートは許可しない trust-vr の AS-path アクセスリストを構成します。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > AS Path: 次のように入力してから **Add** をクリックします。

AS Path Access List ID: 2
Deny: (選択)
AS Path String: 65000$

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > AS Path: 次のように入力してから **Add** をクリックします。

AS Path Access List ID: 2
Permit: (選択)
AS Path String: _65000_

CLI

```
set vrouter trust-vr protocol bgp as-path-access-list 2 deny 65000$
set vrouter trust-vr protocol bgp as-path-access-list 2 permit _65000_
save
```

BGP にルートを追加

BGP でネットワークルートをアドバタイズするよう設定する場合、同じ仮想ルーター (VR) に属するソースプロトコルからアドバタイズに使うプロトコル (すなわち BGP) に、ルートを再配布する必要があります。スタティックルートも BGP に直接追加して構いません。ネットワークプレフィックスが VR から到達可能であれば、BGP がルートをピアにアドバタイズするに当たり、ルートの再配布は必要ありません。ネットワークプレフィックスを BGP に追加するに当たって、いくつか指定できるオプションがあります。

- 「到達性のチェック」を有効にすると、BGP がルートをピアにアドバタイズする前に、*異なる*ネットワークプレフィックスが VR から到達可能でなければならないかどうか指定できるようになります。たとえば、BGP でアドバタイズするプレフィックスが特定のルーターインターフェースを介して到達可能でなければならないとすると、実際に BGP を使ってネットワークをピアにアドバタイズする前に、そのルーターインターフェースが到達可能であることを確認する必要が出てくるでしょう。指定しルーターインターフェースが到着可能であれば、BGP はルートをピアにアドバタイズします。そうでなければ、ルートが BGP に追加されることはなく、したがって BGP ピアにアドバタイズされることもありません。指定したルーターインターフェースが到着不可能になれば、BGP はルートが無効であるとピアに伝えて回収します。

- 「到達性のチェック」を無効にすると、ネットワークプレフィックスが VR から到達可能であるかどうかに関わらず、アドバタイズするようになります。デフォルトでは、BGP がピアにルートをアドバタイズするまでに、ネットワークプリフィッスが VR から到達可能になっていなければなりません。「到達性のチェック」を有効にすると、ルートは接続可能になります。

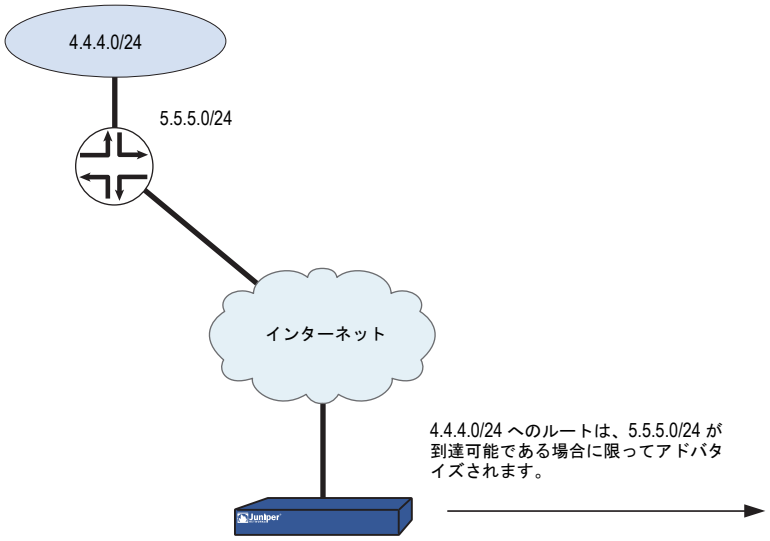
- ネットワークプレフィックスには*重み*を指定することができます。この「重み」は、ルートに対してローカルに割り当てる属性であって、ピアにアドバタイズされることはありません。宛先に到達するルートが複数ある場合、「重み」が大きい方のルートが優先されます。

- ルートの属性は、ルートマップで指定された値を設定することもできます (40 ページの「ルートマップの設定」を参照。)BGP はルートをアドバタイズする際、ルートマップで指定された属性も通知します。

条件付きルートアドバタイズメント

次の例では、ネットワーク 4.4.4.0/24 に静的ルートを追加します。BGP が 4.4.4.0/24 ルートをピアにアドバタイズするために、ルーターインターフェース 5.5.5.0/24 が仮想ルーターから到着できるように指定します。5.5.5.0/24 ネットワークが到達可能でない場合、BGP は 4.4.4.0/24 ネットワークを通知しません。図 16. を参照してください。

図 16: 条件付きルートアドバタイズメントの例



WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Networks: 次のように入力してから **Add** をクリックします。

IP/Netmask: 4.4.4.0/24
Check Reachability:
Yes: (選択), 5.5.5.0/24

CLI

```
set vrouter trust-vr protocol bgp network 4.4.4.0/24 check 5.5.5.0/24
save
```

ルートの重みの設定

次の例ではルート 4.4.4.0/24. に対して 100 の重みを設定します。(重みは 0 から 65535 の間の値を指定することができます)

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Networks: 次のように入力してから **Add** をクリックします。

IP/Netmask: 4.4.4.0/24
Weight: 100

CLI

```
set vrouter trust-vr protocol bgp network 4.4.4.0/24 weight 100
save
```

ルート属性の設定

次の例では、ルートマップ *setattr* を構成し、ルートのメトリックを 100 に設定します。次に BGP において、ルートマップ *setattr* を使用する静的ルートを構成します。(ルートマップをルートエントリのネットワークプレフィックスに合わせる必要はありません。)

WebUI

Network > Routing > Virtual Routers > Route Map (trust-vr) > New: 次のように入力してから **OK** をクリックします。

```
Map Name: setattr
Sequence No.: 1
Action: Permit ( 選択 )
Set Properties:
    Metric: ( 選択 ), 100
```

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Networks: 次のように入力してから **Add** をクリックします。

```
IP/Netmask: 4.4.4.0/24
Route Map: setattr ( 選択 )
```

CLI

```
set vrouter trust-vr route-map name setattr permit 1
set vrouter trust-vr route-map setattr 1 metric 100
set vrouter trust-vr protocol bgp network 4.4.4.0/24 route-map setattr
save
```

Route-Refresh 機能

RFC 2918 に定義されている BGP route-refresh 機能はソフトリセット機構で、BGP ピアと、後に行われるアウトバウンドまたはインバウンドルーティングテーブルの再度アドバタイズとの間で、route refresh 要求やルーティング情報の動的交換を行います。

ルートマップを使用している BGP ピアのルーティングポリシーは、インバウンドまたはアウトバウンドルーティングテーブルの更新に影響を与える場合があります。というのは、ルートポリシーの変更が行われると、BGP セッションがリセットして初めて、新しいポリシーが有効になるからです。BGP セッションはハードまたはソフトリセットを行うとクリアできます。

注 : アクティブな BGP セッションが解体され、それから立ち上がるので、ハードリセットは破壊的です。

ソフトリセットは、アクティブな BGP セッションをクリアすることなく、新しいまたは変更したポリシーの適用ができます。Route-refresh 機能は、近隣ノードに対してソフトリセットを行い、前もって構成を行ったり、追加のメモリを必要としません。

隣接ノードからインバウンドのアップデートを取得するために、動的インバウンドソフトリセットが行われます。隣接ノードに新しいアップデート セットを送るには、アウトバウンドソフトリセットが使われます。アウトバウンドリセットは前もって構成したり、ルーティングテーブルアップデートストレージを必要としません。

Route refresh 機能は、両方の BGP ピアが OPEN メッセージにおいて、route-refresh 機能サポートをアドバタイズする必要があります。Route refresh 機能のネゴシエートに成功すると、どちらの BGP ピアも route-refresh 機能を使って、他方から完全なルーティング情報を要求することができます。

注： **get neighbor** *ip_addr* コマンドを使うと、管理者は route-refresh 機能がネゴシエートされたかチェックできます。このコマンドは route-refresh 要求が何回送信あるいは受信されたかなど、カウンターも表示します。

インバウンドルーティングテーブルアップデートの要求

この例ではソフトインコマンドを使って、10.10.10.10 の隣接するピアのインバウンドルーティングテーブルをローカル BGP ピアの trust-vr に送信します。

注： Route refresh 機能が利用できない場合、管理者が route refresh 機能を使おうとすると、コマンドは例外扱いとします。

WebUI

この機能は WebUI では使用できません。

CLI

clear vrouter trust-vr protocol bgp neighbor 10.10.10.10 soft-in

アウトバウンドルーティングテーブルアップデートの要求

この例ではソフトアウトコマンドを使って、ローカル BGP ピアのアップデートから 10.10.10.10 の隣接ノードに trust-vr の完全なルーティングテーブルを送信します。

WebUI

この機能は WebUI では使用できません。

CLI

clear vrouter trust-vr protocol bgp neighbor 10.10.10.10 soft-out

ルートリフレクションを構成する

IBGP ルーターはある IBGP ピアから得たルートを別の IBGP ピアへ再通知できないため (109 ページの「外部および内部 BGP」を参照)、BGP AS 内の各ルーターがこの AS 内の他のすべてのルーターとピアである場合は IBGP セッションの *フルメッシュ*が必要になります。

注 : フルメッシュにするということは、ルーターのペアそれぞれが直接接続している必要はありませんが、各ルーターがすべての相手方ルーターと IBGP セッションを確立および維持できる必要があるということを意味します。

IBGP セッションのフルメッシュ構成は、拡張性が十分とはいえません。たとえば 8 台のルーターがある AS では、各ルーターが他の 7 台のルーターと使用可能でなければなりません。つまり、ルート数は次の式で表されます。

8 台のルーターからなる AS であれば、フルメッシュ IBGP セッションの数は 28 になります。

ルートリフレクションは、IBGP のスケーラビリティ問題を解決するための方法であり、RFC 1966 に記述されています。*ルートリフレクタ*は、IBGP 取得ルートを指定した IBGP 近隣 (*クライアント*) へ渡すルーターであり、これによりフルメッシュセッションが不要になります。ルートリフレクタとそのクライアントによって*クラスタ*がつくられ、これはクラスタ ID で識別可能です。クラスタの外側のルーターはクラスタ全体を 1 つのエンティティとして扱い、フルメッシュの個々のルーターとインターフェースをとりません。このように配列することで、オーバーヘッドが大きく減ります。クライアントはルートをルートリフレクタと交換し、一方ルートリフレクタはクライアント間のルートを反射します。

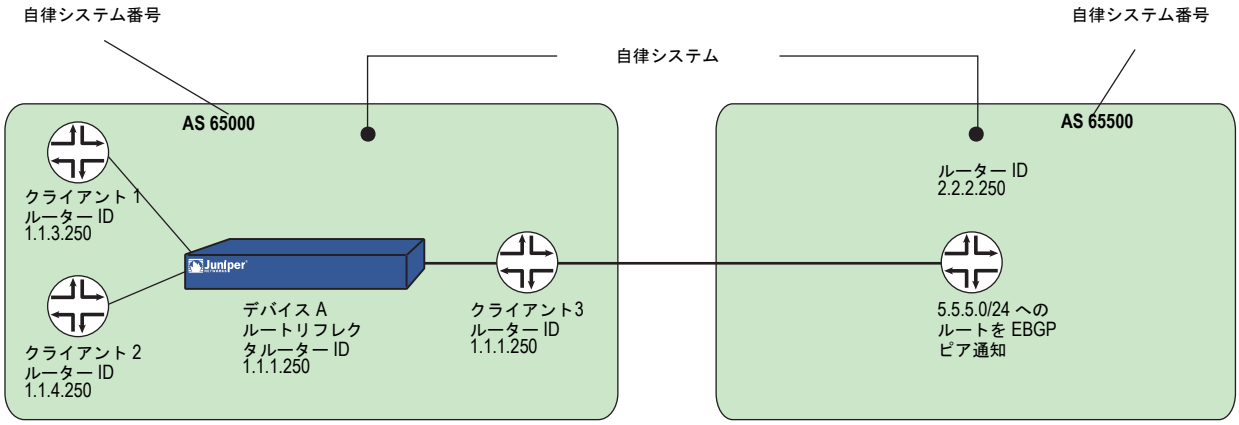
セキュリティデバイスのローカル仮想ルーター (VR) は、ルートリフレクタとして機能することもでき、クラスタ ID を割り当てることもできます。クラスタ ID を指定すると、BGP ルーティングインスタンスはクラスタ ID をルートのクラスタリスト属性に付加します。クラスタ ID は、ローカル BGP ルーティングインスタンスは、そのクラスタ ID がルートのクラスタリストに出現するとルートをドロップするため、ルーティングのループを防ぐ上で役に立ちます。

注 : クラスタ ID を構成する前に、BGP ルーティングインスタンスを使用不可にしてください。

ルートリフレクタをローカル VR で設定したら、次にルートリフレクタのクライアントを定義します。クライアントの個々の IP アドレスかピアグループを指定できます。クライアント上では何も構成する必要はありません。

次の例では、EBGP ルーターは 5.5.5.0/24 プレフィックスをクライアント 3 に通知します。ルートリフレクションがなければ、クライアント 3 はルートを Device-A に通知しますが、Device-A はそのルートをクライアント 1 と 2 に再通知しません。Device-A をルートリフレクタに構成してクライアント 1、2、および 3 をそのクライアントとして構成すると、Device-A はクライアント 3 から受け取ったルートをクライアント 1 と 2 に再通知します。図 17 を参照してください。

図 17: BGP ルートリフレクションの例



WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance: 以下を入力して **Apply** をクリックします。

Route reflector: Enable
Cluster ID: 99

> Neighbors: 次のように入力してから **Add** をクリックします。

AS Number: 65000
Remote IP: 1.1.2.250

次のように入力してから **Add** をクリックします。

AS Number: 65000
Remote IP: 1.1.3.250

次のように入力してから **Add** をクリックします。

AS Number: 65000
Remote IP: 1.1.4.250

> Configure (Remote IP 1.1.2.250): **Reflector Client** を選択して、**OK** をクリックします。

> Configure (Remote IP 1.1.3.250): **Reflector Client** を選択して、**OK** をクリックします。

> Configure (Remote IP 1.1.4.250): **Reflector Client** を選択して、**OK** をクリックします。

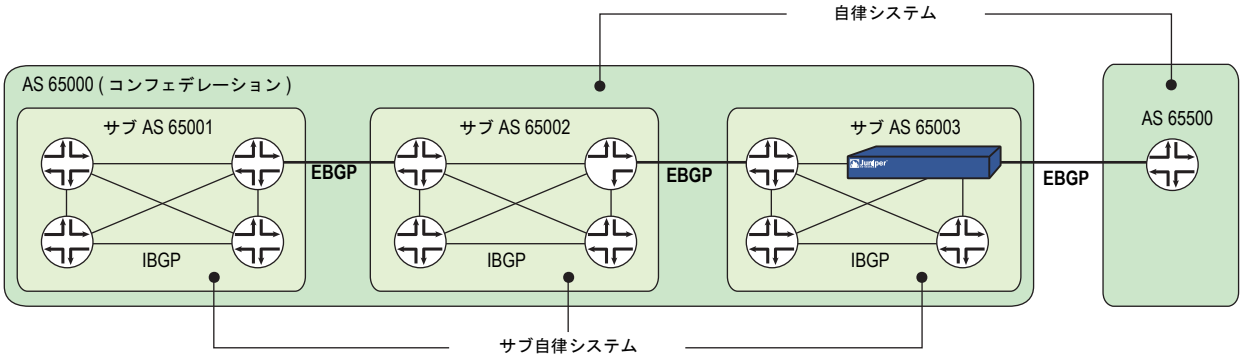
CLI

```
set vrouter trust-vr protocol bgp reflector
set vrouter trust-vr protocol bgp reflector cluster-id 99
set vrouter trust-vr protocol bgp neighbor 1.1.2.250 remote-as 65000
set vrouter trust-vr protocol bgp neighbor 1.1.2.250 reflector-client
set vrouter trust-vr protocol bgp neighbor 1.1.3.250 remote-as 65000
set vrouter trust-vr protocol bgp neighbor 1.1.3.250 reflector-client
set vrouter trust-vr protocol bgp neighbor 1.1.4.250 remote-as 65000
set vrouter trust-vr protocol bgp neighbor 1.1.4.250 reflector-client
save
```

コンフェデレーションの構成

ルートリフレクションと同様 (125 ページの「ルートリフレクションを構成する」を参照)、*コンフェデレーション*は、IBGP 環境のフルメッシュスケーリングの問題を解決するもう 1 つのアプローチで、RFC 1965 に記述されています。コンフェデレーションは、1 つの自律システムを複数の小さな自律システムに分割し、それぞれのサブ AS はフルメッシュの IBGP ネットワークとなります。コンフェデレーションの外側のルーターはコンフェデレーション全体を 1 つの識別子を持つ単一の自律システムであると考え、サブ AS ネットワークはコンフェデレーションの外側からは見えません。同一コンフェデレーション内の異なる 2 つのサブ AS のルーター間のセッションは、EIBGP セッションとして知られ、基本的には自律システム間の EBGP セッションですが、ルーターはルーティング情報をあたかも IBGP ピアであるかのように交換します。図 18 は BGP コンフェデレーションを表す図です。

図 18: BGP コンフェデレーション



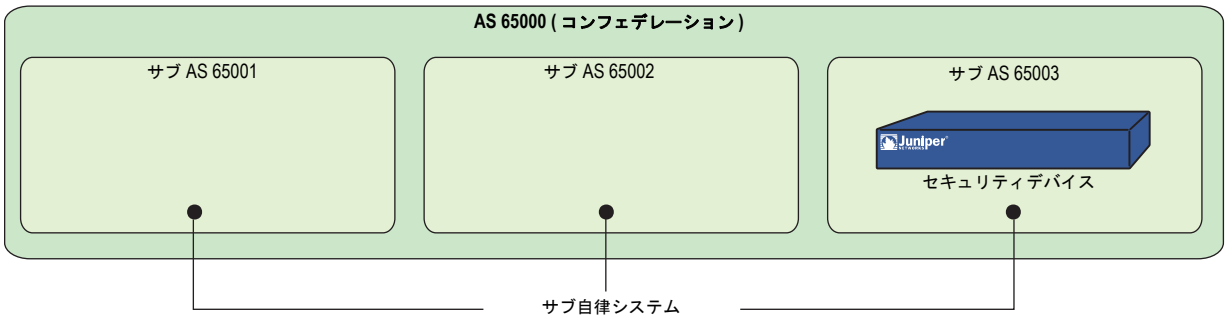
コンフェデレーション内の各ルーターで、以下について指定する必要があります。

- サブ AS 番号 (これは、BGP ルーティングインスタンスを作成するときに指定する AS 番号です)
- サブ AS が所属するコンフェデレーション (これは、コンフェデレーション外部の BGP ルーターに見える AS 番号です)
- コンフェデレーション内のピアサブ AS 番号
- コンフェデレーションが RFC 1965 (デフォルト) か RFC 3065 をサポートするかどうか

注 : AS-Path 属性 (109 ページの「パス属性」を参照) は通常、シーケンスになっています。ルーティングによりトラバースされると AS は更新されます。
RFC 3065 では 、AS-Path 属性が、ルーティングアップデートが行き来するローカルコンフェデレーションのメンバー AS を含むことを可能にしています。

図 19 は、セキュリティデバイスがサブ AS 65003 内の BGP ルーターであることを示しており、サブ AS 65003 はコンフェデレーション 65000 に所属しています。コンフェデレーション 65000 内のピアのサブ AS は 65002 と 65003 です。

図 19: BGP コンフェデレーション構成例



WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Create BGP Instance: 以下を入力して **Apply** をクリックします。

AS Number (**必須**): 65003
> Confederation: 以下を入力して **Apply** をクリックします。

Enable: (**選択**)
ID: 65000
Supported RFC: RFC 1965 (**選択**)

次のように入力してから **Add** をクリックします。

Peer member Area ID: 65001

次のように入力してから **Add** をクリックします。

Peer member Area ID: 65002

> パラメータ **BGP Enable** を選びます

CLI

```
set vrouter trust-vr protocol bgp 65003
set vrouter trust-vr protocol bgp confederation id 65000
set vrouter trust-vr protocol bgp confederation peer 65001
set vrouter trust-vr protocol bgp confederation peer 65002
set vrouter trust-vr protocol bgp enable
save
```

BGP コミュニティ

コミュニティパス属性は、宛先をグループ化する (コミュニティと呼びます) 方法を提供します。このコミュニティを BGP ルーターは使用して受け入れや優先、またはピアへ再配布するルートを管理できます。BGP ルーターはコミュニティをルートの先頭に追加するか (ルートにコミュニティパス属性がない場合)、ルート内のコミュニティを変更 (ルートにコミュニティパス属性が含まれる場合) します。コミュニティパス属性を、IP アドレスプレフィックスまたは AS パス属性に基づいてルート情報を配布する方法の代わりに使用することができます。コミュニティパス属性はいろいろなかたちで使用できますが、本来の目的は複雑なネットワーク環境におけるルーティングポリシーの構成を簡素化することです。

RFC 1997 は、BGP コミュニティの操作について記述しています。AS 管理者は同じルーティング決定を必要とするルートのセットに同一のコミュニティを割り当てることができ、これを*ルート色分け*とよぶこともあります。たとえば、あるコミュニティ値をインターネットへのアクセスを受け入れるルートに割り当て、別のコミュニティ値を受け入れないルートに割り当てることができます。

コミュニティには 2 つの形態があります。

- *特定コミュニティ*は、AS 識別子とコミュニティ識別子からなります。コミュニティ識別子は、AS 管理者が定義します。
- *既知コミュニティ*は、これらのコミュニティ値を含むルートのための特別処理を表わします。以下は、セキュリティデバイスの BGP ルートに指定できる既知のコミュニティ値です。
  - **no-export**: このコミュニティパス属性をもつルートは、BGP コンフェデレーション外部には通知されません。
  - **no-advertise**: このコミュニティパス属性をもつルートは、他の BGP ピアには通知されません。
  - **no-export-subconfed**: このコミュニティパス属性をもつルートは、EBGP ピアには通知されません。

ルートマップを使用して指定したコミュニティリストに一致するルートをフィルタリングしたり、ルート内のコミュニティパス属性を削除や設定したり、コミュニティをルートに追加や削除できます。

たとえば、ISP がインターネット接続を顧客に提供すると、これらの顧客からのすべてのルートには特定のコミュニティ番号を割り当てできます。これらの顧客ルートは、ピア ISP に通知されます。他の ISP からのルートには別のコミュニティ番号が割り当てられ、ピア ISP には通知されません。

ルートの集約

集約とは、ある範囲のルーティングアドレスをひとつのエントリに要約する技法です (*ルートの統合*とも呼ばれている)。集約の設定に当たって指定できるパラメータがいくつかあります。ここではルートを集約する設定例を示します。

異なる AS-Path のルートを集約

ルートの集約を設定する際、BGP AS-Path パス属性の AS-Set フィールドに、集約対象となるすべてのルートの AS パスを入れるよう指定することができます。この指定には集約ルート設定の AS-Set オプションを使います。

注 : 集約されたルートに AS-Set オプションを使うと、集約対象ルートを変更したときに、各ルートのパス属性も変わることがあります。その場合 BGP は、該当する集約ルートを再アドバタイズします。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Aggregate Address: 以下を入力して **Apply** をクリックします。

Aggregate State: Enable (選択)
IP/Netmask: 1.0.0.0/8
AS-Set: (選択)

CLI

```
set vrouter trust protocol bgp
set vrouter trust protocol bgp aggregate
set vrouter trust protocol bgp aggregate 1.0.0.0/8 as-set
set vrouter trust protocol bgp enable
save
```

注 : あらかじめ BGP 集約を有効にしてから BGP を有効にする必要があります。

更新の際、より限定的なルートを除外

集約ルートを設定する際、更新の対象から、より限定的なルートを除くよう指定できます。(BGP ピアは、アドバタイズされたとき、限定的なルートがあれば集約ルートよりも優先して扱います。) その手段には次の 2 とおりがあります。

- 集約ルートの設定の際、Summary-Only オプションを指定して、それよりも限定的なルートをすべて除外。
- 集約ルートの設定の際、Suppress-Map を使って、ルートマップにより特定されたルートを除外。

次の例では、BGP は 1.0.0.0/8 という集約ルートをアドバタイズしますが、これよりも限定的な外向きルートアップデートは除外します。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Aggregate Address: 以下を入力して **Apply** をクリックします。

Aggregate State: Enable (**選択**)
IP/Netmask: 1.0.0.0/8
Suppress Option: Summary-Only (**選択**)

CLI

```
set vrouter trust protocol bgp aggregate 1.0.0.0/8 summary-only
save
```

次の例では 1.2.3.0/24 範囲内のルートを集約ルート 1.0.0.0/8 が含まれているアップデートから除外します。このためには最初に、除外するルート (1.2.3.0/24) を指定するアクセスリストを設定します。次にルートマップ noadvert に 1.2.3.0/24 というルートを許可します。そして集約ルート 1.0.0.0/8 を設定し、ルートマップ noadvert を外向きアップデートの除外対象として指定します。

WebUI

Network > Routing > Virtual Routers > Access List (trust-vr) > New: 次のように入力してから **OK** をクリックします。

Access List ID: 1
Sequence No.: 777
IP/Netmask: 1.2.3.0/24
Action: Permit (**選択**)

Network > Routing > Virtual Routers > Route Map (trust-vr) > New: 次のように入力してから **OK** をクリックします。

Map Name: noadvert
Sequence No.: 2
Action: Permit (選択)
Match Properties:
Access List (選択)、1 (選択)

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Aggregate Address: 以下を入力して **Apply** をクリックします。

Aggregate State: Enable (選択)
IP/Netmask: 1.0.0.0/8
Suppress Option: Route-Map (選択), noadvert (選択)

CLI

```
set vrouter trust-vr access-list 1 permit ip 1.2.3.0/24 777
set vrouter trust-vr route-map name noadvert permit 2
set vrouter trust-vr route-map noadvert 2 match ip 1
set vrouter trust protocol bgp aggregate 1.0.0.0/8 suppress-map noadvert
save
```

パス属性を割り当てるルートの選択

集約ルートを設定する際、その BGP AS-Path パス属性を構築するためにどのルートを使うか、あるいは使わないか、という指定ができます。この目的で使う / 使わないルートは、集約ルート設定の Advertise-Map オプションで指定します。AS-Set オプションと組み合わせれば、AS-Set 属性をつけてアドバタイズされるルートを選択することもできます。

次の例では、集約ルート 1.0.0.0/8 に AS-Set 属性をつけてアドバタイズするよう設定します。アドバタイズされる AS-Set 属性には、1.5.0.0/16 の範囲に入るけれども 1.5.6.0/24 には入らない、より限定的なルートもすべて含まれます。あるプレフィックス範囲を含める / 含めない指定には、ルートマップ advertset を使います。

WebUI

Network > Routing > Virtual Routers > Access List (trust-vr) > New: 次のように入力してから **OK** をクリックします。

Access List ID: 3
Sequence No.: 888
IP/Netmask: 1.5.6.0/24
Action: Deny (選択)

Network > Routing > Virtual Routers > Access List (trust-vr) > New: 次のように入力してから **OK** をクリックします。

Access List ID: 3
Sequence No.: 999
IP/Netmask: 1.5.0.0/16
Action: Permit (選択)

Network > Routing > Virtual Routers > Route Map (trust-vr) > New: 次のように入力してから **OK** をクリックします。

Map Name: advertset
Sequence No.: 4
Action: Permit (選択)
Match Properties:
Access List (選択)、3 (選択)

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Aggregate Address: 以下を入力して **Apply** をクリックします。

Aggregate State: Enable (選択)
IP/Netmask: 1.0.0.0/8
Advertise Map: advertset (選択)

CLI

```
set vrouter trust-vr access-list 3 deny ip 1.5.6.0/24 888
set vrouter trust-vr access-list 3 permit ip 1.5.0.0/16 999
set vrouter trust-vr route-map name advertset permit 4
set vrouter trust-vr route-map advertset 4 match ip 3
set vrouter trust protocol bgp aggregate 1.0.0.0/8 advertise-map advertset
save
```

集約ルートの属性変更

集約ルートの属性は、あるルートマップに基づいて設定することができます。次の例では、集約ルート 1.0.0.0/8 が、外向きアップデートにおいて、メトリック値 1111 でアドバタイズされるよう設定します。

WebUI

Network > Routing > Virtual Routers > Route Map (trust-vr) > New: 次のように入力してから **OK** をクリックします。

Map Name: aggmetric
Sequence No.: 5
Action: Permit (選択)
Set Properties: (選択)
Metric: 1111

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit BGP Instance > Aggregate Address: 以下を入力して **Apply** をクリックします。

Aggregate State: Enable (選択)
IP/Netmask: 1.0.0.0/8
Attribute Map: aggmetric (選択)

CLI

```
set vrouter trust-vr route-map name aggmetric permit 5
set vrouter trust-vr route-map aggmetric 5 metric 1111
set vrouter trust protocol bgp aggregate 1.0.0.0/8 attribute-map aggmetric
save
```

第 6 章

ポリシーベースのルーティング

ポリシーベースのルーティング（PBR）は、ネットワーク管理者が構成したポリシーに基づいてデータパケットを転送するための、柔軟なメカニズムを提供します。

本章のセクションは、以下のようになります。

- 134 ページの「ポリシーベースのルーティングの概要」
  - 134 ページの「拡張アクセスリスト」
  - 134 ページの「適合グループ」
  - 135 ページの「アクショングループ」
- 136 ページの「ポリシーベースのルーティングを使用するルートルックアップ」
- 136 ページの「ポリシーベースのルーティングの構成」
  - 137 ページの「拡張アクセスリストの構成」
  - 138 ページの「適合グループの構成」
  - 139 ページの「アクショングループの構成」
  - 140 ページの「PBR ポリシーの構成」
  - 140 ページの「ポリシーベースのルーティングポリシーのバインディング」
- 141 ページの「ポリシーベースのルーティングの出力の表示」
  - 141 ページの「拡張アクセスリストの表示」
  - 142 ページの「適合グループの表示」
  - 142 ページの「アクショングループの表示」
  - 143 ページの「ポリシーベースのルーティングポリシー構成の表示」
  - 143 ページの「完全なポリシーベースのルーティング構成の表示」
- 144 ページの「高度な PBR の例」
- 148 ページの「可用性およびスケーラビリティが高い、高度な PBR」

ポリシーベースのルーティングの概要

PBR では、パケットに異なった経路を選択的に取らせるポリシーを実装できます。PBR は、アンチウィルス（AV）、徹底監視（DI）、またはアンチスパム、Web フィルタリングなど、アプリケーションレイヤーのサポートに依存するネットワークや、特定のアプリケーションへの自動的なパスを必要とするネットワークに、ルーティングメカニズムを提供します。

パケットがセキュリティデバイスに入ると、ScreenOS は、ルートルックアッププロセスの最初の部分として PBR があるかチェックします。PBR チェックは、非 PBR トラフィックすべてに透過的です。PBR は、インターフェースレベルで使用可能であり、仮想ルーターのコンテキスト内で構成されます。しかし、PBR ポリシーをインターフェース、ゾーン、仮想ルーター（VR）や、インターフェース、ゾーン、または VR の組み合わせにバインドすることもできます。

次の 3 つのビルディングブロックを使用して、PBR ポリシーを作成します。

- 拡張アクセスリスト
- 適合グループ
- アクショングループ

拡張アクセスリスト

拡張アクセスリストは、PBR ポリシーに定義する適合基準を一覧表示します。PBR の適合基準が、特定のデータトラフィックフローのパスを決定します。適合基準には次が含まれます。

- ソース IP アドレス
- 宛先 IP アドレス
- ソースポート
- 宛先ポート
- HTTP などのプロトコル
- サービス品質（QoS）の優先順位（オプション）

適合グループ

適合グループは、拡張アクセスリストを（グループ、名前、および優先順位別に）整理する方法を提供します。適合グループは、拡張アクセスリストの ID 番号を、一意の適合グループ名および適合グループ ID 番号と関連付けます。この適合グループ ID 番号は、セキュリティデバイスが 拡張 ACL リストを処理する順序を定義します。同じ適合グループに複数の拡張アクセスリストを割り当てることができます。

アクショングループ

アクショングループは、パケットに利用させたいルートを指定します。次のインターフェース、次のホップ、またはその両方を定義することにより、そのルートの「アクション」を指定します。

構成された各アクションエントリは、次のように到達可能性が監視されます。

注 : 到達可能性の監視では、レイヤー 3 トラッキングまたはレイヤー 2 アドレス解決プロトコル（ARP）ルックアップを参照しません。

- **次のインターフェースだけの到達可能性**

  アクションエントリを次のインターフェースにだけ関連付けている場合、接続状態が到達可能性を決定します。

  次のインターフェースが稼働中の場合、そのアクションエントリは到着可能です。トンネルインターフェース、統合インターフェース、冗長インターフェースなど、論理インターフェースをすべて含む、ポリシーが存在する VR で見えるインターフェースは、次のインターフェースの候補です。

  たとえば、アクションエントリを NULL インターフェースで構成する場合、そのアクションエントリはいつでも到着可能です。NULL インターフェースが次のインターフェースなので、PBR ルックアップは必ず成功します。ゆえに、ScreenOS はルートルックアップを止めて、パケットを廃棄します。

- **次のホップだけの到達可能性**

  アクショングループを次のホップだけに関連付けている場合、その次のホップは、宛先ルートのルーティングテーブルのルートエントリを通して到着可能でなければなりません。次のホップを解決するため、有効なルートが宛先ルートのルーティングテーブルに存在する限り、構成された次のホップは、到着可能です。

- **次のインターフェース**および**次のホップの到達可能性**

  次のインターフェースおよび次のホップの到達可能性の両方を構成する場合、構成された次のホップは、構成された次のインターフェースを通して到着可能でなければなりません。

  次のホップが次のインターフェースを通して到着可能な場合、そのアクションエントリは到着可能です。トンネルインターフェース、統合インターフェース、冗長インターフェースなど、論理インターフェースをすべて含む、ポリシーが存在する VR で見えるインターフェースは、次のインターフェースの候補です。

  次のホップが到着可能だが次のインターフェースが NULL インターフェースの場合、ScreenOS はパケットをドロップします。アクションエントリを、NULL インターフェースを次のインターフェースとして、次のホップを静的ルートとして構成する場合、ScreenOS はパケットを静的ルートに渡します。

構成の時には、シーケンス番号も割り当てて、アクショングループエントリを処理したい順序を指定します。

ポリシーベースのルーティングを使用するルートルックアップ

インターフェースでポリシーベースのルーティングを使用可能にすると、ScreenOS は、ポリシーベースのルーティングについて、そのインターフェースに送信された全トラフィックをチェックします。パケットがセキュリティデバイスに入ると、ScreenOS は、PBR ポリシー構成がないか、受信インターフェースをチェックします。PBR がその受信インターフェースで有効な場合、次のアクションがパケットに適用されます。

1. ScreenOS は、受信インターフェースにバインドされた PBR ポリシーをそのパケットに適用します。

2. インターフェースレベルの PBR ポリシーが存在しない場合、ScreenOS は、その受信インターフェースに関連付けられたゾーンにバインドされた PBR ポリシーを、そのパケットに適用します。

3. ゾーンレベルの PBR ポリシーが存在しない場合、ScreenOS は、その受信インターフェースに関連付けられた VR にバインドされた PBR ポリシーを、そのパケットに適用します。

ScreenOS は、適合グループの場所を確認して、アクショングループエントリを処理します。有効なルートを持つアクショングループの、最初の到着可能アクションエントリが使用され、パケットが転送されます。到着可能なルートがアクションエントリの間にない場合、通常のルートルックアップが実行されます。

アクションエントリが到着可能な場合、ScreenOS はルートルックアップを実行します。このとき、好ましいインターフェースとして（指定されている場合は）次のインターフェースが、次のホップとして宛先 IP ではなく（指定されている場合は）IP アドレスが使用されます。ルートが指定された次のインターフェースおよび次のホップに適合する場合、ScreenOS はパケットを転送します。適合しない場合、ScreenOS は宛先 IP アドレスを使用します。

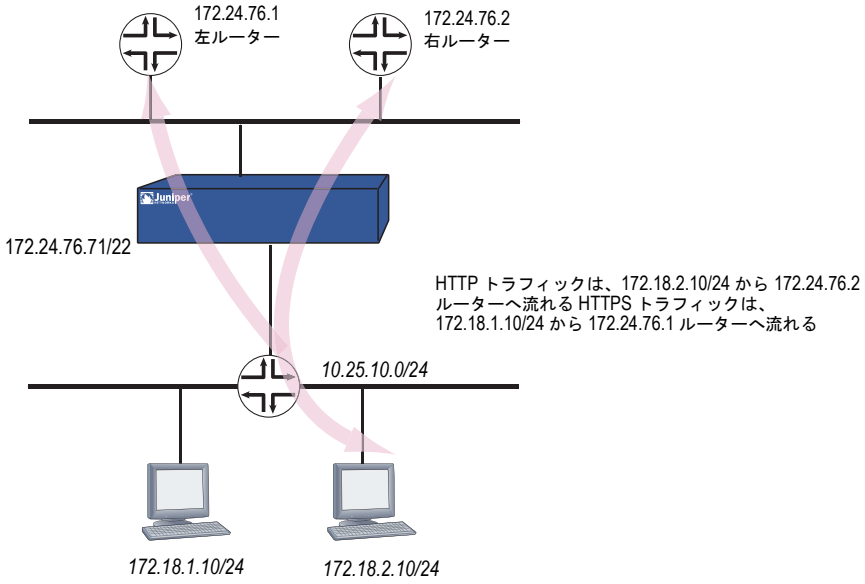
注： ルートルックアップに関する詳細については、*第2 部: 基本*を参照してください。

ポリシーベースのルーティングの構成

Figure 20 は、HTTP トラフィックをあるパスで、HTTPS トラフィックを別のパスで送信することにより、サービストラフィックのパスを区別する方法を示しています。Figure 20 は、172.18.1.10 および 172.18.2.10 という 2 つのノードを示しています。セキュリティデバイスが HTTP トラフィックを受信すると、ScreenOS は、そのトラフィックを 172.24.76.1 のルーターを通るようにルーティングします。また、セキュリティデバイスが HTTPS トラフィックを受信すると、ScreenOS は、そのトラフィックを 172.24.76.2 のルーターを通るようにルーティングします。

172.18.2.10 ノードでは、その逆になります。172.18.2.10 ノードからの HTTP トラフィックは、172.24.76.2 のルーターへ流れ、HTTPS トラフィックは 172.24.76.1 のルーターへ流れます。

図 20: ポリシーベースのルーティングを使用する HTTP および HTTPS トラフィックのルーティング



拡張アクセスリストの構成

拡張アクセスリストは、仮想ルーターのコンテキスト内から、Web ユーザーインターフェース（WebUI）を使用して、またはコマンドラインインターフェース（CLI）を使用して、構成できます。最初に、入口仮想ルーター（VR）で拡張アクセスリストを構成します。

137 ページのこの例では、入口 VR は trust-vr です。CLI を使用する場合、仮想ルーターのコンテキストを入力する必要があります。この例では、2 つのアクセスリスト、10 および 20 が必要です。アクセスシーケンス番号は、1 から 99 までの数です。エントリ 1 および 2 は、各拡張アクセスリストに必要です。

注 : オプションで、サービスのタイプ（TOS）番号を追加できます。これは、1 から 255 までの数になります。TOS 番号はこの例では必要ありません。

アクセスリスト 10 は、ソース IP アドレスを 172.18.1.10、宛先ポートを 80、プロトコルを TCP に定義します。アクセスリスト 10 の宛先ポイントは、宛先 IP アドレスを 172.18.2.10、宛先ポートを 443、プロトコルを TCP に定義します。

アクセスリスト 20 は、ソース IP アドレスを 172.18.2.10、宛先ポートを 443、プロトコルを TCP に定義します。アクセスリスト 10 の宛先ポイントは、宛先 IP アドレスを 172.18.1.10、宛先ポートを 80、プロトコルを TCP に定義します。

CLI で、拡張アクセスリストを構成した後、仮想ルーターのコンテキストから出ます。WebUI の例では、アクセスリスト 10 の作成だけを示します。

WebUI

Network > Routing > PBR > Extended ACL List: ドロップダウンリストから仮想ルーターを選択して、**New** をクリックし、構成ページを表示します。

次の情報を入力して、アクセスリスト 10 のエントリを作成します。

アクセスリスト 10 の作成
Extended ACL ID: 10
Sequence No.: 1
Source IP Address/Netmask: 172.18.1.10/32
Destination Port: 80-80
Protocol: TCP

OK をクリックする。ScreenOS が、アクセスリストの一覧に戻ります。

アクセスリスト 10 の別のエントリを構成するには、**New** をクリックして、次の情報を入力します。

アクセスリスト 10 の作成
Extended ACL ID: 10
Sequence No.: 2
Source IP Address/Netmask: 172.18.2.10/32
Destination Port: 443-443
Protocol: TCP

OK をクリックする。ScreenOS が、アクセスリストの一覧に戻ります。

CLI

```
set vrouter trust-vr
set access-list extended 10 src-ip 172.18.1.10/32 dest-port 80-80 protocol tcp
    entry 1
set access-list extended 10 src-ip 172.18.2.10/32 dest-port 443-443 protocol tcp
    entry 2
set access-list extended 20 src-ip 172.18.2.10/32 dest-port 80-80 protocol tcp
    entry 1
set access-list extended 20 src-ip 172.18.1.10/32 dest-port 443-443 protocol tcp
    entry 2
exit
```

適合グループの構成

仮想ルーターのコンテキスト内から、適合グループを構成できます。

137 ページの例では、2 つの適合グループ、Left Router および Right Router を構成する必要があります。拡張アクセスリスト 10 を Left Router に、拡張アクセスリスト 20 を Right Router にバインドします。適合グループ名は、英数字 31 文字以内の一意の識別子です。

入口 VR は trust-vr です。CLI を使用する場合、仮想ルーターのコンテキストを入力する必要があります。CLI で、拡張アクセスリストを構成した後、仮想ルーターのコンテキストから出ます。

WebUI の例では、左ルーターの適合グループの作成だけを示しています。

WebUI

Network > Routing > PBR > Match Group > ドロップダウンリストから適切な仮想ルーターを選択して、**New** をクリックし、適合グループ構成ページを表示します。次の情報を入力して、Left Router を構成します。

Match Group Name: left_router
Sequence No.: 1
Extended ACL: **ドロップダウンリストから 10 を選択します。**

CLI

```
set vrouter trust-vr
set match-group name left_router
set match-group left ext-acl 10 match-entry 1
set match-group name right_router
set match-group right ext-acl 20 match-entry 1
exit
```

アクショングループの構成

仮想ルーティングのコンテキスト内から、アクショングループを構成できます。

137 ページの例では、2 つのアクショングループが構成できます。セキュリティデバイスは、トラフィックを左ルーターかまたは右ルーターへ転送できます。このため、2 つの異なったアクショングループを構成する必要があります。

これらのアクショングループを構成するには、次のタスクを実行します。

1. 仮想ルーティングのコンテキストを入力します。この例では、仮想ルーターは trust-vr です。

2. アクショングループに意味のある一意の名前を付けます。この例では、**action-right** および **action-left** という名前が、トラフィックフローの説明になります。

3. アクショングループの詳細を構成します。この例では、各アクショングループの次のホップのアドレスを設定し、処理の優先順位を示すため数字を割り当てます。この例では、各アクショングループの優先順位は 1 です。

WebUI

Network > Routing > PBR > Action Group > **New** をクリックして、構成ページを表示します。

CLI

```
set vrouter trust-vr
set action-group name action-right
set action-group action-right next-hop 172.24.76.2 action-entry 1
set action-group name action-left
set action-group action-left next-hop 172.24.76.1 action-entry 1
exit
```

PBR ポリシーの構成

仮想ルーターのコンテキスト内から、PBR ポリシーを構成できます。

各 PBR ポリシーには一意の名前が必要です。この例では、ポリシーに **redirect-policy** という名前が付いています。

PBR ポリシーには、適合グループ名およびアクショングループ名を含めることができます。この例では、トラフィックは 2 つの異なった経路を流れることができます。そのため、シーケンス番号 が 1 の **action-left** およびシーケンス番号 が 2 の **action-right** という、2 つのステートメントが必要になります。シーケンス番号が 1 のポリシーステートメントが最初に処理されます。

WebUI

Network > Routing > PBR > Policy > **New** をクリックして、構成ページを表示します。

CLI

```
set vrouter trust-vr
set pbr policy name redirect-policy
set pbr policy redirect-policy match-group left action-group action-left 1
set pbr policy redirect-policy match-group right action-group action-right 2
exit
```

ポリシーベースのルーティングポリシーのバインディング

仮想ルーターのコンテキスト内から、PBR ポリシーをインターフェース、ゾーン、または仮想ルーターへバインドできます。

ポリシーベースのルーティングポリシーのインターフェースへのバインディング

PBR ポリシー **redirect-policy** を入口インターフェースへバインドできます。この例では、インターフェースは **trust** インターフェースです。

WebUI

Network > Routing > PBR > Policy Binding

CLI

```
set interface trust pbr redirect-policy
```

ポリシーベースのルーティングポリシーのゾーンへのバインディング

PBR ポリシー **redirect-policy** をゾーンへバインドできます。この例では、ゾーンは **Trust** ゾーンです。

WebUI

Network > Routing > PBR > Policy Binding

CLI

```
set zone trust pbr redirect-policy
```

ポリシーベースのルーティングポリシーの仮想ルーターへのバインディング

PBR ポリシー **redirect-policy** を仮想ルーターへバインドできます。この例では、仮想ルーターは **trust-vr** です。

WebUI

Network > Routing > PBR > Policy Binding

CLI

set vrouter trust-vr pbr redirect-policy

ポリシーベースのルーティングの出力の表示

ポリシーベースのルーティング関連の情報を WebUI または CLI で表示できます。

拡張アクセスリストの表示

拡張アクセスリストの全リストを WebUI または CLI で表示できます。

CLI では、1 つの特定の拡張アクセスリストを指定できます。2 番目の CLI の例では、出力例が、2 つの拡張アクセスリストが trust-vr に存在することを示していますが、ユーザーは拡張アクセスリスト 2 を指定しました。指定されたように、ScreenOS は、2 番目の拡張アクセスリストについてだけ、2 つのアクセスリストエントリ 10 および 20 を返しました。

WebUI

Network > Routing > PBR > Access List Ext

CLI 1

get vrouter trust-vr pbr access-list configuration

出力例 :

```
set access-list extended 1 src-ip 172.16.10.10/32 dest-ip 192.169.10.10/32
dest-port 80-80 protocol tcp entry 1
set access-list extended 1 src-port 200-300 entry 2
set access-list extended 2 dest-port 500-600 protocol udp entry 10
set access-list extended 2 dest-ip 50.50.50.0/24 protocol udp entry 20
```

CLI 2

get vrouter trust-vr pbr access-list 2

出力例 :

```
PBR access-list: 2 in vr: trust-vr, number of entries: 2
------------------------------------------------
PBR access-list entry: 10
------------------------
dest port range 500-600
protocols: udp
PBR access-list entry: 20
------------------------
dest ip-address 50.50.50.0/24
protocols: udp
```

適合グループの表示

WebUI または CLI で 適合グループの詳細を表示できます。

WebUI

Network > Routing > PBR > Match Group

CLI

get vrouter trust-vr pbr match-group config

出力例 :

```
set match-group name pbr1_mg
set match-group pbr1_mg ext-acl 1 match-entry 1
set match-group name pbr1_mg2
set match-group pbr1_mg2 ext-acl 2 match-entry 10
```

アクショングループの表示

WebUI または CLI で アクショングループの詳細を表示できます。

WebUI

Network > Routing > PBR > Action Group

CLI 1

get vrouter trust-vr pbr action-group configuration

出力例 :

```
set action-group name pbr1_ag
set action-group pbr1_ag next-interface ethernet2 next-hop 10.10.10.2
    action-entry 1
set action-group name pbr1_ag2
set action-group pbr1_ag2 next-hop 30.30.30.30 action-entry 10
set action-group pbr1_ag2 next-interface ethernet3 action-entry 20
set action-group pbr1_ag2 next-interface ethernet3 next-hop 60.60.60.60
    action-entry 30
```

CLI 2

get vrouter trust-vr pbr match-group name pbr1_ag2

出力例 :

```
device-> get vr tr pbr action-group name pbr1_ag2
PBR action-group: pbr1_ag2 in vr: trust-vr number of entries: 3
------------------------------------------------
PBR action-group entry: 10
next-Interface: N/A, next-hop: 30.30.30.30
------------------------
PBR action-group entry: 20
next-Interface: ethernet3, next-hop: 0.0.0.0
------------------------
PBR action-group entry: 30
next-Interface: ethernet3, next-hop: 60.60.60.60
------------------------
```

ポリシーベースのルーティングポリシー構成の表示

ポリシーベースのルーティングポリシー構成の詳細を WebUI または CLI から表示できます。CLI では、構成を表示するか、ポリシー名を入力して 1 つのポリシーの構成を表示するか、選択できます。

WebUI

Network > Routing > PBR > Policy

CLI

get vrouter trust-vr pbr policy config

出力例 :

```
set pbr policy name pbr1_policy
set pbr policy pbr1_policy match-group pbr1_mg2 action-group pbr1_ag2 50
set pbr policy pbr1_policy match-group pbr1_mg action-group pbr1_ag 256
```

CLI

get vrouter trust-vr pbr policy name pbr1_policy

出力例 :

```
PBR policy: pbr1_policy in vr: trust-vr number of entries: 2
-----------------------------------------------
PBR policy entry: 50
match-group: pbr1_mg2, action-group: pbr1_ag2
------------------------
PBR policy entry: 256
match-group: pbr1_mg, action-group: pbr1_ag
------------------------
```

完全なポリシーベースのルーティング構成の表示

ポリシーベースのルーティング構成を WebUI または CLI から表示できます。

WebUI

Network > Routing > PBR > Access List Ext
Network > Routing > PBR > Match Group
Network > Routing > PBR > Action Group
Network > Routing > PBR > Policy

CLI

get vrouter trust-vr pbr configuration

出力例 :

```
set access-list extended 1 src-ip 172.16.10.10/32 dest-ip 192.169.10.10/32
dest-port 80-80 protocol tcp entry 1
set access-list extended 1 src-port 200-300 entry 2
set access-list extended 2 dest-port 500-600 protocol udp entry 10
set access-list extended 2 dest-ip 50.50.50.0/24 protocol udp entry 20
set match-group name pbr1_mg
set match-group pbr1_mg ext-acl 1 match-entry 1
set match-group name pbr1_mg2
set match-group pbr1_mg2 ext-acl 2 match-entry 10
set action-group name pbr1_ag
```

```
set action-group pbr1_ag next-interface ethernet2 next-hop 10.10.10.2
action-entry 1
set action-group name pbr1_ag2
set action-group pbr1_ag2 next-hop 30.30.30.30 action-entry 10
set action-group pbr1_ag2 next-interface ethernet3 action-entry 20
set action-group pbr1_ag2 next-interface ethernet3 next-hop 60.60.60.60
action-entry 30
set pbr policy name pbr1_policy
set pbr policy pbr1_policy match-group pbr1_mg2 action-group pbr1_ag2 50
set pbr policy pbr1_policy match-group pbr1_mg action-group pbr1_ag 256
```

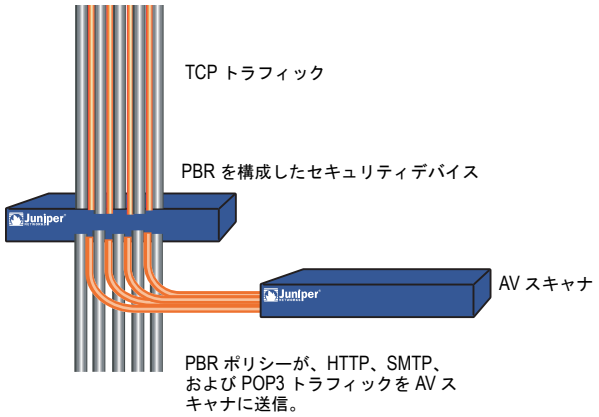
高度な PBR の例

PBR では、ScreenOS が処理する必要のあるタイプのトラフィックだけを定義し、負荷を軽減できます。ウィルス対策（AV）のスキャニングを必要とするトラフィックなど、特定のタイプのトラフィックを処理するときに、ウィルスのスキャンを必要としないパケットタイプをスキャンしてネットワークがボトルネックになる、ということがなくなります。

注： また、アンチスパム、徹底監視（DI）、侵入検出および防止（IDP）、Web フィルタリング、またはキャッシングに特有のトラフィックを送信するよう、PBR を構成できます。

複数のタイプの Juniper Networks セキュリティデバイスを組み合わせて連携させ、サービスを提供しながら、ネットワーク処理速度を高速に、AV スキャニングを管理可能にしておくことができます。Figure 21 は、セキュリティデバイスが、他のすべてのトラフィック（右）から AV トラフィックを分離するため、PBR を実行している様子を示しています。

図 21: トラフィックタイプによる選択的ルーティング



たとえば、PBR を使用して、AV 処理用に HTTP、SMTP、および POP3 トラフィックだけ軽減したい場合、4 つの利用可能な 10/100 インターフェースを持つ少なくとも 1 台のセキュリティデバイスを使用して、ルーティングを行い、1 台のセキュリティデバイスを使用して、アプリケーション（AV）のサポートを提供する必要があります。

注 : 3 つの 10/100 インターフェースしか利用できない場合、2 台のセキュリティデバイスの間にスイッチを置き、VLAN タギング（802.1q）を使用して、トラフィックに同じパスを設定します。

次の例では、次の手順を実行して、ルーティングパスを提供するセキュリティデバイスをセットアップします。

1. ルーティングを構成する。
2. PBR を構成します。
3. PBR ポリシーを適切なインターフェースにバインドします。

次のセクションでは、これらの各手順を説明します。例では、CLI コマンドおよび出力だけを示します。

AV の構成については、*第 4 部 : 攻撃の検出と防衛機能*を参照してください。

ルーティング

この例では、2 つのカスタムゾーンを作成する必要があります。

- trust-vr 用の **av-dmz-1**
- untrust-vr 用の **av-dmz-2**

ゾーンをセットアップするには、次のコマンドを入力します。

```
set zone name av-dmz-1
set zone name av-dmz-2
```

表 15 の情報を使用して、4 つの 10/100 イーサネットインターフェースをセットアップします。

表 15: ルーティング用のインターフェース構成

インターフェース名	ゾーン	Virtual Router	IPv4 アドレス
E1	trust	trust-vr	10.251.10.0/24
E2	av-dmz-1	trust-vr	192.168.100.1/24
E3	av-dmz-2	untrust-vr	192.168.101.1/24
E4	untrust	untrust-vr	172.24.76.127/24

インターフェースをセットアップするには、次のコマンドを入力します。

```
set interface e1 zone trust vrouter trust-vr ip 10.251.10.0/24
set interface e2 zone av-dmz-1 vrouter trust-vr ip 192.168.100.1/24
set interface e3 zone av-dmz-2 vrouter untrust-vr ip 192.168.101.1/24
set interface e4 zone untrust vrouter untrust-vr ip 172.24.76.127/24
```

ゾーン、インターフェース、およびルートをセットアップしたら、次の 2 つのタスクを実行する必要があります。

1. untrust-vr から trust-vr へ静的ルートを構成します。ゲートウェイ IP アドレスに 10.251.10.0/24 を、エントリの優先度値に 20 を割り当てます。

   set vrouter "untrust-vr"
   set route 10.251.10.0/24 vrouter "trust-vr" preference 20
   exit

2. NULL インターフェースを構成します。Trust インターフェースから Untrust インターフェースへ、優先度値に、ゼロより大きな値を割り当てます。

   set vrouter "trust-vr"
   set route 0.0.0.0/0 vrouter "untrust-vr" preference 20
   exit

get route コマンドで、変更を確認できます。

```
Routing Table (ルーティングテーブル):
IPv4 Dest-Routes for <untrust-vr> (6 entries)
------------------------------------------------------------------------------
   ID          IP-Prefix      Interface         Gateway   P Pref    Mtr     Vsys
------------------------------------------------------------------------------
*   6           0.0.0.0/0           eth4     172.24.76.1   C    0      1     Root
*   3      10.251.10.0/24            n/a       trust-vr   S   20      0     Root
*   4      172.24.76.0/22          eth4          0.0.0.0   C    0      0     Root
*   2   192.168.101.1/32          eth3          0.0.0.0   H    0      0     Root
*   5   172.24.76.127/32          eth4          0.0.0.0   H    0      0     Root
*   1   192.168.101.0/24          eth3          0.0.0.0   C    0      0     Root

IPv4 Dest-Routes for <trust-vr> (5 entries)
------------------------------------------------------------
   ID          IP-Prefix      Interface         Gateway   P Pref    Mtr     Vsys
------------------------------------------------------------
*  5           0.0.0.0/0            n/a      untrust-vr    S   20      0     Root
*  1      10.251.10.0/24           eth1          0.0.0.0    C   0      0     Root
*  4    192.168.100.1/32           eth2          0.0.0.0    H   0      0     Root
*  3    192.168.100.0/24           eth2          0.0.0.0    C   0      0     Root
*  2      10.251.10.1/32           eth1          0.0.0.0    H   0      0     Root
```

これで PBR を構成する準備ができました。

PBR 要素

インターフェースおよびルートを構成した後で、PBR を構成します。PBR が正しく機能するためには、trust-vr について次の項目を構成する必要があります。

- 拡張アクセスリスト
- 適合グループ
- アクショングループ
- PBR ポリシー

拡張アクセスリスト

この例では、AV 処理のため、HTTP（ポート 80）、SMTP（ポート 110）、および POP3（ポート 25）のトラフィックを送信します。これらの 3 つのタイプのパケットをセキュリティデバイスに送信するには、trust-vr で拡張アクセスリストをセットアップします。

注 : 戻りトラフィックの拡張アクセスリストはセットアップする必要がありません。セキュリティデバイスは、ルートルックアップの前にセッションルックアップを行ってから、必要に応じて PBR ポリシーを適用するからです。戻りトラフィックには既存のセッションが含まれます。

10.251.10.0/24 サブネットのクライアントが、TCP を使用するポート 80、110、または 25 へのトラフィックを開始すると、ScreenOS に、そのトラフィックを拡張アクセスリストの基準と照合して、アクセスリストに関連付けられたアクションを実行させたいとします。このアクションは、ScreenOS に、指定したように他のトラフィックとは異なるルートへトラフィックをルーティングさせます。各アクセスリストには、対象とする各タイプの TCP トラフィックに 1 つずつ、3 つのエントリが必要です。

trust-vr 用の拡張アクセスリストを構成するには、次のコマンドを入力します。

```
set vrouter "trust-vr"
set access-list extended 10 src-ip 10.251.10.0/24 dest-port 80-80 protocol tcp
    entry 1
set access-list extended 10 src-ip 10.251.10.0/24 dest-port 110-110 protocol
    tcp entry 2
set access-list extended 10 src-ip 10.251.10.0/24 dest-port 25-25 protocol tcp
    entry 3
exit
```

適合グループ

適合グループは、拡張アクセスリストを、PBR ポリシーで参照される意味のある名前と関連付けます。最初に、仮想ルーターのコンテキストを入力して、適合グループを作成し、最後に、新しく作成した適合グループ名をアクセスリストおよびエントリ番号と関連付けるエントリを追加します。

trust-vr で適合グループを作成するには、次のコマンドを入力します。

```
set vrouter trust-vr
set match-group name av-match-trust-vr
set match-group av-match-trust-vr ext-acl 10 match-entry 1
exit
```

アクショングループ

次に、パケットの送信先を示す、アクショングループを作成します。この例では、trust-vr 用のアクショングループを作成します。アクションは、次のホップへトラフィックを送信するように設定します。



注意 : アクションが次のインターフェースへトラフィックを送信する場合、接続状態の変化により、ルーティングポリシーが有効になったり無効になったりします。

次のホップでは、アクションがアドレス解決プロトコル（ARP）を使用して解決します。

trust-vr では、次のコマンドを入力して、次のホップステートメントを持つトラフィックを 192.168.100.254 通ってリダイレクトします。

```
set vrouter trust-vr
set action-group name av-action-redirect-trust-vr set action-group
    av-action-redirect-trust-vr next-hop 192.168.100.254 action-entry 1
exit
```

PBR ポリシー

次に、PBR を定義します。次の要素が必要です。

- PBR ポリシーの名前
- 適合グループ名
- アクショングループ名

PBR ポリシーを構成するには、次のコマンドを入力します。

```
set vrouter trust-vr
set pbr policy name av-redirect-policy-trust-vr
set pbr policy av-redirect-policy-trust-vr match-group av-match-trust-vr
    action-group av-action-redirect-trust-vr 1
exit
```

インターフェースのバインディング

最後に、PBR ポリシーを入口インターフェース e1 にバインドします。

PBR ポリシーをその入口インターフェースにバインドするには、次のコマンドを入力します。

```
set interface e1 pbr av-redirect-policy-trust-vr
```

可用性およびスケーラビリティが高い、高度な PBR

前の PBR の例を基礎として使用し、ネットワークに回復力を追加し、高可用性（HA）やスケーラビリティを実現できます。

回復力のある PBR ソリューション

堅固な PBR ソリューションは、次のデバイス構成を含む場合があります。

- ネットワークを提供する 2 台のセキュリティデバイス
- AV スキャニングを提供する他の 2 台のセキュリティデバイス

デバイスの各ペアは、フォールオーバー保護を提供するため、アクティブ / パッシブ構成で NetScreen 冗長プロトコル（NSRP）を実行します。ルーティングを行う 2 台のセキュリティデバイスでは、ハードウェアの故障が発生した場合、1 台がルーティング機能を引き継ぎます。AV スキャニングを提供するペアの場合、1 台で障害が発生した場合、もう 1 台がスキャニング機能を引き継ぎます。

注 : 詳細については、“ 第 11 部 : 高可用性 ” を参照してください。

スケーラブルな PBR ソリューション

PBR ソリューションは規模を調整できます。容量がさらに必要な場合、セキュリティデバイスを追加できます。/24 サブネットを 2 つの /25 サブネットに分割することにより、下の /25 サブネットと上の /25 サブネットにそれぞれ別の拡張アクセスリストを構成できます。それから、2 台のセキュリティデバイスを追加して、DMZ でのスキャニングサービスを提供します。

アクティブ / アクティブ NSRP 構成を作成した場合、ロードバランスの実装もできます。1 台のデバイスが、下の /25 サブネットからのトラフィックを処理し、もう 1 台のデバイスが、上の /25 サブネットからのトラフィックを処理するようにできます。各デバイスが、もう 1 台のデバイスのバックアップを行います。

第 7 章

マルチキャストルーティング

この章では、マルチキャストルーティングの基本的な概念を紹介します。本章のセクションは、以下のようになります。

- 151 ページの「概要」
  - 152 ページの「マルチキャストアドレス」
  - 152 ページの「逆方向パス転送」
- 153 ページの「セキュリティデバイスによるマルチキャストルーティング」
  - 153 ページの「マルチキャストルーティングテーブル」
  - 154 ページの「静的マルチキャストルートの設定」
  - 155 ページの「アクセスリスト」
  - 155 ページの「トンネルインターフェース上に一般ルーティングのカプセル化を構成する」
- 157 ページの「マルチキャストポリシー」

概要

企業はマルチキャストルーティングを使用して、データや動画ストリームなどのトラフィックを 1 つのソースから受信側のグループへ同時に送信することができるのです。ソースはいずれのホストでも構わず、受信側はインターネット上のどこにあっても構いません。

マルチキャスト対応ルーターは、マルチキャストトラフィックを受信しようとしているホストにのみ転送するため、IP マルチキャストルーティングは複数のホストにトラフィックを送信する効率の良い手段を提供します。各ホストがデータを受信するためには、それを望んでいる旨を通知し、マルチキャストグループに参加する必要があります。マルチキャスト対応ルーターは、マルチキャストトラフィックを受信しようとしているホストにのみ転送します。

マルチキャスト情報を転送するためには、次のような要素を満たすマルチキャストルーティング環境が必要です。

- ホストやルーター間で、マルチキャストグループのメンバーシップ情報をやり取りできること。セキュリティデバイスは IGMP (Internet Group Management Protocol) version 1 ～ 3 に対応しています。ルーターやホストは IGMP を使って、メンバーシップ情報を交換します。トラフィックそのものの伝送には使いません。（IGMP の詳細については、159 ページの「IGMP (Internet Group Management Protocol)」を参照してください。）

- マルチキャストルーティングプロトコル。マルチキャストルーティングテーブルをやり取りし、ネットワークを介してホストにデータを転送するために必要です。Juniper Networks セキュリティデバイスでは、Protocol Independent Multicast - Sparse Mode (PIM-SM) および Protocol Independent Multicast - Source Specific Multicast (PIM-SSM) をサポートします。（PIM-SM および PIM-SSM の詳細については 187 ページの「プロトコル独立マルチキャスト」を参照ください。）

  別法として、IGMP Proxy 機能を使ってマルチキャストトラフィックを伝送することもできます。マルチキャストルーティングプロトコルを稼動させる必要がないので、CPU に対する負荷が増えません。(詳細については、168 ページの「IGMP プロキシ」を参照してください) 。

以下、マルチキャストルーティングに使われている基本的な概念を紹介します。

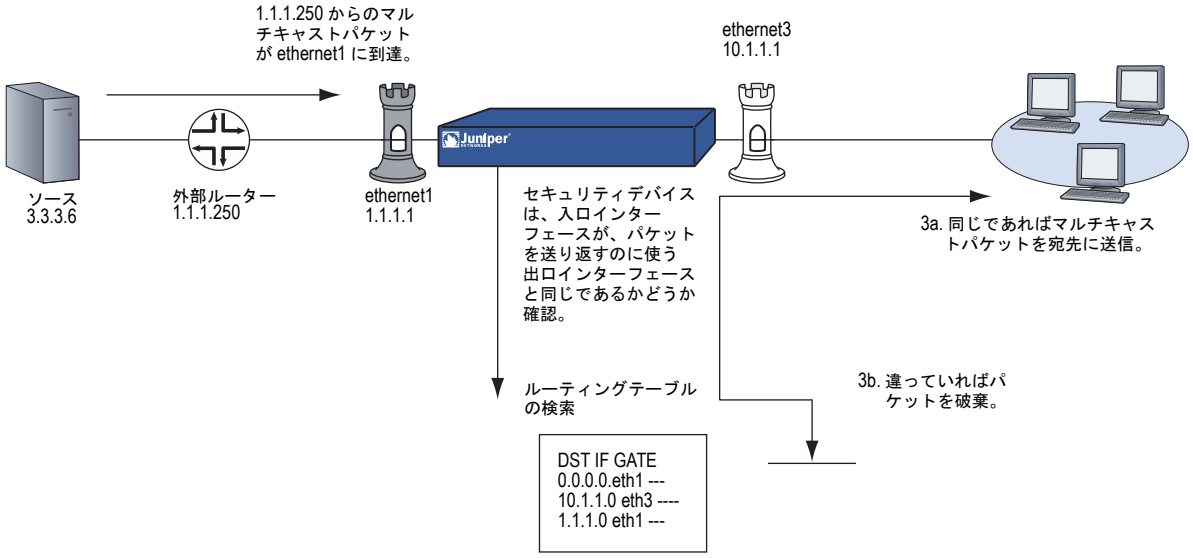
マルチキャストアドレス

マルチキャストトラフィックの宛先は、マルチキャストグループアドレスでなければなりません。これはクラス D に属する、224.0.0.0 ～ 239.255.255.255 の範囲のアドレスです。

逆方向パス転送

マルチキャストルーターは、マルチキャストパケットを受け取ると、逆方向パス転送 (Reverse Path Forwarding、RPF) という処理によりパケットの有効性を確認します。マルチキャストルートを決める前に、ルーターはユニキャストルーティングテーブルを参照して、パケットを受け取るインターフェース (ingress インターフェース) が、送信元にパケットを送り返すためのインターフェースと同じであるかどうかを確認します。同じであればマルチキャストルートのエントリを作成し、次ホップのルーターにパケットを転送します。そうでなければパケットを破棄します。マルチキャストルーターは静的ルートに対しては、この RPF チェックを行いません。図 22 はセキュリティデバイスとマルチキャストパケットプロセスフローを示します。

図 22: 逆方向パス転送



セキュリティデバイスによるマルチキャストルーティング

Juniper Networks セキュリティデバイスには、2 つの定義済み仮想ルーター (VR) があります。trust-vr と untrust-vr です。いずれも、ユニキャスト用、マルチキャスト用のルーティングテーブルを独自に管理している、独立したルーティングコンポーネントです。(ユニキャストルーティングテーブルについては 1 ページの「静的ルーティング」を参照してください。) セキュリティデバイスは、マルチキャストパケットを受け取ると、マルチキャストルーティングテーブルを検索します。

マルチキャストルーティングテーブル

マルチキャストルーティングテーブルの配布には、静的ルートか、マルチキャストルーティングプロトコルにより認識したルートを使います。セキュリティデバイスは、マルチキャストトラフィックを転送するために、マルチキャストルーティングテーブルから得られた情報を使います。セキュリティデバイスは仮想ルーターのルーティングプロトコルごとに、独立にマルチキャストルーティングテーブルを管理しています。

マルチキャストルーティングテーブルには、ルーティングプロトコルに固有の情報に加え、次のような情報が管理されています。

- 各エントリの最初は転送状態を表します。転送状態は、次のいずれかです。(*, G) または (S, G).「(*, G)」という形式は「スター、カンマ、G」と読み、「*」は任意の転送元、「G」は特定のマルチキャストグループのアドレスになります。一方「(S, G)」という形式は「S、カンマ、G」と読み、「S」は転送元 IP アドレス、「G」はマルチキャストグループのアドレスを表します。
- アップストリーム / ダウンストリームインターフェース。
- 逆方向パス転送 (RPF) の近隣ノード。

次に trust-vr 仮想ルーターの PIM-SM マルチキャストルーティングテーブルの例を示します。

```
trust-vr - PIM-SM routing table
------------------------------------------------------------------------------
Register - R, Connected members - C, Pruned - P, Pending SPT Alert - G
Forward - F, Null - N , Negative Cache - E, Local Receivers - L
SPT - T, Proxy-Register - X, Imported - I, SGRpt state - Y, SSM Range Group - S
Turnaround Router - K
------------------------------------------------------------------------------
Total PIM-SM mroutes: 2
(*, 236.1.1.1)  RP 20.20.20.10         00:06:24/-         Flags: LF
  Zone: Untrust
  Upstream        : ethernet1/2         State          : Joined
  RPF Neighbor    : local               Expires        : -
  Downstream      :
  ethernet1/2  00:06:24/00:02:57  Join         0.0.0.0          FC
(20.20.20.200/24, 236.1.1.1)           00:06:24/00:00:36  Flags: TXLF  Register Prune
  Zone: Untrust
  Proxy register  : (10.10.10.1, 238.1.1.1) of zone Trust
  Upstream        : ethernet1/1         State          : Joined
  RPF Neighbor    : local               Expires        : -
  Downstream      :
  ethernet1/2  00:06:24/-         Join         236.1.1.1          20.20.20.200 FC
```

静的マルチキャストルートの設定

ソースからマルチキャストグループへの静的マルチキャストルート (S, G) のほか、ソースまたはマルチキャストグループの一方または両方がワイルドカードになっているルートも定義できます。静的マルチキャストルートは一般に、IGMP ルータープロキシモードのインターフェース上のホストから、IGMP ホストモードのインターフェース上の上流ルーターに、マルチキャストデータを転送するために使います。(詳細については、168 ページの「IGMP プロキシ」を参照してください)。また、ドメイン内マルチキャスト転送にも静的マルチキャストルートが使えます。(S, G) ペアの静的ルートは、どの入力 / 出力インターフェースに対しても作成できます。また、「0.0.0.0」を指定することにより、静的ルートのソースまたはマルチキャストグループをワイルドカードにすることも可能です。静的ルートの出力インターフェースには、本来のマルチキャストグループアドレスに加え、それとは別のマルチキャストグループアドレスを指定することもできます。

この例では、ソース IP アドレス 20.20.20.200 からマルチキャストグループ 238.1.1.1 への静的マルチキャストルートを設定します。セキュリティデバイスの設定により、出力インターフェース上のマルチキャストグループを 238.1.1.1 から 238.2.2.1 に変換します。

WebUI

Network > Routing > MCast Routing > New: 次のように入力してから **OK** をクリックします。

Source IP: 20.20.20.200
MGroup: 238.1.1.1
Incoming Interface: ethernet1 (選択)
Outgoing Interface: ethernet3 (選択)
Translated MGroup: 238.2.2.1

CLI

```
set vrouter trust-vr mroute mgroup 238.1.1.1 source 20.20.20.200 iif ethernet1
    oif ethernet3 out-group 238.2.2.1
save
```

アクセスリスト

アクセスリストは一連のステートメントから成り、これをルート情報と比較するようになっています。各文には、ネットワークプレフィックスの IP アドレス / ネットマスクと、転送を許可するか拒否するかの区別が指定されています。マルチキャストルーティングでは、ステートメントにマルチキャストグループアドレスも指定できます。マルチキャストルーティングでは、特定のマルチキャストグループまたはホストに対するマルチキャストトラフィックだけを許可するよう、アクセスリストで制御できます。したがって、アクションや転送状態は常に Permit になります。あるグループやホストを拒否するようなアクセスリストは作成できません。（アクセスリストに関する詳細情報は 43 ページの「アクセスリストの構成」を参照してください。）

トンネルインターフェース上に一般ルーティングのカプセル化を構成する

マルチキャストパケットをユニキャストパケット内にカプセル化する方法は、マルチキャスト用の設定がなされていないネットワークや、IPSec トンネルを介して、マルチキャストパケットを転送するために広く使われています。Generic Routing Encapsulation (GRE) version 1 は、任意のタイプのパケットを IPv4 ユニキャストパケットにカプセル化するための機構です。Juniper Networks セキュリティデバイスは、IP パケットを IPv4 ユニキャストパケットにカプセル化する、この GREv1 に対応しています。GRE について詳しくは、RFC 1701, *Generic Routing Encapsulation (GRE)* を参照してください。

セキュリティデバイスでは、トンネルインターフェース上で GRE によるカプセル化を有効にするようになっています。

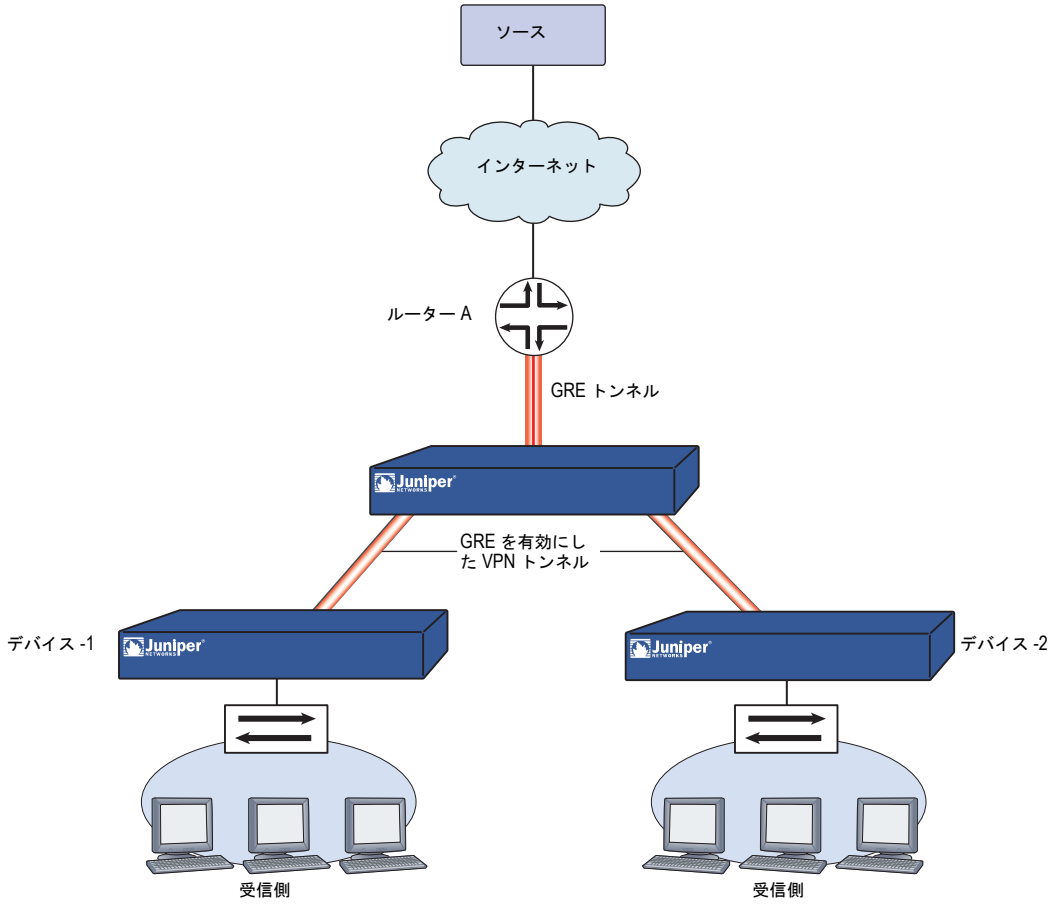
注 : (ループバックインターフェースにバインドされたトンネルインターフェース上で GRE を有効にするためには、このループバックインターフェースが出力インターフェースと同じゾーンになければなりません。ループバックインターフェースについては、**2**-58 ページの「ループバックインターフェース」を参照してください。

マルチキャストパケットを、Juniper Networks セキュリティデバイスと他社製のデバイスやルーターとの間を結ぶ IPSec VPN トンネルを介して転送するためには、GRE を有効にする必要があります。

セキュリティデバイスには、マルチキャストパケットの転送に使う出力インターフェースの数に関して、プラットフォームごとに制限があります。大規模なハブ - スポーク型 VPN 環境で、セキュリティデバイスがハブの位置にある場合は、ハブ側セキュリティデバイスのルーター上流からスポーク側のセキュリティデバイスに GRE トンネルを作成することにより、この制限を回避できます。

図 23 では、Router-A は Device-A の上流です。Router-A は 2 つの GRE トンネルがあり、それは Device-1 と Device-2 で終了します。Device-A は VPN トンネルを介して Device-1 と Device-2 に接続されています。Router-A はマルチキャストパケットを送信する際、これを IPv4 ユニキャストパケットにカプセル化します。Device-A はこれをユニキャストパケットの形で受け取り、Device-1 および Device-2 に送信します。

図 23: トンネルインターフェースの GRE



この例では、Device-1 のトンネルインターフェースを設定します。次の手順を行います。

1. tunnel.1 インターフェースを作成し、ethernet3 および trust-vr 上の Untrust ゾーンにバインドします。
2. tunnel.1 で GRE カプセル化を有効にします。
3. GRE トンネルの起点 (ローカル側) と終点 (リモート側) を指定します。

この例ではセキュリティデバイスの GRE 設定のみ示します。(VPN の詳細については、*第 5 部: 仮想プライベート ネットワーク* を参照してください。)

WebUI

Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (選択)
Interface: ethernet3 (trust-vr)

Network > Interfaces > Tunnel (tunnel.1): 以下を入力して **Apply** をクリックします。

Encap: GRE (選択)
Local Interface: ethernet3
Destination IP: 3.3.3.1

CLI

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
set interface tunnel.1 tunnel encap gre
set interface tunnel.1 tunnel local-if ethernet3 dst-ip 3.3.3.1
save
```

マルチキャストポリシー

デフォルトでは、Juniper Networks セキュリティデバイスは、クロスセキュリティデバイスに対する IGMP や PIM メッセージなど、マルチキャスト制御トラフィックを許可しないようになっています。ゾーン間のマルチキャスト制御トラフィックを許可するためには、マルチキャストポリシーとして次のような事項の設定が必要です。

- **Source** - トラフィックを発するゾーン
- **Destination** - トラフィックの送り先となるゾーン
- **Multicast group** - セキュリティデバイスがマルチキャスト制御トラフィックを許可するようにしたいマルチキャストグループ。次のいずれかで指定します。
  - マルチキャストグループの IP アドレス
  - ホストが参加するマルチキャストグループを定義したアクセスリスト
  - キーワード **any**。どのマルチキャストグループに対するマルチキャスト制御トラフィックをも許可する場合
- **Multicast control traffic** - マルチキャスト制御メッセージのタイプ、IGMP メッセージまたは PIM メッセージがあります。（IGMP の詳細については、159 ページの「IGMP (Internet Group Management Protocol)」を参照してください。）（PIM に関しては、187 ページの「プロトコル独立マルチキャスト」を参照してください。）

さらに次のような事項も指定できます。

- **Translated multicast address** - セキュリティデバイスは、内部ゾーンに属するマルチキャストグループアドレスを、egress インターフェース上の別のアドレスに変換できます。グループアドレスを変換するためには、マルチキャストポリシーでアドレス間の対応（元のマルチキャストアドレスと変換されたマルチキャストグループアドレス）を指定する必要があります。
- **Bi-directional** - 両方向のトラフィックに対して適用する、両方向ポリシーも作成できます。

注： マルチキャストポリシーは、マルチキャスト制御トラフィックのみのフローを制御します。ゾーン間のデータトラフィック (ユニキャスト、マルチキャストとも) を許可するためには、これとは別にファイアウォールポリシーを設定する必要があります。（ポリシーの詳細については、*第 2 部: 基本* を参照してください。）

ファイアウォールポリシーのように、マルチキャストポリシーは、いくつか並べた場合それが順に適用されるわけではありません。相反するポリシーがあっても、新しい方が優先されるのではないのです。そうではなく、最長一致のポリシーを選択するようになっています。これは他のルーティングプロトコルに倣ったものです。要求に合致する、より範囲の狭いサブネットがあれば、それに対応するポリシーを適用します。

注： IGMP メッセージ用のマルチキャストポリシーを設定する例については、173 ページの「IGMP 用のマルチキャストグループポリシーの作成」を参照してください。PIM メッセージ用のマルチキャストポリシーを設定する例については、198 ページの「PIM-SM のマルチキャストグループポリシーの定義」を参照してください。

第 8 章

IGMP (Internet Group Management Protocol)

この章では、Juniper Networks セキュリティデバイスで、IGMP(インターネットグループ管理プロトコル) マルチキャストプロトコルを使う方法について解説します。本章のセクションは、以下のようになります。

- 160 ページの「概要」
  - 161 ページの「ホスト」
  - 161 ページの「マルチキャストルーター」
- 162 ページの「セキュリティデバイスで稼動する IGMP」
  - 162 ページの「BGP をインターフェースで使用可能・不可にする」
  - 163 ページの「ホストの参加を許可するグループを列挙したアクセスリストの設定」
  - 164 ページの「IGMP の構成」
  - 166 ページの「IGMP に関する設定事項の確認」
  - 167 ページの「IGMP 運用パラメータ」
- 168 ページの「IGMP プロキシ」
  - 170 ページの「IGMP プロキシの設定」
  - 171 ページの「インターフェース上で IGMP プロキシを設定する」
  - 173 ページの「IGMP および IGMP プロキシ設定のマルチキャストポリシー」
  - 180 ページの「IGMP 送信元プロキシの設定」

概要

インターネットグループ管理プロトコル (IGMP) マルチキャストプロトコルは、ホストやルーター間で、マルチキャストグループメンバーの確立および維持のために使います。セキュリティデバイスは次の IGMP バージョンをサポートしています。

- IGMPv1: RFC 1112 *Host Extensions for IP Multicasting*に定義されているもので、マルチキャストグループのメンバーシップ情報に関する基本的な操作ができます。
- IGMPv2: RFC 2236 、*Internet Group Management Protocol* 、*Version 2* に定義されており、IGMPv1 の機能を拡張したものです。
- IGMPv3: RFC 3376 、*Internet Group Management Protocol* 、*Version 3* 、に定義されており、ソースフィルタリングの機能が加わっています。IGMPv3 を搭載したホストは、参加するマルチキャストグループやマルチキャストトラフィックを受信するソースを示します。IGMPv3 は、SSM (Source-Specific Multicast) モードで PIM (Protocol Independent Multicast) を稼動させる場合に必要です。(詳細については、194 ページの「PIM-SM」を参照してください) 。

ホストやルーターは IGMP を使って、マルチキャストグループに属するノードを管理できます。PIM などのマルチキャストルーティングプロトコルは、IGMP を使ってメンバーシップ情報を取得し、その情報をマルチキャストルーティングテーブルに追加したり、ネットワークを介してマルチキャストトラフィックをホストに転送したりします。

以下、ホストやルーターが、グループのメンバーシップ情報を維持するためにネットワークを介して交換する、さまざまな IGMP メッセージについて解説します。IGMP の新バージョンが稼動しているホストやルーターは、旧バージョンが動作するホストやルーターとも情報を交換できます。

ホスト

ホストは IGMP メッセージを送ってマルチキャストグループに参加し、その状態を維持します。ルーターは、ローカルネットワークで IGMP メッセージを監視して、どのホストがマルチキャストグループのメンバーか確認します。表 16 はホストが送信する IGMP メッセージおよびその宛先をリストします。

表 16: IGMP ホストメッセージ

IGMP のバージョン	IGMP メッセージ	宛先
IGMPv1 および v2	ホストは、マルチキャストグループに参加する際に IGMP メッセージを送るほか、参加後も定期的に、グループに属している旨のレポートを送信します。IGMP メッセージには、参加しようとするマルチキャストグループのアドレスを記載します。	ホストが参加しようとしているマルチキャストグループの IP アドレス
IGMPv3	ホストは、マルチキャストグループに参加する際に IGMP メッセージを送るほか、参加後も定期的に、グループに属している旨のレポートを送信します。このメッセージにはグループアドレスのほか、フィルタモード (include または exclude)、ソースリストも指定します。フィルタモードが include ならば、ソースリストに記載されいてるアドレスから届いたパケットを受け入れることになります。一方、exclude であれば、ソースリストに記載されていないアドレスからのパケットを受け入れます。	224.0.0.22
IGMPv2	ホストは、マルチキャストグループから離脱し、このグループ宛のデータを受け取らないことにしようとする場合、Leave Group メッセージを送信します。	「すべてのルーター」を表すアドレス (224.0.0.2)

マルチキャストルーター

ルーターは IGMP を使って、ローカルネットワーク上のどのホストがどのマルチキャストグループに属しているかを把握します。各ネットワークはそのための代表ルーターを選びます。これをクエリア (querier) と呼びます。通常、ネットワークごとに 1 台のクエリアがあります。クエリアはネットワーク上の全ホストに IGMP メッセージを送ってメンバーシップ情報を収集します。ホストがグループに属している旨の応答を返せば、ルーターはこれをもとに、グループとこれに属するホストの対応表 (インターフェースごとに管理) を更新します。IGMPv3 対応ルーターは、マルチキャストグループのアドレス、フィルタモード (include または exclude)、ソースリストの表を管理します。

注 : IGMPv1 の場合、ネットワークのクエリアを決めるのは、各マルチキャストルーティングプロトコルです。IGMPv2、v3 の場合は、ネットワーク上で最小の IP アドレスのルーターインターフェースがクエリアになります。

表 17 はクエリアが送信するメッセージおよびその宛先を説明します。

表 17: IGMP クエリアメッセージ

IGMP のバージョン	IGMP メッセージ	[Destination]
IGMPv1、v2、v3	クエリアは定期的に、メンバーシップ情報を問い合わせるためのゼネラルクエリを送ります。	「すべてのホスト」を表すアドレス (224.0.0.1)
IGMPv2、v3	クエリアは、IGMPv2 の Leave Group メッセージ、または所属ノードが変わった旨を表す IGMPv3 のレポートを受け取ると、当該グループに対して問い合わせを送信します。所定の時間内に応答がなければ、ローカルネットワーク上にはそのグループに属するホストがなくなったと看做し、マルチキャストトラフィックの転送を停止します。	ホストが離脱しようとしているマルチキャストグループ
IGMPv3	クエリアは、ある送信元からのトラフィックを受信するホストがグループ内に存在するかどうか確認するため、当該グループ / ソースに対して問い合わせを送信します。	ホストが離脱しようとしているマルチキャストグループ

セキュリティデバイスで稼動する IGMP

マルチキャストルーティングプロトコルを有効にすると、自動的に IGMP が有効になるルーターもあります。しかし Juniper Networks セキュリティデバイスの場合、IGMP と他のマルチキャストルーティングプロトコルは独立で、それぞれ明示的に有効にしなければなりません。

BGP をインターフェースで使用可能・不可にする

デフォルトでは、どのインターフェースでも IGMP は無効になっています。ホストに接続されているインターフェースすべてについて、ルーターモードで IGMP を有効にしなければなりません。セキュリティデバイスは、ルーターモードにすると自動的に IGMPv2 が稼動します。設定変更により、IGMPv1 が稼動する、IGMPv2 および v3 が稼動する、あるいは IGMPv3 のみが稼動するようにすることもできます。

あるインターフェース上で IGMP を稼動させる

この例では、ホストに接続されている ethernet1 インターフェース上で、ルーターモードで IGMP を稼動させます。

WebUI

Network > Interfaces > Edit (ethernet1) > IGMP: 以下を入力して **Apply** をクリックします。

IGMP Mode: Router (選択)
Protocol IGMP: Enable (選択)

CLI

```
set interface ethernet1 protocol igmp router
set interface ethernet1 protocol igmp enable
save
```

インターフェース上の IGMP を停止する

この例では、IGMP をインターフェース ethernet1 で使用不可にします。IGMP に関する設定事項は残したままで無効にします。

WebUI

Network > Interfaces > Edit (ethernet1) > IGMP: **Protocol IGMP Enable** をオフ にし、**Apply** をクリックします。

CLI

```
unset interface ethernet1 protocol igmp enable
save
```

IGMP に関する設定事項を消去したい場合は、**unset interface** *interface* **protocol igmp router** というコマンドを使ってください。

ホストの参加を許可するグループを列挙したアクセスリストの設定

IGMP を稼動させる場合、セキュリティについても考慮しなければなりません。攻撃のために、IGMP クエリやメンバーシップレポート、離脱メッセージを不正に送りつけられる恐れがあります。セキュリティデバイスでは、マルチキャストトラフィックを所定のホストやマルチキャストグループだけに制限することができます。また、ネットワークごとに、クエリアとなりうるルーターを指定することも可能です。この制限は、アクセスリストを作成し、これを各インターフェースに適用することによって行います。

アクセスリストとは、IP アドレスと転送状態（許可 / 拒否の別）を列挙したリストです。IGMP の場合、指定できるのは「**許可**」だけです。IP アドレスとしては次のいずれかを指定します。

- ホストが参加できるマルチキャストグループ
- 送信元ホスト。IGMP ルーターインターフェースに IGMP メッセージを送るホスト
- クエリア。IGMP ルーターインターフェースに IGMP メッセージを送るルーター

次に、作成したアクセスリストを、各インターフェースに適用します。するとそのインターフェースは、アクセスリストに指定されたホストやルーターから届いたトラフィックしか受け付けないようになります。したがって、あるマルチキャストやホスト、クエリアからのトラフィックを拒否するためには、そのアドレスを除外したアクセスリストを用意すればよいことになります。（アクセスリストについて詳しくは 43 ページの「アクセスリストの構成」を参照。）

ここでは trust-vr 上にアクセスリストを作成します。アクセスリストには次のような事項を設定します。

- アクセスリスト ID は 1。
- マルチキャストグループ 224.4.4.1/32 からのトラフィックを許可。
- このステートメントのシーケンス番号は 1。

すると ethernet1 上のホストは、ここに指定されたマルチキャストグループにのみ参加できるようになります。

WebUI

Network > Routing > Virtual Routers > Access List: > New (trust-vr): 次のように入力してから **OK** をクリックします。

Access List ID: 1
Sequence No: 1
IP/Netmask: 224.4.4.1/32
Action: Permit (選択)

Network > Interfaces > Edit (ethernet1) > IGMP: 次のように入力してから **OK** をクリックします。

Accept Group's Access List ID: 1

CLI

```
set vrouter trust-vr access-list 1 permit ip 224.4.4.1/32 1
set interface ethernet1 protocol igmp accept groups 1
save
```

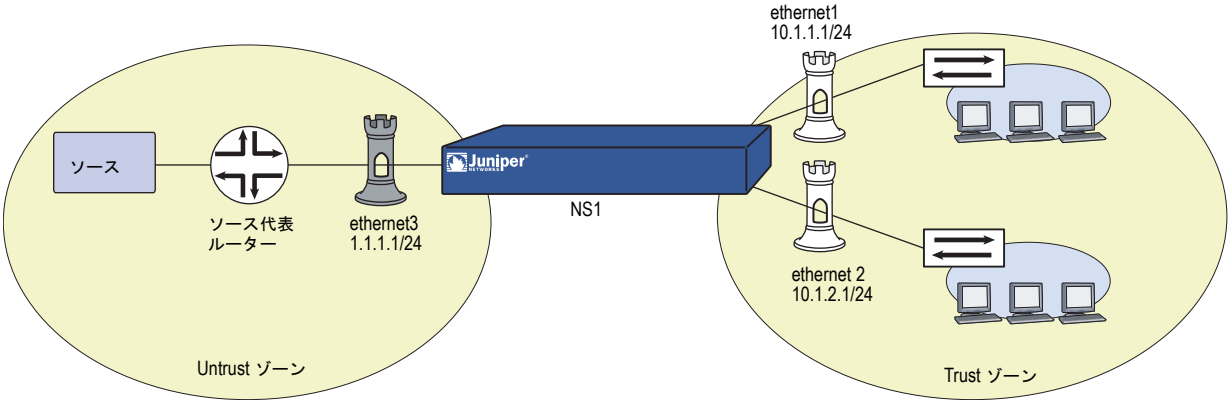
IGMP の構成

セキュリティデバイスで IGMP を稼動させるためには、ホストが直接接続されたインターフェース上で、ルーターモードで IGMP を有効にします。ネットワークのセキュリティを確保するため、アクセスリストを使って、トラフィックを特定のマルチキャストグループ、ホスト、ルーターに制限します。

図 24 では、セキュリティデバイス NS1 で保護された Trust ゾーン上のホストが、Untrust ゾーンからのマルチキャストストリームを受信できるようにします。インターフェース ethernet1 および ethernet2 がホストにつながっています。マルチキャストデータは、マルチキャストグループ 224.4.4.1 に対して送られます。ホストに接続された各インターフェース上で IGMP を設定する手順を示します。

1. インターフェースに IP アドレスを割り当て、ゾーンにバインドします。
2. アクセスリストを作成し、マルチキャストグループ 224.4.4.1/32 を指定します。
3. ethernet1、ethernet2 で、ルーターモードで IGMP を稼動させます。
4. マルチキャストグループ 224.4.4.1/32 からの IGMP メッセージしか受け取らないよう、ethernet1、ethernet2 の各インターフェースを制限します。

図 24: IGMP 構成例



WebUI

1. **ゾーンおよびインターフェース**
   Network > Interfaces > Edit (ethernet1): 次のように入力してから **OK** をクリックします。

   Zone Name: Trust
   IP Address/Netmask: 10.1.1.1/24

   Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

   Zone Name: Trust
   IP Address/Netmask: 10.1.2.1/24

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   IP Address/Netmask: 1.1.1.1/24

2. **アクセスリスト**
   Network > Routing > Virtual Routers > Access List: > New (trust-vr): 次のように入力してから **OK** をクリックします。

   Access List ID: 1
   Sequence No: 1
   IP/Netmask: 224.4.4.1/32
   Action: Permit

3. **IGMP**
   Network > Interfaces > Edit (ethernet1) > IGMP: 以下を入力して **Apply** をクリックします。

   IGMP Mode: Router (選択)
   Protocol IGMP: Enable (選択)
   Accept Group's Access List ID: 1

Network > Interfaces > Edit (ethernet2) > IGMP: 以下を入力して **Apply** をクリックします。

IGMP Mode: Router (選択)
Protocol IGMP: Enable (選択)
Accept Group's Access List ID: 1

CLI

1. **ゾーンおよびインターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet2 zone trust
   set interface ethernet2 ip 10.2.1.1/24

2. **アクセスリスト**
   set vrouter trust access-list 1 permit ip 224.4.4.1/32 1

3. **IGMP**
   set interface ethernet1 protocol igmp router
   set interface ethernet1 protocol igmp accept groups 1
   set interface ethernet1 protocol igmp enable
   set interface ethernet2 protocol igmp router
   set interface ethernet2 protocol igmp accept groups 1
   set interface ethernet2 protocol igmp enable
   save

ethernet1、ethernet2 で IGMP を設定した後、PIM などのマルチキャストルーティングプロコトルで、マルチキャストトラフィックを転送するよう設定します。(PIM に関しては、187 ページの「プロトコル独立マルチキャスト」を参照してください。)

IGMP に関する設定事項の確認

正しく接続され、IGMP が稼動していることを確認するために、何種類かの **exec** コマンドや **get** コマンドが使えます。

- あるインターフェースに対して、ゼネラルクエリや、グループに関する情報の問い合わせを送信するには、**exec igmp interface** *interface* **query** というコマンドを使います。たとえば ethernet2 を介してゼネラルクエリを送信するコマンドは次のようになります。

  exec igmp interface ethernet2 query

  また、ethernet2 からマルチキャストグループ 224.4.4.1 に関する情報を問い合わせる場合は次のようになります。

  exec igmp interface ethernet2 query 224.4.4.1

- あるインターフェース上のメンバーシップレポートを送信するには、**exec igmp interface** *interface* **report** というコマンドを使います。たとえば ethernet2 を介してゼネラルクエリを送信するコマンドは次のようになります。

  exec igmp interface ethernet2 report 224.4.4.1

あるインターフェースの IGMP パラメータは、次のコマンドで表示できます。

```
device-> get igmp interface
Interface trust support IGMP version 2 router.It is enabled.
IGMP proxy is disabled.
Querier IP is 10.1.1.90, it has up 23 seconds.I am the querier.
There are 0 multicast groups active.
    Inbound Router access list number: not set
    Inbound Host access list number: not set
    Inbound Group access list number: not set
    query-interval: 125 seconds
    query-max-response-time 10 seconds
    leave-interval 1 seconds
    last-member-query-interval 1 seconds
```

This output lists the following information:

- IGMP バージョン (2)
- クエリアステータス（自分がクエリアである。）
- パラメータを設定および設定解除する

マルチキャストグループに関する情報は、次の CLI コマンドで表示できます。

```
device-> get igmp group

total groups matched: 1
multicast group  interface    last reporter   expire ver
*224.4.4.1       trust        0.0.0.0         ------ v2
```

IGMP 運用パラメータ

あるインターフェース上で、IGMP をルーターモードで有効にすると、そのインターフェースはクエリアとして動作を始めます。この時点ではデフォルトのパラメータで動作しますが、これは変更可能です。このレベルでパラメータを設定すると、指定したインターフェースにのみ有効です。表 18 はクエリアインターフェースパラメータおよびデフォルトを列挙します。

表 18: IGMP クエリアインターフェースパラメータおよびデフォルト値

IGMP インターフェースパラメータ	説明	デフォルト値
General query interval	クエリアインターフェースが「すべてのホスト」を表すアドレス (224.0.0.1) にゼネラルクエリを送信する時間間隔。	125 秒
Maximum response time	ゼネラルクエリの送信後、応答を待っている最大時間。	10 秒
Last Member Query Interval	グループごとの情報を問い合わせる時間間隔。2 回めのクエリに対して時間内に応答がなければ、当該グループに属するメンバーが、このローカルネットワーク上にはないと看做します。	1 秒

IGMPv2/v3 対応ルーターは、デフォルトでは、router-alert IP オプションつきの IGMP パケットしか受け取らず、そうでないパケットは破棄するようになっています。IGMPv1 パケットにはこのオプションがないので、セキュリティデバイスで IGMPv2/v3 が稼動していれば、このようなパケットをすべて破棄することに

なります。IGMPv1 ルーターとの後方互換性を保つため、この機能を無効にし、IGMP パケットをすべて受け取るようにすることも可能です。たとえば ethernet1 インターフェースで、IGMP パケットをすべて受け取るよう設定する手順は次のようになります。

WebUI

Network > Interfaces > Edit (ethernet1) > IGMP: 次のように選択してから **OK** をクリックします。

Packet Without Router Alert Option: Permit (**選択**)

CLI

```
set interface ethernet1 protocol igmp no-check-router-alert
save
```

IGMP プロキシ

ルーターが IGMP メッセージを監視 / 送信する対象は、直接接続されているホストのみです。ローカルネットワーク以外に IGMP メッセージを転送することはありません。しかし、あるインターフェースで IGMP プロキシ機能を有効にすれば、次ホップのネットワークに IGMP メッセージを転送できます。この機能を使えば、マルチキャストルーティングプロトコルを稼動させるために CPU を消費することなく、上流 (マルチキャストのソース) に IGMP メッセージを転送できます。

セキュリティデバイスで IGMP プロキシを稼動させると、ホストに接続されているインターフェースはルーターとして、また、上流ルーターに接続されているインターフェースはホストとして機能します。ホスト / ルーターインターフェースは一般に、別のゾーンに属します。IGMP メッセージがゾーン間をまたがって受け渡しされるよう、マルチキャストポリシーを設定する必要があります。さらに、マルチキャストデータトラフィックをゾーン間で転送するため、ファイアウォールポリシーも設定しなければなりません。

複数の仮想システムに対応しているデバイスでは、いずれか 1 つのインターフェースをルート仮想システム (vsys)、他のインターフェースを別の独立した vsys で設定しなければなりません。こうしておいて、マルチキャスト制御トラフィックが 2 つの仮想システム間で転送されるよう、マルチキャストポリシーを作成することになります。(仮想システムについて詳しくは、*第 10 部: 仮想 システム* を参照してください。)

IGMP メンバーシップ情報を転送するため、各インターフェースはマルチキャストルーティングテーブルに、どの仮想ルーターがバインドされているかを登録し、受信者からソースへのマルチキャスト配布ツリーを構築します。以下、IGMP ホスト / ルーターがソースに IGMP メンバーシップ情報を転送する手順、マルチキャストデータをソースから受信者に転送する手順を解説します。

メンバーシップレポートをソースに転送する手順

セキュリティデバイスのルーターインターフェースに接続されたホストは、マルチキャストグループに参加するために、メンバーシップレポートを送信します。ルーターインターフェースはこれを受け取ると、当該ホストがマルチキャストグループに登録されているかどうか確認します。その上で、次のいずれかの処理を行います。

- 既に登録済みであれば、レポートを無視します。
- 未登録であれば、グループのマルチキャストポリシーを参照して、レポートをどのゾーンに送ればよいかを確認します。
  - マルチキャストポリシーがない場合は、レポートを転送しません。
  - マルチキャストポリシーがあれば、マルチキャストグループに当該ホストを登録し、ポリシーで指定されたゾーンに属するプロキシホストインターフェースに、メンバーシップレポートを転送します。

プロキシホストインターフェースは、メンバーシップレポートを受け取ると、該当するマルチキャストグループに (*, G) 型エントリがあるかどうか確認します。

- エントリがあれば、ホストインターフェースは対応する egress インターフェースのリストに、ルーターインターフェースを追加します。
- ない場合は新たに作成します。ingress はプロキシホストインターフェース、egress はルーターインターフェースになります。次いでプロキシホストインターフェースは、レポートを上流ルーターに転送します。

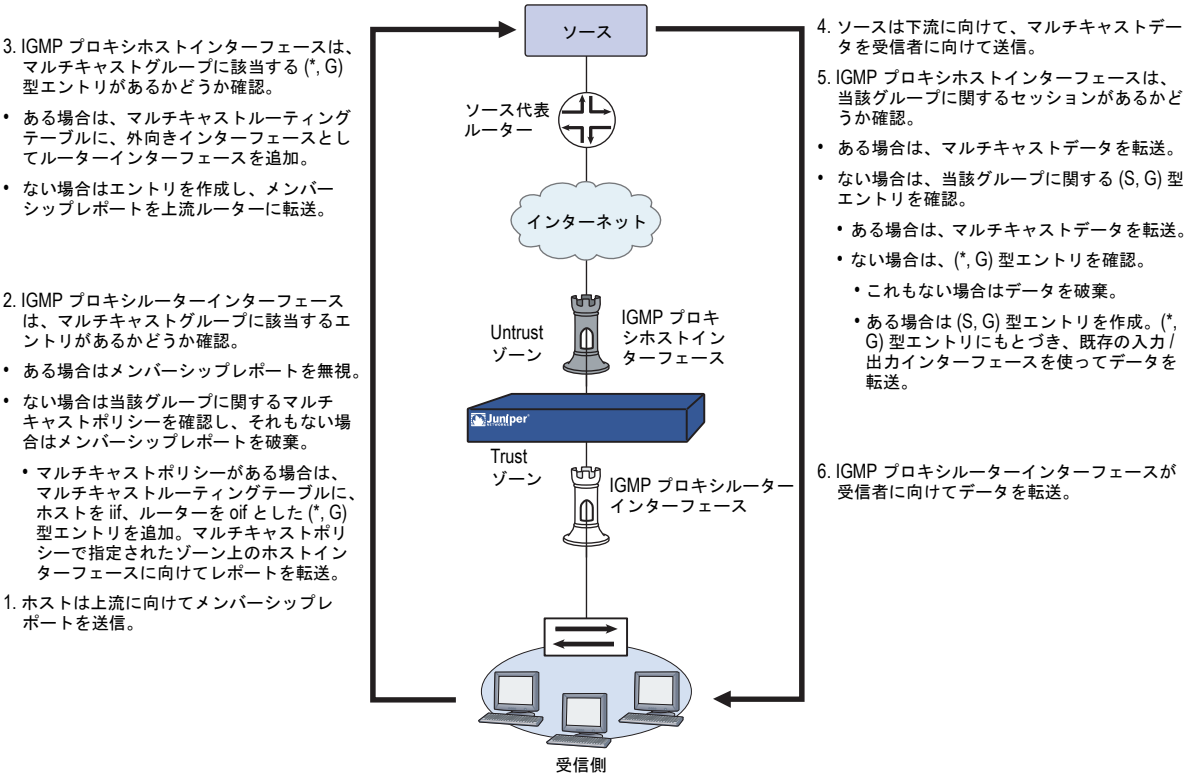
マルチキャストデータを受信者に送る手順

セキュリティデバイスのホストインターフェースは、マルチキャストグループ宛のマルチキャストデータを受け取ると、当該グループと接続するセッションがあるかどうか確認します。

- ある場合は、そのセッション情報にもとづいてデータを転送します。
- ない場合は、マルチキャストルーティングテーブルに (S, G) 型エントリがあるかどうか確認します。
  - ある場合はそれに従ってマルチキャストデータを転送します。
  - ない場合は (*, G) 型エントリがあるかどうか確認します。
  - ない場合はパケットを破棄します。
  - ある場合は、(S, G) 型エントリを作成します。これ以降、同じグループ宛のマルチキャストパケットを受け取ると、インターフェースはこのトラフィックをルーターインターフェース (egress) に転送します。これが最終的に宛先ホストに転送されることになります。

図 25 は IGMP プロキシホスト設定の例です。

図 25: IGMP プロキシホストの設定



IGMP プロキシの設定

ここでは Juniper Networks セキュリティデバイスで IGMP プロキシを設定する基本的な手順を説明します。

1. 上流に向かうインターフェースで、ホストモードで IGMP を有効にします。IGMP プロキシは、ホストインターフェース上で、デフォルトで有効になっています。
2. 下流に向かうインターフェースで、ルーターモードで IGMP を有効にします。
3. ルーターインターフェース上で IGMP プロキシを有効にします。
4. マルチキャスト制御トラフィックがゾーン間で転送されるよう、マルチキャストポリシーを設定します。
5. データトラフィックがゾーン間で転送されるよう、ポリシーを設定します。

インターフェース上で IGMP プロキシを設定する

セキュリティデバイスで IGMP プロキシを稼動させる場合、下流インターフェースはルーターモード、上流インターフェースはホストモードに設定します。(インターフェースはホストモード、ルーターモードのいずれか一方にすることしかできず、兼用はできません。) さらに、マルチキャストトラフィックを転送するルーターインターフェースについては、ローカルネットワークにおけるクエリアとする必要があります。クエリアでないインターフェースを使ってマルチキャストトラフィックを転送するためには、IGMP を有効にする際、**always** というキーワードを指定しなければなりません。

デフォルトでは、IGMP インターフェースはこれが属するサブネット内からの IGMP メッセージのみ受け付けるようになっています。外部ソースからの IGMP メッセージは無視します。IGMP プロキシを稼動させる場合は、他のサブネットからの IGMP メッセージも受け付けるよう、設定を変える必要があります。

この例では、インターフェース ethernet1 の IP アドレスは 10.1.2.1/24 で、ここから上流ルーターに接続されているとします。ethernet1 を次のように設定します。

- IGMP をホストモードで稼動。
- すべてのサブネットからの IGMP メッセージを受け付け。

さらに、インターフェース ethernet3 の IP アドレスが 10.1.1.1/24 で、ホストに接続されているとします。ethernet3 を次のように設定します。

- IGMP をルーターモードで稼動。
- クエリアでなくてもマルチキャストトラフィック転送を許可。
- 他のサブネットからの IGMP メッセージも許可。

WebUI

1. ゾーンおよびインターフェース

Network > Interfaces > Edit (ethernet1): 次のように入力してから **OK** をクリックします。

Zone Name: Trust
IP Address/Netmask: 10.1.2.1/24

Network > Interfaces > Edit (ethernet3): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
IP Address/Netmask: 10.1.1.1/24

2. IGMP

Network > Interfaces > Edit (ethernet1) > IGMP: 以下を入力して **Apply** をクリックします。

IGMP Mode: Host (選択)
Protocol IGMP: Enable (選択)
Packet From Different Subnet: Permit (選択)

Network > Interfaces > Edit (ethernet3) > IGMP: 次のように入力してから **OK** をクリックします。

IGMP Mode: Router (選択)
Protocol IGMP: Enable (選択)
Packet From Different Subnet: Permit (選択)
Proxy: (選択)
Always (選択)

CLI

1. **ゾーンおよびインターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.2.1/24
   set interface ethernet3 zone trust
   set interface ethernet1 ip 10.1.1.1/24

2. **IGMP**
   set interface ethernet1 protocol igmp host
   set interface ethernet1 protocol igmp enable
   set interface ethernet1 protocol igmp no-check-subnet
   set interface ethernet3 protocol igmp router
   set interface ethernet3 protocol igmp proxy
   set interface ethernet3 protocol igmp proxy always
   set interface ethernet3 protocol igmp enable
   set interface ethernet3 protocol igmp no-check-subnet
   save

IGMP および IGMP プロキシ設定のマルチキャストポリシー

セキュリティデバイスは通常、直接接続されたホストとの間でのみ IGMP メッセージを交換します。しかし IGMP プロキシを稼動させた場合、他のゾーンに属するホストやルーターにも IGMP メッセージを送信することになります。そのため、これを許可するようマルチキャストポリシーを設定します。マルチキャストポリシーには次のような事項を指定します。

- **Source** - トラフィックを発するゾーン
- **Destination** - トラフィックの送り先となるゾーン
- **Multicast group** - (単独の) マルチキャストグループ、マルチキャストグループを列挙したアクセスリスト、キーワード any のいずれかを指定

さらに、上流向け、下流向け両方のトラフィックに適用する場合、ポリシーを両方向と指定する必要があります。

IGMP 用のマルチキャストグループポリシーの作成

この例では、ルーターインターフェースは Trust ゾーン、ホストインターフェースは Untrust ゾーンに属するとします。マルチキャストグループ 224.2.202.99/32 に関する IGMP メッセージが、Trust ゾーンと Untrust ゾーンをまたがって転送されるよう、マルチキャストポリシーを設定します。また、bi-directional というキーワードを指定して、両方向のトラフィックに適用されるようにします。

WebUI

MCast Policies (From: Trust, To: Untrust) > New: 次のように入力してから **OK** をクリックします。

MGroup Address: IP/Netmask (選択) 224.2.202.99/32
Bidirectional: (選択)
IGMP Message: (選択)

CLI

```
set multicast-group-policy from trust mgroup 224.2.202.99/32 to untrust
    igmp-message bi-directional
save
```

IGMP プロキシ設定の作成

図 26 では、セキュリティデバイス NS1 および NS2 で、IGMP プロキシの設定をします。この 2 つは VPN トンネル経由でつながっています。それぞれについて、次の手順で設定します。

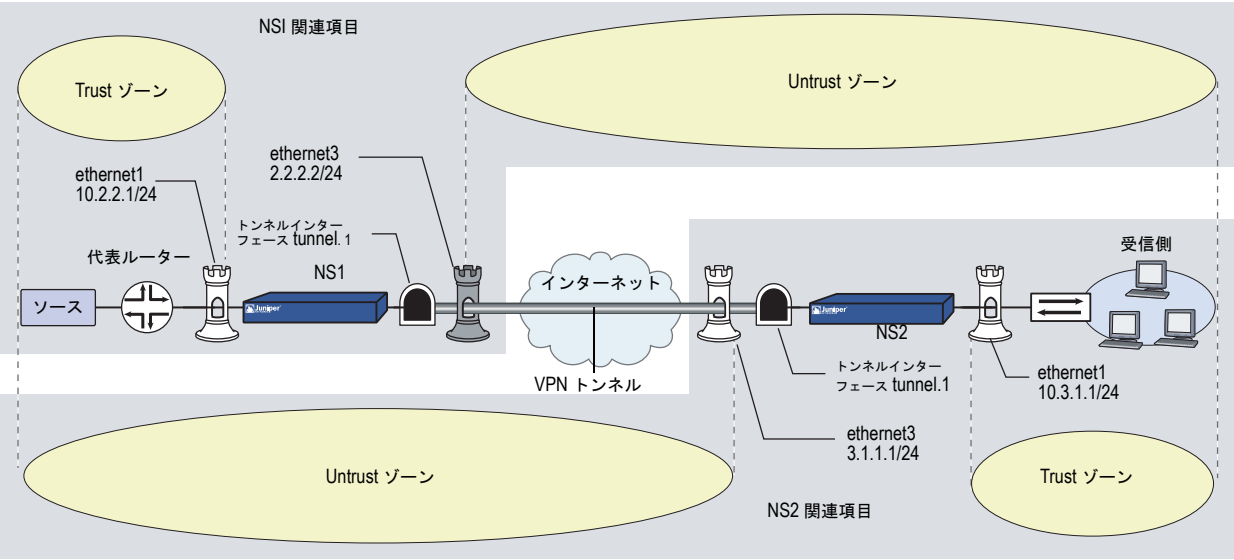
1. セキュリティゾーンにバインドされている物理インターフェースに IP アドレスを割り当てます。
2. アドレスオブジェクトを作成します。
3. ホストインターフェース、ルーターインターフェースで IGMP を有効にし、ルーターインターフェースでは IGMP プロキシも有効にします。(IGMP プロキシは、ホストインターフェース上で、デフォルトで有効になっています。)

a. NS1 の ethernet1 では、キーワード **always** を指定して、クエリアでなくてもマルチキャストトラフィックを転送するようにします。

b. デフォルトでは、IGMP インターフェースはこれが属するサブネット内からの IGMP パケットのみ受け付けるようになっています。この例では、インターフェースはそれぞれ別のサブネットに属します。IGMP を有効にする際、どのサブネットからの IGMP パケット (問い合わせ、メンバーシップレポート、離脱メッセージなど) でも受け付けるようインターフェースを設定します。

4. ルートを設定します。
5. VPN トンネルの設定をします。
6. データトラフィックがゾーン間で転送されるよう、ファイアウォールポリシーを設定します。
7. IGMP メッセージをゾーン間で受け渡しするよう、マルチキャストポリシーを設定します。この例では、マルチキャストトラフィックをマルチキャストグループ (224.4.4.1/32) だけに制限します。

図 26: 2 つのデバイス間の IGMP プロキシの設定



WebUI (NS1)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.2.2.1/24
次のように選択してから **OK** をクリックします。
Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (選択)
Interface: ethernet3 (trust-vr)

2. アドレス

Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

Address Name: branch
IP Address/Domain Name:
IP/Netmask: (選択), 10.3.1.0/24
Zone: Untrust

3. IGMP

Network > Interfaces > Edit (ethernet1) > IGMP: 以下を入力して **Apply** をクリックします。

IGMP Mode: Host (選択)
Protocol IGMP: Enable (選択)
Packet From Different Subnet: Permit (選択)

Network > Interfaces > Edit (tunnel.1) > IGMP: 以下を入力して **Apply** をクリックします。

IGMP Mode: Router (選択)
Protocol IGMP: Enable (選択)
Packet From Different Subnet: Permit (選択)
Proxy (選択): Always (選択)

4. ルート

Network > Routing > Routing Entries > New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.3.1.0/24
Gateway (選択):
Interface: tunnel.1 (選択)

5. VPN

VPN > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: To_Branch
Security Level: Compatible
Remote Gateway Type:
Static IP Address: (選択), IP Address/Hostname: 3.1.1.1
Preshared Key: fg2g4h5j
Outgoing Interface: ethernet3

> > Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Compatible
Phase 1 Proposal (Compatible Security Level): pre-g2-3des-sha
Mode (Initiator): Main (ID Protection)

6. **ポリシー**
   Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

   Source Address:
   　Address Book Entry: (選択), branch
   Destination Address:
   　Address Book Entry: (選択), any (選択)
   Service: any
   Action: Permit

7. **マルチキャストポリシー**
   MCast Policies > (From: Trust, To: Untrust) > New: 次のように入力してから **OK** をクリックします。

   MGroup Address: IP/Netmask (選択): 224.4.4.1/32
   Bidirectional: (選択)
   IGMP Message: (選択)

WebUI (NS2)

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 次のように入力してから **OK** をクリックします。

   Zone Name: Trust
   IP Address/Netmask: 10.3.1.1/24

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   IP Address/Netmask: 3.1.1.1/24

   Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

   Tunnel Interface Name: tunnel.1
   Zone (VR): Untrust (trust-vr)
   Unnumbered: (選択)
   　Interface: ethernet3 (trust-vr)

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

   Address Name: mgroup1
   IP Address/Domain Name:
   　IP/Netmask: (選択), 224.4.4.1/32
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

   Address Name: source-dr
   IP Address/Domain Name:
   　IP/Netmask: (選択), 10.2.2.1/24
   Zone: Untrust

3. IGMP

Network > Interfaces > Edit (ethernet1) > IGMP: 以下を入力して **Apply** をクリックします。

IGMP Mode: Router (選択)
Protocol IGMP: Enable (選択)
Proxy (選択): Always (選択)

Network > Interfaces > Edit (tunnel.1) > IGMP: 以下を入力して **Apply** をクリックします。

IGMP Mode: Host (選択)
Protocol IGMP: Enable (選択)
Packet From Different Subnet: Permit (選択)

4. ルート

Network > Routing > Routing Entries > New (trust-vr): 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.2.2.0/24
Gateway (選択):
Interface: tunnel.1 (選択)

5. VPN

VPN > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: To_Corp
Security Level: Compatible
Remote Gateway Type:
Static IP Address: (選択), IP Address/Hostname: 1.1.1.1
Preshared Key: fg2g4hvj
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Compatible
Phase 1 Proposal (Compatible Security Level): pre-g2-3des-sha
Mode (Initiator): Main (ID Protection)

6. ポリシー

Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), source-dr
Destination Address:
Address Book Entry: (選択), mgroup1
Service: ANY
Action: Permit

7. **マルチキャストポリシー**
   MCast Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

   MGroup Address: IP/Netmask (選択): 224.4.4.1/32
   Bidirectional: (選択)
   IGMP Message: (選択)

CLI (NS1)

1. **インターフェース**
   Set interface ethernet1 zone trust
   set interface ethernet1 ip 10.2.2.1/24
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 2.2.2.2/24
   set interface tunnel.1 zone untrust
   set interface tunnel.1 ip unnumbered interface ethernet3

2. **アドレス**
   set address untrust branch1 10.3.1.0/24

3. **IGMP**
   set interface ethernet1 protocol igmp host
   set interface ethernet1 protocol igmp enable
   set interface ethernet1 protocol igmp no-check-subnet
   set interface tunnel.1 protocol igmp router
   set interface tunnel.1 protocol igmp proxy
   set interface tunnel.1 protocol igmp proxy always
   set interface tunnel.1 protocol igmp enable
   set interface tunnel.1 protocol igmp no-check-subnet

4. **ルート**
   set route 10.3.1.0/24 interface tunnel.1

5. **VPN トンネル**
   set ike gateway To_Branch address 3.1.1.1 main outgoing-interface ethernet3
   preshare fg2g4h5j proposal pre-g2-3des-sha
   set vpn Corp_Branch gateway To_Branch sec-level compatible
   set vpn Corp_Branch bind interface tunnel.1
   set vpn Corp_Branch proxy-id local-ip 10.2.2.0/24 remote-ip 10.3.1.0/24 any

6. **ポリシー**
   set policy name To_Branch from untrust to trust branch1 any any permit

7. **マルチキャストポリシー**
   set multicast-group-policy from trust mgroup 224.4.4.1/32 to untrust
   igmp-message bi-directional
   save

CLI (NS2)

1. **インターフェース**
   Set interface ethernet1 zone trust
   set interface ethernet1 ip 10.3.1.1/24
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 3.1.1.1/24
   set interface tunnel.1 zone untrust
   set interface tunnel.1 ip unnumbered interface ethernet3

2. **アドレス**
   set address trust mgroup1 224.4.4.1/32
   set address untrust source-dr 10.2.2.1/24

3. **IGMP**
   set interface ethernet1 protocol igmp router
   set interface ethernet1 protocol igmp proxy
   set interface ethernet1 protocol igmp proxy always
   set interface ethernet1 protocol igmp enable
   set interface tunnel.1 protocol igmp host
   set interface tunnel.1 protocol igmp enable
   set interface tunnel.1 protocol igmp no-check-subnet

4. **ルート**
   set route 10.2.2.0/24 interface tunnel.1

5. **VPN トンネル**
   set ike gateway To_Corp address 2.2.2.2 main outgoing-interface ethernet3
   preshare fg2g4hvj proposal pre-g2-3des-sha
   set vpn Branch_Corp gateway To_Corp sec-level compatible
   set vpn Branch_Corp bind interface tunnel.1
   set vpn Branch_Corp proxy-id local-ip 10.3.1.0/24 remote-ip 10.2.2.0/24 any

6. **ポリシー**
   set policy from untrust to trust source-dr mgroup1 any permit

7. **マルチキャストポリシー**
   set multicast-group-policy from untrust mgroup 224.4.4.1/32 to trust
   igmp-message bi-directional
   save

IGMP 送信元プロキシの設定

IGMP プロキシを使うと、マルチキャストトラフィックは通常、ホストインターフェース (上流) からルーターインターフェース (下流) に流れます。ソースがルーターインターフェースと同じネットワーク上にある場合もあります。IGMP ルータープロキシインターフェースと同じネットワークにあるインターフェースに接続されたソースがマルチキャストトラフィックを送信する場合、セキュリティデバイスは次の点を確認します。

- マルチキャストグループポリシーにより、ソースゾーンから IGMP プロキシホストインターフェースのゾーンへのトラフィックが許可されていること
- アクセスリストに正当なソースとして登録されていること

ソースゾーンとプロキシ IGMP インターフェースのゾーンとの間にマルチキャストポリシーがない、あるいはソースがアクセスリストに載っていない場合、セキュリティデバイスはトラフィックを破棄します。ソースゾーンとプロキシ IGMP インターフェースのゾーンとの間にマルチキャストポリシーがあり、しかもソースがアクセスリストに載っている場合、デバイスはマルチキャストルーティングテーブルに、当該インターフェースに対する (S, G) 型エントリを追加します。入力インターフェースはソースがつながっているインターフェース、出力インターフェースは IGMP プロキシホストインターフェースになります。次いでセキュリティデバイスは、IGMP プロキシホストインターフェースにデータを送ります。データはここからすべてのプロキシルーターインターフェースに送られることになります (インターフェースがソースにつながっている場合を除く)。

図 27 は送信元プロキシの例です。

図 27: IGMP 送信元プロキシ

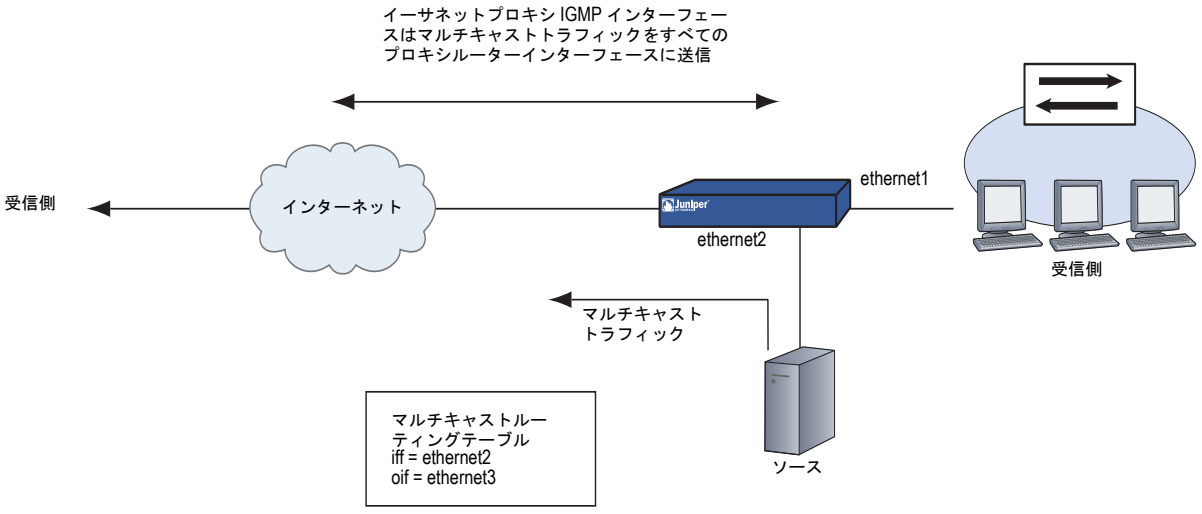
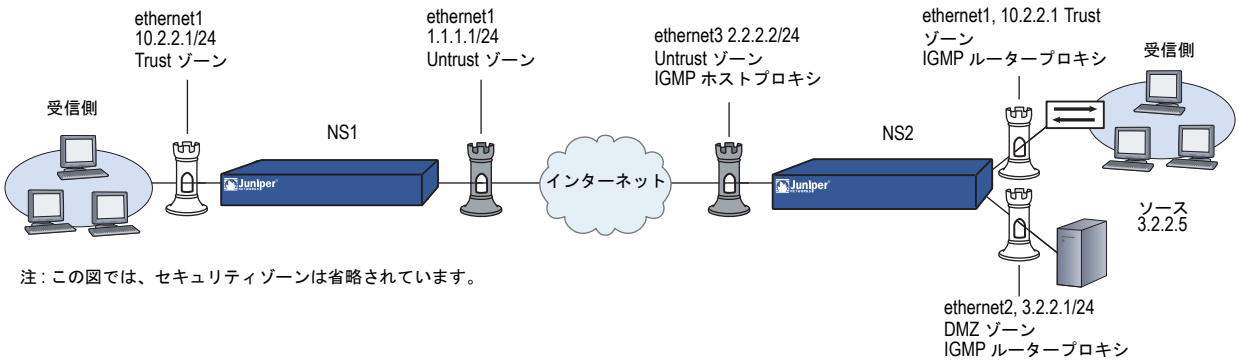


図 28 では、ソースが ethernet2 インターフェースにつながり、これが NS2 の DMZ ゾーンにバインドされているとします。そこでは、マルチキャストトラフィックがマルチキャストグループ 224.4.4.1/32 に送信されます。そして NS2 上の Trust ゾーンにバインドされている ethernet1 インターフェースに受信者が接続されています。ethernet1、ethernet2 とも、IGMP プロキシルーターインターフェースです。NS2 の Untrust ゾーンにバインドされた ethernet3 インターフェースは、IGMP プロキシホストインターフェースです。NS1 の Trust ゾーンにバインドされた、ethernet1 インターフェースに接続されている受信者もいます。NS2 上で次のように操作します。

1. セキュリティゾーンにバインドされているインターフェースに IP アドレスを割り当てます。
2. アドレスオブジェクトを作成します。
3. ethernet1、ethernet2 を次のように設定します。
   a. IGMP をルーターモードで有効にし、IGMP プロキシも有効にします。
   b. キーワード **always** を指定して、クエリアでなくてもマルチキャストトラフィックを転送するようにします。
4. ethernet3 では、ホストモードで IGMP を有効にします。
5. デフォルトルートを設定します。
6. ゾーン間のファイアウォールポリシーを設定します。
7. ゾーン間のマルチキャストポリシーを設定します。

注 : この例では NS2 の設定手順のみ示します。NS1 の設定手順には触れていません。

図 28: IGMP 送信元プロキシネットワーク例



WebUI (NS2)

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.2.2.1/24
   次のように選択してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

   Zone Name: DMZ
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 3.2.2.1/24

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 2.2.2.2/24

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

   Address Name: mgroup1
   IP Address/Domain Name:
   IP/Netmask: (選択), 224.4.4.1/32
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

   Address Name: source-dr
   IP Address/Domain Name:
   IP/Netmask: (選択), 3.2.2.5/32
   Zone: DMZ

   Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

   Address Name: proxy-host
   IP Address/Domain Name:
   IP/Netmask: (選択), 2.2.2.2/32
   Zone: Untrust

3. IGMP

Network > Interfaces > Edit (ethernet1) > IGMP: 以下を入力して **Apply** をクリックします。

IGMP Mode: Router (選択)
Protocol IGMP: Enable (選択)
Proxy (選択): Always (選択)

Network > Interfaces > Edit (ethernet2) > IGMP: 以下を入力して **Apply** をクリックします。

IGMP Mode: Router (選択)
Protocol IGMP: Enable (選択)
Proxy (選択): Always (選択)

Network > Interfaces > Edit (ethernet3) > IGMP: 以下を入力して **Apply** をクリックします。

IGMP Mode: Host (選択)
Protocol IGMP: Enable (選択)
Packet From Different Subnet: Permit (選択)

4. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
    Interface: ethernet3
    Gateway IP Address: 2.2.2.250

5. ポリシー

Policies > (From: DMZ, To: Trust) > New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: source-dr
Destination Address:
    Address Book Entry: (選択), mgroup1
Service: ANY
Action: Permit

Policies > (From: DMZ, To: Untrust) > New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), source-dr
Destination Address:
    Address Book Entry: (選択), mgroup1
Service: ANY
Action: Permit

Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), proxy-host
Destination Address:
Address Book Entry: (選択), mgroup1
Service: ANY
Action: Permit

6. マルチキャストポリシー

MCast Policies > (From: DMZ, To: Untrust) > New: 次のように入力してから **OK** をクリックします。

MGroup Address: IP/Netmask (選択): 224.4.4.1/32
Bidirectional: (選択)
IGMP Message: (選択)

MCast Policies > (From: DMZ, To: Trust) > New: 次のように入力してから **OK** をクリックします。

MGroup Address: IP/Netmask (選択): 224.4.4.1/32
Bidirectional: (選択)
IGMP Message: (選択)

MCast Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

MGroup Address: IP/Netmask (選択): 224.4.4.1/32
Bidirectional: (選択)
IGMP Message: (選択)

CLI (NS2)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat
set interface ethernet2 zone dmz
set interface ethernet2 ip 3.2.2.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
```

2. アドレス

```
set address trust mgroup1 224.4.4.1/32
set address dmz source-dr 3.2.2.5/32
set address untrust proxy-host 2.2.2.2/32
```

3. IGMP

```
set interface ethernet1 protocol igmp router
set interface ethernet1 protocol igmp proxy always
set interface ethernet1 protocol igmp enable
set interface ethernet2 protocol igmp router
set interface ethernet2 protocol igmp proxy always
set interface ethernet2 protocol igmp enable
set interface ethernet3 protocol igmp host
set interface ethernet3 protocol igmp no-check-subnet
set interface ethernet3 protocol igmp enable
```

4. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250

5. **ポリシー**
   set policy from dmz to trust source-dr mgroup1 any permit
   set policy from dmz to untrust source-dr mgroup1 any permit
   set policy from untrust to trust proxy-host mgroup1 any permit

6. **マルチキャストポリシー**
   set multicast-group-policy from dmz mgroup 224.4.4.1/32 to untrust
   igmp-message bi-directional
   set multicast-group-policy from dmz mgroup 224.4.4.1/32 to trust igmp-message
   bi-directional
   set multicast-group-policy from trust mgroup 224.4.4.1/32 to untrust
   igmp-message bi-directional
   save

第 9 章

プロトコル独立マルチキャスト

本章では、Juniper Networks セキュリティデバイス上のプロトコル独立マルチキャスト (PIM) について説明します。本章のセクションは、以下のようになります。

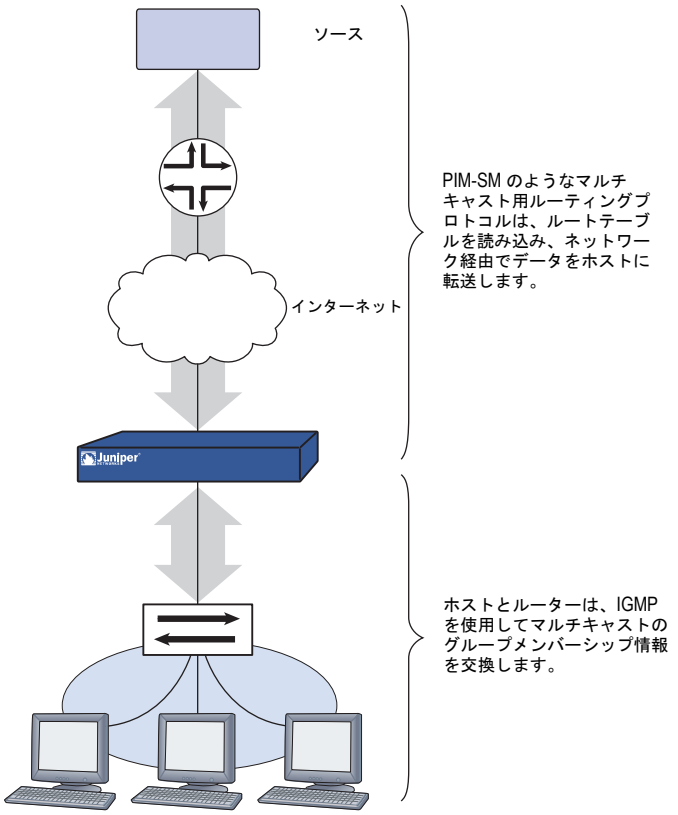
- 188 ページの「概要」
  - 190 ページの「PIM-SM」
  - 190 ページの「マルチキャスト配布ツリー」
  - 191 ページの「代表ルーター」
  - 191 ページの「集合地点のグループへのマッピング」
  - 192 ページの「配布ツリーでのトラフィックの転送」
- 195 ページの「セキュリティデバイスで PIM-SM を構成する方法」
  - 195 ページの「VR 上に PIM-SM インスタンスを有効にし、削除します。」
  - 196 ページの「PIM-SM をインターフェースで使用可能・不可にする」
  - 197 ページの「マルチキャストグループポリシー」
- 198 ページの「PIM-SM の基本設定」
- 203 ページの「設定内容の確認」
- 205 ページの「集合地点の設定」
  - 205 ページの「静的集合地点の設定」
  - 206 ページの「Candidate 集合地点の設定」
- 207 ページの「セキュリティ検討事項」
  - 207 ページの「マルチキャストグループの制限」
  - 208 ページの「マルチキャストソースの制限」
  - 209 ページの「集合地点の制限」

- 210 ページの「PIM-SM インターフェースパラメータ」
  - 210 ページの「Neighbor Policy を定義する」
  - 211 ページの「Bootstrap Border を定義する」
- 212 ページの「プロキシ集合地点の設定」
- 221 ページの「PIM-SM および IGMPv3」

概要

プロトコル独立マルチキャスト (PIM) とは、ルーター間で動作するマルチキャスト用のルーティングプロトコルです。インターネットグループ管理プロトコル IGMP (IGMP) がホストとルーター間で動作して、マルチキャストのグループメンバーシップ情報を交換するのに対し、PIM はルーター間で動作して、ネットワーク経由でマルチキャストトラフィックをマルチキャストグループのメンバーに転送します（IGMP の詳細については、159 ページの「IGMP (Internet Group Management Protocol)」を参照してください。）

図 29: IGMP



PIM を利用する場合は、静的ルートか動的ルーティングプロトコルのいずれかを設定しなければなりません。PIM が*プロトコルから独立*とされる理由は、ユニキャストルーティングを基本とするルーティングテーブルを使用して RPF (reverse path forwarding) チェックを実行しているにもかかわらず、ユニキャストルーティングプロトコルの機能には依存していないためです (RPF の詳細については、152 ページの「逆方向パス転送」を参照してください)。

PIM は以下のモードで動作します。

- PIM-DM (PIM-Dense Mode) では、ネットワーク経由でマルチキャストトラフィックをフラッドして、受信を希望しない受信側へのルートを取り除きます。
- PIM-Sparse Mode (PIM-SM) では、要求を出した受信側にのみマルチキャストトラフィックを転送します。PIM-SM で稼働しているルーターは、共有パスツリーまたは最短パスツリー (SPT) を利用して、マルチキャスト情報を転送します (詳細については、190 ページの「マルチキャスト配布ツリー」を参照してください) 。
- PIM-Source Specific Multicast Mode (PIM-SSM) は、PIM-SM の派生モードです。PIM-SM 同様、受信しようとしている受信側にのみマルチキャストトラフィックを転送します。PIM-SM と異なる点は、直ちにソースへの SPT を確立することです。

  Juniper Networks セキュリティデバイスは、*draft-ietf-pim-sm-v2-new-06* に定義されるように PIM-SM に対応しています。また、RFC 3569 、*Source-Specific Multicast (SSM) の概要*に定義されるように PIM-SSM にも対応しています。PIM-SM についての情報は、「PIM-SM」を参照してください。PIM-SSM についての情報は、194 ページの「PIM-SM」を参照してください。

PIM-SM

PIM-SM は、受信しようとしている受信側にのみマルチキャストトラフィックを転送する、マルチキャスト用ルーティングプロトコルです。共有配布ツリーまたは最短パスツリー (SPT) を利用して、ネットワーク経由でマルチキャストトラフィックを転送します (マルチキャスト配布ツリーの詳細については、190 ページの「マルチキャスト配布ツリー」を参照してください。) デフォルトでは、PIM-SM は ツリーのルートに集合地点 (RP) のある共有配布ツリーを使用します。グループ内のソースはすべて、RP にパケットを送信し、RP はネットワーク内のすべての受信側への共有配布ツリーにデータを送信します。構成されたしきい値に達すると、受信側はソースへの SPT を確立して、マルチキャストデータの受信に要する時間を短縮します。

注 : デフォルトでは、Juniper Networks セキュリティデバイスは最初のバイトを受信すると、SPT に切り替わります。

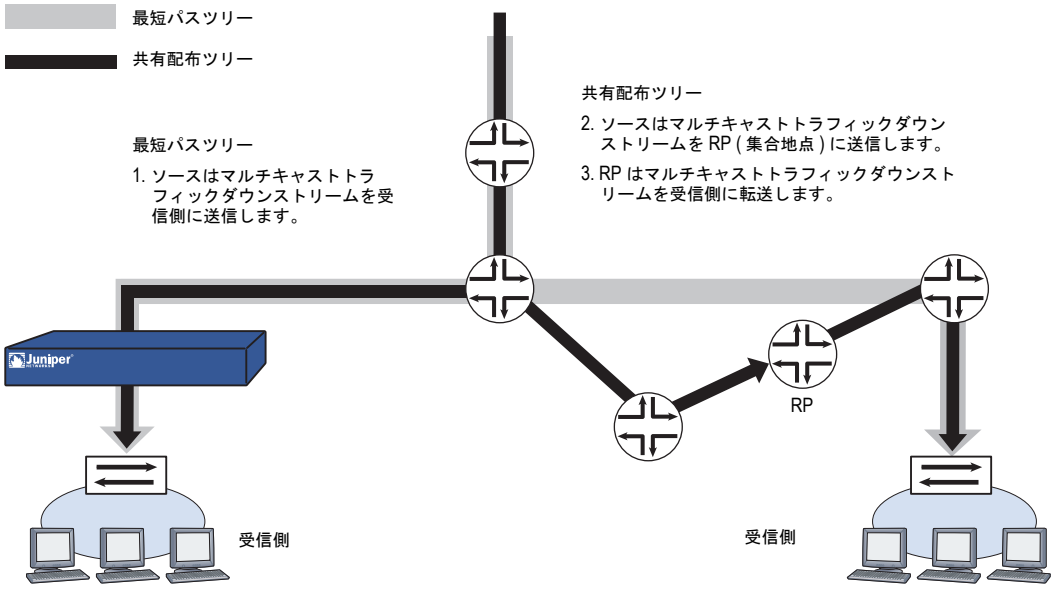
配布トラフィックに使用されるツリーに関係なく、マルチキャストグループに明示的に参加している受信側のみがそのグループのトラフィックを受信できます。PIM-SM はユニキャストルートテーブルを使用して、マルチキャスト制御メッセージを受信すると reverse path forwarding (RPF) ルックアップを実行し、同時に、受信側に対してマルチキャストデータトラフィックを送信します。

マルチキャスト配布ツリー

マルチキャストルーターは、マルチキャスト配布ツリーを経由して、ソースから受信側にマルチキャストトラフィックダウンストリームを転送します。マルチキャスト配布ツリーには、次の 2 種類があります。

- 最短パスツリー (SPT) - 送信元はツリーのルートにあり、各受信側にマルチキャストデータダウンストリームを転送します。これは、source-specific tree とも呼ばれます。
- 共有配布ツリー - ソースは、通常ネットワークコアに置かれたルーターにある集合地点 (RP) にマルチキャストトラフィックを送信します。そして、RP は配布ツリー上の受信側に対してトラフィックダウンストリームを転送します。

図 30: PIM



代表ルーター

マルチアクセス LAN (ローカルエリアネットワーク) にマルチキャストルーターが複数ある場合、ルーターは 代表ルーター (DR) を選択します。ソースの LAN 上にある DR が、マルチキャストパケットをソースから RP と source-specific 配布ツリー上の受信側に送信する役割を果たします。一方、受信側の LAN 上にある DR は、受信側から RP に join-prune メッセージを転送し、LAN の受信側にマルチキャストデータトラフィックを送信する役割を果たしています。受信側は、マルチキャストグループに参加したり、抜ける場合に、join-prune メッセージを送信します。

DR は選定プロセスを経て選択されます。LAN の PIM-SM ルーターにはそれぞれ、ユーザーが設定可能な DR 優先順位が付いています。PIM-SM ルーターは、DR の優先順位について、隣接ノードを定期的に送信しているハローメッセージで通知します。ルーターはハローメッセージを受信すると、最も優先順位の高いルーターを LAN の DR として選択します。優先順位の高いルーターが複数ある場合は、IP アドレスの最も高いルーターが DR となります。

集合地点のグループへのマッピング

集合地点 (RP) は特定のマルチキャストグループにマルチキャストパケットを送信します。PIM-SM ドメインとは、RP グループの同一マッピングを持つ PIM-SM ルーターのグループです。マルチキャストグループを RP にマッピングするには、静的手法および動的手法の 2 通りがあります。

静的 RP マッピング

RP とマルチキャストグループ間の静的マッピングを作成するには、ネットワークの各ルーター上のマルチキャストグループに RP を設定しなければなりません。RP のアドレスが変わるたびに、RP のアドレスを再設定してください。

動的 RP マッピング

PIM-SM には、マルチキャストグループへの動的 RP マッピングを行うメカニズムもあります。最初に、各マルチキャストグループの candidate rendezvous points (C-RPs) を設定します。次に、C-RP は、LAN 上にあるブートストラップルーター (BSR) と呼ばれるルーターに Candidate-RP 通知を送信します。通知には、RP となるルーターおよび C-RP の優先順位のマルチキャストグループが含まれています。

BSR は、こうした C-RP 通知を収集し、BSR メッセージに入れて、ドメイン内の全ルーターに送信します。ルーターは BSR メッセージを収集すると、有名なハッシュアルゴリズムを使って、マルチキャストグループごとにアクティブな RP を 1 つ選択します。選択した RP が失敗すると、ルーターは candidate RP の中から新しい RP グループマッピングを選択します。BSR の選定プロセスの詳細については、*draft-ietf-pim-sm-bsr-03.txt* を参照してください。

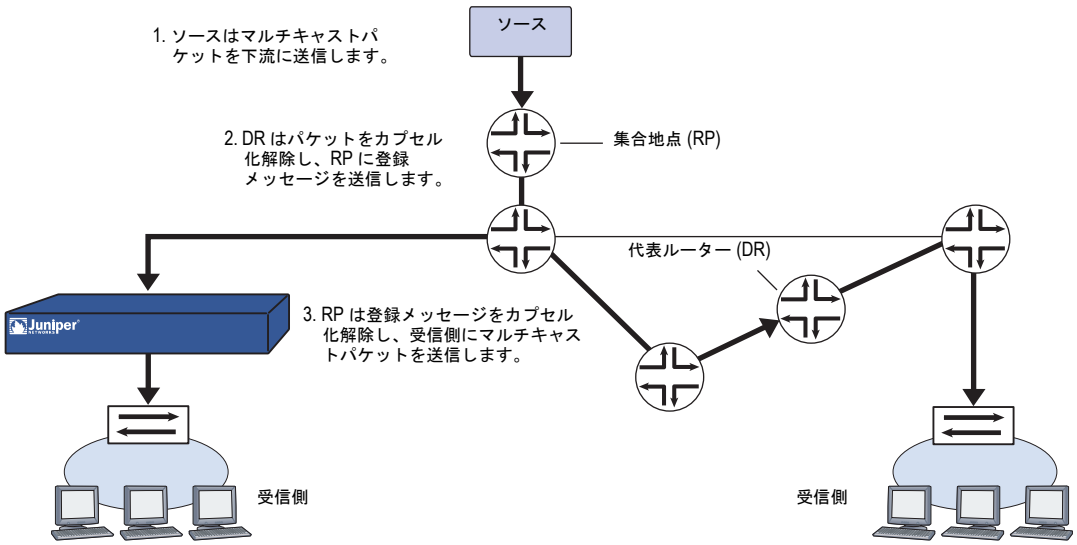
配布ツリーでのトラフィックの転送

このセクションでは、PIM-SM ルーターが参加メッセージを集合地点 (RP) に送信する方法、および RP がマルチキャストデータをネットワーク内の受信側に送信する方法について説明します。マルチキャストネットワーク環境では、セキュリティデバイスは、ソースネットワーク、受信側ネットワーク、または中間ルーターのいずれでも、RP 、代表ルーター として機能します。

グループにデータを送信するソース

ソースがマルチキャストパケットの送信を開始すると、ネットワークでパケットを伝送します。LAN 上の DR がマルチキャストパケットを受信すると、ユニキャストルートテーブルで、出力インターフェースおよび RP への次のホップ点の IP アドレスのルックアップを実行します。DR はマルチキャストパケットを登録メッセージと呼ばれるユニキャストパケットにカプセル化し、次のホップ点の IP アドレスに転送します。RP は登録メッセージを受信すると、パケットのカプセル化を解除して、受信側への配布ツリーにマルチキャストパケットを送信します。

図 31: ソース送信データ

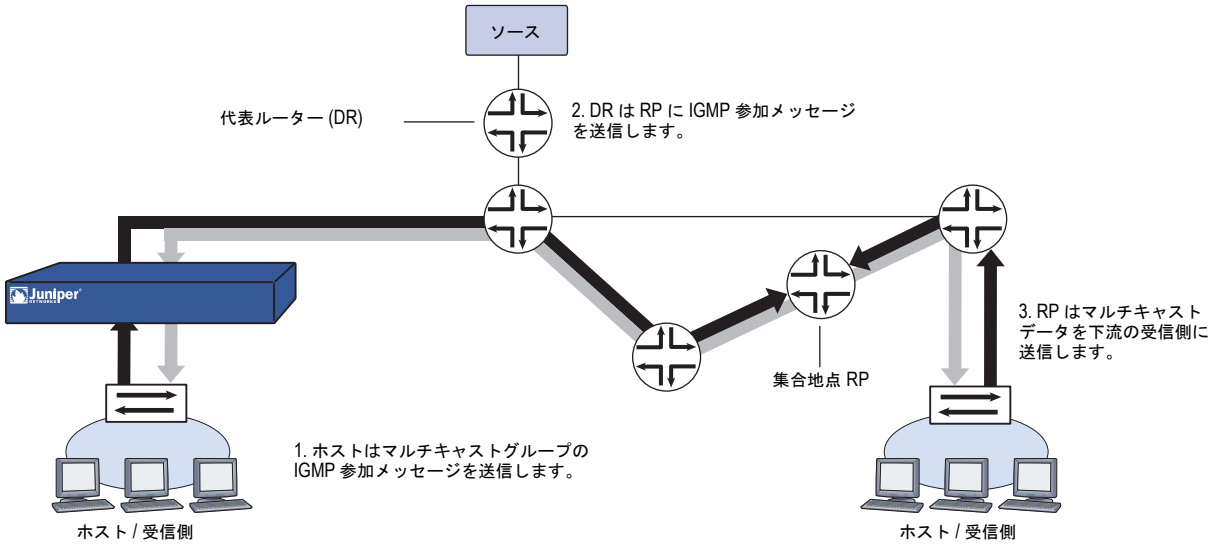


ソースの DR からのデータレートが設定したしきい値に達すると、RP は ソースの DR に PIM-SM 参加メッセージを送信して、登録メッセージではなく元のマルチキャストデータを受信できるようになります。ソースの DR は参加メッセージを受信すると、RP に対してマルチキャストパケットと登録メッセージを送信します。RP はマルチキャストパケットを DR から受信すると、DR に登録中止メッセージを送信します。DR は登録中止メッセージを受信すると、登録メッセージの送信を中止し、元のマルチキャストデータを送信して、ダウンストリームを受信側に送信します。

グループに参加するホスト

ホストはマルチキャストグループに参加すると、マルチキャストグループに IGMP 参加メッセージを送信します。ホスト側の LAN 上の DR が IGMP 参加メッセージを受信すると、グループの RP のルックアップを実行します。ホストはマルチキャストルートテーブルに (*,G) エントリを作成し、RPF 隣接ノードの上流に PIM-SM 参加メッセージを送信します。上流ルーターが PIM-SM 参加メッセージを受信すると、同じルックアップ手順を実行し、RPF 隣接ノードから参加メッセージが来たかどうかもチェックします。参加メッセージが来ていた場合は、それを RP に転送します。これは、PIM-SM 参加メッセージが RP に到着するまで続行します。RP は参加メッセージを受信すると、マルチキャストデータダウンストリームを受信側に送信します。

図 32: グループに参加するホスト



マルチキャストデータを受信すると、各ダウンストリームルーターは RPF チェックを実行します。各ルーターは、トラフィックの RP への送信に使用する同一インターフェースからマルチキャストパケットを受信しているかどうかをチェックします。RFP チェックが成功すると、次にルーターは、マルチキャストルートテーブル内の一致する (*, G) 転送エントリを検索します。(*, G) エントリが見つかると、そこにソースを格納して (S, G) エントリとなります。また、マルチキャストパケットダウンストリームを転送します。このプロセスは、ホストがマルチキャストデータを受信するまで継続します。

トラフィックレートが、設定したしきい値に達すると、ホスト側の LAN 上の DR がマルチキャストソースに直接最短パスツリーを形成します。DR はソースから直接トラフィックの受信を開始し、RP に対して source-specific prune メッセージを上流送信します。中間ルーターはそれぞれ、prune メッセージが RP に到着するまで、配布ツリーからホストへのリンクを取り除き、それにより配布ツリーの特定の枝へのマルチキャストトラフィックの送信が停止します。

PIM-SM

PIM-SM だけでなく、セキュリティデバイスも PIM-Source-Specific Multicast (SSM) に対応しています。PIM-SSM は source-specific model (SSM) に従い、マルチキャストトラフィックは、マルチキャストグループだけでなくチャネルに送信されます。チャネルには、ソースとマルチキャストグループが含まれます。受信側は、ソースとマルチキャストグループが分かっているチャネルに加入します。また、IGMPv3 を経由して、ソースに関する情報も提供します。LAN 上の代表ルーターは、集合地点 (RP) ではなく、ソースにメッセージを送信します。

IANA は、IPv4 の SSM サービスに、232/8 の範囲のマルチキャストアドレスを予約済みです。IGMPv3 が、PIM-SM と共にデバイスでも稼働している場合、PIM-SSM の動作はこのアドレスの範囲内であれば保証されます。セキュリティデバイスは、232/8 のアドレス範囲内にあるマルチキャストグループの IGMPv3 メンバーシップレポートを、以下のように処理します。

- レポートにフィルタモードを含める場合、デバイスはレポートをソース一覧内のソースに直接送信します。
- レポートに除外フィルタモードがある場合、デバイスはレポートをドロップします。232/8 のアドレス範囲内にあるマルチキャストグループの (*、G) レポートは処理しません。

セキュリティデバイスで PIM-SSM を設定する手順は、以下の項目を除き、PIM-SM と同様です。

- 受信側に接続するインターフェースには、IGMPv3 を設定してください (セキュリティデバイスでは、デフォルトで IGMPv2 が有効になっています)。
- マルチキャストグループポリシーを設定する場合は、join-prune メッセージを許可してください (ブートストラップメッセージは使用しません)。
- 集合地点を設定しないでください。

次のセクションでは、セキュリティデバイスで PIM-SM を構成する方法を説明します。

セキュリティデバイスで PIM-SM を構成する方法

Juniper Networks セキュリティデバイスには、2 つの定義済み仮想ルーター (VR) があります。trust-vr と untrust-vr です。各仮想ルーターは、独自のルートテーブルを持つ個別のルーティングコンポーネントです。Protocol Independent Multicast - Sparse Mode (PIM-SM) は、仮想ルーターのルートテーブルを使用しており、そこでは、reverse path forwarding (RPF) インターフェースと次のホップ点の IP アドレスのルックアップを実行するよう設定されています。そのため、セキュリティデバイス上で PIM-SM を動かすには、まず仮想ルーター上で静的ルートか動的ルーティングプロトコルを設定する必要があります。そして次に同じ仮想ルーター上で PIM-SM を設定します。（仮想ルーターについて詳しくは、15 ページの「ルーティング」を参照してください。）セキュリティデバイスは、以下の動的ルーティングプロトコルに対応しています。

- OSPF (Open Shortest Path First) - 詳細については、49 ページの「オープンショーテストパスファースト (OSPF)」を参照してください。
- RIP (Routing Information Protocol) - 詳細については、77 ページの「ルーティング情報プロトコル (RIP)」を参照してください。
- BGP (Border Gateway Protocol) - 詳細については、107 ページの「境界ゲートウェイプロトコル」を参照してください。

次のセクションでは、セキュリティデバイスで PIM-SM を構成する基本的な手順を説明します。

- VR 上に PIM-SM インスタンスを作成し使用可能にする
- インターフェース上で PIM-SM を使用可能にする
- マルチキャストポリシーを設定して、PIM-SM メッセージがセキュリティデバイスを横断できるようにする

VR 上に PIM-SM インスタンスを有効にし、削除します。

各仮想ルーターには、1 つの PIM-SM インスタンスを設定することができます。PIM-SM は、仮想ルーターのユニキャストルートテーブルを使用して RPF チェックを実行します。仮想ルーターに PIM-SM ルーティングインスタンスを作成して、有効にしてから、インターフェース上で PIM-SM を有効にします。

PIM-SM インスタンスを有効にする

この例では、trust-vr 仮想ルーターの PIM-SM インスタンスを作成して、有効にします。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Create PIM Instance: Select **Protocol PIM: Enable** を選択し、次に **Apply** をクリックします。

CLI

```
device-> set vrouter trust-vr
device(trust-vr)-> set protocol pim
device(trust.vr/pim)-> set enable
device(trust.vr/pim)-> exit
device(trust-vr)-> exit
save
```

PIM-SM インスタンスの削除

この例では、trust-vr 仮想ルーターの PIM-SM インスタンスを削除します。仮想ルーターの PIM-SM インスタンスを削除すると、セキュリティデバイスはインターフェース上の PIM-SM を無効にし、PIM-SM インターフェースパラメータをすべて削除します。

WebUI

Network > Routing > Virtual Routers (trust-vr) > Edit > Delete PIM Instance を実行。確認プロンプトが現れるので **OK** をクリック。

CLI

```
unset vrouter trust-vr protocol pim
deleting PIM instance, are you sure? y/[n] y
save
```

PIM-SM をインターフェースで使用可能・不可にする

デフォルトでは、PIM-SM は全インターフェース上で無効になっています。仮想ルーターで PIM-SM を作成し、有効にしたら、マルチキャストトラフィックを送信する仮想ルーターのインターフェースでは、PIM-SM を有効にしなければなりません。インターフェースが受信側に接続されている場合は、そのインターフェースのルーターモードの IGMP も設定する必要があります（IGMP の詳細については、159 ページの「IGMP (Internet Group Management Protocol)」を参照してください。）

ゾーンにバインドされたインターフェースの PIM-SM を有効にすると、PIM-SM はそのインターフェースが属するゾーンで自動的に有効となります。それから、そのゾーンの PIM-SM パラメータを設定してください。同様に、ゾーンのインターフェースの PIM-SM パラメータを無効にすると、そのゾーンに関連するすべての PIM-SM パラメータが自動的に削除されます。

インターフェース上の PIM-SM を有効にする

この例では、PIM-SM をインターフェース ethernet1 で有効にします。

WebUI

Network > Interfaces > Edit (ethernet1) > PIM: 以下を入力して **Apply** をクリックします。

PIM Instance: (選択)
Protocol PIM: Enable (選択)

CLI

```
set interface ethernet1 protocol pim
set interface ethernet1 protocol pim enable
save
```

インターフェース上の PIM-SM を無効にする

この例では、PIM-SM をインターフェース ethernet1 で無効にします。PIM-SM を有効にした他のインターフェースでは、まだ PIM-SM パケットの送信および処理が続いています。

WebUI

Network > Interfaces > Edit (ethernet1) > PIM: **Protocol PIM Enable** をオフにし、**Apply** をクリックします。

CLI

```
unset interface ethernet1 protocol pim enable
save
```

マルチキャストグループポリシー

デフォルトでは、セキュリティデバイスは、PIM-SM メッセージなどのマルチキャスト制御トラフィックをゾーン間にパスさせないようになっています。ゾーン間の PIM-SM メッセージを許可するには、マルチキャストグループポリシーを設定する必要があります。マルチキャストグループポリシーは、次の 2 種類の PIM-SM メッセージを制御します。static-RP-BSR メッセージと join-prune メッセージです。

Static-RP-BSR メッセージ

Static-RP-BSR メッセージには、静的集合地点 (RP) および dynamic RP-group マッピングに関する情報が含まれます。ゾーン間の静的 RP マッピングとブートストラップ (BSR) メッセージを許可するマルチキャストポリシーを設定すると、セキュリティデバイスは仮想ルーター内、または 2 つの仮想ルーター間のゾーンで RP-group マッピングを共有できるようになります。ルーターは他のゾーンから RP-group マッピングを学習できるため、すべてのゾーンで RP を設定する必要はありません。

セキュリティデバイスは BSR メッセージを受信すると、reverse path forwarding (RPF) 隣接ノードから来たかどうかを確認します。そして、BSR メッセージにマルチキャストグループのマルチキャストポリシーがあるかどうかをチェックします。ここで、マルチキャストポリシーで許可されていないグループを遮断して、許可されたグループの BSR メッセージをポリシーが許可するすべての宛先ゾーンに送信します。

Join-Prune メッセージ

マルチキャストグループポリシーは、join-prune メッセージも制御します。セキュリティデバイスが、ダウンストリームインターフェースでソースとグループまたはソースと RP の join-prune メッセージを受信すると、ユニキャストルーティングテーブルの RPF 隣接ノードとインターフェースをルックアップします。

- RPF インターフェースがダウンストリームインターフェースとして同一ゾーンにある場合は、マルチキャストポリシーの検証は必要ありません。
- RPF インターフェースが別のゾーンにある場合は、セキュリティデバイスが、ダウンストリームインターフェースのゾーンと RPF インターフェースのゾーンの間のグループに join-prune メッセージを許可するマルチキャストポリシーがあるかどうかをチェックします。

- 2 つのゾーン間に join-prune メッセージを許可するマルチキャストポリシーがある場合、メッセージを RPF インターフェースに転送します。
- 2 つのゾーン間に join-prune メッセージを許可するマルチキャストポリシーがない場合、join-prune メッセージはドロップされます。

PIM-SM のマルチキャストグループポリシーの定義

この例では、グループ 224.4.4.1 の Trust および Untrust ゾーン間で PIM-SM メッセージをすべて許可する双方向マルチキャストグループポリシーを定義しています。

WebUI

Policies (From: Trust, To: Untrust) > New: 次のように入力してから **OK** をクリックします。

MGroup Address: IP/Netmask (**選択**) 224.4.4.1/32
Bidirectional: (**選択**)
PIM Message: (**選択**)
BSR-Static RP: (**選択**)
Join/Prune: (**選択**)

CLI

```
set multicast-group-policy from trust mgroup 224.4.4.1/32 to untrust
    pim-message bsr-static-rp join-prune bi-directional
save
```

PIM-SM の基本設定

セキュリティデバイスは、集合地点 (RP)、代表ルーター (DR)、受信側 DR、中間ルーターとして機能します。ブートストラップルーターとしては機能しません。

PIM-SM は、1 つの仮想ルーター (VR) または 2 つの仮想ルーター上に構成できます。1 つの仮想ルーター上に PIM-SM を設定するには、以下の手順を実行します。

1. ゾーンとインターフェースを設定します。
2. セキュリティデバイスの特定の仮想ルーター上に、静的ルート、または Routing Information Protocol (RIP) 、境界ゲートウェイプロトコル (BGP) 、Open Shortest Path First (OSPF) などの動的ルーティングプロトコルを設定します。
3. ファイアウォールポリシーを作成して、ゾーン間をユニキャストおよびマルチキャストデータトラフィックがパスするようにします。
4. 静的ルートまたは動的ルーティングプロトコルを設定した同一仮想ルーター上に、PIM-SM ルーティングインスタンスを作成し、有効にします。
5. インターフェース上で PIM-SM を有効にして、ソースや RP に対しトラフィック上流を、そして受信側に下流を転送します。
6. ホストに接続されたインターフェース上で IGMP を有効にします。
7. マルチキャストポリシーを設定して、ゾーン間の PIM-SM メッセージを許可します。

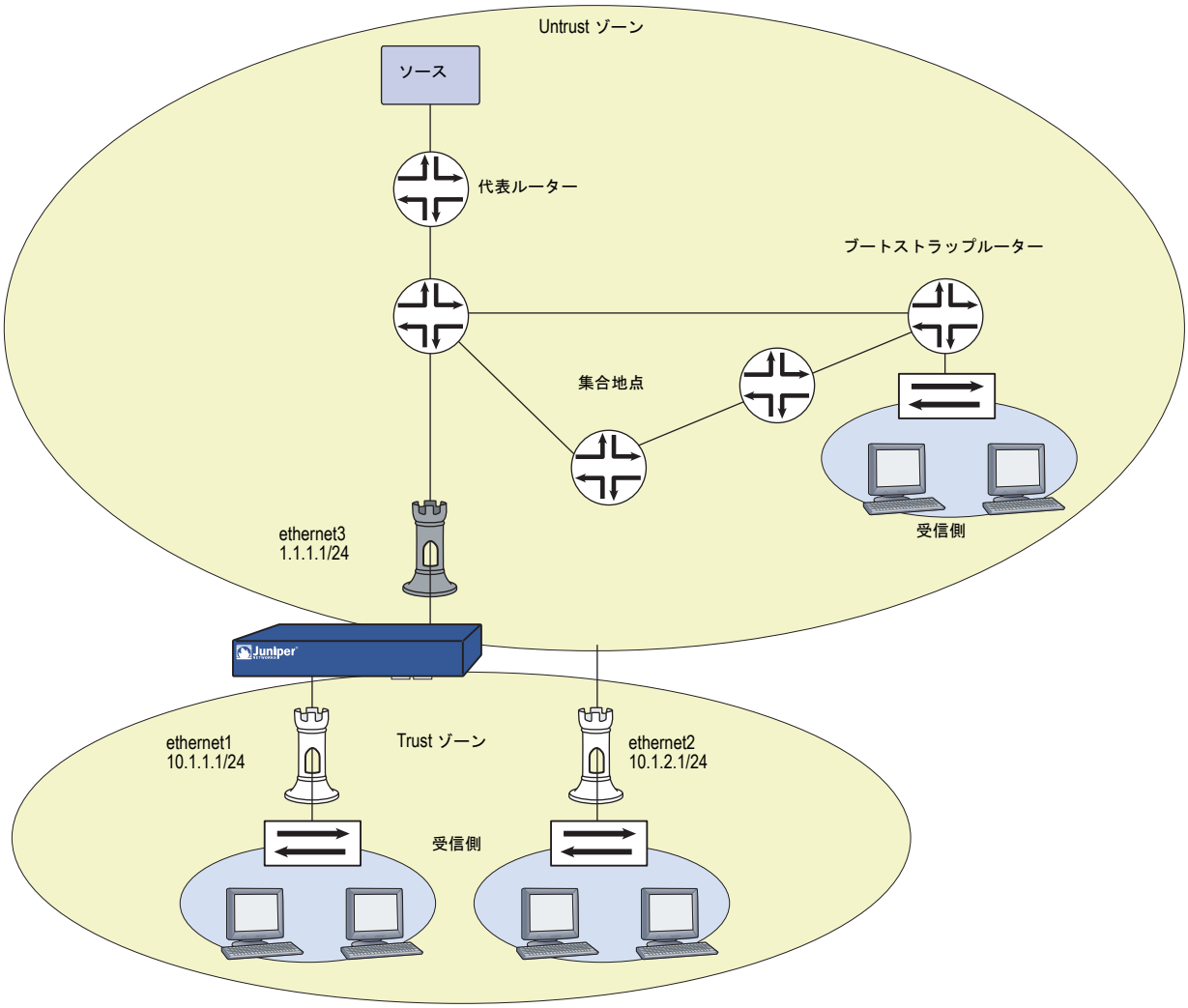
2 つの仮想ルーターで PIM-SM を設定する場合は、RP がある仮想ルーターのゾーンに RP を設定してください。そして、マルチキャストグループポリシーを設定して、各仮想ルーターのゾーン間での join-prune メッセージと BSR-static-RP メッセージを許可します。さらに、2 つの仮想ルーター間でユニキャストルートをエクスポートして、reverse path forwarding (RPF) 情報の精度を確認してください。ルートのエクスポートに関しては、45 ページの「仮想ルーター間でルート情報をエクスポート / インポート」を参照してください。

注 : セキュリティデバイスを複数の仮想ルーターに設定する場合は、すべて同じ PIM-SM オプションにする必要があります。

Juniper Networks セキュリティデバイスには、複数の仮想システムをサポートするものがあります（仮想システムについて詳しくは、*第 10 部 : 仮想 システム* を参照してください。）仮想システムに PIM-SM を設定する場合は、ルートシステムの PIM-SM と同じ設定になります。異なる仮想システムにある 2 つの仮想ルーターに PIM-SM を設定する場合は、プロキシ RP を設定しなければなりません（プロキシ RP の設定については、212 ページの「プロキシ集合地点の設定」を参照してください。）

この例では、trust-vr に PIM-SM を設定します。Trust ゾーンのホストで、マルチキャストグループ 224.4.4.1/32 のマルチキャストトラフィックを受信するものとします。ユニキャストルーティングプロトコルとして trust-vr に RIP を設定し、ファイアウォールポリシーを作成して、Trust および Untrust ゾーン間にデータトラフィックをパスさせます。trust-vr に PIM-SM インスタンスを作成し、Trust ゾーンの ethernet1 と ethernet2、および Untrust ゾーンの ethernet3 で PIM-SM を有効にします。インターフェースはすべて Route モードです。次に、受信側に接続した ethernet1 と ethernet2 で IGMP を設定します。最後に、ゾーン間の static-RP-BSR メッセージと join-prune メッセージを許可するマルチキャストポリシーを作成します。

図 33: PIM-SM の基本設定



WebUI

1. **ゾーンおよびインターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24

   次のように選択してから **OK** をクリックします。

   Interface Mode: NAT

Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.2.1/24
次のように選択してから **OK** をクリックします。
Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
IP Address/Netmask: 1.1.1.1/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

Address Name: mgroup1
IP Address/Domain Name:
IP/Netmask: (選択), 224.4.4.1/32
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

Address Name: source-dr
IP Address/Domain Name:
IP/Netmask: (選択), 6.6.6.1/24
Zone: Untrust

3. IGMP

Network > Interfaces > Edit (ethernet1) > IGMP: 次のように入力してから **OK** をクリックします。

IGMP Mode: Router (選択)
Protocol IGMP: Enable (選択)

Network > Interfaces > Edit (ethernet2) > IGMP: 次のように入力してから **OK** をクリックします。

IGMP Mode: Router (選択)
Protocol IGMP: Enable (選択)

4. RIP

Network > Routing > Virtual Router (trust-vr) > Edit > Create RIP Instance: **Enable RIP** を選択して **OK** をクリックします。

Network > Interfaces > Edit (for ethernet3) > RIP: 以下を入力して **Apply** をクリックします。

RIP Instance: (選択)
Protocol RIP: Enable (選択)

5. PIM-SM

Network > Routing > Virtual Router (trust-vr) > Edit > Create PIM Instance: 次のように選択してから **OK** をクリックします。

Protocol PIM: Enable (選択)

Network > Interfaces > Edit (ethernet1) > PIM: 以下を入力して **Apply** をクリックします。

PIM Instance: (選択)
Protocol PIM: Enable (選択)

Network > Interfaces > Edit (ethernet2) > PIM: 以下を入力して **Apply** をクリックします。

PIM Instance: (選択)
Protocol PIM: Enable (選択)

Network > Interfaces > Edit (ethernet3) > PIM: 以下を入力して **Apply** をクリックします。

PIM Instance: (選択)
Protocol PIM: Enable (選択)

6. ポリシー

Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), source-dr
Destination Address:
    Address Book Entry: (選択), mgroup1
Service: any
Action: Permit

7. マルチキャストポリシー

MCast Policies (From: Trust, To: Untrust) > New: 次のように入力してから **OK** をクリックします。

MGroup Address: IP/Netmask (選択) 224.4.4.1/32
Bidirectional: (選択)
PIM Message: (選択)
BSR Static RP: (選択)
Join/Prune: (選択)

CLI

1. ゾーンおよびインターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet2 zone trust
set interface ethernet2 ip 10.1.2.1/24
set interface ethernet2 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. **アドレス**
   set address trust mgroup1 224.4.4.1/32
   set address untrust source-dr 6.6.6.1/24

3. **IGMP**
   set interface ethernet1 protocol igmp router
   set interface ethernet1 protocol igmp enable
   set interface ethernet2 protocol igmp router
   set interface ethernet2 protocol igmp enable

4. **RIP**
   set vrouter trust-vr protocol rip
   set vrouter trust-vr protocol rip enable
   set interface ethernet3 protocol rip enable

5. **PIM-SM**
   set vrouter trust-vr protocol pim
   set vrouter trust-vr protocol pim enable
   set interface ethernet1 protocol pim
   set interface ethernet1 protocol pim enable
   set interface ethernet2 protocol pim
   set interface ethernet2 protocol pim enable
   set interface ethernet3 protocol pim
   set interface ethernet3 protocol pim enable

6. **ポリシー**
   set policy from untrust to trust source-dr mgroup1 any permit

7. **マルチキャストポリシー**
   set multicast-group-policy from trust mgroup 224.4.4.1/32 any to untrust
   pim-message bsr-static-rp join bi-directional
   save

設定内容の確認

PIM-SM の設定を確認するには、以下のコマンドを実行します。

```
device-> get vrouter trust protocol pim
PIM-SM enabled
Number of interfaces : 1
SPT threshold        : 1 Bps
PIM-SM Pending Register Entries Count : 0
Multicast group accept policy list: 1
Virtual Router trust-vr - PIM RP policy
--------------------------------------------------
Group Address      RP access-list
Virtual Router trust-vr - PIM source policy
--------------------------------------------------
Group Address      Source access-list
```

マルチキャストルートエントリを表示するには、以下のコマンドを実行します。

```
device-> get igmp group
total groups matched: 1
multicast group  interface    last reporter   expire ver
*224.4.4.1       trust        0.0.0.0         ------ v2

device->get vrouter trust protocol pim mroute
trust-vr - PIM-SM routing table
------------------------------------------------------------------------------
Register - R, Connected members - C, Pruned - P, Pending SPT Alert - G
Forward - F, Null - N , Negative Cache - E, Local Receivers - L
SPT - T, Proxy-Register - X, Imported - I, SGRpt state - Y, SSM Range Group - S
Turnaround Router - K
------------------------------------------------------------------------------
Total PIM-SM mroutes: 2

(*, 236.1.1.1)  RP 20.20.20.10         01:54:20/-         Flags: LF
  Zone: Untrust
  Upstream        : ethernet1/2         State          : Joined
  RPF Neighbor    : local               Expires        : -
  Downstream      :
  ethernet1/2  01:54:20/-         Join         0.0.0.0          FC

(10.10.10.1/24, 238.1.1.1)             01:56:35/00:00:42  Flags: TLF  Register Prune
  Zone: Trust
  Upstream        : ethernet1/1         State          : Joined
  RPF Neighbor    : local               Expires        : -
  Downstream      :
  ethernet1/2  01:54:20/-         Join         236.1.1.1          20.20.20.200 FC
```

ルートエントリごとに以下の項目を確認できます。

- (S、G) 状態または (*、G) 転送状態
- 転送状態が (*、G) の場合は RP の IP アドレスとなり、(S、G) の場合は ソースの IP アドレスとなります。
- ルートを持つゾーン
- 「join」ステータスと入力および出力インターフェース
- タイマーの値

各ゾーンの集合地点を表示するには、以下のコマンドを実行します。

```
device-> get vrouter trust protocol pim rp
Flags: I - Imported, A - Always(override BSR mapping)
       C - Static Config, P - Static Proxy
------------------------------------------------------------------------------
Trust
  238.1.1.1/32       RP: 10.10.10.10     192    Static  -     C
    Registering : 0
    Active Groups : 1
                238.1.1.1
Untrust
  236.1.1.1/32       RP: 20.20.20.10     192    Static  -     P
    Registering : 0
    Active Groups : 1
                236.1.1.1
```

RPF (Reverse Path Forwarding) の隣接ノードがあるかどうかを確認するには、以下のコマンドを実行します。

```
device-> get vrouter trust protocol pim rpf
Flags: RP address - R, Source address - S
Address         RPF Interface      RPF Neighbor    Flags
-----------------------------------------------------------
10.10.11.51     ethernet3          10.10.11.51     R
10.150.43.133   ethernet3          10.10.11.51     S
```

仮想ルーターでセキュリティデバイスが各隣接ノードに送信する join-prune メッセージのステータスを表示するには、以下のコマンドを実行します。

```
device-> get vrouter untrust protocol pim join
Neighbor        Interface       J/P          Group           Source
-------------------------------------------------------------------------
1.1.1.1         ethernet4:1    (S,G)     J  224.11.1.1      60.60.0.1
                               (S,G)     J  224.11.1.1      60.60.0.1
```

集合地点の設定

特定の集合地点 (RP) を 1 つ以上のマルチキャストグループにバインドする場合は、静的集合地点を設定します。複数の静的集合地点を設定する場合、各 RP を異なるマルチキャストグループにマッピングできます。

ネットワークにブートストラップルーターがない場合は、静的集合地点を設定してください。セキュリティデバイスはブートストラップメッセージを受信、処理できますが、ブートストラップルーターとしては機能しません。

RP をマルチキャストグループに動的にマッピングする場合は、仮想ルーターを candidate RP (C-RP) として設定します。C-RP は、ゾーンごとに 1 つ作成できます。

静的集合地点の設定

静的 RP を設定する場合は、以下の項目を指定します。

- 静的 RP のゾーン
- 静的 RP の IP アドレス
- 静的 RP のマルチキャストグループを定義するアクセスリスト（アクセスリストの詳細については、155 ページの「アクセスリスト」を参照。）

アクセスリストのマルチキャストグループが常に同じ RP を使うようにするには、キーワード **always** を入れてください。このキーワードを入れないまま、同じマルチキャストグループに動的にマッピングされた別の RP が見つかると、セキュリティデバイスは動的 RP を使用します。

この例では、マルチキャストグループ 224.4.4.1 のアクセスリストを作成し、そのグループの静的 RP を作成します。静的 RP の IP アドレスは 1.1.1.5/24 です。キーワード **always** を指定して、セキュリティデバイスが常に同じ RP を使用するようにしてください。

WebUI

Network > Routing > Virtual Routers > Access List: > New (trust-vr): 次のように入力してから **OK** をクリックします。

Access List ID: 2
Sequence No.: 1
IP/Netmask: 224.4.4.1/32
Action: Permit

Network > Routing > Virtual Router (trust-vr) > Edit > Edit PIM Instance > RP Address > New: 次のように選択してから **OK** をクリックします。

Zone: Trust (選択)
Address: 1.1.1.5
Access List: 2
Always: (選択)

CLI

```
set vrouter trust-vr access-list 2 permit ip 224.4.4.1/32 1
set vrouter trust-vr protocol pim zone trust rp address 1.1.1.5 mgroup-list 2 always
save
```

Candidate 集合地点の設定

仮想ルーターを C-RP として設定するには、以下の項目を指定します。

- C-RP を設定するゾーン
- C-RP として通知するインターフェースの IP アドレス
- C-RP のマルチキャストグループを定義するアクセスリスト
- 通知した C-RP の優先順位

この例では、Trust ゾーンにバインドされている ethernet1 インターフェースで PIM-SM を有効にします。C-RP のマルチキャストグループを定義するアクセスリストを作成します。そして、trust-vr の Trust ゾーンで C-RP を作成します。C-RP の優先順位は 200 に設定します。

WebUI

Network > Interfaces > Edit (ethernet1) > PIM: 以下を入力して **Apply** をクリックします。

PIM Instance: (選択)
Protocol PIM: Enable (選択)

Network > Routing > Virtual Routers > Access List: > New (trust-vr): 次のように入力してから **OK** をクリックします。

Access List ID: 1
Sequence No.: 1
IP/Netmask: 224.2.2.1/32
Action: Permit

Select Add Seq No: 次のように入力してから **OK** をクリックします。

Sequence No.: 2
IP/Netmask: 224.3.3.1/32
Action: Permit

Network > Routing > Virtual Router (trust-vr) > Edit > Edit PIM Instance > RP Candidate > Edit (Trust Zone): 次のように選択してから **OK** をクリックします。

Interface: ethernet1 (選択)
Access List: 1 (選択)
Priority: 200

CLI

```
set interface ethernet1 protocol pim
set interface ethernet1 protocol pim enable
set vrouter trust-vr access-list 1 permit ip 224.2.2.1/32 1
set vrouter trust-vr access-list 1 permit ip 224.3.3.1/32 2
set vrouter trust-vr protocol pim zone trust rp candidate interface ethernet1
    mgroup-list 1 priority 200
save
```

セキュリティ検討事項

PIM-SM を動作させる場合、仮想ルーターとのトラフィックを制御するために、仮想ルーターのレベルを設定する特定のオプションがあります。仮想ルーターのレベルに定義した設定は、PIM-SM が動作している全インターフェースに影響します。

インターフェースが別のゾーンからマルチキャスト制御トラフィック (IGMP または PIM-SM メッセージ) を受信すると、最初に、セキュリティデバイスはトラフィックを許可するマルチキャストポリシーがあるかどうかをチェックします。そうしたマルチキャストポリシーが見つかると、セキュリティデバイスはトラフィックに適用する PIM-SM オプションがないか仮想ルーターをチェックします。例えば、アクセスリストに指定されたマルチキャストグループから join-prune メッセージを受け取るよう仮想ルーターを設定すると、セキュリティデバイスはトラフィックがリストにあるマルチキャストグループのものかどうかをチェックします。その結果、初めてデバイスはトラフィックを許可します。そのグループのものでない場合、トラフィックはドロップされます。

マルチキャストグループの制限

仮想ルーターに制限をかけることにより、PIM-SM の join-prune メッセージが特定のマルチキャストグループだけに転送されるようにすることができます。許可するマルチキャストグループは、アクセスリストに指定します。この機能を使うと、仮想ルーターはアクセスリストにないグループへの join-prune メッセージをドロップします。

この例では、次のマルチキャストグループを許可する ID 1 を持つアクセスリストを作成します。224.2.2.1/32 および 224.3.3.1/32 です。さらに、trust-vr 仮想ルーターを設定して、アクセスリストにあるマルチキャストグループからの join-prune メッセージを受け取れるようにします。

WebUI

Network > Routing > Virtual Routers > Access List: > New (trust-vr): 次のように入力してから **OK** をクリックします。

Access List ID: 1
Sequence No: 1
IP/Netmask: 224.2.2.1/32
Action: Permit

Select Add Seq No: 次のように入力してから **OK** をクリックします。

Sequence No: 2
IP/Netmask: 224.3.3.1/32
Action: Permit

Network > Routing > Virtual Router (trust-vr) > Edit > Edit PIM Instance: 以下を選択して **Apply** をクリックします。

Access Group: 1 (**選択**)

CLI

```
set vrouter trust-vr access-list 1 permit ip 224.2.2.1/32 1
set vrouter trust-vr access-list 1 permit ip 224.3.3.1/32 2
set vrouter trust-vr protocol pim accept-group 1
save
```

マルチキャストソースの制限

マルチキャストグループがデータを受信するソースは制御することができます。アクセスリストで許可されているソースを識別し、マルチキャストグループにリンクします。これにより、認証されていないソースからネットワークへのデータ送信を防止できます。この機能を使うと、セキュリティデバイスはリストにないソースからのマルチキャストデータをドロップします。仮想ルーターがゾーンの集合地点にある場合は、アクセスリストをチェックした後に、ソースからの登録メッセージを受信します。登録メッセージが、許可したソースからのものでない場合は、ドロップされます。

この例では、最初に、許可されたソース 1.1.1.1/32 を指定する ID 5 のアクセスリストを作成します。次に、trust-vr 仮想ルーターを設定して、アクセスリストに指定したソースからマルチキャストグループ 224.4.4.1/32 のマルチキャストデータを受信できるようにします。

WebUI

Network > Routing > Virtual Routers > Access List: > New (trust-vr): 次のように入力してから **OK** をクリックします。

Access List ID: 5
Sequence No: 1
IP/Netmask: 1.1.1.1/32
Action: Permit

Network > Routing > Virtual Router (trust-vr) > Edit > Edit PIM Instance > MGroup: 次のように選んでから **Add** をクリックします。

MGroup: 224.4.4.1/32
Accept Source: 5 (**選択**)

CLI

```
set vrouter trust-vr access-list 5 permit ip 1.1.1.1/32 1
set vrouter trust-vr protocol pim mgroup 224.4.4.1/32 accept-source 5
save
```

集合地点の制限

マルチキャストグループにマッピングする集合地点 (RP) は制御することができます。アクセスリストで許可されている RP を識別し、マルチキャストグループにリンクします。仮想ルーターが特定のグループへのブートストラップメッセージを受信すると、そのグループに許可された RP の一覧をチェックします。一覧にない場合は、マルチキャストグループの RP は選択されません。

この例では、許可されたソース 2.1.1.1/32 を指定する ID 6 のアクセスリストを作成します。次に、trust-vr 仮想ルーターを設定して、マルチキャストグループ 224.4.4.1/32 のアクセスリストにある RP を受信できるようにします。

WebUI

Network > Routing > Virtual Routers > Access List: > New (trust-vr): 次のように入力してから **OK** をクリックします。

Access List ID: 6
Sequence No: 1
IP/Netmask: 2.1.1.1/32
Action: Permit

Network > Routing > Virtual Router (trust-vr) > Edit > Edit PIM Instance > MGroup: 次のように選んでから **Add** をクリックします。

MGroup: 224.4.4.1/32
Accept RP: 6 (選択)

CLI

```
set vrouter trust-vr access-list 6 permit ip 2.1.1.1/32 1
set vrouter trust-vr protocol pim mgroup 224.4.4.1/32 accept-rp 6
save
```

PIM-SM インターフェースパラメータ

PIM-SM が有効になっているインターフェースでは、特定のデフォルト値を変更することができます。このレベルでパラメータを設定すると、指定したインターフェースにのみ影響します。

表 19 は PIM-SM インターフェースパラメータとその初期値を示します。

表 19: PIM-SIM パラメータ

PIM-SIM インターフェースパラメータ	説明	デフォルト値
Neighbor policy	隣接ノードの隣接関係を制御します。詳細については、210 ページの「Neighbor Policy を定義する」を参照してください。	無効
Hello interval	インターフェースが隣接ノードのルーターにハローメッセージを送信すする間隔を指定します。	30 秒
Designates router priority	代表ルーターを選ぶための、インターフェースの優先順位を指定します。	1
Join-Prune interval	インターフェースが join-prune メッセージを送信する間隔を秒単位で指定します。	60 秒
Bootstrap border	インターフェースが bootstrap border であることを指定します。詳細については、211 ページの「Bootstrap Border を定義する」を参照してください。	無効

Neighbor Policy を定義する

インターフェースが隣接関係を確立できる隣接ノードは制御することができます。PIM-SM ルーターは定期的にハローメッセージを送信することにより、自身が PIM-SM ルーターであることを知らせます。この機能を使うと、インターフェースは隣接ノードが許可されているかどうかをチェックし、許可されているノードと隣接関係を確立します。

この例では、以下の項目を指定するアクセスリストを作成します。

- ID 番号は 1 。
- 1 行目のステートメントで 2.1.1.1/24 を許可。
- 2 行目のステートメントで 2.1.1.3/24 を許可。

そして、ethernet 1 がアクセスリストにある隣接ノードと隣接関係を確立するよう指定します。

WebUI

Network > Routing > Virtual Routers > Access List: > New (trust-vr): 次のように入力してから **OK** をクリックします。

Access List ID: 1
Sequence No: 1
IP/Netmask: 2.1.1.1/24
Action: Permit

Select Add Seq No: 次のように入力してから **OK** をクリックします。

Sequence No: 2
IP/Netmask: 2.1.1.3/24
Action: Permit

Network > Interfaces > Edit (ethernet1) > PIM: 以下を入力して **Apply** をクリックします。

Accepted Neighbors: 1

CLI

```
set vrouter trust-vr access-list 1 permit ip 2.1.1.1/24 1
set vrouter trust-vr access-list 1 permit ip 2.1.1.3/24 2
set interface ethernet1 protocol pim neighbor-policy 1
save
```

Bootstrap Border を定義する

ブートストラップ (BSR) ボーダーであるインターフェースは BSR メッセージを受信し、処理しますが、ゾーン間の BSR メッセージを許可するマルチキャストグループポリシーがあっても、このメッセージを他のインターフェースへは転送しません。これにより、RP とグループとのマッピングが常にゾーン内にとどまります。

この例では、bootstrap border として ethernet1 を定義します。

WebUI

Network > Interfaces > Edit (ethernet1) > PIM: **Bootstrap Border** を選択して **Apply** をクリックします。

CLI

```
set interface ethernet1 protocol pim boot-strap-border
save
```

プロキシ集合地点の設定

PIM-SM ドメインとは、RP グループの同じ集合地点 (RP) グループマッピングを持つ PIM-SM ルーターのグループです。動的 RP グループマッピングを持つ PIM-SM ドメインでは、ルーターは同じブートストラップルーター (BSR) からメッセージを受信して、RP グループマッピングを選択します。静的 RP グループマッピングを持つ PIM-SM ドメインでは、ドメイン内の各ルーターに静的 RP を設定しなければなりません（RP グループマッピングについては、205 ページの「集合地点の設定」を参照してください。）

Juniper Networks セキュリティデバイスでは、レイヤー 3 ゾーンにバインドされたインターフェースは、NAT モードと Route モードのいずれでも動作します。それ以外のモードで動作するインターフェースのデバイス上で PIM-SM を稼働させる場合、各ゾーンは異なる PIM-SM ドメインになければなりません。例えば、Trust ゾーンのインターフェースが NAT モードで、Untrust ゾーンのインターフェースが Route モードの場合、各ゾーンは別々の PIM-SM ドメインにある必要があります。さらに、別々の仮想システム上にある 2 つの仮想ルーターに PIM-SM を設定する場合、各仮想ルーターも別々の PIM-SM ドメイン上になければなりません。

1 つの PIM-SM ドメインから別のドメインへと、マルチキャストグループを通知するには、プロキシ RP を設定します。プロキシ RP は、マルチキャストグループポリシーが許可する静的 RP またはブートストラップメッセージを通じて、他の PIM-SM ドメインから学習し、マルチキャストグループの RP として動作します。ドメイン内にある受信側の共有ツリーのルートとして機能し、ソースへの最短パスツリーを形成します。

仮想ルーターでは、ゾーンごとに 1 つのプロキシ RP を設定できます。ゾーンにプロキシ RP を設定するには、そのゾーンに candidate-RP (C-RP) を設定しなければなりません。すると、セキュリティデバイスは、C-RP の IP アドレスをプロキシ RP のアドレスとして通知します。C-RP を設定する場合は、マルチキャストグループリストにマルチキャストグループを指定しないでください。こうすることにより、C-RP が他のゾーンからインポートされたグループのプロキシ RP として動作するようになります。ここでマルチキャストグループを指定すると、C-RP はリストに指定されたグループの実際の RP として機能します。

ゾーン内に BSR があると、プロキシ RP は他のゾーンからインポートされたマルチキャストグループの RP として自分自身を通知します。ゾーン内に BSR がない場合、プロキシ RP は他のゾーンからインポートされたマルチキャストグループの静的 RP として動作します。その場合、C-RP の IP アドレスを、ゾーン内にある他のルーターすべての静的 RP として設定する必要があります。

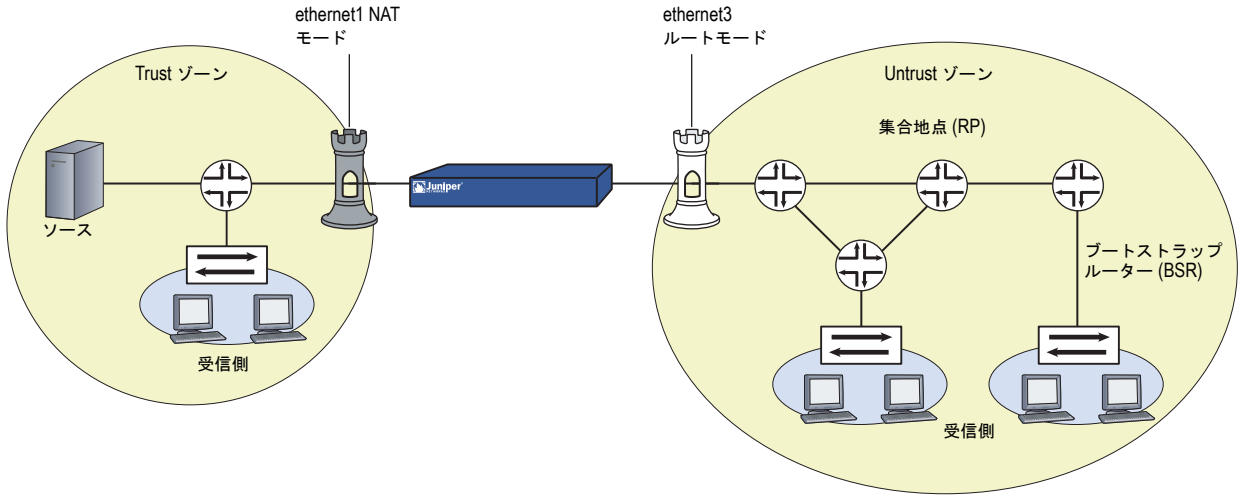
プロキシ RP は、ソースアドレス変換のためのマップ IP (MIP) 利用をサポートしています。MIP とは、ある IP アドレスから別の IP アドレスに、1 対 1 で直接対応づけるマッピングのことです。MIP を設定できるのは、セキュリティデバイスに、ゾーン内のインターフェースが NAT モードである非公開アドレスを別のアドレスに変換させる場合です。プロキシ RP のゾーンにある MIP ホストが登録メッセージを送信する場合、セキュリティデバイスはソース IP アドレスを MIP アドレスに変換し、新しい登録メッセージを実際の RP に送信します。セキュリティデバイスは MIP アドレスの join-prune メッセージを受信すると、MIP を元のソースアドレスにマッピングして、ソースに送信します。

プロキシ RP も、ゾーン間のマルチキャストグループアドレスの変換をサポートしています。元のマルチキャストグループアドレスと変換後のマルチキャストグループアドレスを指定するマルチキャストポリシーを設定することができます。セキュリティデバイスはプロキシ RP のゾーンにあるインターフェース上で join-prune メッセージを受信すると、必要に応じて、マルチキャストグループを変換し、参加メッセージを実際の RP に送信します。

以下のシナリオを考察してみます。

- Trust ゾーンの ethernet1 は NAT モードになっており、Untrust ゾーンの ethernet3 は Route モードになっています。
- Trust ゾーンにはソースの MIP があります。
- Trust ゾーンのソースは、マルチキャストトラフィックをマルチキャストグループ 224.4.4.1/32 に送信します。
- Trust ゾーンと Untrust ゾーンの両方に受信側があります。
- Trust ゾーンと Untrust ゾーンの間に、PIM-SM メッセージを許可するマルチキャストポリシーがあります。
- Trust ゾーンをプロキシ RP として設定します。
- RP および BSR は Untrust ゾーンにあります。

図 34: プロキシの集合地点例



以下にデータフローを示します。

1. ソースはデータをマルチキャストグループ 224.4.4.1/32 に送信します。
2. 代表ルーター (DR) はデータをカプセル化し、RP に登録メッセージを送信します。
3. Trust ゾーンの RP プロキシが登録メッセージを受信し、元のソース IP アドレスを MIP の IP アドレスに変更します。そして、そのメッセージをマルチキャストグループの RP に転送します。

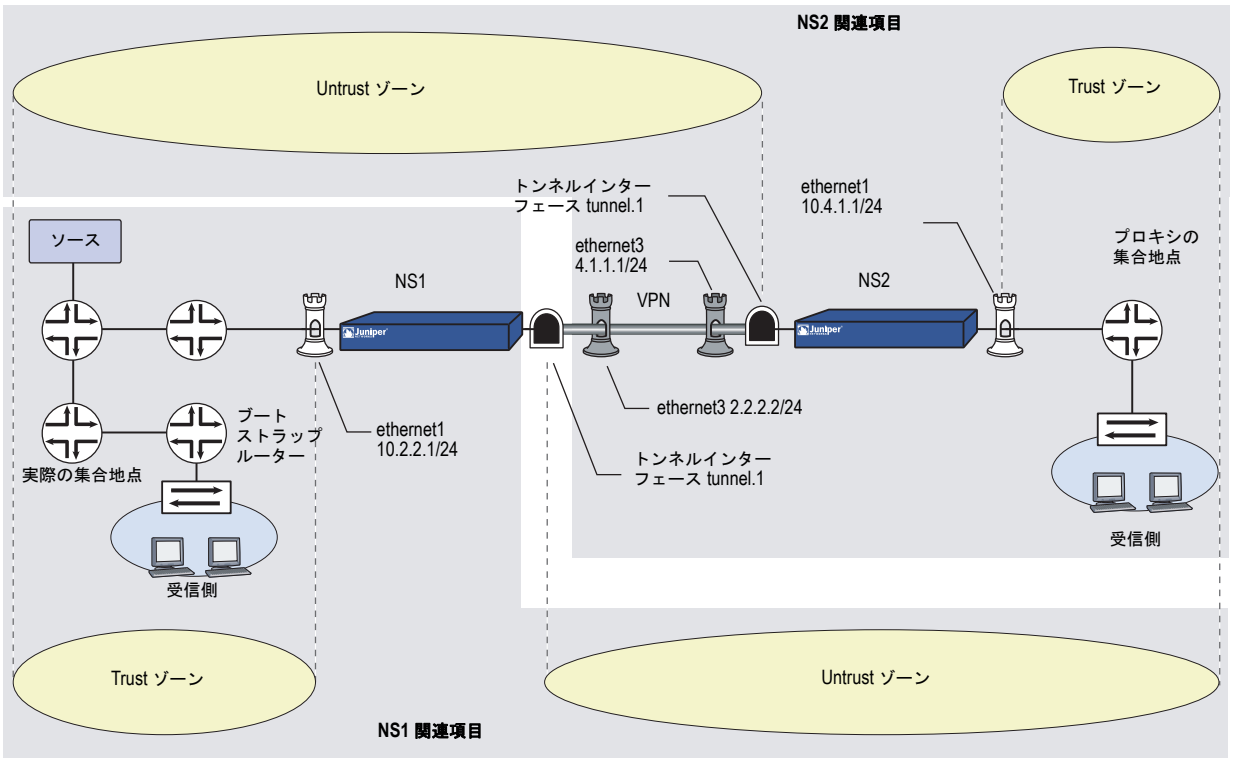
4. プロキシ RP は (*、G) 参加メッセージを実際の RP に送信します。
5. Trust ゾーンにある受信側は、参加メッセージをプロキシ RP に送信します。
6. プロキシ RP は、Trust ゾーンにある受信側にマルチキャストパケットを送信します。

プロキシ RP を設定するには、以下の内容を実行します。

1. 特定の仮想ルーター上に PIM-SM インスタンスを作成します。
2. 適切なインターフェース上で PIM-SM を有効にします。
3. プロキシ RP のゾーンに C-RP を設定します。
4. プロキシ RP を設定します。

この例では、セキュリティデバイス NS1 および NS2 が VPN トンネル経由で接続されています。どちらのデバイスでも、動的ルーティングプロトコル、BGP が作動しています。NS1 および NS2 の ethernet1 と tunnel.1 に PIM-SM を設定します。次に、NS2 上で、静的 RP として ethernet1 を設定し、trust-vr の Trust ゾーンにプロキシ RP を作成します。

図 35: プロキシ RP を設定する例



WebUI (NS1)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 次のように入力してから **OK** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.2.2.1/24
次のように選択してから **OK** をクリックします。
Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (選択)
Interface: ethernet3 (trust-vr)

2. アドレス

Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

Address Name: mgroup1
IP Address/Domain Name:
IP/Netmask: (選択), 224.4.4.1/32
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

Address Name: branch
IP Address/Domain Name:
IP/Netmask: (選択), 10.4.1.0/24
Zone: Untrust

3. PIM-SM

Network > Routing > Virtual Router (trust-vr) > Edit > Create PIM Instance: Select **Protocol PIM: Enable** にしてから **OK** をクリックします。

Network > Interfaces > Edit (ethernet1) > PIM: 以下を入力して **Apply** をクリックします。

PIM Instance: (選択)
Protocol PIM: Enable (選択)

Network > Interfaces > Edit (tunnel.1) > PIM: 以下を入力して **Apply** をクリックします。

PIM Instance: (選択)
Protocol PIM: Enable (選択)

4. VPN

VPN > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: To_Branch
Security Level: Compatible
Remote Gateway Type:
Static IP Address: (**選択**), IP Address/Hostname: 4.1.1.1
Preshared Key: fg2g4h5j
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Compatible
Phase 1 Proposal (Compatible Security Level): pre-g2-3des-sha
Mode (Initiator): Main (ID Protection)

5. BGP

Network > Routing > Virtual Router (trust-vr) > Edit: 次のように入力してから **OK** をクリックします。

Virtual Router ID: Custom (**選択**)
テキストボックスに 0.0.0.10 **を入力します。**

Network > Routing > Virtual Router (trust-vr) > Edit: **Create BGP Instance** を選択します。

AS Number (**必須**): 65000
BGP Enabled: (**選択**)

Network > Routing > Virtual Router (trust-vr) > Edit > Edit BGP Instance > Neighbors: 次のように入力してから **Add** をクリックします。

AS Number: 65000
Remote IP: 4.1.1.1
Outgoing Interface: ethernet3

Network > Routing > Virtual Router (trust-vr) > Edit > Edit BGP Instance > Neighbors > Configure (ここで追加したピア): **Peer Enabled** を選択し、**OK** をクリックします。

Network > Routing > Virtual Router (trust-vr) > Edit > Edit BGP Instance > Networks: IP/Netmask フィールドに **2.2.2.0/24** と入力し、**Add** をクリックします。IP/Netmask フィールドに 10.2.2.0/24 と入力し、もう一度 **Add** をクリックします。

Network > Interfaces > Edit (ethernet3) > BGP: 以下を入力して **Apply** をクリックします。

Protocol BGP: Enable (**選択**)

6. ポリシー

Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), branch
Destination Address:
    Address Book Entry: (選択), mgroup1
Service: any
Action: Permit

7. マルチキャストポリシー

MCast Policies (From: Trust, To: Untrust) > New: 次のように入力してから **OK** をクリックします。

MGroup Address: IP/Netmask (選択) 224.4.4.1/32
Bidirectional: (選択)
PIM Message: (選択)
BSR Static IP: (選択)
Join/Prune: (選択)

WebUI (NS2)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.4.1.1/24
NAT を選択して **Apply** をクリックします。

> IGMP: 以下を入力して **Apply** をクリックします。

IGMP Mode: Router
Protocol IGMP: Enable (選択)

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 4.1.1.1/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (選択)
    Interface: ethernet3 (trust-vr)

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

   Address Name: mgroup1
   IP Address/Domain Name:
   IP/Netmask: (選択), 224.4.4.1/32
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

   Address Name: corp
   IP Address/Domain Name:
   IP/Netmask: (選択), 2.2.2.0/24
   Zone: Untrust

3. **PIM-SM**
   Network > Routing > Virtual Router (trust-vr) > Edit > Create PIM Instance: Select **Protocol PIM: Enable** にしてから **OK** をクリックします。

   Network > Interfaces > Edit (ethernet1) > PIM: 以下を入力して **Apply** をクリックします。

   PIM Instance: (選択)
   Protocol PIM: Enable (選択)
   Network > Interfaces > Edit (tunnel.1) > PIM: 以下を入力して **Apply** をクリックします。

   PIM Instance: (選択)
   Protocol PIM: Enable (選択)

   Network > Routing > Virtual Router (trust-vr) > Edit > Edit PIM Instance > RP Address > New: 次のように選択してから **OK** をクリックします。

   Zone: Trust (選択)
   Address: 10.4.1.1/24

4. **VPN**
   VPN > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

   Gateway Name: To_Corp
   Security Level: Compatible
   Remote Gateway Type:
   Static IP Address: (選択), IP Address/Hostname: 2.2.2.2
   Preshared Key: fg2g4h5j
   Outgoing Interface: ethernet3

   > Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

   Security Level: Compatible
   Phase 1 Proposal (Compatible Security Level): pre-g2-3des-sha
   Mode (Initiator): Main (ID Protection)

5. **BGP**

Network > Routing > Virtual Router (trust-vr) > Edit: 次のように入力してから **OK** をクリックします。

Virtual Router ID: Custom (選択)
テキストボックスに 0.0.0.10 を入力します。

Network > Routing > Virtual Router (trust-vr) > Edit: **Create BGP Instance** を選択します。

AS Number (必須): 65000
BGP Enabled: (選択)

Network > Routing > Virtual Router (trust-vr) > Edit > Edit BGP Instance > Neighbors: 次のように入力してから **Add** をクリックします。

AS Number: 65000
Remote IP: 2.2.2.2
Outgoing Interface: ethernet3

Network > Routing > Virtual Router (trust-vr) > Edit > Edit BGP Instance > Neighbors > Configure (ここで追加したピア): **Peer Enabled** を選択し、**OK** をクリックします。

Network > Routing > Virtual Router (trust-vr) > Edit > Edit BGP Instance > Networks:

IP/Netmask フィールドに **4.1.1.0/24** と入力し、**Add** をクリックします。

IP/Netmask フィールドに **10.4.1.0/24** と入力し、**Add** をクリックします。

Network > Interfaces > Edit (ethernet3) > BGP: Select **Protocol BGP: Enable** を選択し、次に **Apply** をクリックします。

6. **ポリシー**

Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), corp
Destination Address:
    Address Book Entry: (選択), mgroup1
Service: any
Action: Permit

7. **マルチキャストポリシー**

MCast Policies (From: Trust, To: Untrust) > New: 次のように入力してから **OK** をクリックします。

MGroup Address: IP/Netmask (選択) 224.4.4.1/32
Bidirectional: (選択)
PIM Message: (選択)
BSR Static IP: (選択)
Join/Prune: (選択)

CLI (NS1)

1. インターフェース

```
Set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. アドレス

```
set address trust mgroup1 224.4.4.1/32
set address untrust branch 10.4.1.0/24
```

3. PIM-SM

```
set vrouter trust-vr
set vrouter trust-vr protocol pim enable
set interface ethernet1 protocol pim
set interface ethernet1 protocol pim enable
set interface tunnel.1 protocol pim
set interface tunnel.1 protocol pim enable
```

4. VPN トンネル

```
set ike gateway To_Branch address 4.1.1.1 main outgoing-interface ethernet3
    preshare fg2g4h5j proposal pre-g2-3des-sha
set vpn Corp_Branch gateway To-Branch3 sec-level compatible
set vpn Corp_Branch bind interface tunnel.1
set vpn Corp_Branch proxy-id local-ip 10.2.2.0/24 remote-ip 10.4.1.0/24
```

5. BGP

```
set vrouter trust-vr router-id 10
set vrouter trust-vr protocol bgp 6500
set vrouter trust-vr protocol bgp enable
set vrouter trust-vr protocol bgp neighbor 4.1.1.1
set vrouter trust-vr protocol bgp network 2.2.2.0/24
set vrouter trust-vr protocol bgp network 10.2.2.0/24
set interface ethernet3 protocol bgp enable
set interface ethernet3 protocol bgp neighbor 4.1.1.1
```

6. ポリシー

```
set policy name To-Branch from untrust to trust branch any any permit
```

7. マルチキャストポリシー

```
set multicast-group-policy from trust mgroup 224.4.4.1/32 any to untrust
    pim-message bsr-static-rp join bi-directional
save
```

CLI (NS2)

1. インターフェース

```
set interface ethernet 1 zone trust
set interface ethernet 1 ip 10.4.1.1/24
set interface ethernet 1 protocol igmp router
set interface ethernet 1 protocol igmp enable
set interface ethernet 3 zone untrust
set interface ethernet 3 ip 4.1.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. **アドレス**
   set address trust mgroup1 224.4.4.1/32
   set address untrust corp 2.2.2.0/24

3. **PIM-SM**
   set vrouter trust protocol pim
   set interface ethernet1 protocol pim
   set interface ethernet1 protocol pim enable
   set interface tunnel.1 protocol pim
   set interface tunnel.1 protocol pim enable
   set vrouter trust protocol pim zone trust rp proxy
   set vrouter trust protocol pim zone trust rp candidate interface ethernet1
   set vrouter trust protocol pim enable

4. **VPN トンネル**
   set ike gateway To_Corp address 2.2.2.2 main outgoing-interface ethernet3
   preshare fg2g4h5j proposal pre-g2-3des-sha
   set vpn Branch_Corp gateway To_Corp sec-level compatible
   set vpn Branch_Corp bind interface tunnel.1
   set vpn Branch_Corp proxy-id local-ip 10.4.1.0/24 remote-ip 10.2.2.0/24

5. **BGP**
   set vrouter trust-vr router-id 10
   set vrouter trust-vr protocol bgp 6500
   set vrouter trust-vr protocol bgp enable
   set vrouter trust-vr protocol bgp neighbor 2.2.2.2
   set vrouter trust-vr protocol bgp network 4.1.1.0/24
   set vrouter trust-vr protocol bgp network 10.4.1.0/24
   set interface ethernet3 protocol bgp neighbor 2.2.2.2

6. **ポリシー**
   set policy name To-Corp from untrust to trust corp any any permit

7. **マルチキャストポリシー**
   set multicast-group-policy from trust mgroup 224.4.4.1/32 any to untrust
   pim-message bsr-static-rp join bi-directional
   save

PIM-SM および IGMPv3

PIM-SM は、Internet Group Management Protocol (IGMP) バージョン 1、2 または 3 を搭載したインターフェースで動作します。IGMPv1 または v2 を搭載したインターフェースで PIM-SM を動作させると、マルチキャストグループのデータを受信するホストは、マルチキャストグループにデータを送信するソースからデータを受信することが可能です。IGMPv1 および v2 のメンバーシップレポートは、ホストが参加しようとしているマルチキャストグループだけを示します。このレポートには、マルチキャストトラフィックのソースに関する情報は含まれません。PIM-SM は IGMPv1 および v2 のメンバーシップレポートを受信すると、マルチキャストグループテーブルに (*、G) エントリを作成し、ソースに対しマルチキャストグループへの送信の許可を出します。これを any-source-multicast model (ASM) と言い、グループにデータを送信するソースが分からないまま、受信側はマルチキャストグループに参加します。ネットワークはソースに関する情報を保持します。

IGMPv3 を搭載したホストは、参加するマルチキャストグループやマルチキャストトラフィックを受信するソースを示します。IGMPv3 のメンバーシップレポートには、マルチキャストグループアドレス、フィルタモード、どちらを含めるか除外するか、ソースの一覧が含まれています。

フィルタモードを含めると、受信側はマルチキャストトラフィックをソース一覧にあるアドレスからのみ受け入れます。PIM-SM はソース一覧とフィルタモードを含めた IGMPv3 メンバーシップレポートを受信すると、ソース一覧にある全ソースのマルチキャストルートテーブルに (S、G) エントリを作成します。

フィルタモードを除外すると、受信側は一覧にあるソースからのマルチキャストトラフィックを受け入れず、それ以外のすべてのソースからのマルチキャストトラフィックを受け入れます。PIM-SM は ソース一覧と除外フィルタモードの入った IGMPv3 メンバーシップレポートを受信すると、グループの (*、G) エントリを作成し、ソース一覧にあるソースの prune メッセージを送信します。この場合、受信側でソースのアドレスが分からない場合は、集合地点を設定する必要があります。

第 10 章

ICMP ルーター検出プロトコル

本章では、RFC 1256 で定義されている、インターネット制御メッセージプロトコル（ICMP）ルーター検出プロトコルについて説明します。本章のセクションは、以下のようになります。

- 223 ページの「概要」
- 224 ページの「ICMP ルーター検出プロトコルの構成」
  - 224 ページの「ICMP ルーター検出プロトコルを使用可能にする」
  - 224 ページの「WebUI からの ICMP ルーター検出プロトコルの構成」
  - 225 ページの「CLI からの ICMP ルーター検出プロトコルの構成」
- 227 ページの「IRDP を使用不可にする」
- 227 ページの「IRDP 設定の表示」

概要

ICMP ルーター検出プロトコル（IRDP）は、ホストとルーターとの間の ICMP メッセージの交換を行います。セキュリティデバイスがルーターであり、定期的にあるいは要求に応じて、指定されたインターフェースの IP アドレスを通知します。ホストがリッスンするように構成されている場合、セキュリティデバイスを定期的な通知を送信するように構成できます。ホストが明示的にルーター要請を送信する場合、セキュリティデバイスが要求に応じて応答するように構成できます。

注： IRDP を利用できないプラットフォームがあります。この機能がお使いのセキュリティデバイスで利用できるかどうか、データシートを見て確認してください。

ScreenOS は、インターフェースごとに IRDP をサポートします。そのインターフェースで IRDP を利用する前に、IP アドレスを割り当てる必要があります。デフォルトでは、この機能は無効です。この機能は、NetScreen 冗長プロトコル（NSRP）を使って、高可用性（HA）環境で構成できます。

ICMP ルーター検出プロトコルの構成

WebUI または CLI で、IRDP を使用可能および使用不可にしたり、IRDP の設定を構成または表示したりできます。

ICMP ルーター検出プロトコルを使用可能にする

IRDP をインターフェースで使用可能にすると、ScreenOS は、ネットワークへの IRDP 通知を即座に開始します。インターフェースの構成に関する情報については、2-35 ページの「インターフェース」を参照してください。

次の例では、Trust インターフェースについて IRDP を構成します。

WebUI

Network > Interfaces (edit) > IRDP: IRDP 使用可能チェックボックスを選択します。

CLI

```
set interface trust protocol irdp enable
```

WebUI からの ICMP ルーター検出プロトコルの構成

WebUI から IRDP を構成するには、次を行います。

Network > Interface > Edit > IRDP: 希望の設定を入力して **OK** をクリックします。

表 20 に、IRDP のパラメータ、デフォルト値、および利用可能な設定を一覧表示します。

表 20: IRDP の WebUI による設定

パラメータ	デフォルトの設定	その他の設定
IPv4 address	■ 1 次および 2 次 IP アドレスの通知 ■ 管理および webauth IP アドレスの非通知	通知－希望の値を追加可能（-1 ～ 2147483647）
Broadcast-address	無効	有効
Init Advertise Interval	16 秒	1 ～ 32 秒
Init Advertise Packet	3	1 ～ 5
Lifetime	Max Advertise Interval 値の 3 倍	9000 秒までの Max Advertise Interval 値
Max Advertise Interval	600 秒	4 ～ 1800 秒
Min Advertise Interval	Max Advertise Interval 値の 75%	3 ～ Max Advertise Interval 値
Response Delay	2 秒	0 ～ 4 秒

CLI からの ICMP ルーター検出プロトコルの構成

通知および要請動作を制御するため、CLI から IRDP パラメータを構成できます。

インターフェースの通知

デフォルトでは、ScreenOS は、セキュリティデバイスの 1 次 IP アドレスを通知します。しかし、WebAuth および管理については、IP アドレスは通知されません。

セキュリティデバイスの優先度状況も関連付けできます。優先度状況は、-1 ～ 2147483647 までの数です。数が大きいほど優先度は高くなります。異なったセキュリティデバイスには異なった優先度値を割り当てることができます。たとえば、主にネットワークトラフィックを処理するセキュリティデバイス優先度値を高く割り当てることができます。バックアップのセキュリティデバイスには、低い優先度値を割り当てることができます。

IP アドレスが 10.10.10.10 で、優先度が 250 の Untrust インターフェースを通知するには、次のコマンドを入力します。

```
set interface untrust protocol irdp 10.10.10.10 advertise
set interface untrust protocol irdp 10.10.10.10 preference 250
save
```

アドレスのブロードキャスト

デフォルトでは、IRDP が使用可能になったときの最初のブロードキャスト通知メッセージ以外に、インターフェースはブロードキャスト通知を送信しません。デフォルトのアドレスは 224.0.0.1（ネットワーク上の全ホスト）です。

Untrust インターフェースのデフォルトのブロードキャストアドレスを構成するには、次のコマンドを入力します。

```
set interface untrust protocol irdp broadcast-address
```

最大通知間隔の設定

最大通知間隔は、ICMP 通知と ICMP 通知の間に経過する最大秒数です。この間隔には、4 ～ 1800 秒の値を使用できます。デフォルト値は 600 秒です。

Untrust インターフェースの最大通知間隔を 800 秒に設定するには、次のコマンドを入力します。

```
set interface untrust protocol irdp max-adv-interval 800
save
```

最小通知間隔の設定

最小通知間隔は、通知間隔の下限（秒単位）です。最大通知間隔の 75 パーセントとして計算されます。最小通知間隔の値の範囲は、3 から最大通知間隔の値までです。最大通知間隔を変更すると、最小通知間隔の値は自動的に計算されます。

最大通知間隔を 800 秒に設定すると、ScreenOS は自動的に再計算を行い、最小通知間隔を 600 秒と計算します。

Untrust インターフェースの最小通知間隔を 500 秒に設定するには、次のコマンドを入力します。

```
set interface untrust protocol irdp min-adv-interval 500
save
```

通知寿命値の設定

デフォルトでは、通知寿命値は、最大通知間隔の 3 倍です。通知寿命値を設定できます。値の範囲は、最大通知間隔の値（4 ～ 1800 秒）から 9000 秒までです。

Untrust インターフェースの通知寿命値を 5000 秒に設定するには、次のコマンドを入力します。

```
set interface untrust protocol untrust lifetime 5000
save
```

応答遅延の設定

デフォルトでは、セキュリティデバイスは、0 ～ 2 秒待ってから、クライアント要請要求に応答します。応答遅延設定を、遅延なし（0 秒）から 4 秒の応答遅延の範囲で変更できます。たとえば、応答遅延を 4 秒に構成する場合、セキュリティデバイスは 0 ～ 4 秒待ってから応答します。

Untrust インターフェースへの応答遅延値を 4 秒に設定するには、次のコマンドを入力します。

```
set interface untrust protocol irdp response-delay 4
save
```

初期通知間隔の設定

初期通知間隔は、通知に割り当てられた IRDP 起動期間の秒数です。デフォルトでは、この間隔は 16 秒です。この間隔の値の範囲は、1 ～ 32 秒です。

Untrust インターフェースの初期通知間隔を 24 秒に設定するには、次のコマンドを入力します。

```
set interface untrust protocol irdp init-adv-interval
save
```

初期通知パケット数の設定

デフォルトでは、セキュリティデバイスは、指定された起動期間に、3 つの通知パケットを送信します。この設定を 1 ～ 5 の範囲で変更できます。

送信する初期パケットの数を 5 に変更するには、次のコマンドを入力します。

```
set interface untrust protocol irdp init-adv-packet 5
save
```

IRDP を使用不可にする

インターフェースで IRDP を使用不可にできます。しかし、そうすると、ScreenOS は、元の構成から関連する設定をすべて削除します。

Trust インターフェースで IRDP を使用不可にするには、次のコマンドを入力します。

unset interface trust protocol irdp enable

IRDP 設定の表示

WebUI または CLI で IRDP 情報を表示できます。

IRDP 設定を表示するには、**get irdp** または **get irdp interface** *interface_name* コマンドを入力します。

WebUI

Network > Interface > Edit > IRDP: IRDP が使用可能かどうかを表示できます。

CLI 1

device> **get irdp**

```
Total 1 IRDP instance enabled
------------------------------------------------------------------
interface    dest-addr       lifetime adv-interval Next-Adv(sec)
------------------------------------------------------------------
untrust      255.255.255.255     6000 450 to 600   358
```

CLI 2

device-> **get irdp interface untrust**

```
IRDP enabled on untrust:
    advertisement interval       : 450 to 600 sec
    next advertisement in        : 299 sec
    advertisement lifetime       : 6000 sec
    advertisement address        : 255.255.255.255
    initial advertise interval   : 16 sec
    initial advertise packet     : 3
    solicitation response delay  : 4 sec
    10.100.37.90                 : pref 250, advertise YES
```

索引

B

BGP
- AS-path アクセスリスト 120
- external 109
- 仮想ルーター、インスタンスの作成 111
- 近隣ノード、認証 117
- 構成、確認 116
- コミュニティ 128
- コンフェデレーション 127
- 正規表現 120
- 設定、セキュリティ 117
- 内部 109
- パス属性 109
- パラメータ 118
- プロトコルの概要 108
- メッセージタイプ 108
- ロードバランス 39

BGP 使用可能
- VR での 111
- インターフェース上 112

BGP ルート
- おもみ、設定 122
- 再配布 120
- 条件付きアドバタイズメント 122
- 除外 130
- 属性、設定 123
- 追加 121
- デフォルト、拒否 118
- リフレクション 125

BGP ルート、集約
- AS-Path の 131
- AS-Set の 129
- の属性 132

BGP 、構成
- peers 113
- ステップ 110
- ピアグループ 113

BGP ルート
- 集約 129

E

ECMPECMP 39, 62

I

IGMP
- アクセスリスト、利用 163
- インターフェース、稼動 162
- クエリア 161
- 構成、確認 166
- 設定、基本 164
- パラメータ 166, 167
- ホストメッセージ 161
- ポリシー、マルチキャスト 173

IGMP (Internet Group Management Protocol)
- IGMP を参照

IGMP プロキシ 168
- インターフェース上 170
- 送信側 180

O

OSPF
- ECMP への対応 62
- Hello プロトコル 51
- LSA の省略 71
- LSA フラッディングの省略 L 71
- Tunnel インターフェース 72
- インターフェースパラメータ 66
- インターフェース、エリアに割り当て 57
- 仮想リンク 63
- 近隣ノード、認証 68
- 近隣ノード、フィルタリング 69
- 準スタブエリア 51
- スタブエリア 51
- セキュリティ設定 68
- 接続状態の通知 50
- 設定の手順 53
- 大域パラメータ 62
- フラッディングの回避 70
- ブロードキャストネットワーク 52
- ポイントツーポイントネットワーク 52
- ポイントツーマルチポイント 72
- リンクタイプ、設定 73
- ロードバランス 39

OSPF エリア 50
- インターフェース、エリアに割り当て 57
- 定義 55

OSPF ルーター
VR 上にインスタンス作成 54
種類 51
代表 51
バックアップ代表 51
隣接関係 51
OSPF ルート
route-deny 機能、無効化 73
再配布 60
再配布、要約 61
デフォルト、拒否 70

P

PIM-SM 190, 194
IGMPv3 221
インスタンス、作成 195
インターフェースパラメータ 210
集合地点 191
集合地点の設定 205
セキュリティ設定 207
設定の手順 195
代表ルーター 191
トラフィック、転送 192
プロキシ RP 212

R

RIP
インスタンス、VR で作成 80
インターフェースパラメータ 89
インターフェース、稼動 81
近隣ノードの認証 90
大域パラメータ 87
データベース 97
バージョン 94
バージョン、プロトコル 94
フラッディングの回避 92
プレフィックスサマリ 96
ポイントツーマルチポイント 100
要求回路の設定 99
隣接ノードのフィルタリング 91
ロードバランス 39
RIP ルート
再配布 81
代替 97
デフォルトを拒否 92
要約、設定 96
RIP 、設定
ステップ 79
デマンド回線 99
セキュリティ 90
RIP 、表示
インターフェース詳細 86
近隣ノード情報 85
データベース 84
プロトコル詳細 84

V

VR 40–45
2 つを使用 26
BGP 110–117
ECMPECMP 39
OSPF 53–71
RIP 79–94
SBR 19
SIBR 22
vsys 上の 29
アクセスリスト 43
設定変更 24
ルーター ID 25
ルートのメトリック 34
VR 、ルーティングテーブル
最大エントリ 32
VR 、ルーティングテーブル VR 、
複数の仮想ルーターにおけるルックアップ 36
VR 、ルート VR
選択 32
マップ 41
インポート 45
エキスポート中 45
フィルタリング 42
優先度 33
再配布 40

あ

アクセスリスト
IGMP 163
PIM-SM 207
マルチキャストルーティング 155
ルートの 43

い

インターフェース、IGMP 上で稼動 162

お

オープンショーテストパスファースト (OPSF)
OSPF を参照

か

仮想ルーター
VR を参照

し

自律システム (AS) 番号 111

せ

静的ルーティング 2–10, 1
Null インターフェースで転送する 11
構成 5
使用 3
マルチキャスト 154
接続状態 (LSA) の通知抑止 71

そ

ソースのインターフェースベースのルーティング (SIBR) 22
ソースベースのルーティング (SBR) 19

は

パスのコストによるロードバランス 39, 62
汎用ルーティングのカプセル化 (GRE) 155

ふ

プロトコル独立マルチキャスト
PIM を参照

ほ

ポイントツーマルチポイント構成
OSPF 72
ポリシー
マルチキャスト 157

ま

マルチキャスト
IGMP のポリシー 173
アドレス 152
逆方向パス転送 152
静的ルーティング 154
配布ツリー 190
ポリシー 157
ルーティングテーブル 153
マルチキャストルーティング
IGMP 159
PIM 187

よ

要求回路 、RIP 99

る

ルーティング情報プロトコル (RIP)
RIP を参照
ルーティングテーブル 17
種類 17
複数の仮想ルーターにおけるルックアップ 36
マルチキャスト 153
ルートの選択 32
ルーティング、マルチキャスト 151
ルート
インポート 45
エキスポート中 45
再配布 40
選択 32
フィルタリング 42
マップ 41
メトリック 34
優先度 33
ルートルックアップ
順序 34
複数の仮想ルーター 36
ルートを定義する Null インターフェース 11

概念と用例
ScreenOS リファレンス ガイド

第 8 部 :
アドレス変換

リリース 6.0.0、改訂 02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

品番 : 530-017774-01-JP, 改訂 02

Copyright Notice

Copyright © 2007 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

目次

本編について v

ドキュメントの規則 v
Web ユーザーインターフェースの規則 vi
コマンドラインインターフェースの規則 vi
ネーミング規則および文字タイプ vii
説明図の規則 viii
技術ドキュメントおよびテクニカルサポート ix

第 1 章 アドレス変換 1

アドレス変換の概要 1
ソースネットワークアドレス変換 1
宛先ネットワークアドレス変換 3
ポリシーベースの NAT-Dst 4
マップ IP: 6
仮想 IP 6
ポリシーベースの変換のさまざまな形態 7
例 : NAT-Src - DIP プールからアドレス取得、PAT 機能あり 7
例 : NAT-Src - DIP プールからアドレス取得、PAT 機能あり 8
例 : NAT-Src - DIP プールからアドレスシフティングによりアドレス取得 8
例 : NAT-Src - Egress インターフェース IP アドレスに変換 9
例 : NAT-Dst を特定の IP アドレスに変換、ポートマッピングあり 9
例 : NAT-Dst を特定の IP アドレスに変換、ポートマッピングなし 9
例 : 所定の IP アドレス範囲を特定の IP アドレスに変換した NAT-Dst 10
例 : IP アドレス範囲間の NAT-Dst 10
NAT-Src と NAT-Dst の適用方向 10

第 2 章 ソースネットワークアドレス変換 13

NAT-Src の概要 13
NAT-Src - DIP プールからアドレス取得、PAT 機能あり 14
例 : PAT を有効にした NAT-Src の設定 15
NAT-Src - DIP プールからアドレス取得、PAT 機能なし 18
例 : PAT を無効にした NAT-Src の設定 18
NAT-Src - DIP プールからアドレスシフティングによりアドレス取得 19
例 : アドレスシフティングによる NAT-Src の設定 20
NAT-Src - Egress インターフェース IP アドレスに変換 23
例 : DIP プールを使わない NAT-Src の設定 23

第 3 章 宛先ネットワークアドレス変換 27

NAT-Dst の概要 28
NAT-Dst のパケットフロー 29
NAT-Dst のルーティング 32
例 : 同じインターフェースに接続されたアドレス 33

例 : 同じインターフェースに接続されているが、ルーターにより分離されたアドレス 33
例 : 別々のインターフェースに接続されたアドレス 34
NAT-Dst-1 対 1 のマッピング 35
例 : 1 対 1 の宛先アドレス変換 35
単一のアドレスから複数のアドレスへの変換 38
例 : 1 対多の宛先アドレス変換 38
NAT-Dst- 多対 1 のマッピング 40
例 : 多対 1 の宛先アドレス変換 40
NAT-Dst- 多対多のマッピング 43
例 : 多対多の宛先アドレス変換 44
ポートマッピングを伴う NAT-Dst 46
例 : ポートマッピングを伴う NAT-Dst 46
１つのポリシーで NAT-Src と NAT-Dst を適用 49
例 : NAT-Src と NAT-Dst の組み合わせ 49

第 4 章 マップアドレスと仮想アドレス 61

マップ IP アドレス 61
MIP と Global ゾーン 62
例 : Untrust ゾーンインターフェース上の MIP 63
例 : 別のゾーンから MIP に到達するトラフィック 65
例 : MIP をトンネルインターフェースに追加 68
MIP を Untrust ゾーンとして扱うインターフェース 69
例 : Untrust ゾーンインターフェース上の MIP 69
MIP とループバックインターフェース 71
例 : 2 つのトンネルインターフェースに対する MIP 72
MIP グルーピング 78
例 : マルチセルポリシーにおける MIP グルーピング 78
仮想 IP アドレス 79
VIP と Global ゾーン 81
例 : 仮想 IP サーバーの設定 81
例 : VIP 設定の編集 83
例 : VIP 設定の削除 83
例 : カスタムサービス、複数のポートを使うサービスに対応した VIP 83

索引 ..... IX-I

本編について

*第 8 部 : アドレス変換*では、ScreenOS で実行できるさまざまなアドレス変換方式を取り上げます。本編は、それぞれの変換を行うためのセキュリティデバイスの設定方法を説明した、以下の章で構成されています。

- 第 1 章「アドレス変換」、はさまざまな変換オプションの概要。詳細は、これ以降の各章で説明します。
- 第 2 章 「ソースネットワークアドレス変換」、はソース IP アドレスのパケットのヘッダーの変換 (NAT-src) を説明しています。ポートアドレス変換 (PAT) の有無についても説明しています。
- 第 3 章 「宛先ネットワークアドレス変換」、は宛先 IP アドレスのパケットのヘッダーの変換 (NAT-dst) について説明しています。宛先ポートアドレスのマッピングの有無についても説明しています。このセクションでは、NAT-src を実行する場合のパケットフロー情報、ルーティングの留意点、アドレスシフティングについても説明しています。
- 第 4 章 「マップアドレスと仮想アドレス」、はある宛先 IP アドレスから別のアドレスへの、IP アドレス単体 (マップ IP) に基づくマッピング、または宛先 IP アドレスと宛先ポート番号に基づくマッピング (仮想 IP) について説明しています。

注 : インターフェースベースのソースネットワークアドレス変換 (単純に *NAT* と呼ばれます) については、**2**-94 ページの「NAT モード」を参照してください。

ドキュメントの規則

このドキュメントは、次のセクションで説明されている規則を使用しています。

- vi ページの「Web ユーザーインターフェースの規則」
- vi ページの「コマンドラインインターフェースの規則」
- vii ページの「ネーミング規則および文字タイプ」
- viii ページの「説明図の規則」

Web ユーザーインターフェースの規則

WebUI（Web ユーザーインターフェース）では、各作業の操作指示は、操作手順と構成設定値に分かれています。構成設定を入力できる WebUI ページを開くには、画面の左側にあるナビゲーション ツリーのメニュー項目をクリックして、そのページに移動します。先へ進むと、ナビゲーション パスが画面の上部に表示されます。各ページは角括弧で分離されています。

WebUI のパスおよびアドレスを定義するためのパラメータは、以下のとおりです。

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.2.2.5/32
Zone: Untrust

構成設定のオンラインヘルプを開くには、画面の左上にある疑問符（?）をクリックします。

ナビゲーションツリーにも、Help > Config Guide 構成ページがあり、セキュリティポリシーおよび IPSec （インターネットプロトコルセキュリティ）の構成に役立ちます。ドロップダウンメニューからオプションを選択して、そのページの指示に従います。構成設定のオンラインヘルプを開くには、左上にある **?** 文字をクリックします。

コマンドラインインターフェースの規則

次の規則は、例とテキストにおいて、コマンドラインインターフェース（CLI）コマンドの構文を示すために使用されます。

例においては、次のように使用されます。

- 角括弧 [ ] 内にあるものはすべてオプションです。
- 中括弧 { } 内にあるものはすべて必須です。
- 選択肢が複数ある場合、各選択肢はパイプ (|) で区切られています。次に例を示します。

  set interface { ethernet1 | ethernet2 | ethernet3 } manage

- 変数は*斜体*で表示されます。

  set admin user *name1* password *xyz*

テキストにおいては、コマンドは**太字**で、変数は*斜体*で表示されます。

注： キーワード入力時には、単語を間違いなく識別できる数の文字を入力すれば十分です。**set admin user wheezer j12fmt54** というコマンドを入力する際には、**set adm u whee j12fmt54** と入力するだけで十分です。ただし、本編に記載されたコマンドはすべて本来の形式で記載されています。

ネーミング規則および文字タイプ

ScreenOS はオブジェクトの名前 (アドレス、管理ユーザー、認証サーバー、IKE ゲートウェイ、仮想システム、VPN トンネルおよびゾーンなど、ScreenOS 構成に定義されているもの) に関して、次の規則に従います。

- 名前文字列に 1 つまたは複数のスペースが含まれる場合、文字列全体を二重引用符で囲む必要があります。例 :

  set address trust “local LAN” 10.1.1.0/24

- 二重引用符で囲まれた文字列の先頭または末尾のスペースを取り除きます。たとえば、**「 local LAN 」**は**「local LAN」**となります。

- 連続した複数のスペースは、一つのスペースとして扱われます。

- CLI キーワードの多くはケースセンシティブではありませんが、名前文字列はケースセンシティブです。たとえば、**「local LAN」**は**「local lan」**とは異なります。

ScreenOS は、次の文字タイプをサポートします。

- 1 バイト文字セット (SBCS) およびマルチバイト文字セット (MBCS)。SBCS の例に、ASCII、欧州言語、およびヘブライ語があります。2 バイト文字セット (DBCS) とも呼ばれる MBCS の例に、中国語、韓国語、および日本語があります。

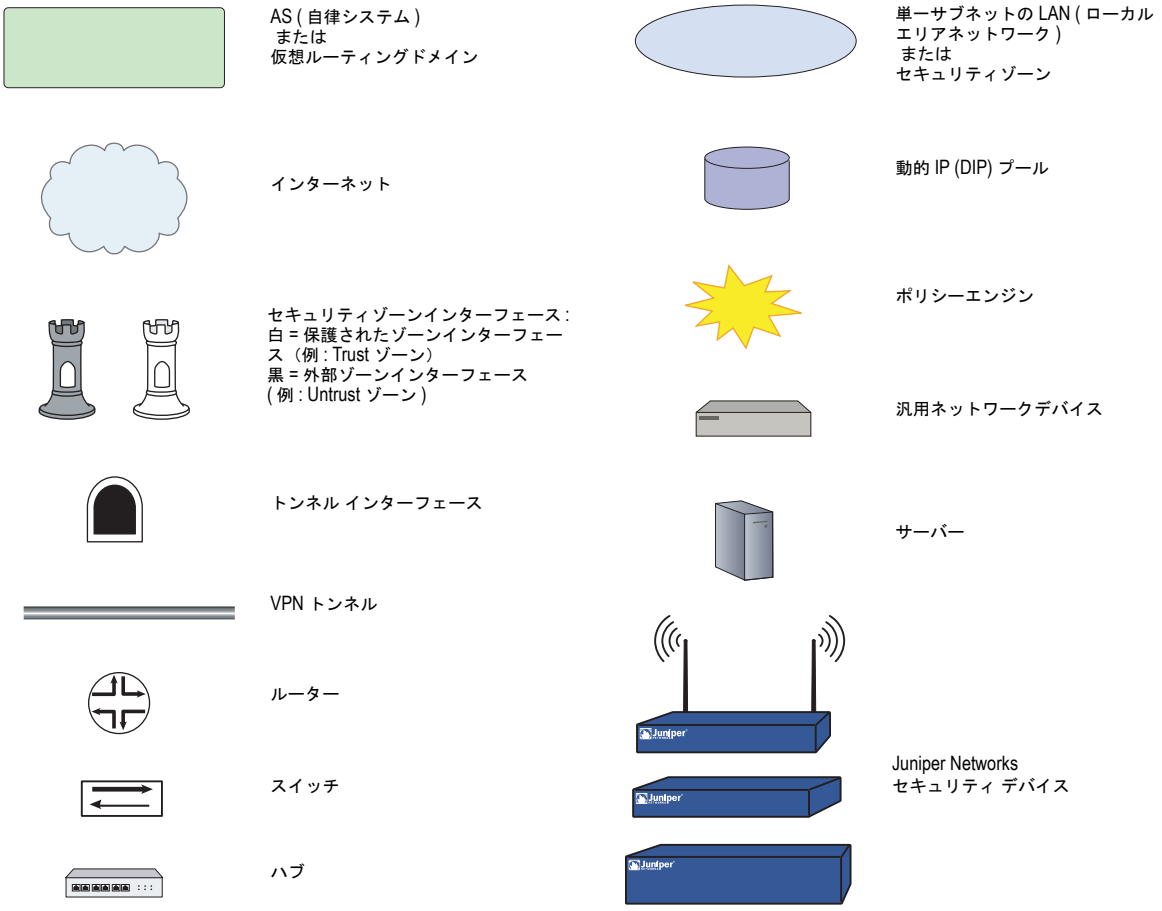
- ASCII 文字の 32（16 進数の 0x20）から 255（0xff)。ただし二重引用符 (“) は、スペースを含む名前文字列の先頭と末尾を示す特殊な意味をもつため、例外とします。

注 : コンソール接続では、SBCS のみがサポートされます。ご利用のブラウザがサポートする文字セットに応じて、WebUI は SBCS および MBCS の両方をサポートします。

説明図の規則

次の図は、本編を通して説明図に使用されている画像の基本的なものです。

図 1: 説明図の画像



技術ドキュメントおよびテクニカルサポート

Juniper Networks 製品のいずれかの技術ドキュメントを入手するには、www.juniper.net/techpubs/ をご覧になってください。

テクニカルサポートについては、http://www.juniper.net/customers/support/ にある Case Manager を使って事例サポートを開くか、1-888-314-JTAC (米国内) か 1-408-745-9500 (その他の国) までお問い合わせください。

本書に間違いや欠落があった場合は、techpubs-comments@juniper.net までお知らせください。

第 1 章
アドレス変換

ScreenOS には、宛先 IP アドレスと宛先ポートアドレスを変換する方式が、いくつも組み込まれています。本章ではさまざまなアドレス変換方式を、次の節に分けて解説します。

- 1 ページの「アドレス変換の概要」
  - 1 ページの「ソースネットワークアドレス変換」
  - 3 ページの「宛先ネットワークアドレス変換」
- 7 ページの「ポリシーベースの変換のさまざまな形態」
- 10 ページの「NAT-Src と NAT-Dst の適用方向」

アドレス変換の概要

ScreenOS には、ネットワークアドレス変換 (NAT) の方式が何種類か組み込まれています。NAT は IP パケットヘッダーのインターネットプロトコル (IP) アドレスの変換、そしてオプションとしてトランスミッションコントロールプロトコル (TCP) のポート番号の変換またはユーザーデータグラムプロトコル (UDP) データグラムヘッダーの変換を含みます。変換の対象となるのは、ソースアドレス（および場合によりソースポート番号）と宛先アドレス（および場合により宛先ポート番）または変換された要素の組み合わせです。

ソースネットワークアドレス変換

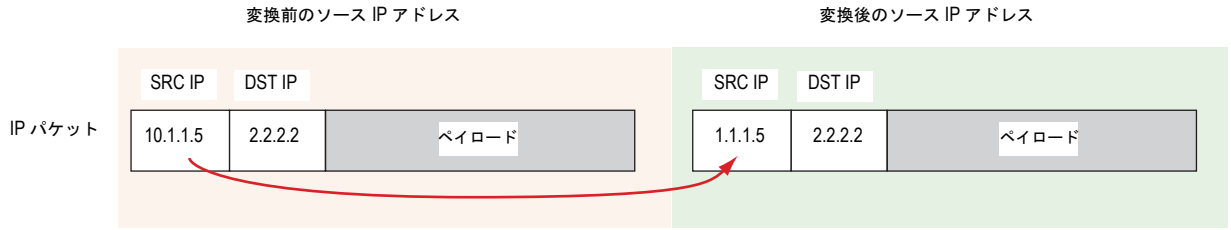
ソースネットワークアドレス変換 (NAT-src) では、あるソース IP アドレスを別のアドレスに変換する、という処理を行います。変換後のアドレスは、動的 IP (DIP) プール、またはセキュリティデバイスの egress インターフェースから取得します。DIP プールから取得する場合、その具体的なアドレスは不定である場合と、予測がつく場合があります。すなわち、DIP プールに確保されている中からランダムに選ぶか、あるいは元のソース IP アドレスから所定の計算により求めることになります。

注： 変換後のアドレスがあらかじめ予測できる決定性のアドレス変換では、アドレスシフティングという技法を使います。これについては後述します。これについては後述します。アドレスシフティングにより NAT-src を適用する手法については、19 ページの「NAT-Src - DIP プールからアドレスシフティングによりアドレス取得」を参照してください。また、同じアドレスシフティングで NAT-dst を適用する手法については、49 ページの「1 つのポリシーで NAT-Src と NAT-Dst を適用」を参照してください。

Egress インターフェースから変換後のアドレスを取得した場合は、すべてのパケットについて、ソース IP アドレスを当該インターフェースの IP アドレスに変換します。NAT-src の適用については、セキュリティデバイス側で、インターフェースレベルかポリシーレベルかを設定できます。NAT-src を適用するポリシーを設定した場合、ingress インターフェースが NAT モードになっていれば、インターフェースベースの NAT であったとしても、強制的にポリシーベースの NAT-src の設定になります (本章ではポリシーベースの NAT-src についてのみ解説します。インターフェースベースの NAT-src、あるいは NAT 全般については、**2**-94 ページの「NAT モード」を参照してください。DIP プールの詳細については、**2**-143 ページの「動的 IP プール」を参照してください。)

注： ポリシーベースの NAT-src は、ingress インターフェースが Route モードまたは NAT モードの場合に適用できます。NAT モードの場合は、ポリシーレベル NAT-src パラメータが、インターフェースレベル NAT パラメータよりも優先します。

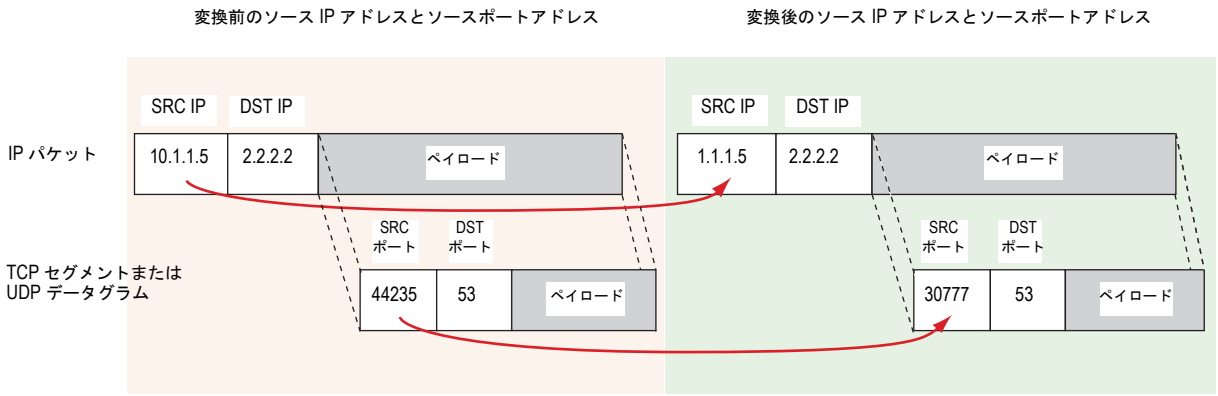
図 2: ソース IP アドレス変換



ポリシーベースの NAT-src では、元のソースポート番号に対してポートアドレス変換 (PAT、Port Address Translation) を施すよう、セキュリティデバイスを設定することも可能です。PAT を有効にした場合、セキュリティデバイスは、最大 64,500 とおりの IP アドレスを単一の IP アドレスに変換できます。元の IP アドレスに応じて、変換後のポート番号は 64,500 とおりになります。IP アドレスは同じであっても、元の IP アドレスごとに別々のポート番号を与えているので、それぞれのセッション状態を区別できるのです。インターフェースベースの NAT-src (単に「NAT」と言えば一般にこのことを指す) では、自動的に PAT が有効になります。セキュリティデバイスは元の IP アドレスが何であっても同じ (egress インターフェースの) IP アドレスに変換するので、そのパケットが属するセッションを区別するためには、変換後のポート番号を使用します。同様に、DIP プールに IP アドレスが 1 つしか確保されていない場合も、セキュリティデバイスで複数のホストに NAT-src を適用しようとすれば、同じ理由で PAT が必要になります。

注 : PAT を有効にした場合は、DIP プールから IP アドレスを取得するのと同様に、未使用ポート番号のプールを管理します。最大 64,500 とおりというのは、ポート番号の最大値である 65,535 から、「よく知られているサービス」用のポート (well-known ports) として予約された番号の最大値である 1,023 を引いた値です。したがって、DIP プールに IP アドレスが 1 つしか用意されていない場合、セキュリティデバイスで PAT を有効にすれば、最大 64,500 とおりの IP アドレスを単一の IP アドレスに変換できますが、元々あったポート番号の区別はなくなってしまいます。

図 3: ソース IP とソースポート宛先変換



特定のポート番号を想定したアプリケーションの場合、PAT を有効にすると正常に動作しなくなります。そのような場合は PAT を無効にしてください。

注 : NAT-src について詳しくは 13 ページの「ソースネットワークアドレス変換」を参照してください。

宛先ネットワークアドレス変換

Screen OS には、宛先ネットワークアドレス変換 (NAT-dst) を施すしくみが 3 とおり組み込まれています。

- **Policy-based NAT-dst**: 4 ページの「ポリシーベースの NAT-Dst」を参照してください
- **MIP**: 6 ページの「マップ IP:」を参照してください
- **VIP**: 6 ページの「仮想 IP」を参照してください

どれも IP パケットヘッダー中の宛先 IP アドレスを別のアドレスに変換します。ポリシーベースの NAT-dst および VIP では、オプションとしてポートマッピングを使うこともできます。

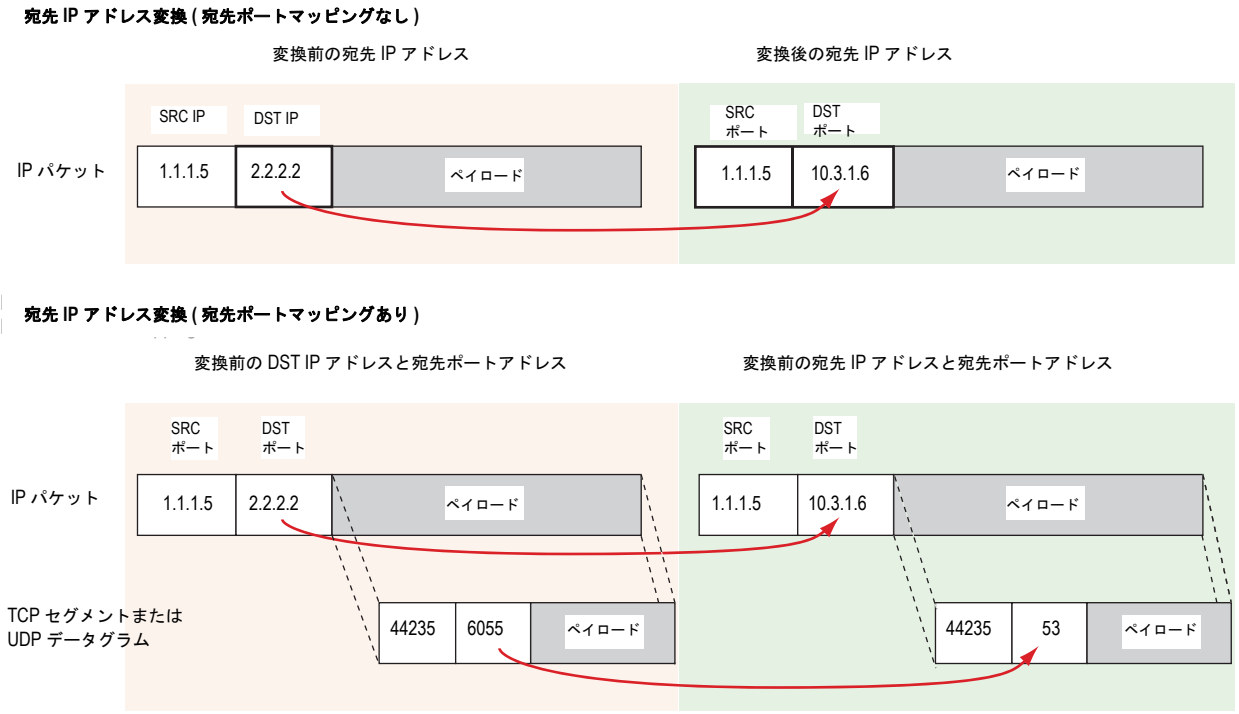
注： ポートマッピングについては 4 ページの「ポリシーベースの NAT-Dst」と 27 ページの「宛先ネットワークアドレス変換」を参照してください。

ScreenOS では、ポリシーベースの NAT-dst を、MIP や VIP と組み合わせて使うことはできません。MIP や VIP を構成した場合、ポリシーベースの NAT-dst を適用したトラフィックに対しても、重ねて MIP や VIP を適用してしまいます。つまり間違って、同じトラフィックに対して両方を同時に設定した場合、NAT-dst を適用したとしても、その効果は MIP や VIP によって無効になってしまうのです。

ポリシーベースの NAT-Dst

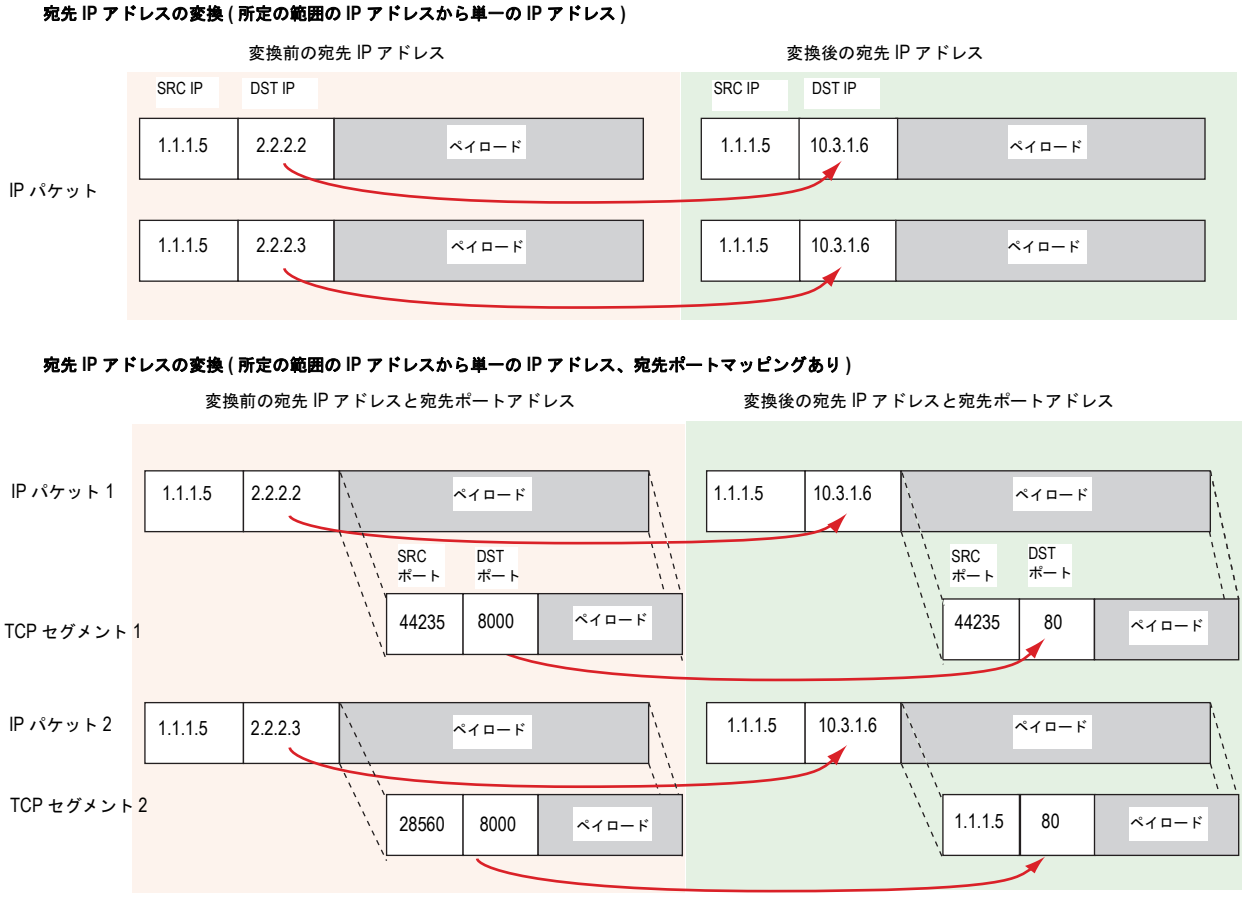
ある IP アドレスを別のアドレスに変換する、所定の範囲の IP アドレスをある特定の IP アドレスに変換する、所定の範囲の IP アドレスを所定の範囲の IP アドレスに変換する、などといった、変換のポリシー (条件規則) を設定することができます。単一の宛先 IP アドレスが他の IP アドレスに変換されたり、所定の範囲の IP アドレスが単一の IP アドレスに変換された場合、ScreenOS はポートマッピングの有無にかかわらず NAT-dst をサポートすることができます。ポートマッピングは一つの宛先ポート番号から他の特定の番号への変換で、その対応関係は予測可能 (決定性) です。これは PAT とは異なります。PAT とは、ホスト側でランダムに割り当てられたソースポート番号を、セキュリティデバイス側でランダムに割り当てたポート番号に変換する、というものです。

図 4: 宛先 IP アドレス変換



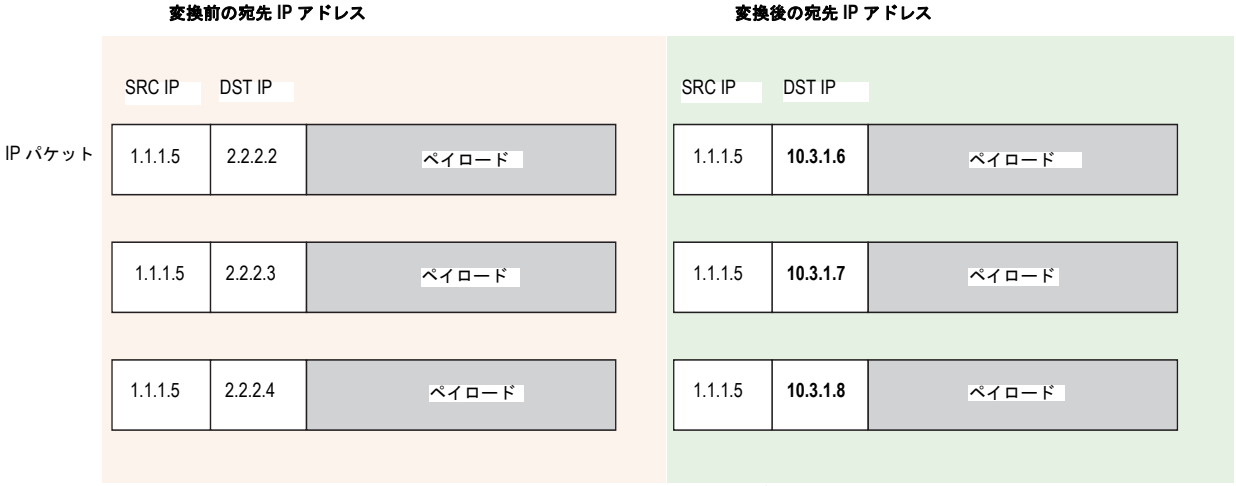
所定の範囲のアドレスを単一のアドレスに変換する、というポリシーを設定して NAT-dst を適用した場合、セキュリティデバイスはユーザーが定義した範囲の宛先 IP アドレスを、ある特定のアドレスに変換します。ポートマッピングも可能です。

図 5: 所定の IP アドレス範囲を特定の IP アドレスに変換した NAT-Dst



所定の範囲の IP アドレスを所定の範囲の IP アドレスに変換する、というポリシーを設定して NAT-dst を適用した場合、アドレスシフティングという方法により、ある範囲の宛先アドレスが別のアドレスに変換されます。変換後のアドレスは予測が可能です。

図 6: アドレスシフティングによる NAT-Dst の設定



ある範囲の IP アドレスに対して NAT-dst を適用する場合、セキュリティデバイスは、変換前と変換後のアドレスの対応関係を管理します。

注： NAT-src と NAT-dst の両方を適用するポリシーも設定可能です。アドレス変換はそれぞれ独立に行われ、しかも一方向にのみ作用します。すなわち、たとえばゾーン 1 からゾーン 2 へのトラフィックに対して NAT-dst を適用するとしても、明示的に指定しない限り、ゾーン 2 からゾーン 1 へのトラフィックに対して NAT-src を適用することはありません。詳細については、10 ページの「NAT-Src と NAT-Dst の適用方向」を参照してください。NAT-dst に関する詳細については 27 ページの「宛先ネットワークアドレス変換」を参照してください。

マップ IP:

マップインターネットプロトコル (MIP) は、一つの IP アドレスから他の IP アドレスを対応づけるマッピングのことです。同じサブネットに属するアドレスを 1 つ、インターフェース IP アドレスとして定義しておきます。それ以外のアドレスは、トラフィックの宛先となるホストに割り当てます。MIP は両方向に働きます。すなわち、インバウンドトラフィックの宛先 IP アドレスはすべて MIP アドレスからホスト IP アドレスに変換し、逆にアウトバウンドトラフィックのソース IP アドレスについては、ホスト IP アドレスから MIP アドレスに変換します。ポートマッピングは行いません。MIP について詳しくは、61 ページの「マップ IP アドレス」を参照してください。

仮想 IP

VIP 仮想インターネットプロトコル (VIP) では、宛先ポート番号をもとに、ある IP アドレスから別の IP アドレスへのマッピングを行います。同じサブネットに属するアドレスを 1 つ、インターフェース IP アドレスとして定義しておきます。これを使って、宛先ポート番号で区別される各種のサービスを、別々のホストに割り当てることができます。VIP はポートマッピングにも対応しています。MIP と異なり、VIP のアドレス変換は一方向です。セキュリティデバイスは、インバウンドトラフィックの宛先 IP アドレスはすべて VIP アドレスからホスト IP アドレスに変換します (宛先 IP アドレスが、Untrust ゾーンにバインドされたインターフェースに到着するパケットの VIP にバインドされているかだけをチェックします)。VIP ホストからその VIP アドレスに向かう、アウトバウンドトラフィックの本来のソース IP アドレスは変換されません。事前に設定していれば、

代わりにインターフェースベースまたはポリシーベースの NAT-src を適用します。そうでない場合は、VIP ホストを起点とするトラフィック上では NAT-src を実行しません。VIP について詳しくは 79 ページの「仮想 IP アドレス」を参照してください。

注 : セキュリティデバイスの機種によっては、インターフェース IP アドレスと同じ値を VIP アドレスとして定義することもできます。この機能は、セキュリティデバイスに割り当てられた IP アドレスが 1 つだけ、そして IP アドレスが動的に割り当てられる場合に便利です。

MIP や VIP の場合は、インバウンド、アウトバウンドの両方向でアドレス変換を行います。一方、ポリシーベースの NAT-src や NAT-dst では、インバウンドとアウトバウンドで独立にアドレス変換を施すようにして、細かい制御ができるようにすると同時に、安全性 (セキュリティ) の向上も図っています。たとえば Web サーバーに MIP を適用した場合、更新やパッチ取得のためサーバー側からアウトバウンドトラフィックを送出すると、情報が洩れて攻撃に悪用される恐れがあります。これに対し、ポリシーベースのアドレス変換ならば、Web サーバーに対するトラフィック (NAT-dst を適用) と、サーバー側から送出するトラフィック (NAT-src を適用) とで、別々のアドレスマッピングを定義できます。サーバー側の動作状況を隠蔽することにより、攻撃の準備段階としてさまざまな情報を収集されることのないよう防御する、という狙いがあるのです。最新の ScreenOS では、ポリシーベースの NAT-src、NAT-dst が強化され、インターフェースベースの MIP や VIP の機能を完全に包含しています。

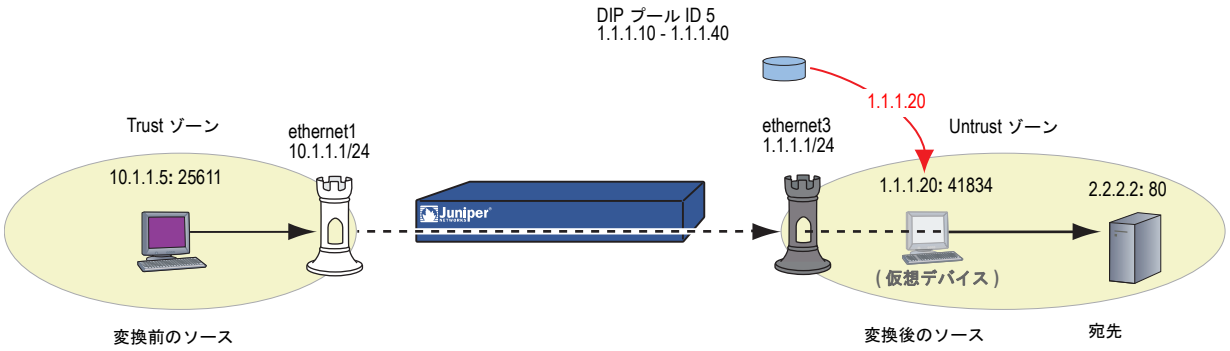
ポリシーベースの変換のさまざまな形態

ScreenOS は次の方法を用いて、ソースネットワークアドレス変換 (NAT-src) と宛先ネットワークアドレス変換 (NAT-dst) を適用しています。なお、NAT-src と NAT-dst の両方を適用するポリシーも設定可能です。

例 : NAT-Src - DIP プールからアドレス取得、PAT 機能あり

セキュリティデバイスは元のソース IP アドレスを動的 IP (DIP) プールから取得したアドレスに変換します。さらに、ソースポートアドレス変換 (PAT) も施します。詳細については、14 ページの「NAT-Src - DIP プールからアドレス取得、PAT 機能あり」を参照してください。

図 7: NAT-Src でポートアドレス変換

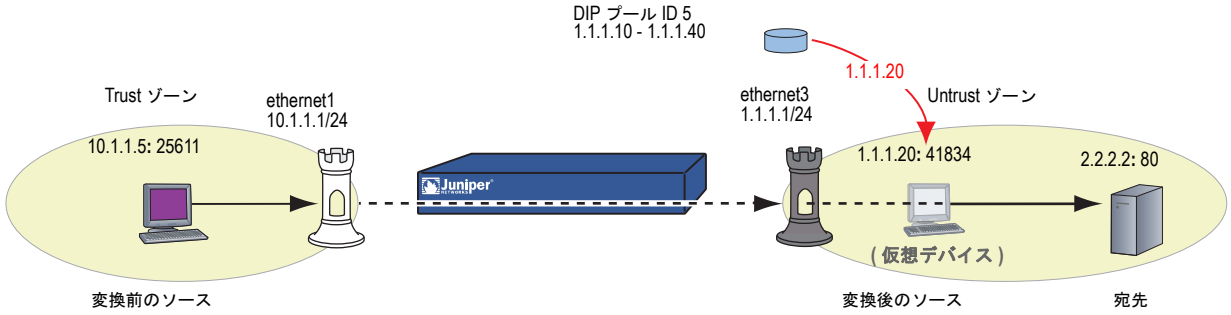


注： 図 7 およびこれ以降の図では、変換後のソースアドレスや宛先アドレスが実在のデバイスに割り当てられていない場合、「仮想デバイス」として表します。

例：NAT-Src - DIP プールからアドレス取得、PAT 機能あり

セキュリティデバイスは元のソース IP アドレスを DIP プールから取得したアドレスに変換します。PAT は施しません。詳細については、18 ページの「NAT-Src - DIP プールからアドレス取得、PAT 機能なし」を参照してください。

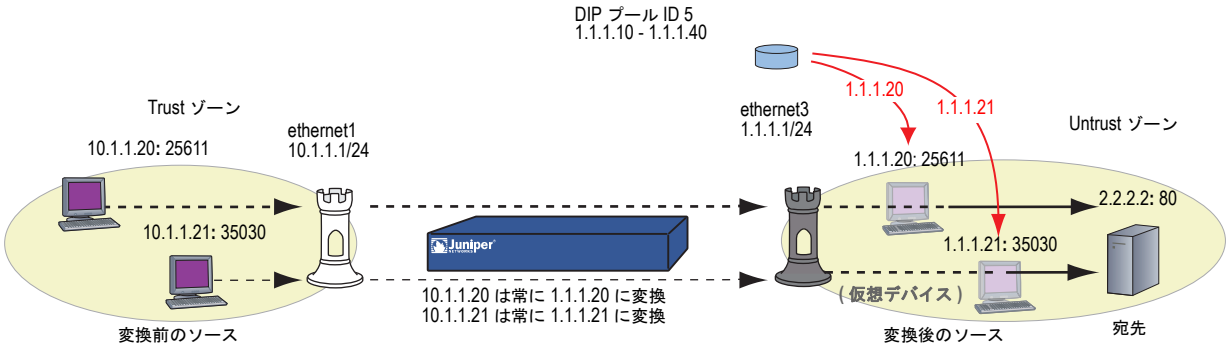
図 8: NAT-Src 、ポートアドレス変換なし



例：NAT-Src - DIP プールからアドレスシフティングによりアドレス取得

セキュリティデバイスは元のソースアドレスを動的 IP (DIP) プールから取得したアドレスに変換します。変換前のアドレスが同じならば、変換後のアドレスも常に同じです。ソースポートアドレス変換 (PAT) は施しません。詳細については、19 ページの「NAT-Src - DIP プールからアドレスシフティングによりアドレス取得」を参照してください。

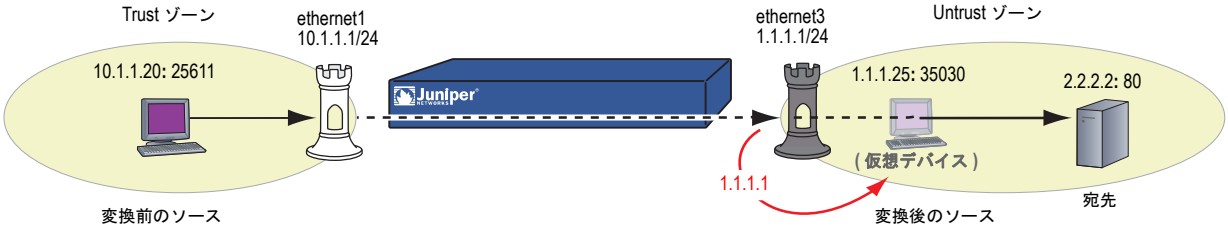
図 9: アドレスシフティングによる NAT-Src の設定



例 : NAT-Src - Egress インターフェース IP アドレスに変換

セキュリティデバイスは元のソース IP アドレスを egress インターフェースのアドレスに変換します。さらに、PAT も施します。詳細については、23 ページの「NAT-Src - Egress インターフェース IP アドレスに変換」を参照してください。

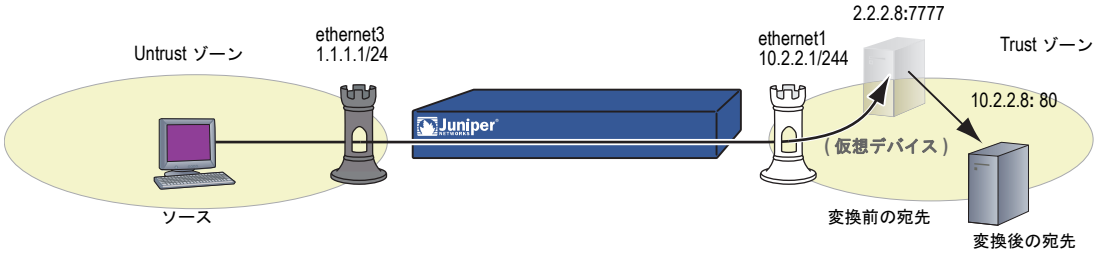
図 10: NAT-Src - Egress インターフェース IP アドレスを使用



例 : NAT-Dst を特定の IP アドレスに変換、ポートマッピングあり

セキュリティデバイスは宛先ネットワークアドレス変換 (NAT-dst) と宛先ポートマッピングを行います。詳細については、46 ページの「ポートマッピングを伴う NAT-Dst」を参照してください。

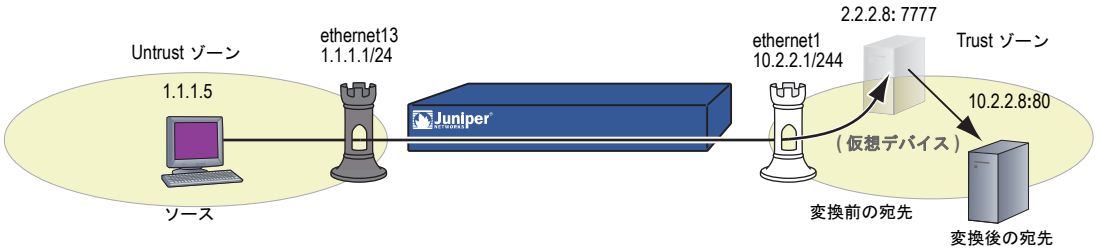
図 11: ポートマッピングを伴う NAT-Dst



例 : NAT-Dst を特定の IP アドレスに変換、ポートマッピングなし

セキュリティデバイスは NAT-dst を実行しますが、元の宛先ポート番号は変更しません。詳細については、27 ページの「宛先ネットワークアドレス変換」を参照してください。

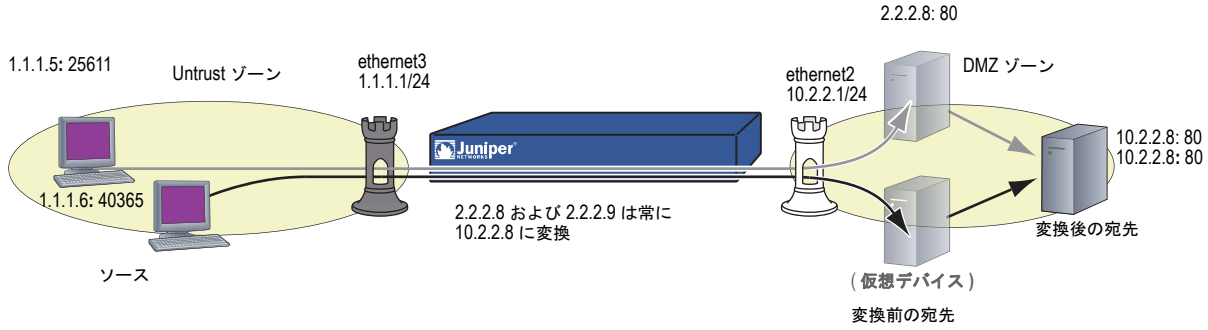
図 12: ポートマッピングを伴わない NAT-Dst



例 : 所定の IP アドレス範囲を特定の IP アドレスに変換した NAT-Dst

セキュリティデバイスは NAT-dst を実行し、所定の IP アドレス範囲を特定の IP アドレスに変換します。ポートマッピングも有効にした場合は、宛先ポート番号を別のナンバーに変換します。詳細については、40 ページの「NAT-Dst- 多対 1 のマッピング」を参照してください。

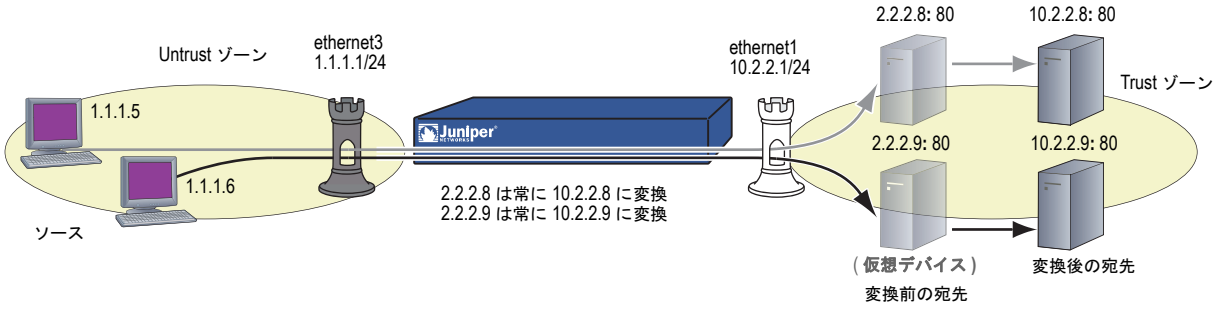
図 13: 所定の IP アドレス範囲を特定の IP アドレスに変換した NAT-Dst



例 : IP アドレス範囲間の NAT-Dst

NAT-dst では、ある範囲の宛先 IP アドレスを、アドレスシフティングという方法で、別の範囲の IP アドレスに変換します。変換前のアドレスが同じならば、変換後のアドレスも常に同じです。ただしポートマッピングには対応していません。詳細については、43 ページの「NAT-Dst- 多対多のマッピング」を参照してください。

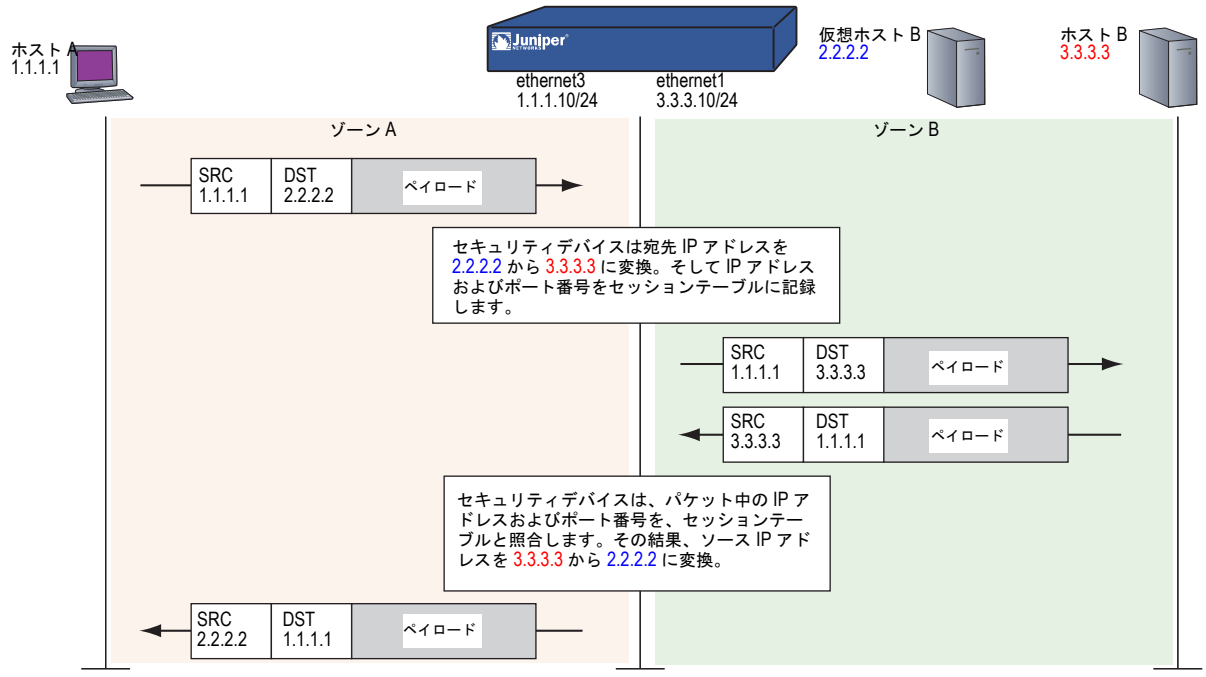
図 14: アドレス範囲間の NAT-Dst



NAT-Src と NAT-Dst の適用方向

NAT-src と NAT-dst は、独立に適用されます。トラフィックの向きに応じ、どちらを適用するか、ポリシーとして設定することができます。たとえば、ホスト A から仮想ホスト B へのトラフィックに対して NAT-dst を適用するよう設定すれば、変換前の宛先 IP アドレスがセキュリティデバイスで 2.2.2.2 から 3.3.3.3 に変換されます (逆にその応答トラフィックでは、ソース IP アドレスを 3.3.3.3 から 2.2.2.2 に変換します。)

図 15: NAT-Dst のパケットフロー

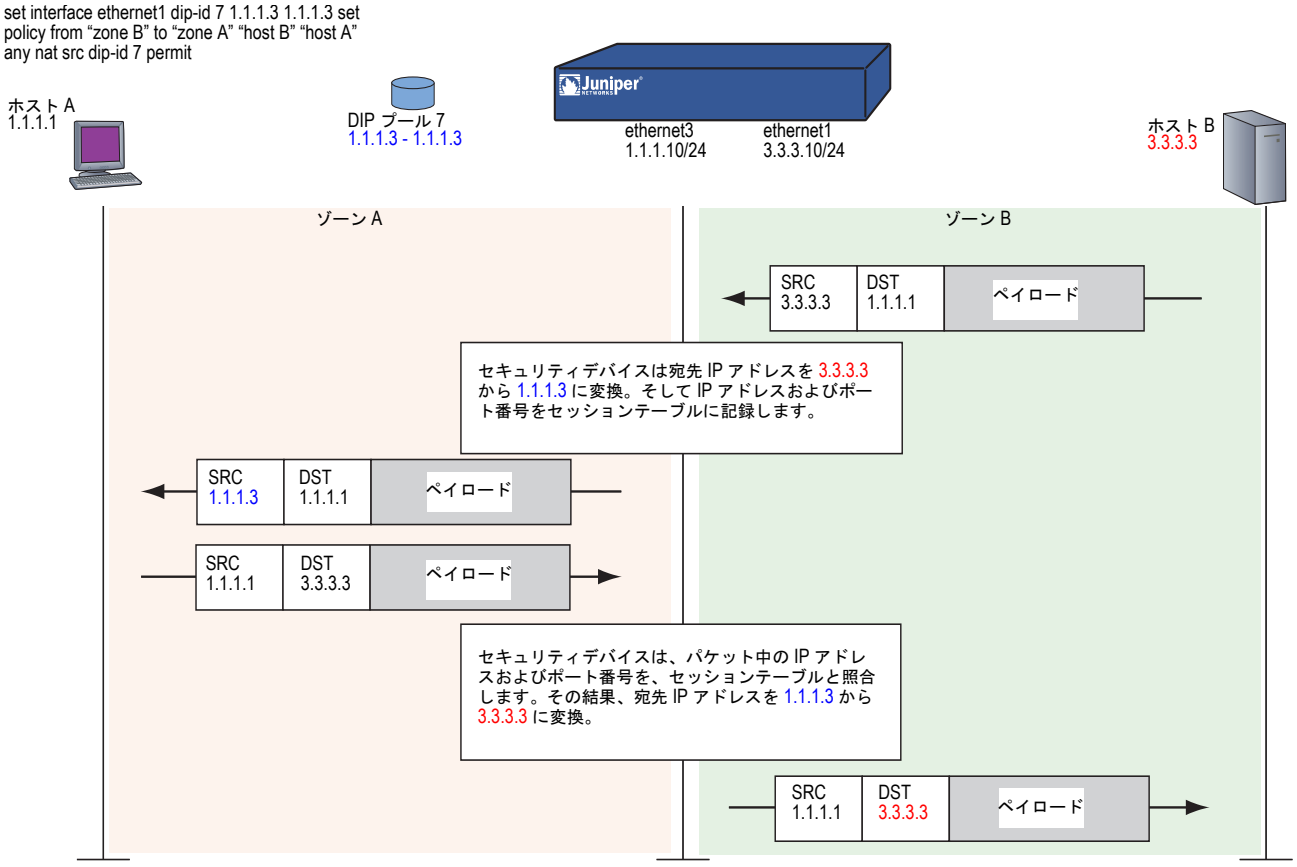


注 : 2.2.2.2/32 (仮想ホスト B) へのルートを設定して、セキュリティデバイスがこれを検索し、宛先ゾーンを判断できるようにしておく必要があります。NAT-dst におけるルーティングの問題について詳しくは、32 ページの「NAT-Dst のルーティング」を参照してください。

しかしながら、上記のようにホスト A からホスト B への NAT-dst を行うポリシーを設定しただけでは、ホスト B 側からホスト A に向かって送出した (ホスト A への応答ではない) トラフィックのソース IP アドレスは変換されません。このような変換も施すようにしたい場合は、別のポリシーとして、ホスト B からホスト A への NAT-src を設定する必要があります (これは MIP の場合とは異なります。61 ページの「マップ IP アドレス」を参照してください。)

注 : ここでは IP アドレス変換に着目するため、ポートアドレス変換 (PAT) については省略しています。DIP プールに IP アドレスが 1 つしかない場合、固定ポート番号を指定すれば、同時に 1 台のホストしかそのプールを使えないことになります。上記のポリシーではソースアドレスとして「ホスト B 」のみを指定しています。DIP プール 7 を使うホストがホスト B だけであれば、PAT を有効にする必要はありません。

図 16: ソース IP アドレス変換のパケットフロー



第 2 章

ソースネットワークアドレス変換

ScreenOS には、ソースネットワークアドレス変換 (NAT-src) とソースポートアドレス変換 (PAT) を実行する方式が、いくつも組み込まれています。本章ではさまざまなアドレス変換方式を、次の節に分けて解説します。

- 13 ページの「NAT-Src の概要」
- 14 ページの「NAT-Src - DIP プールからアドレス取得、PAT 機能あり」
- 18 ページの「NAT-Src - DIP プールからアドレス取得、PAT 機能なし」
- 19 ページの「NAT-Src - DIP プールからアドレスシフティングによりアドレス取得」
- 23 ページの「NAT-Src - Egress インターフェース IP アドレスに変換」

NAT-Src の概要

セキュリティデバイスで、IP パケットヘッダー中のソース IP アドレスを、別のアドレスに変換しなければならない場合があります。たとえば、プライベート IP アドレスを割り当てられたホストが、公開アドレス空間に向かってトラフィックを送出する場合、このプライベートアドレスを公開アドレスに変換しなければなりません。あるいは、プライベートアドレス空間から同じアドレス空間へのトラフィックが VPN を経由する場合も、両側のトンネル終端で、ソース IP アドレス、宛先 IP アドレスを変換する必要があります。

注 : 公開 IP アドレス、プライベート IP アドレスについて詳しくは、2-47 ページの「公開 IP アドレス」および 2-48 ページの「非公開 IP アドレス」を参照してください。

動的 (DIP) アドレスプールには、ソースネットワークアドレス変換 (NAT-src) の際、変換後のアドレスをセキュリティデバイスに供給する働きがあります。ある DIP プールを参照して NAT-src を施す、というポリシーが設定されていれば、セキュリティデバイスはアドレス変換にあたり、当該 DIP プールから変換先アドレスを取得します。

注： DIP プールは、ポリシーとして設定された宛先ゾーンのデフォルトインターフェースと、同じサブネットに属するアドレスを供給するものでなければなりません。宛先ゾーンインターフェースのサブネットに属さないアドレスを供給するようにしたい場合は、この DIP プールを拡張インターフェース上に定義する必要があります。詳細については、**2**-146 ページの「異なるサブネットでの DIP の使用」を参照してください。

DIP プールから常に同じ IP アドレスが供給されるという場合でも、ポートアドレス変換 (PAT) を有効にすれば、同時に 64,500 台までのホストに対応できます。すべてのパケットが DIP プールから受け取る新しいソース IP アドレスは毎回同じですが、ポート番号はその都度異なります。したがって、変換後の IP アドレスとポート番号を組にしてセッションテーブルで管理すれば、どのパケットがどのセッションに属し、どのセッションがどのホストに対するものであるか、を追跡できるのです。

注： ポートアドレス変換を有効にした場合、DIP プールから IP アドレスを取得するのと同様に、セキュリティデバイスは未使用ポート番号のプールも管理します。最大 64,500 とおりというのは、ポート番号の最大値である 65,535 から、「よく知られているサービス」用のポート (well-known ports) として予約された番号の最大値である 1,023 を引いた値です。

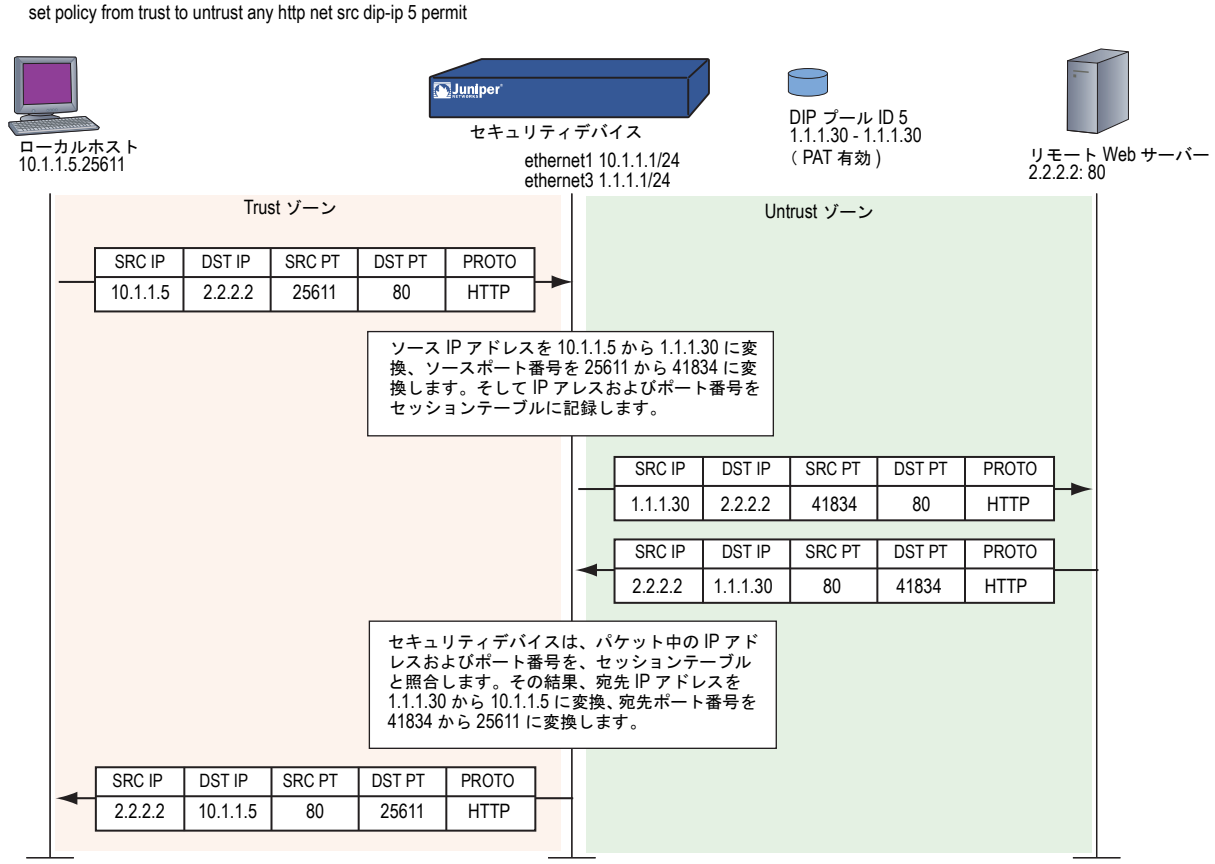
NAT-src を適用する設定であっても、DIP プールを指定しなければ、セキュリティデバイスはソース IP アドレスを、宛先ゾーンの egress インターフェースのアドレスに変換するようになります。この場合 PAT は必須であり、特に指定しなくても有効になります。

特定のソースポート番号を固定的に使うアプリケーションがある場合は、PAT を無効にしなければなりません。同時に稼動しうるホスト数以上の IP アドレスを供給できるよう、DIP プールを設定してください。ポート番号が固定なので、同じホスト上で並行して動作するセッションに対しても、すべて同じポート番号を割り当てることになります。一方、DIP プールで PAT を有効にした場合、同じホストに対し、並行しているセッションごとに別々のポート番号に変換することがありえます。ただし「スティッキー」DIP アドレス機能を有効にした場合を除きます (**2**-145 ページの「スティッキー DIP アドレス」を参照)。

NAT-Src - DIP プールからアドレス取得、PAT 機能あり

ソースネットワークアドレス変換 (NAT-src) で、ポートアドレス変換 (PAT) も有効にした場合、セキュリティデバイスは IP アドレスとポート番号を変換した上で、図 17 のようなパケット状態監視 (stateful inspection) を行います (IP パケットヘッダー、TCP セグメントヘッダーのうち、NAT-src に関係のあるものだけを示します)。

図 17: NAT-Src - DIP プールを使用、PAT 機能あり



例 : PAT を有効にした NAT-Src の設定

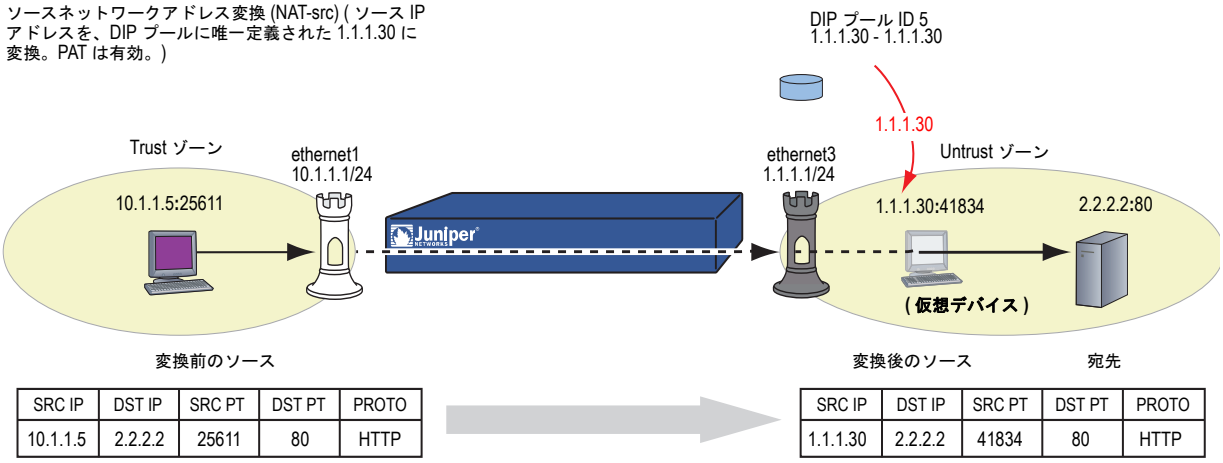
この例では、Untrust ゾーンに向かうインターフェースである ethernet3 に、DIP プール 5 を定義しています。この DIP プールには IP アドレスが 1.1.1.30 だけしかないため、自動的に PAT が有効になっています。

注 : DIP プールを定義すると、自動的に PAT も有効になります。無効にしたい場合は、CLI コマンドの末尾に fix-port と指定するか、WebUI の DIP 設定ページで、Port Translation オプションをオフにしてください。たとえば、**set interface ethernet3 dip 5 1.1.1.30 1.1.1.30 fix-port** または Network > Interfaces > Edit (ethernet3) > DIP: ID: 5; Start: 1.1.1.30; End: 1.1.1.30; Port Translation:（オフ）のように設定します。

ここで、セキュリティデバイスが次のような処理をするよう、ポリシーを設定します。

- Trust ゾーンの任意のアドレスから、Untrust ゾーンの任意のアドレスへの HTTP トラフィックを許可
- IP パケット中のソース IP アドレスは、DIP プール 5 に唯一存在する 1.1.1.30 に変換
- TCP セグメントヘッダーや UDP データグラムヘッダー中のソースポート番号は、一意的なポート番号を取得して変換
- ソース IP アドレスおよびポート番号を変換した HTTP トラフィックを、ethernet3 経由で Untrust ゾーンに転送

図 18: PAT を有効にした NAT-Src の設定



SRC IP	DST IP	SRC PT	DST PT	PROTO
10.1.1.5	2.2.2.2	25611	80	HTTP

SRC IP	DST IP	SRC PT	DST PT	PROTO
1.1.1.30	2.2.2.2	41834	80	HTTP

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24

   次のように選択してから **OK** をクリックします。

   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. DIP

Network > Interfaces > Edit (ethernet3) > DIP > New: 次のように入力してから **OK** をクリックします。

ID: 5
IP Address Range: (**選択**), 1.1.1.30 ～ 1.1.1.30
Port Translation: (**選択**)
In the same subnet as the interface IP or its secondary IPs: (**選択**)

3. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), Any
Service: HTTP
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: (**選択**)
(DIP on): 5 (1.1.1.30 - 1.1.1.30)/X-late

CLI

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. DIP

```
set interface ethernet3 dip 5 1.1.1.30 1.1.1.30
```

3. ポリシー

```
set policy from trust to untrust any any http nat src dip-id 5 permit
save
```

NAT-Src - DIP プールからアドレス取得、PAT 機能なし

設定や状況によっては、IP アドレスについてはソースネットワークアドレス変換 (NAT-src) を行うけれども、ソースポート番号のポートアドレス変換 (PAT) は行わないということがあります。例えばカスタムアプリケーションの場合、ソースポートアドレスに特定の番号が必要なことがあります。このような場合、セキュリティデバイスでは、PAT 機能なしの NAT-src を施す、というポリシーを設定します。

例 : PAT を無効にした NAT-Src の設定

この例では、Untrust ゾーンに向かうインターフェースである ethernet3 に、DIP プール 6 を定義しています。DIP プールには 1.1.1.50 ～ 1.1.1.150 の範囲の IP アドレスが用意されています。PAT は無効です。ここで、セキュリティデバイスが次のような処理をするよう、ポリシーを設定します。

- Trust ゾーンの任意のアドレスから、Untrust ゾーンの任意のアドレスへの、「 e-stock 」というユーザー定義サービスのトラフィックを許可。

注 : 財務サービス「 e-stock 」が定義済みであると想定します。このサービスは、e-stock トランザクションが特定のソースポート番号から要求されるものと想定しています。したがって DIP プール 6 の PAT は無効にしなければなりません。

- IP パケットヘッダー中のソース IP アドレスを、DIP プール 6 から取得したアドレスに変換。
- TCP セグメントヘッダー、UDP データグラムヘッダー中のソースポート番号は、元の値のまま。
- ソース IP アドレスを変換し、ポート番号は元のまま残した e-stock トラフィックを、ethernet3 経由で Untrust ゾーンに転送。

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように選択してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. DIP

Network > Interfaces > Edit (ethernet3) > DIP > New: 次のように入力してから **OK** をクリックします。

ID: 6
IP Address Range: (**選択**), 1.1.1.50 ～ 1.1.1.150
Port Translation:（**オフ**）
In the same subnet as the interface IP or its secondary IPs: (**選択**)

3. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), Any
Service: e-stock
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Source Translation: (**選択**)
DIP on: (**選択**), 6 (1.1.1.50 - 1.1.1.150)

CLI

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. DIP

```
set interface ethernet3 dip 6 1.1.1.50 1.1.1.150 fix-port
```

3. ポリシー

```
set policy from trust to untrust any any e-stock nat src dip-id 6 permit
save
```

NAT-Src - DIP プールからアドレスシフティングによりアドレス取得

所定の範囲のソース IP アドレスについて、変換後の IP アドレスと 1 対 1 の対応がつくように設定することができます。このようなマッピングを定義した場合、その範囲内であれば常に、同じソース IP アドレスは DIP プール内の同じアドレスに変換されることになります。この範囲の幅（アドレス数) も任意に設定できます。あるサブネット全体を別のサブネットにマップすることも可能です。サブネット内の各アドレスが、もう一方のサブネットに、1 対 1 で対応します。

このアドレスシフティングによる NAT-src を適用すると、あるサイトのセキュリティデバイスでアドレス変換されたトラフィックをもう一方のサイトで受け取る場合に、よりきめ細かなポリシー設定ができるようになります。たとえば、サイト A にあるデバイス A が、サイト間 VPN トンネルを介してサイト B にあるデバ

イス B と通信するとして、サイト A 内のホストのソースアドレスを変換するポリシーの定義を考えてみます。アドレスシフティングをしないとすれば、デバイス A 側では、DIP プールから取得したアドレスに変換することになるでしょう。この場合、デバイス B はサイト A から許可しているトラフィックに関して、汎用ポリシーしか設定できません。デバイス B の管理者が指定された変換後の IP アドレスを知らない限り、デバイス A DIP プールから取得したソースアドレスの範囲に対して、インバウンドポリシーしか設定できません。他方、デバイス B の管理者が（アドレスシフティングのため）変換後のソースアドレスを知っている場合、デバイス B の管理者はサイト A からのインバウンドトラフィックに対して設定するポリシーに、より制限を設けることができます。

具体的にどのような IP アドレスに変換されるのかは予測できないので、NetScreen-A の DIP プールに確保されている範囲のソースアドレス全体に関して、十把一絡げのポリシーを設定することしかできないのです。この場合、セキュリティデバイスはポリシーが許可しているすべてのソースアドレスからのトラフィックを通過させ、DIP 範囲内のアドレスにアドレスシフティングを有効にした NAT-src を適用します。しかしながら、DIP プール範囲外のアドレスに関しては、これを適用しません。常に NAT-src が適用されるようにしたい場合は、ソースアドレスの取りうる範囲が、DIP プールの範囲以下になるようにしてください。

注： アドレスシフティングとソースポートアドレス変換 (PAT) を同時に適用することはできません。

例：アドレスシフティングによる NAT-Src の設定

この例では、Untrust ゾーンに向かうインターフェースである ethernet3 に、DIP プール 10 を定義しています。10.1.1.11 ～ 10.1.1.15 の 5 つのアドレスを 1.1.1.101 ～ 1.1.1.105 に変換し、変換前と変換後のアドレスの関係も維持したいとします。

表 1: アドレスシフティングによる NAT-Src の設定

変換前のソース IP アドレス	変換後のソース IP アドレス
10.1.1.11	1.1.1.101
10.1.1.12	1.1.1.102
10.1.1.13	1.1.1.103
10.1.1.14	1.1.1.104
10.1.1.15	1.1.1.105

Trust ゾーンにある 5 台のホストのアドレスを定義し、これを「 group1 」というアドレスグループに追加します。このアドレスを、10.1.1.11、10.1.1.12、10.1.1.13、10.1.1.14、10.1.1.15 としましょう。Trust ゾーンから Untrust ゾーンへのトラフィックに適用するポリシーを、「DIP プール 10 を使って、上記アドレスグループに NAT-src を施す」と設定してみます。group1 に属するホストから Untrust ゾーンのアドレスに宛てて HTTP トラフィックを送る場合、セキュリティデバイスは NAT-src を適用することになります。さらに、この NAT-src では、たとえば 10.1.1.13 は常に 1.1.1.103 に変換されるというように、アドレスの対応は常に一定です。

ここで、セキュリティデバイスが次のような処理をするよう、ポリシーを設定します。

- Trust ゾーンの group1 に属するアドレスから、Untrust ゾーンの任意のアドレスへの HTTP トラフィックを許可。
- IP パケットヘッダー中のソース IP アドレスを、DIP プール 10 から取得した、対応するアドレスに変換。
- ソース IP アドレスおよびポート番号を変換した HTTP トラフィックを、ethernet3 経由で Untrust ゾーンに転送。

WebUI

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24
次のように選択してから **OK** をクリックします。
Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

2. DIP

Network > Interfaces > Edit (ethernet3) > DIP > New: 次のように入力してから **OK** をクリックします。

ID: 10
IP Shift: (選択)
From: 10.1.1.11
To: 1.1.1.101 ~ 1.1.1.105
In the same subnet as the interface IP or its secondary IPs: (選択)

3. アドレス

Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

Address Name: host1
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.11/32
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

Address Name: host2
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.12/32
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

Address Name: host3
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.13/32
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

Address Name: host4
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.14/32
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

Address Name: host5
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.15/32
Zone: Trust

Policy > Policy Elements > Addresses > Group > (Zone: Trust) New: 以下のグループ名を入力して、以下のアドレスを移動し、**OK** をクリックします。

Group Name: group1

host1 を選択し、< < ボタンを使用して Available Members 列から Group Members 列にアドレスを移動します。

host2 を選択し、< < ボタンを使用して Available Members 列から Group Members 列にアドレスを移動します。

host3 を選択し、< < ボタンを使用して Available Members 列から Group Members 列にアドレスを移動します。

host4 を選択し、< < ボタンを使用して Available Members 列から Group Members 列にアドレスを移動します。

host5 を選択し、< < ボタンを使用して Available Members 列から Group Members 列にアドレスを移動します。

4. **ポリシー**

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), group1
Destination Address:
Address Book Entry: (選択), Any
Service: HTTP
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

```
NAT:
  Source Translation: ( 選択 )
  (DIP on): 10 (1.1.1.101 - 1.1.1.105)
```

CLI

1. **インターフェース**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. **DIP**

```
set interface ethernet3 dip 10 shift-from 10.1.1.11 to 1.1.1.101 1.1.1.105
```

3. **アドレス**

```
set address trust host1 10.1.1.11/32
set address trust host2 10.1.1.12/32
set address trust host3 10.1.1.13/32
set address trust host4 10.1.1.14/32
set address trust host5 10.1.1.15/32

set group address trust group1 add host1
set group address trust group1 add host2
set group address trust group1 add host3
set group address trust group1 add host4
set group address trust group1 add host5
```

4. **ポリシー**

```
set policy from trust to untrust group1 any http nat src dip-id 10 permit
save
```

NAT-Src - Egress インターフェース IP アドレスに変換

ポリシーとして NAT-src を指定しても、DIP プールを指定しなかった場合、セキュリティデバイスは、ソース IP アドレスを egress インターフェースの IP アドレスに変換するようになります。この場合は常に PAT が適用されます。

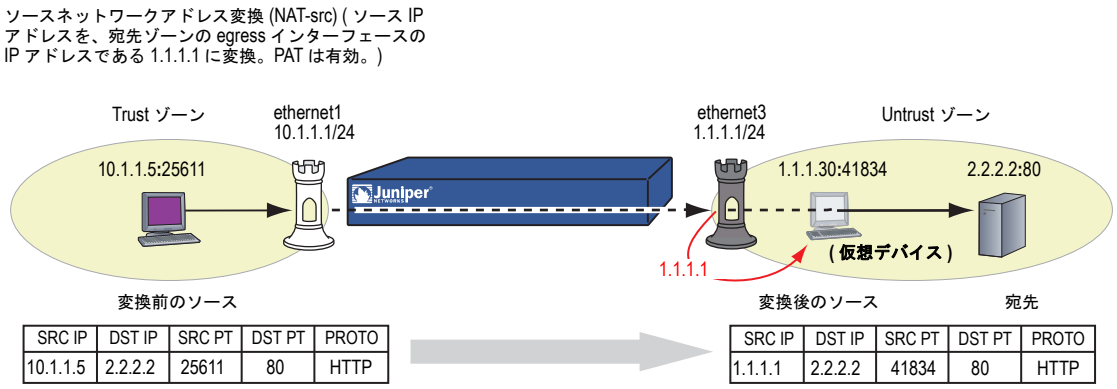
例 : DIP プールを使わない NAT-Src の設定

ここでは、セキュリティデバイスが次のような処理をするよう、ポリシーを設定します。

- Trust ゾーンの任意のアドレスから、Untrust ゾーンの任意のアドレスへの HTTP トラフィックを許可。
- IP パケットヘッダー中のソース IP アドレスを 1.1.1.1 に変換。これは Untrust ゾーンに向かうインターフェースである ethernet3 の IP アドレスであり、したがって Untrust ゾーン内のアドレスを宛先とするトラフィックがすべて通過する、egress インターフェースの IP アドレスでもあります。

- TCP セグメントヘッダーや UDP データグラムヘッダー中のソースポート番号は、一意的なポート番号を取得して変換。
- ソース IP アドレスおよびポート番号を変換したトラフィックを、ethernet3 経由で Untrust ゾーンに転送。

図 19: DIP プールを使わない NAT-Src の設定



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように選択してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. **ポリシー**
   Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Any
   Destination Address:
   Address Book Entry: (選択), Any
   Service: HTTP
   Action: Permit

   > Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

   NAT:
   Source Translation: (選択)
   (DIP on): None (Use Egress Interface IP)

CLI

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **ポリシー**
   set policy from trust to untrust any any http nat src permit
   save

第 3 章

宛先ネットワークアドレス変換

ScreenOS には、宛先ネットワークアドレス (NAT-dst) 変換と宛先ポートアドレスをマッピングする方式が、いくつも組み込まれています。本章では、さまざまなアドレス変換方式について、次の節に分けて解説します。

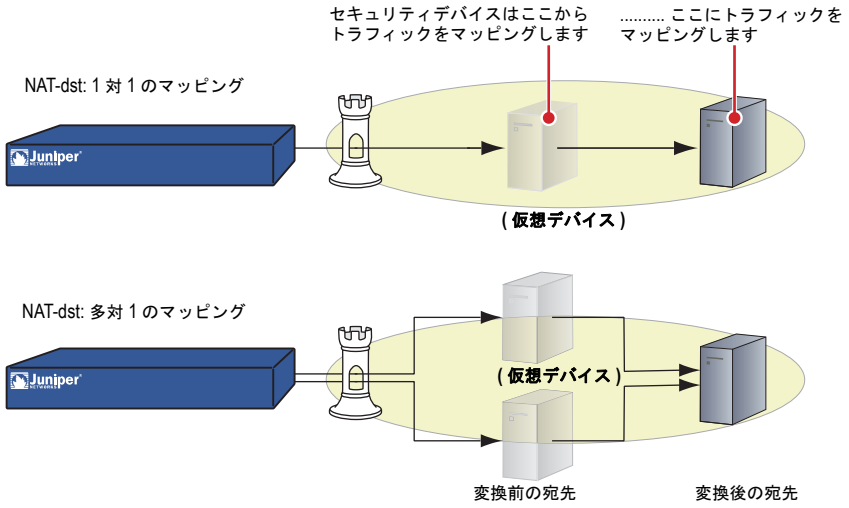
- 28 ページの「NAT-Dst の概要」
  - 29 ページの「NAT-Dst のパケットフロー」
  - 32 ページの「NAT-Dst のルーティング」
- 35 ページの「NAT-Dst-1 対 1 のマッピング」
  - 38 ページの「単一のアドレスから複数のアドレスへの変換」
- 40 ページの「NAT-Dst- 多対 1 のマッピング」
- 43 ページの「NAT-Dst- 多対多のマッピング」
- 46 ページの「ポートマッピングを伴う NAT-Dst」
- 49 ページの「1 つのポリシーで NAT-Src と NAT-Dst を適用」

注 : マップ IP (MIP) または仮想 IP (VIP) アドレスを使用した宛先アドレス変換の詳細については、61 ページの「マップアドレスと仮想アドレス」を参照してください。

NAT-Dst の概要

宛先アドレスについても、ある IP アドレスから別の IP アドレスに変換する、というポリシーを定義することができます。通常必要になるのは、公開 IP アドレスからプライベート IP アドレスへの変換でしょう。変換前アドレスと変換後アドレスとの対応には、1 対 1 、多対 1 、多対多の関係がありえます。図 20 は 1 対 1 、多対 1 の NAT-dst 関係の概念を示します。

図 20: NAT-Dst: 1 対 1 および多対 1 のマッピング

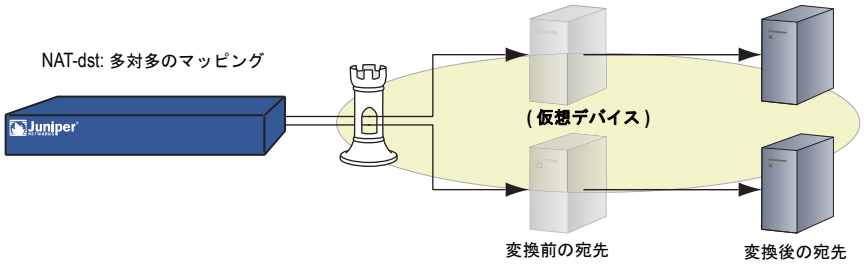


注 : 変換前、変換後とも、宛先 IP アドレスは同じセキュリティゾーンに属するものでなければなりません。

図 20 に示されているいずれの場合も、宛先ポートマッピングが可能です。ポートマッピングとは、ある宛先ポート番号から特定のポート番号への変換で、その対応関係は予測可能 (決定性) です。この関係は、ポートアドレス変換 (PAT) の対応とは異なります。ポートマッピングの場合、変換前と変換後のポート番号の対応関係はあらかじめ決まっています。一方 PAT では、ランダムに割り当てられたソースポート番号を、別のランダムに決まるポート番号に変換します。

覧所定の範囲の宛先アドレスを別の範囲のアドレスに (たとえばあるサブネットを別のサブネットに)、アドレスシフティングという方法で変換することができます。この場合セキュリティデバイスは、変換前宛先アドレスが同じならば、常に同じアドレスに変換します。セキュリティはアドレスシフティングを利用しているポートマッピングをサポートしていません。図 21 は NAT-dst の多対多関係の概念を示します。

図 21: NAT-Dst-: 多対多



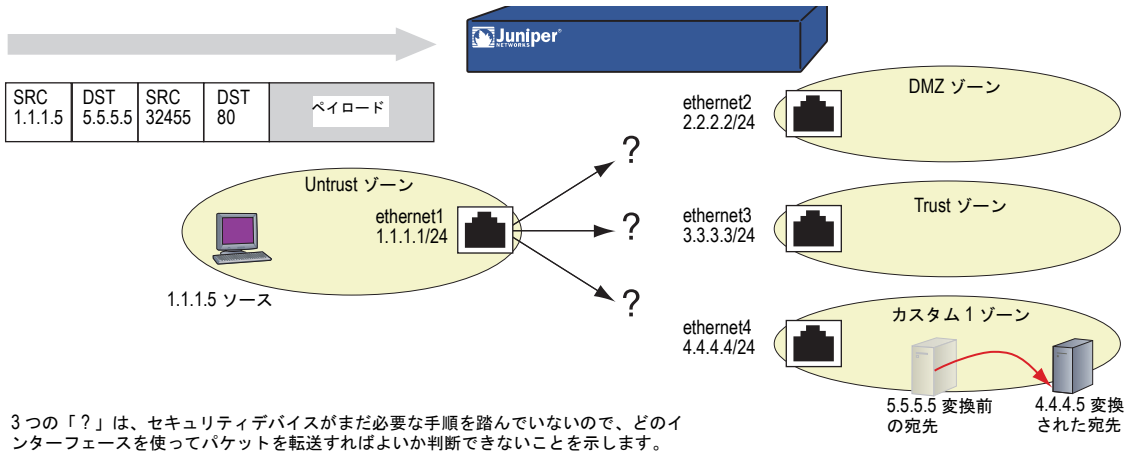
変換前、変換後とも、宛先 IP アドレスはルートテーブルに載っているものでなければなりません。セキュリティデバイスは、変換前の宛先 IP アドレスをもとにルートテーブルを検索して宛先ゾーンを求め、さらにこれを基準として、どのポリシーを適用するかを判定します。次に変換後のアドレスをもとにルートテーブルを検索し、パケットの送り先を決定します。ポリシーに沿ってルーティングを制御できるよう、変換前、変換後とも、宛先 IP アドレスは同じセキュリティゾーンに属するものでなければなりません (宛先 IP アドレス、ルート検索、ポリシー検索の関係については、29 ページの「NAT-Dst のパケットフロー」を参照してください)。

NAT-Dst のパケットフロー

セキュリティデバイスを経由するパケットの流れと、NAT-dst を施す細かな手順を以下に示します。

1. HTTP パケットが ethernet1 に届きました。ソース IP アドレスはポート番号 1.1.1.5:32455、宛先 IP アドレスはポート番号は 5.5.5.5:80 で、Untrust ゾーンにバインドされているパケットです。

図 22: NAT-Dst パケットの流れ - パケットの到着



3 つの「?」は、セキュリティデバイスがまだ必要な手順を踏んでいないので、どのインターフェースを使ってパケットを転送すればよいか判断できないことを示します。

2. Untrust ゾーンに対して SCREEN オプションが有効になっていれば、セキュリティデバイスはこの時点で SCREEN モジュールをアクティブにします。SCREEN モジュールによるチェックの結果は、次の 3 つのうちいずれかになります。

- SCREEN 機構が異常な動きを検出し、パケットを拒否する場合、NetScreen デバイスはパケットを破棄し、イベントログにその旨を記録します。
- SCREEN 機構が異常な動きを検出し、イベントを記録するように構成されていてもパケットをブロックするようには構成されていない場合、セキュリティデバイスはイベントを ingress インターフェースの SCREEN カウンタリストに記録し、次の手順に進みます。
- SCREEN 機構が異常な動きを検出しない場合、セキュリティデバイスはそのまま次の段階に進みます。

Untrust ゾーンに対して SCREEN オプションを何も有効にしていなかった場合は、セキュリティデバイスは何もせずに次に進みます。

3. セッションモジュールは、パケットを既存のセッションと一致させるためセッションルックアップを実行します。

   パケットが既存のセッションと一致しない場合は、先頭パケットに対し、以下のような処理を行います。

   逆に該当するセッションが見つかれば、既存のセッションエントリの情報を参照して、パケットを高速処理します。高速処理の場合、最後の手順まで飛ばします。このセッションの先頭パケットを処理した段階で必要な情報は得られているので、省略しても構わないのです。

4. アドレスマッピングモジュールが、マップ IP (MIP) または仮想 IP (VIP) の設定で宛先 IP アドレス 5.5.5.5 が使われていないかどうかを確認します。

注： Untrust ゾーンにバインドされたインターフェースに到着する場合に限り、宛先 IP アドレスが VIP 設定で使用されているかどうかをチェックします。

   使われていれば、MIP または VIP により変換後の宛先 IP アドレスを求め、これをもとにルートを検索します。次に Untrust ゾーン、Global ゾーンについてポリシーを検索します。トラフィックを許可する旨のポリシーに合致すれば、ルート検索により見つかった egress インターフェースを経由してパケットを転送します。

   5.5.5.5 が MIP でも VIP でも使われていなければ次に進みます。

5. 宛先ゾーンを求めるため、ルートモジュールは変換前の宛先 IP アドレスをもとにルートテーブルを検索します。つまり ethernet1 に到着したパケットのヘッダーに示されている IP 宛先アドレスを使います。(ルートモジュールは ingress インターフェースを使って、ルートルックアップにどの仮想ルーターを使うか判断します。) この例では、5.5.5.5/32 が ethernet4 経由で Custom1 ゾーンに向かうルートであることがわかりました。

trust-vr ルートテーブル			
アクセス先 :	**使用するインターフェース :**	**ゾーン :**	**使用するゲートウェイ :**
0.0.0.0/0	ethernet1	Untrust	1.1.1.250
1.1.1.0/24	ethernet1	Untrust	0.0.0.0
2.2.2.0/24	ethernet2	DMZ	0.0.0.0
3.3.3.0/24	ethernet3	Trust	0.0.0.0
4.4.4.0/24	ethernet4	Custom1	0.0.0.0
5.5.5.5/32	**ethernet4**	Custom1	**0.0.0.0**

6. ポリシーエンジンは、(対応する ingress、egress インターフェースで求められた) Untrust ゾーン、Custom1 ゾーンについて、条件に合致するポリシーを検索します。ソース IP アドレス、宛先 IP アドレスおよびサービスは、HTTP トラフィックを 5.5.5.5 から 4.4.4.5 にリダイレクトするポリシーと一致します。

   set policy from untrust to custom1 any v-server1 http nat dst ip 4.4.4.5 permit

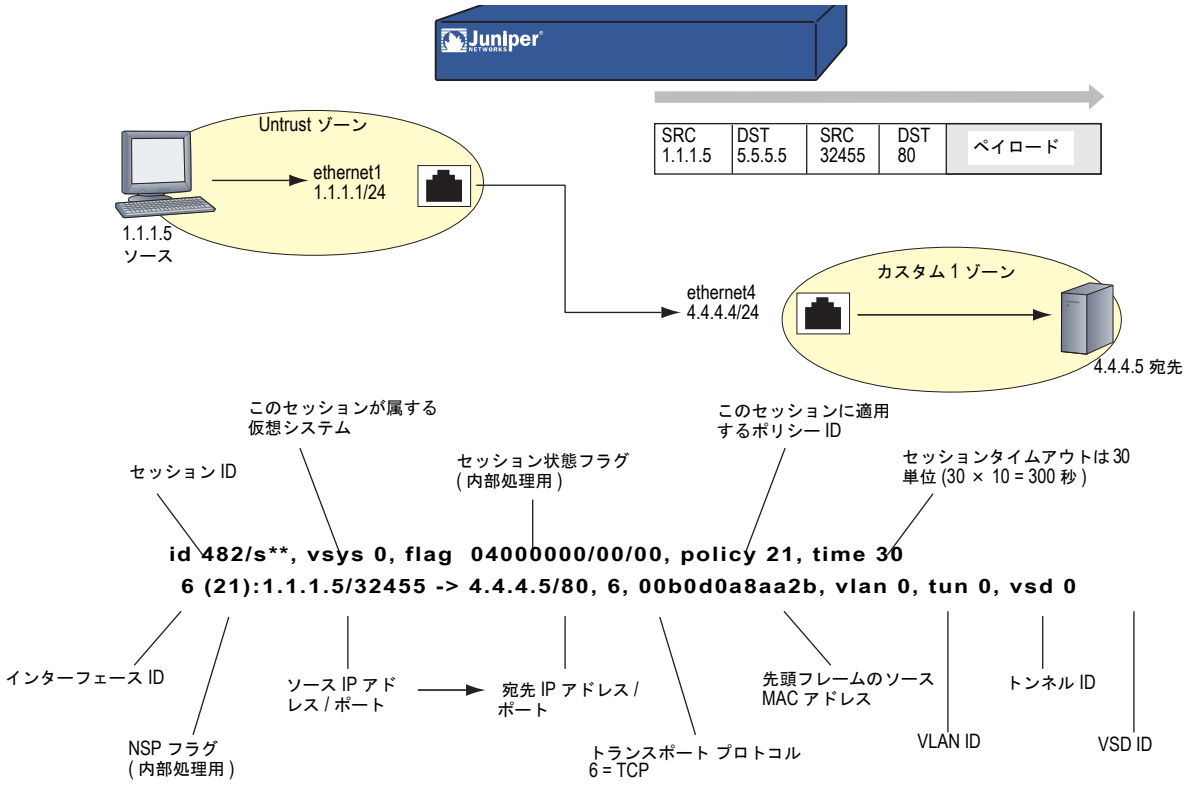
   (ここでアドレス「v-server1」は、IP アドレス 5.5.5.5/32 のことであるとあらかじめ定義されているとします。これは Custom1 ゾーンに属します。)

   セキュリティデバイスは宛先 IP アドレスを 5.5.5.5 から 4.4.4.5 に変換します。ポリシーは NAT-src と PAT-dst のいずれも必要でないことを示しています。

7. セキュリティデバイスは変換後の IP アドレスについてもう一度ルートテーブルを検索し、4.4.4.5/32 へは ethernet4 経由で到達できることを認識します。

8. アドレスマッピングモジュールは、パケットヘッダー中の宛先 IP アドレスを 4.4.4.5 に変換します。セキュリティデバイスはこのパケットを ethernet4 経由で送出し、セッションテーブルに記録します (ただし既存のセッションに属するパケットの場合は記録済みなので不要)。

図 23: NAT-Dst パケットの流れ - パケットの転送



注: このセッションは仮想システム、VLAN、VPN トンネル、仮想セキュリティデバイス (VSD) のいずれも加わっていないので、当該 ID はすべて 0 になっています。

NAT-Dst のルーティング

NAT-dst に使うアドレスを設定する際は、セキュリティデバイスのルーティングテーブルに、パケットヘッダーに現れる変換前の宛先アドレスと、変換後のアドレス (すなわち当該パケットのリダイレクト先) の、両方のルートが設定されている必要があります。29 ページの「NAT-Dst のパケットフロー」でも説明したように、セキュリティデバイスは変換前のアドレスをもとにルートを検索し、どの egress インターフェースを使うか判断します。覧すると egress インターフェースの先にある宛先ゾーンがわかるので、セキュリティデバイスはこれをもとに、どのポリシーを適用するか検索する、というわけです。条件に合致するポリシーが見つかると、そこには宛先アドレスをどのように変換するかが定義されています。セキュリティデバイスはもう一度ルーティングテーブルを検索して、新しい宛先アドレスに到達するためにはどのインターフェースにパケットを転送すればよいか、を判断します。以上のように、元の宛先アドレスへのルートはポリシーの検索方法を提供し、新しい宛先アドレスへのルートはセキュリティデバイスがパケットを転送する egress インターフェースを指定します。

以下に解説する 3 とおりの設定例では、ポリシーに記載された宛先アドレスまわりのネットワークトポロジーに応じて、静的ルートの設定が必要かどうかが異なります。

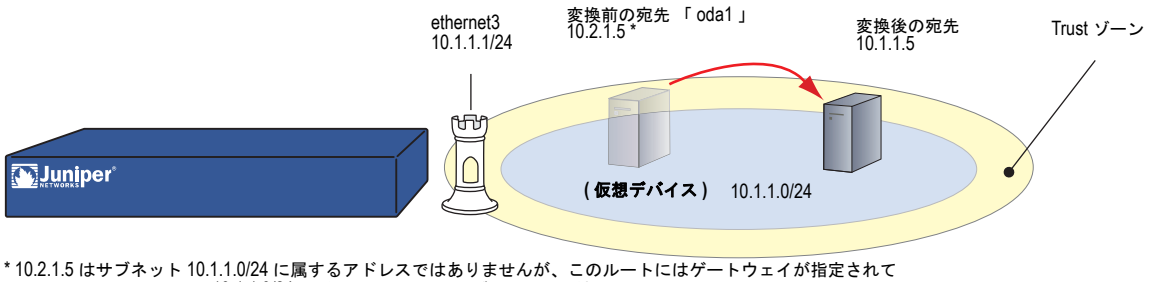
set policy from untrust to trust any oda1 http nat dst ip 10.1.1.5 permit

ここで「oda1」は変換前の宛先アドレス 10.2.1.5 を表します。また、変換後の宛先アドレスは 10.1.1.5 となります。

例 : 同じインターフェースに接続されたアドレス

この例では、変換前および変換後の宛先アドレスはどちらも、同じ ethernet3 というインターフェースを経由するようになっています。ethernet3 インターフェースのアドレスを 10.1.1.1/24 と設定すると、セキュリティデバイスには、ethernet3 を通って 10.1.1.0/24 に到達するルートも自動的に追加されたことになります。ルーティングが可能になるよう、ethernet3 を通って 10.2.1.5/32 に到達するルートも追加設定しなければなりません。

図 24: 同じ Egress インターフェースを使用した変換前および変換後のアドレス



* 10.2.1.5 はサブネット 10.1.1.0/24 に属するアドレスではありませんが、このルートにはゲートウェイが指定されていないので、図の上では、10.1.1.0/24 アドレス空間と同じサブネットに接続されているように表しています。

WebUI

Network > Routing > Destination > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.2.1.5/32
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 0.0.0.0

CLI

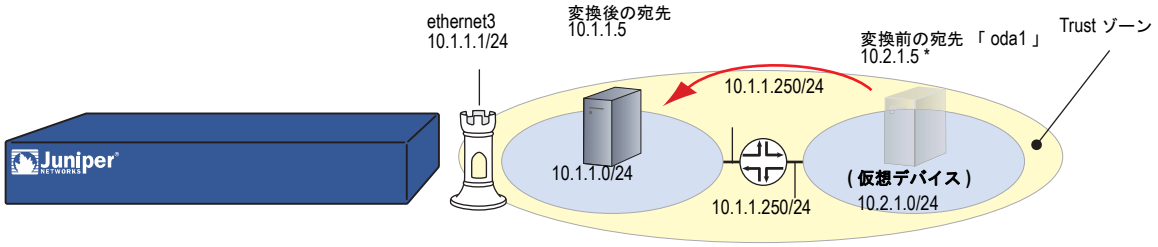
```
set vrouter trust-vr route 10.2.1.5/32 interface ethernet3
save
```

例 : 同じインターフェースに接続されているが、ルーターにより分離されたアドレス

この例でもやはり変換前および変換後の宛先アドレスはどちらも、同じ ethernet3 というインターフェースを通って到達できます。ethernet3 インターフェースのアドレスを 10.1.1.1/24 と設定すると、セキュリティデバイスには、ethernet3 を通って 10.1.1.0/24 に到達するルートも自動的に追加されたことになります。ルーティングが可能になるよう、ethernet3 を通って 10.2.1.0/24 に到達するルート、サブネット 10.1.1.0/24 および 10.2.1.0/24 を中継するゲートウェイも追加設定しなければなりません。

注： このルートはサブネット 10.2.1.0/24 に属するどのアドレスにも到達できる必要があるので、既に設定済みかも知れません。その場合は、改めてルートを追加しなくてもポリシーは、10.2.1.5 に変換する NAT-dst を適用できます。

図 25: ルーターにより分離された変換前および変換後のアドレス



WebUI

Network > Routing > Destination > (trust-vr) New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.2.1.0/24
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 10.1.1.250

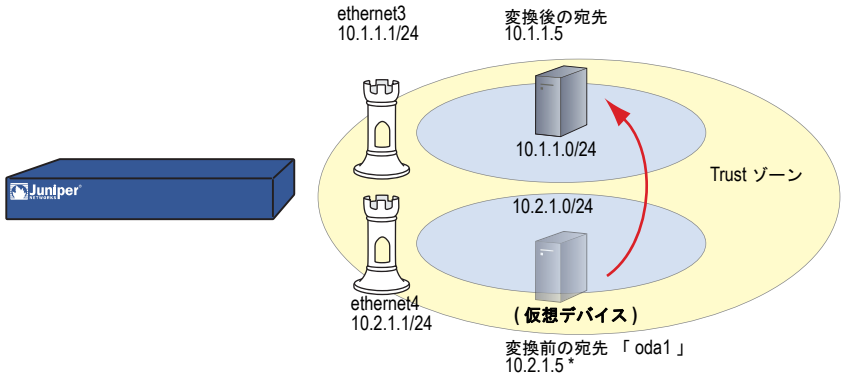
CLI

```
set vrouter trust-vr route 10.2.1.0/24 interface ethernet3 gateway 10.1.1.250
save
```

例：別々のインターフェースに接続されたアドレス

この例では Trust ゾーンに向かうインターフェースが 2 つあります。すなわち、ethernet3 (IP アドレスは 10.1.1.1/24) と ethernet4 (IP アドレスは 10.2.1.1/24) です。このインターフェースの IP アドレスをそれぞれ設定すれば、セキュリティデバイスには、ethernet3 を通って 10.1.1.0/24 に到達するルート、ethernet4 を通って 10.2.1.0/24 に到達するルートも自動的に追加されたことになります。変換前のアドレスをサブネット 10.2.1.0/24、変換後のアドレスをサブネット 10.1.1.0/24 に配置すれば、これ以外にはルートを追加することなく、たとえば 10.1.1.5 から 10.2.1.5 に変換する NAT-dst を適用することができます。

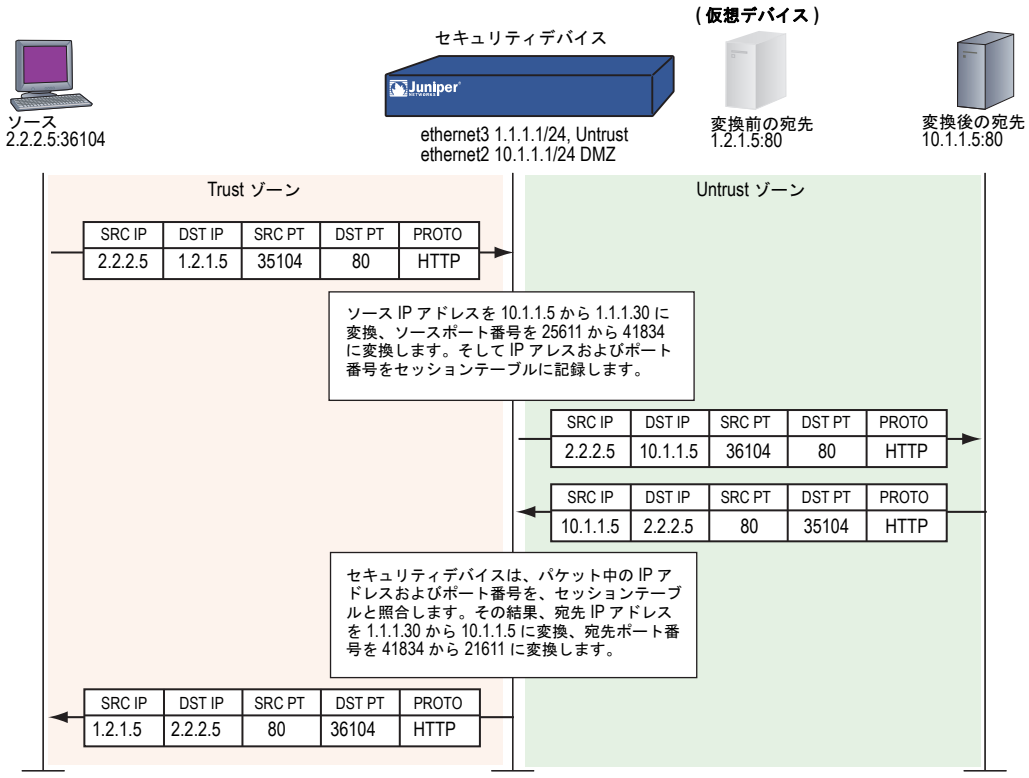
図 26: 異なる Egress インターフェースを使用した変換前および変換後のアドレス



NAT-Dst-1 対 1 のマッピング

宛先ネットワークアドレス変換 (NAT-dst) で、ポートアドレス変換 (PAT) を無効にした場合、セキュリティデバイスは宛先 IP アドレスを変換した上で、図 27 のようなパケット状態監視 (stateful inspection) を行います (IP パケットヘッダー、TCP セグメントヘッダーのうち、NAT-dst に関係のあるものだけを示します)。

図 27: NAT-Dst 1 対 1



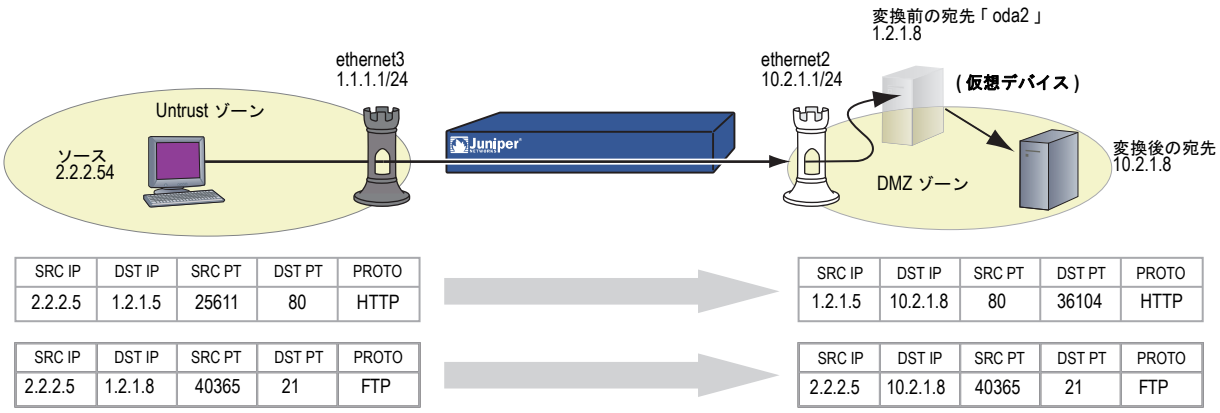
例 : 1 対 1 の宛先アドレス変換

この例では、1 対 1 の宛先ネットワークアドレス変換 (NAT-dst) を施す、というポリシーを設定します。宛先ポートアドレスは変更しません。次のような処理を行うポリシーです。

- Untrust ゾーン内の任意のアドレスから、「 oda2 」という変換前の宛先アドレスに向かう、FTP および HTTP のトラフィック (サービスグループ 「 http-ftp 」として定義) を許可。「 oda2 」のアドレスは 1.2.1.8 で、これは DMZ ゾーンにあります。
- IP パケットヘッダー中の宛先 IP アドレスを 1.2.1.8 から 10.2.1.8 に変換。
- TCP セグメントヘッダー中の宛先ポート番号は元のまま (HTTP ならば 80、FTP ならば 21)
- HTTP および FTP トラフィックを、DMZ ゾーンにある 10.2.1.8 に転送。

ethernet3 を Untrust ゾーンにバインドし、1.1.1.1/24 という IP アドレスを割り当てます。同様に、ethernet2 を DMZ ゾーンにバインドし、10.2.1.1/24 という IP アドレスを割り当てます。また、元の宛先アドレスである 1.2.1.8 へのルートを ethernet2 経由で定義します。Untrust ゾーン、DMZ ゾーンはともに、trust-vr ルーティングドメインに属します。

図 28: NAT-Dst - 1 対 1



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

   Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

   Zone Name: DMZ
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.2.1.1/24

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

   Address Name: oda2
   IP Address/Domain Name:
   IP/Netmask: (選択), 1.2.1.8/32
   Zone: DMZ

3. **サービスグループ**
   Policy > Policy Elements > Services > Groups: 以下のグループ名を入力して、以下のサービスを移動し、**OK** をクリックします。

   Group Name: HTTP-FTP

   HTTP を選択し、< < ボタンを使って Available Members 列から Group Members 列にサービスを移動します。

FTP を選択し、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

4. **ルート**
   Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 1.2.1.8/32
   Gateway: (**選択**)
   Interface: ethernet2
   Gateway IP Address: 0.0.0.0

5. **ポリシー**
   Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), Any
   Destination Address:
   Address Book Entry: (**選択**), oda2
   Service: HTTP-FTP
   Action: Permit

   > Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

   NAT:
   Destination Translation: (**選択**)
   Translate to IP: (**選択**), 10.2.1.8
   Map to Port:（**オフ**）

CLI

1. **インターフェース**
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24
   set interface ethernet2 zone dmz
   set interface ethernet2 ip 10.2.1.1/24

2. **アドレス**
   set address dmz oda2 1.2.1.8/32

3. **サービスグループ**
   set group service http-ftp
   set group service http-ftp add http
   set group service http-ftp add ftp

4. **ルート**
   set vrouter trust-vr route 1.2.1.8/32 interface ethernet2

5. **ポリシー**
   set policy from untrust to dmz any oda2 http-ftp nat dst ip 10.2.1.8 permit
   save

単一のアドレスから複数のアドレスへの変換

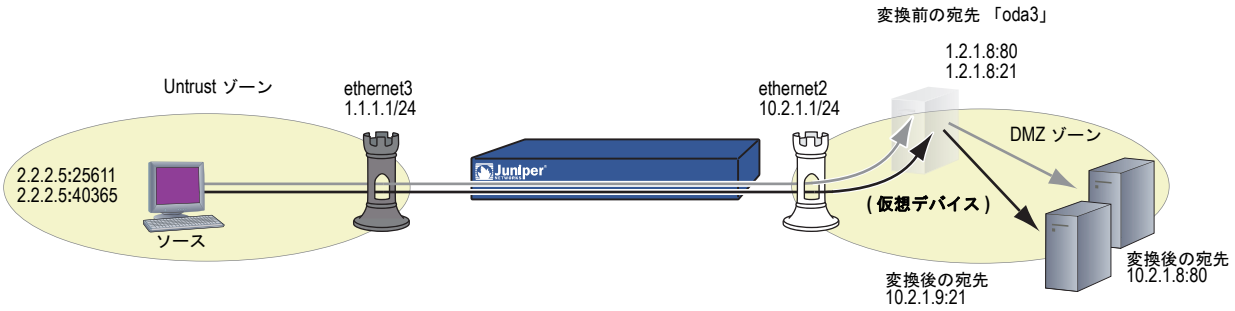
同じ宛先アドレスを、ポリシーによって異なるアドレスに変換することも可能です。サービスタイプやソースアドレスを基準としてポリシーを使い分けます。HTTP トラフィックは 1.2.1.8 から 10.2.1.8 に、一方 FTP トラフィックは 1.2.1.8 から 10.2.1.9 にリダイレクトする、というような設定ができます (以下に述べる例を参照)。あるいは、host1 から 1.2.1.8 への HTTP トラフィックは 10.2.1.8 にリダイレクトし、同じ 1.2.1.8 宛の HTTP トラフィックでも、host2 からのものであれば 10.2.1.37 にリダイレクトする、という設定も可能です。どちらの場合も、変換前の宛先アドレスは同じですが、変換後の宛先アドレスは異なります。

例 : 1 対多の宛先アドレス変換

この例では、変換前の宛先アドレスが同じ (1.2.1.8) ポリシーを 2 つ設定します。サービスタイプによってポリシーを使い分け、異なる宛先アドレスに変換するものとします。次のような処理を行うポリシーです。

- Untrust ゾーン内の任意のアドレスから、ユーザー定義アドレス「 oda3 」に向かう、FTP および HTTP のトラフィックを許可。「 oda3 」は DMZ ゾーンにあります。
- HTTP トラフィックについては、IP パケットヘッダー中の宛先 IP アドレスを 1.2.1.8 から 10.2.1.8 に変換。
- FTP トラフィックについては、IP パケットヘッダー中の宛先 IP アドレスを 1.2.1.8 から 10.2.1.9 に変換。
- TCP セグメントヘッダー中の宛先ポート番号は元のまま (HTTP ならば 80、FTP ならば 21)。
- HTTP トラフィックを 10.2.1.8、FTP トラフィックを 10.2.1.9 に転送。どちらも DMZ ゾーン。

図 29: NAT-Dst - 1 対多



SRC IP	DST IP	SRC PT	DST PT	PROTO
2.2.2.5	1.2.1.8	25611	80	HTTP

SRC IP	DST IP	SRC PT	DST PT	PROTO
2.2.2.5	1.2.1.8	40365	21	FTP

SRC IP	DST IP	SRC PT	DST PT	PROTO
2.2.2.5	10.2.1.8	25611	80	HTTP

SRC IP	DST IP	SRC PT	DST PT	PROTO
2.2.2.5	10.2.1.9	40365	21	FTP

ethernet3 を Untrust ゾーンにバインドし、1.1.1.1/24 という IP アドレスを割り当てます。同様に、ethernet2 を DMZ ゾーンにバインドし、10.2.1.1/24 という IP アドレスを割り当てます。また、元の宛先アドレスである 1.2.1.8 へのルートを ethernet2 経由で定義します。Untrust ゾーン、DMZ ゾーンはともに、trust-vr ルーティングドメインに属します。

WebUI

1. インターフェース

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

Zone Name: DMZ
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.2.1.1/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

Address Name: oda3
IP Address/Domain Name:
IP/Netmask: (選択), 1.2.1.8/32
Zone: DMZ

3. ルート

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 1.2.1.8/32
Gateway: (選択)
Interface: ethernet2
Gateway IP Address: 0.0.0.0

4. ポリシー

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), oda3
Service: HTTP
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Destination Translation: (選択)
Translate to IP: (選択), 10.2.1.8
Map to Port:（オフ）

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), oda3
Service: FTP
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Destination Translation: (**選択**)
Translate to IP: (**選択**), 10.2.1.9
Map to Port:（**オフ**）

CLI

1. **インターフェース**
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24
   set interface ethernet2 zone dmz
   set interface ethernet2 ip 10.2.1.1/24
2. **アドレス**
   set address dmz oda3 1.2.1.8/32
3. **ルート**
   set vrouter trust-vr route 1.2.1.8/32 interface ethernet2
4. **ポリシー**
   set policy from untrust to dmz any oda3 http nat dst ip 10.2.1.8 permit
   set policy from untrust to dmz any oda3 ftp nat dst ip 10.2.1.9 permit
   save

NAT-Dst- 多対 1 のマッピング

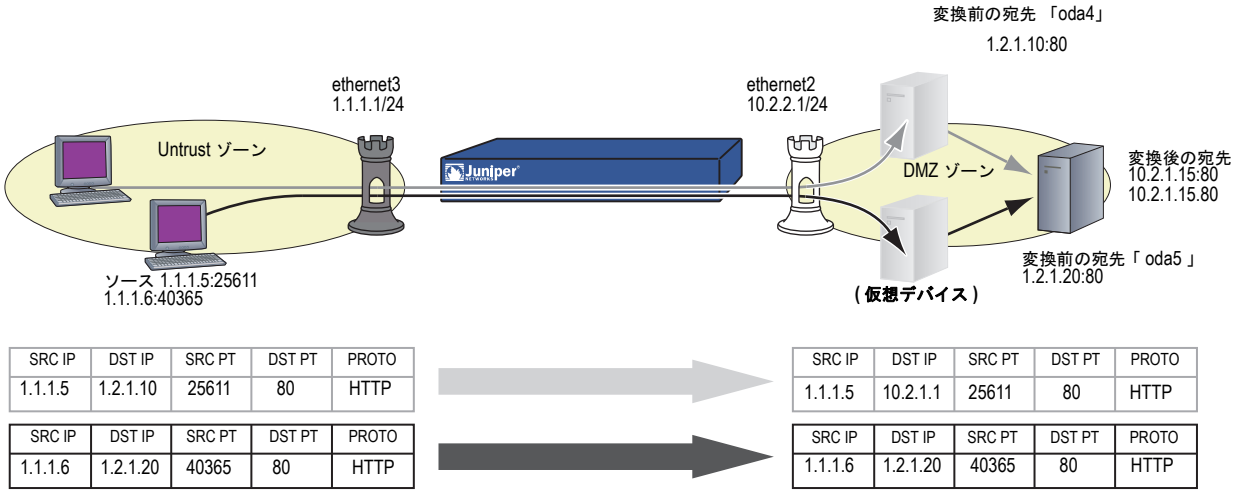
変換前と変換後の宛先アドレスが多対 1 の関係になるような設定も可能です。この場合、変換前の宛先アドレスが違っていても、同じ宛先アドレスに変換することになります。さらに、宛先ポートマッピングを指定することもできます。

例: 多対 1 の宛先アドレス変換

この例では、元の宛先アドレスが異なる (1.2.1.10、1.2.1.20) トラフィックを、同じ宛先アドレスに変換する、というポリシーを設定します。次のような処理を行うポリシーです。

- Untrust ゾーン内の任意のアドレスから、「 oda45 」というユーザー定義アドレスグループに向かう、HTTP のトラフィックを許可。「 oda4 」(1.2.1.10) および 「 oda5 」(1.2.1.20) は DMZ ゾーンにあります。
- IP パケットヘッダー中の宛先 IP アドレスを、1.2.1.10 または 1.2.1.20 から 10.2.1.15 に変換。
- TCP セグメントヘッダー中の宛先ポート番号は元のまま (HTTP ならば 80)。
- HTTP トラフィックを DMZ ゾーンにある 10.2.1.15 に転送。

図 30: NAT-Dst - 多対 1



ethernet3 を Untrust ゾーンにバインドし、1.1.1.1/24 という IP アドレスを割り当てます。同様に、ethernet2 を DMZ ゾーンにバインドし、10.2.1.1/24 という IP アドレスを割り当てます。また、元の宛先アドレスである 1.2.1.10 および 1.2.1.20 へのルートを ethernet2 経由で定義します。Untrust ゾーン、DMZ ゾーンはともに、trust-vr ルーティングドメインに属します。

WebUI

1. インターフェース

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

Zone Name: DMZ
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.2.1.1/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

Address Name: oda4
IP Address/Domain Name:
IP/Netmask: (選択), 1.2.1.10/32
Zone: DMZ

Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

Address Name: oda5
IP Address/Domain Name:

IP/Netmask: (選択), 1.2.1.20/32
Zone: DMZ

Policy > Policy Elements > Addresses > Groups > (Zone: DMZ) New: 以下のグループ名を入力して、以下のアドレスを移動し、**OK** をクリックします。

Group Name: oda45

アドレス **oda4** を選択し、< < ボタンで Available Members 列から Group Members 列に移動します。

アドレス **oda5** を選択し、< < ボタンで Available Members 列から Group Members 列に移動します。

3. ルート

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 1.2.1.10/32
Gateway: (選択)
Interface: ethernet2
Gateway IP Address: 0.0.0.0

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 1.2.1.20/32
Gateway: (選択)
Interface: ethernet2
Gateway IP Address: 0.0.0.0

4. ポリシー

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), oda45
Service: HTTP
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Destination Translation: (選択)
Translate to IP: (選択), 10.2.1.15
Map to Port:（オフ）

CLI

1. インターフェース

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet2 zone dmz
set interface ethernet2 ip 10.2.1.1/24
```

2. **アドレス**
   set address dmz oda4 1.2.1.10/32
   set address dmz oda5 1.2.1.20/32
   set group address dmz oda45 add oda4
   set group address dmz oda45 add oda5

3. **ルート**
   set vrouter trust-vr route 1.2.1.10/32 interface ethernet2
   set vrouter trust-vr route 1.2.1.20/32 interface ethernet2

4. **ポリシー**
   set policy from untrust to dmz any oda45 http nat dst ip 10.2.1.15 permit
   save

NAT-Dst- 多対多のマッピング

ある範囲の IP アドレスを別の範囲の IP アドレスに変換する、という宛先ネットワークアドレス変換 (NAT-dst) も利用できます。この範囲は、サブネット全体でも、その一部であっても構いません。アドレスシフティングというしくみで、変換前と変換後のアドレスの対応を管理することになります。たとえば変換前アドレスの範囲が 10.1.1.1 - 10.1.1.50 で、変換後アドレス範囲の先頭が 10.100.3.101 であれば、次のように変換されます。

- 10.1.1.1 - 10.100.3.101
- 10.1.1.2 - 10.100.3.102
- 10.1.1.3 - 10.100.3.103

  …

- 10.1.1.48 - 10.100.3.148
- 10.1.1.49 - 10.100.3.149
- 10.1.1.50 - 10.100.3.150

たとえば、ゾーン A に属する任意のアドレスからアドレスグループ “addr1-50” に向かう、HTTP トラフィックに適用するポリシーを設定するとしましょう。“addr1-50” には、ゾーン B に属する、10.1.1.1 から 10.1.1.50 のアドレスが含まれています。この場合、次のような CLI コマンドで設定します。

```
set policy id 1 from zoneA to zoneB any addr1-50 http nat dst ip 10.100.3.101
    10.100.3.150 permit
```

ゾーン A の任意のホストが、ゾーン B の定義された範囲内のアドレス、たとえば 10.1.1.37 宛に HTTP トラフィックを送ると、セキュリティデバイスはこのポリシーを適用して、宛先アドレスを 10.100.3.137 に変換します。

NAT-dst が適用されるのは、ソースおよび宛先ゾーン、ソースおよび宛先アドレス、サービスタイプのすべてが、ポリシーの条件と合致した場合に限ります。たとえば、ゾーン A の任意のホストからゾーン B の任意のホストへのトラフィックも許可させたい場合は、もう 1 つ、次のようなポリシーを作成してポリシー 1 の後に追加してください。

```
set policy id 1 from zoneA to zoneB any addr1-50 http nat dst ip 10.100.3.101
    10.100.3.150 permit
set policy id 2 from zoneA to zoneB any any any permit
```

このように構成した 2 つのポリシーによって、ゾーン A からゾーン B に向かう次のようなトラフィックは、NAT-dst を適用されることなくそのまま通過します。

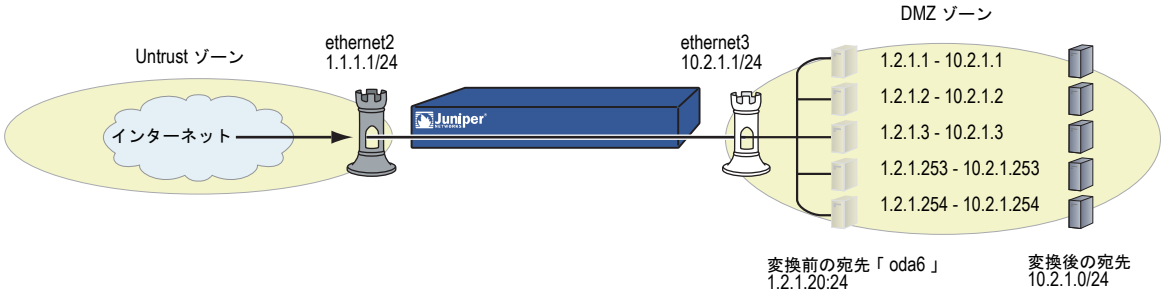
- ゾーン A 内のホストが、ゾーン B に属する 10.1.1.37 宛の、HTTP 以外のトラフィックを送出した場合。サービスタイプが HTTP ではないので、ポリシー 2 を適用し、宛先アドレスを変換することなくそのまま通過させます。
- ゾーン A 内のホストが、ゾーン B に属する 10.1.1.51 宛の、HTTP トラフィックを送出した場合。宛先アドレスが “addr1-50” アドレスグループに属さないので、やはりポリシー 2 を適用し、宛先アドレスを変換することなくそのまま通過させます。

例: 多対多の宛先アドレス変換

この例では、あるサブネットに属する任意のホストを宛先とする、任意のトラフィックに対して NAT-dst を適用するポリシーを設定します。

- Untrust ゾーンの任意のアドレスから DMZ ゾーンの任意のアドレスへのあらゆるタイプのトラフィックを許可。
- サブネット 1.2.1.0/24 に属している、変換前の宛先アドレス「 oda6 」を、サブネット 10.2.1.0/24 の対応するアドレスに変換。
- TCP セグメントヘッダー中の宛先ポート番号は元のまま。
- HTTP トラフィックは DMZ に属する変換後のアドレスに転送。

図 31: NAT-Dst-: 多対多



ethernet3 を Untrust ゾーンにバインドし、1.1.1.1/24 という IP アドレスを割り当てます。同様に、ethernet2 を DMZ ゾーンにバインドし、10.2.1.1/24 という IP アドレスを割り当てます。さらに、ethernet2 を通って、変換前の宛先アドレスが属するサブネット 1.2.1.0/24 に到達するルートを定義します。Untrust ゾーン、DMZ ゾーンはともに、trust-vr ルーティングドメインに属します。

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

Zone Name: DMZ
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.2.1.1/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

Address Name: oda6
IP Address/Domain Name:
IP/Netmask: (選択), 1.2.1.0/24
Zone: DMZ

3. ルート

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 1.2.1.0/24
Gateway: (選択)
Interface: ethernet2
Gateway IP Address: 0.0.0.0

4. ポリシー

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), oda6
Service: ANY
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Destination Translation: (選択)
Translate to IP Range: (選択), 10.2.1.0 - 10.2.1.254

CLI

1. インターフェース

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet2 zone dmz
set interface ethernet2 ip 10.2.1.1/24
```

2. アドレス

```
set address dmz oda6 1.2.1.0/24
```

3. ルート

```
set vrouter trust-vr route 1.2.1.0/24 interface ethernet2
```

4. ポリシー

```
set policy from untrust to dmz any oda6 any nat dst ip 10.2.1.1 10.2.1.254 permit
save
```

ポートマッピングを伴う NAT-Dst

宛先ネットワークアドレス変換 (NAT-dst) に加え、ポートマッピングを有効にすることもできます。1 台のホストで、同じサービスタイプであっても、複数のサーバープロセスを稼動させたいような場合に有用です。たとえば同じホスト上で Web サーバーを 2 つ動かし、ポート 80 番および 8081 番で待ち受けるとします。HTTP サービス 1 に対しては、ポートマッピングを施すことなく NAT-dst を適用します (dst port 80 -> 80)。

一方 HTTP サービス 2 に対しては、ポートマッピングを有効にして NAT-dst を同じ宛先 IP アドレスに適用します (dst port 80 -> 8081)。このようにすれば、どちらの Web サーバーに対する HTTP トラフィックかを、ポート番号で区別できるようになります。

注 : アドレスシフティングによる NAT-dst の場合、ポートマッピングをサポートしません。43 ページの「NAT-Dst- 多対多のマッピング」を参照してください。

例 : ポートマッピングを伴う NAT-Dst

この例では、Trust ゾーンおよび Untrust ゾーンから、DMZ ゾーン内の Telnet サーバーに向かう Telnet トラフィックに対して、NAT-dst およびポートマッピングを施す 2 つのポリシーを設定します。次のような処理を行うポリシーです。

- Untrust ゾーンおよび Trust ゾーンに属する任意のアドレスから、DMZ ゾーン内の 1.2.1.15 に向かう Telnet トラフィックを許可。
- 宛先 IP アドレス「 oda7 」を、1.2.1.15 から 10.2.1.15 に変換。
- TCP セグメントヘッダー中の宛先ポート番号を、23 から 2200 に変換。
- Telnet トラフィックは DMZ ゾーンに属する変換後のアドレスに転送。

次のように、各インターフェースを対応するゾーンにバインドし、IP アドレスを割り当てます。

- ethernet1: Trust ゾーン、10.1.1.1/24
- ethernet2: DMZ ゾーン、10.2.1.1/24
- ethernet3: Untrust ゾーン、1.1.1.1/24

アドレスエントリー「 oda7 」を、DMZ ゾーンに属する 1.2.1.15/32 と定義します。さらに、ethernet2 を通って、変換前の宛先アドレスである 1.2.1.15 に到達するルートを定義します。Trust、Untrust、DMZ の各ゾーンはすべて、trust-vr ルーティングドメインに属します。

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように選択してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

   Zone Name: DMZ
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.2.1.1/24

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 以下を入力して **OK** をクリックします。

   Address Name: oda7
   IP Address/Domain Name:
   IP/Netmask: (選択), 1.2.1.15/32
   Zone: DMZ

3. **ルート**
   Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 1.2.1.15/32
   Gateway: (選択)
   Interface: ethernet2
   Gateway IP Address: 0.0.0.0

4. **ポリシー**
   Policies > (From: Trust, To:DMZ) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Any
   Destination Address:
   Address Book Entry: (選択), oda7
   Service: Telnet
   Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Destination Translation: (選択)
Translate to IP: (選択), 10.2.1.15
Map to Port: (選択), 2200

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), oda7
Service: Telnet
Action: Permit

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

NAT:
Destination Translation: (選択)
Translate to IP: (選択), 10.2.1.15
Map to Port: (選択), 2200

CLI

1. **インターフェース**
```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet2 zone dmz
set interface ethernet2 ip 10.2.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```
2. **アドレス**
```
set address dmz oda7 1.2.1.15/32
```
3. **ルート**
```
set vrouter trust-vr route 1.2.1.15/32 interface ethernet2
```
4. **ポリシー**
```
set policy from trust to dmz any oda7 telnet nat dst ip 10.2.1.15 port 2200 permit
set policy from untrust to dmz any oda7 telnet nat dst ip 10.2.1.15 port 2200
    permit
save
```

1 つのポリシーで NAT-Src と NAT-Dst を適用

ソースネットワークアドレス変換 (NAT-src) と宛先ネットワークアドレス変換 (NAT-dst) を同じポリシーに組み合わせることができます。このようにすれば、ソースおよび宛先 IP アドレスの両方を、データパス上の一箇所で変換することができます。

例 : NAT-Src と NAT-Dst の組み合わせ

図 32 では、サービスプロバイダーの顧客とサーバーファームの間に設置された、セキュリティデバイス（デバイス 1 ）を設定します。顧客は ethernet1 経由でデバイス 1 に接続します。ethernet1 の IP アドレスは 10.1.1.1/24 で、その先は Trust ゾーンにつながっています。デバイス 1 は、2 つあるルートベースの VPN トンネルのうちいずれかを経由して、トラフィックを目的のサーバーに送ります。トンネルに向かうトンネルインターフェースは Untrust ゾーンに属します。Untrust ゾーン、DMZ ゾーンはともに、trust-vr ルーティングドメインに属します。

注 : ポリシーベースの VPN では NAT-dst を実現できません。NAT-dst を適用したい場合はルートベースの VPN にする必要があります。

顧客側のアドレスが接続先サーバーのアドレスと同じである可能性があるので、デバイス 1 ではソースアドレスと宛先アドレスの両方を変換する必要があります（NAT-src と NAT-dst の併用）。アドレス割り当ての独立性や柔軟性を保つため、サーバーファーム（デバイス A および デバイス B ）を保護する、別のセキュリティデバイスで NAT-dst を適用します。サービスプロバイダーは顧客およびサーバーファームの管理者に対し、10.173.10.1 - 10.173.10.7、10.173.20.0/24、10.173.30.0/24、10.173.40.0/24、10.173.50.0/24 の各アドレスはこの目的のために予約されている旨を伝えます。このアドレスは次のように使われます。

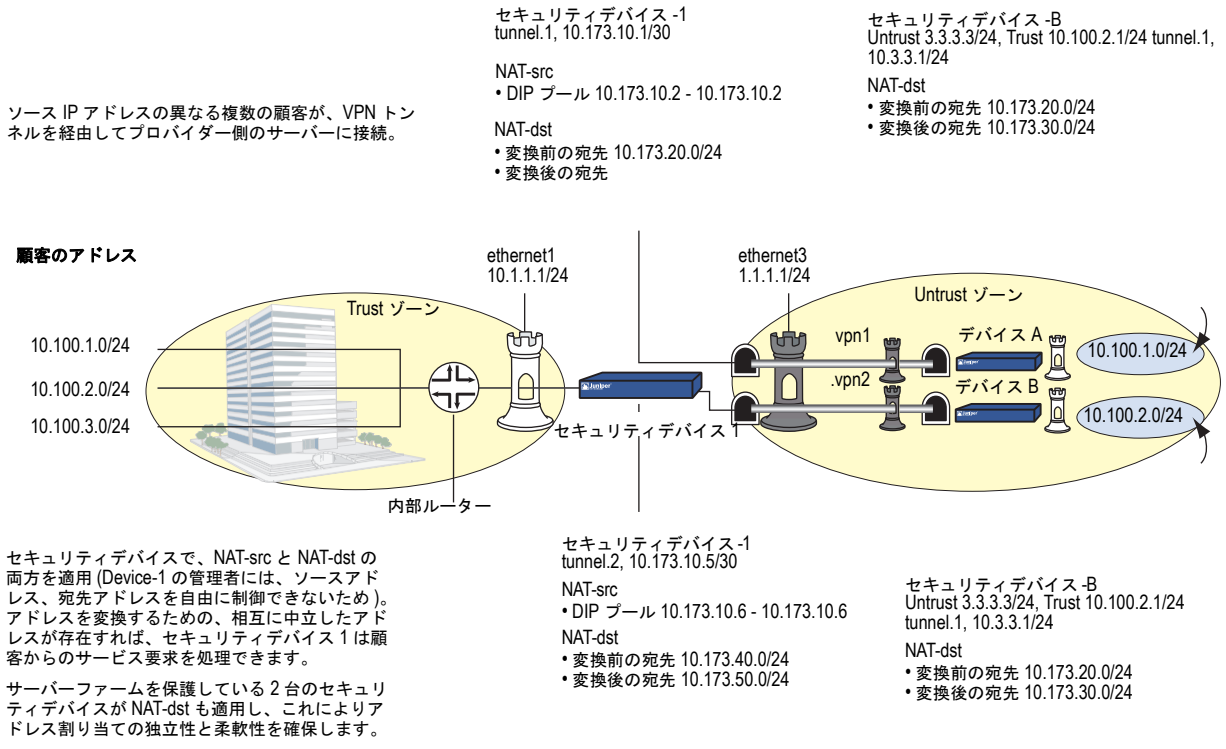
- 2 つのトンネルインターフェースに次のアドレスを割り当て。
  - tunnel.1, 10.173.10.1/30
  - tunnel.2, 10.173.10.5/30
- 各トンネルインターフェースは、次のような DIP プールを管理 (PAT つき)。
  - tunnel.1, DIP ID 5: 10.173.10.210.173.10.2
  - tunnel.2, DIP ID 6: 10.173.10.610.173.10.6
- デバイス 1 が NAT-dst を適用する場合、アドレスシフティングにより次のように宛先アドレスを変換。
  - 10.173.20.0/24 → 10.173.30.0/24
  - 10.173.40.0/24 → 10.173.50.0/24

注 : アドレスシフティングによる NAT-dst については、43 ページの「NAT-Dst- 多対多のマッピング」を参照してください。

トンネル vpn1 および vpn2 は、次のようなパラメータで設定します。すなわち、AutoKey IKE、事前共有鍵（ vpn1 は「 device1 」、vpn2 は「 device2 」）を設定し、セキュリティレベルは、フェーズ 1、フェーズ 2 のプロポーザルとも、「 Compatible 」としてあらかじめ定義しておいたレベルとします。(これらのプロポーザルに関する詳細については、5-8 ページの「トンネルネゴシエーション」を参照してください)。プロキシー ID は、vpn1、vpn2 とも、0.0.0.0/0 - 0.0.0.0/0 - any です。

注 : 最初にデバイス 1 の設定を示します。次いで、完全を期すため、デバイス A およびデバイス B の VPN 設定を示します。

図 32: NAT-Src と NAT-Dst の組み合わせ



WebUI （セキュリティデバイス 1 ）

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24
次のように選択してから **OK** をクリックします。
Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Fixed IP: (選択)
IP Address/Netmask: 10.173.10.1/30

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Fixed IP: (選択)
IP Address/Netmask: 10.173.10.5/30

2. DIP プール

Network > Interfaces > Edit (tunnel.1) > DIP > New: 次のように入力してから **OK** をクリックします。

ID: 5
IP Address Range: (選択), 10.173.10.2 ～ 10.173.10.2
Port Translation: (選択)
In the same subnet as the interface IP or its secondary IPs: (選択)

Network > Interfaces > Edit (tunnel.2) > DIP > New: 次のように入力してから **OK** をクリックします。

ID: 6
IP Address Range: (選択), 10.173.10.6 ～ 10.173.10.6
Port Translation: (選択)
In the same subnet as the interface IP or its secondary IPs: (選択)

3. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: serverfarm-A
IP Address/Domain Name:
IP/Netmask: (選択), 10.173.20.0/24
Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: serverfarm-B
IP Address/Domain Name:
IP/Netmask: (選択), 10.173.40.0/24
Zone: Untrust

4. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway:Create a Simple Gateway: (**選択**)
Gateway Name: gw-A
Type: Static IP: (**選択**), Address/Hostname: 2.2.2.2
Preshared Key: device1
Security Level: Compatible
Outgoing Interface: ethernet3

注 : ここでは出力インターフェースに、トンネルインターフェースの先にあるゾーンを指定していますが、必ずしもそうでなくても構いません。

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to Tunnel Interface: (**選択する**), tunnel.1
Proxy-ID: (**選択**)
Local IP / Netmask: 0.0.0.0/0
Remote IP / Netmask: 0.0.0.0/0
Service: ANY

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn2
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (**選択**)
Gateway Name: gw-B
Type: Static IP: (**選択**), Address/Hostname: 3.3.3.3
Preshared Key: device2
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to Tunnel Interface: (**選択**), tunnel.2
Proxy-ID: (**選択**)
Local IP / Netmask: 0.0.0.0/0
Remote IP / Netmask: 0.0.0.0/0
Service: ANY

5. ルート

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.173.20.0/24
Gateway: (**選択**)
Interface: tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.173.30.0/24
Gateway: (**選択**)
Interface: tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.173.40.0/24
Gateway: (**選択**)
Interface: tunnel.2
Gateway IP Address: 0.0.0.0

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.173.50.0/24
Gateway: (**選択**)
Interface: tunnel.2
Gateway IP Address: 0.0.0.0

6. ポリシー

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), Any
Destination Address:
Address Book Entry: (**選択**), serverfarm-A
Service: ANY
Action: Permit
Position at Top: (**選択**)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

NAT:
Source Translation: (**選択**)
(DIP on): 5 (10.173.10.2-10.173.10.2)/X-late
Destination Translation: (**選択**)
Translate to IP Range: (**選択**), 10.173.30.0 - 10.173.30.255

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), serverfarm-B
Service: ANY
Action: Permit
Position at Top: (選択)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

NAT:
Source Translation: (選択)
(DIP on): 6 (10.173.10.6-10.173.10.6)/X-late
Destination Translation: (選択)
Translate to IP Range: (選択), 10.173.50.0 - 10.173.50.255

CLI （セキュリティデバイス 1 ）

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.173.10.1/30
set interface tunnel.2 zone untrust
set interface tunnel.2 ip 10.173.10.5/30
```

2. DIP プール

```
set interface tunnel.1 dip-id 5 10.173.10.2 10.173.10.2
set interface tunnel.2 dip-id 6 10.173.10.6 10.173.10.6
```

3. アドレス

```
set address untrust serverfarm-A 10.173.20.0/24
set address untrust serverfarm-B 10.173.40.0/24
```

4. VPN

```
set ike gateway gw-A ip 2.2.2.2 main outgoing-interface ethernet3 preshare
    device1 sec-level compatible
set vpn vpn1 gateway gw-A sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set ike gateway gw-B ip 3.3.3.3 main outgoing-interface ethernet3 preshare
    device2 sec-level compatible
set vpn vpn2 gateway gw-B sec-level compatible
set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

5. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.173.20.0/24 interface tunnel.1
set vrouter trust-vr route 10.173.30.0/24 interface tunnel.1
set vrouter trust-vr route 10.173.40.0/24 interface tunnel.2
set vrouter trust-vr route 10.173.50.0/24 interface tunnel.2
```

6. ポリシー

set policy top from trust to untrust any serverfarm-A any nat src dip-id 5 dst ip 10.173.30.0 10.173.30.255 permit
set policy top from trust to untrust any serverfarm-B any nat src dip-id 6 dst ip 10.173.50.0 10.173.50.255 permit
save

WebUI (セキュリティデバイス A_)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.100.1.1/24

次のように選択してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Fixed IP: (選択)
IP Address/Netmask: 10.2.2.1/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: serverfarm-A
IP Address/Domain Name:
IP/Netmask: (選択), 10.173.30.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: customer1
IP Address/Domain Name:
IP/Netmask: (選択), 10.173.10.0/32
Zone: Untrust

3. **VPN**

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (選択)
Gateway Name: gw-1
Type: Static IP: (選択), Address/Hostname: 1.1.1.1
Preshared Key: device1
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to Tunnel Interface:(選択する), tunnel.1
Proxy-ID: (選択)
Local IP / Netmask: 0.0.0.0/0
Remote IP / Netmask: 0.0.0.0/0
Service: ANY

4. **ルート**

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 2.2.2.250

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.173.10.2/32
Gateway: (選択)
Interface: tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.173.30.0/24
Gateway: (選択)
Interface: ethernet1
Gateway IP Address: 0.0.0.0

5. **ポリシー**

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), customer1
Destination Address:
Address Book Entry: (選択), serverfarm-A
Service: ANY
Action: Permit
Position at Top: (選択)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

NAT:
Destination Translation: (選択)
Translate to IP Range: (選択), 10.100.1.0 - 10.100.1.255

CLI (セキュリティデバイス A)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.100.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.2.2.1/24
```

2. アドレス

```
set address trust serverfarm-A 10.173.30.0/24
set address untrust customer1 10.173.10.2/32
```

3. VPN

```
set ike gateway gw-1 ip 1.1.1.1 main outgoing-interface ethernet3 preshare
    device1 sec-level compatible
set vpn vpn1 gateway gw-1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter trust-vr route 10.173.10.2/32 interface tunnel.1
set vrouter trust-vr route 10.173.30.0/24 interface ethernet1
```

5. ポリシー

```
set policy top from untrust to trust customer1 serverfarm-A any nat dst ip
    10.100.1.0 10.100.1.255 permit
save
```

WebUI (セキュリティデバイス B)

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.100.2.1/24
次のように選択してから **OK** をクリックします。
Interface Mode: NAT

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 3.3.3.3/24

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Fixed IP: (**選択**)
IP Address/Netmask: 10.3.3.1/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: serverfarm-B
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.173.50.0/24
Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: customer1
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.173.10.6/32
Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (**選択**)
Gateway Name: gw-1
Type: Static IP: (**選択**), Address/Hostname: 1.1.1.1
Preshared Key: device2
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to Tunnel Interface: (**選択する**), tunnel.1
Proxy-ID: (**選択**)
Local IP / Netmask: 0.0.0.0/0
Remote IP / Netmask: 0.0.0.0/0
Service: ANY

4. ルート

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: ethernet3
Gateway IP Address: 3.3.3.250

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.173.10.6/32
Gateway: (選択)
Interface: tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.173.50.0/24
Gateway: (選択)
Interface: ethernet1
Gateway IP Address: 0.0.0.0

5. ポリシー

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), customer1
Destination Address:
Address Book Entry: (選択), serverfarm-B
Service: ANY
Action: Permit
Position at Top: (選択)

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本ポリシー構成ページに戻ります。

NAT:
Destination Translation: (選択)
Translate to IP Range: (選択), 10.100.2.0 - 10.100.2.255

CLI (セキュリティデバイス B)

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.100.2.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.3.3.1/24
```

2. アドレス

```
set address trust serverfarm-B 10.173.50.0/24
set address untrust customer1 10.173.10.6/32
```

3. VPN

```
set ike gateway gw-1 ip 1.1.1.1 main outgoing-interface ethernet3 preshare
    device2 sec-level compatible
set vpn vpn2 gateway gw-1 sec-level compatible
set vpn vpn2 bind interface tunnel.1
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 3.3.3.250
   set vrouter trust-vr route 10.173.10.6/32 interface tunnel.1
   set vrouter trust-vr route 10.173.50.0/24 interface ethernet1

5. **ポリシー**
   set policy top from untrust to trust customer1 serverfarm-B any nat dst ip
   10.100.2.0 10.100.2.255 permit
   save

第 4 章

マップアドレスと仮想アドレス

ScreenOS には、宛先 IP アドレスと宛先ポートアドレス（PAT）を変換する方式が、いくつも組み込まれています。本章では、マップ IP (MIP) や仮想 IP (VIP) アドレスの使用方法を、次のセクションに分けて解説します。

- 61 ページの「マップ IP アドレス」
  - 62 ページの「MIP と Global ゾーン」
  - 69 ページの「MIP を Untrust ゾーンとして扱うインターフェース」
  - 71 ページの「MIP とループバックインターフェース」
  - 78 ページの「MIP グルーピング」
- 79 ページの「仮想 IP アドレス」
  - 81 ページの「VIP と Global ゾーン」

マップ IP アドレス

マップ IP (MIP) とは、ある IP アドレスから別の IP アドレスに、1 対 1 で直接対応づけるマッピングのことです。セキュリティデバイスは、宛先が MIP であるトラフィックを受け取ると、その MIP に対応するアドレスのホストに転送します。MIP は実際には、静的な宛先アドレス変換、すなわち、IP パケットヘッダー中の宛先 IP アドレスを別の静的 IP アドレスに対応づける変換です。逆に MIP ホストがアウトバウンドトラフィックを発信した場合、セキュリティデバイスはホストのソース IP アドレスの方を MIP アドレスに変換します。このように、対称性を持つ両方向の変換である点で、ソースアドレス変換 (NAT-src) や宛先アドレス変換 (NAT-dst) とは動作が異なります (10 ページの「NAT-Src と NAT-Dst の適用方向」を参照)。

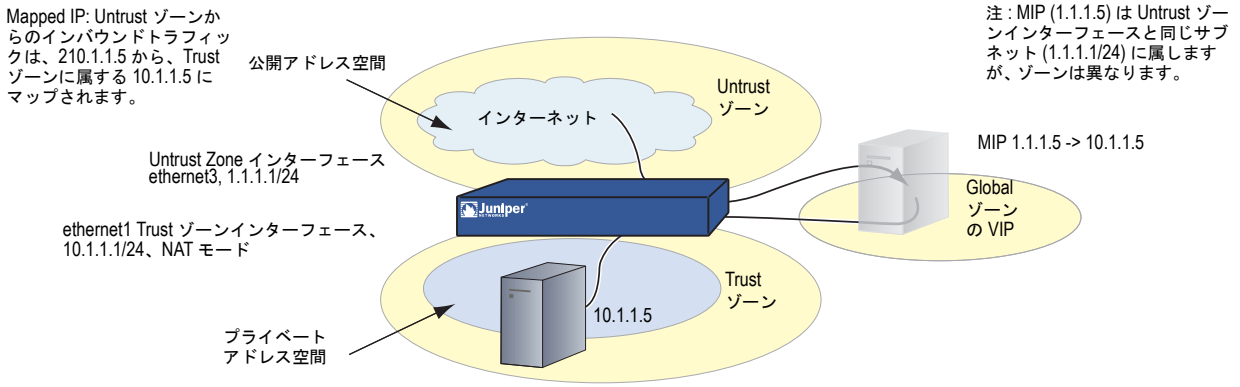
MIP はインバウンドトラフィックが、インターフェースが NAT モードであるゾーンのプライベートアドレスに到達することを許可します。MIP を使えば、VPN トンネルがつなぐ 2 つのサイトで重複するアドレス空間の問題の一部を解決することもできます (この問題の完全な解決法については、5-137 ページの「アドレスがオーバーラップする VPN サイト」を参照してください)。

注 : ここでいう「アドレス空間の重複」とは、2 つのネットワークで、IP アドレス範囲の一部または全部が一致してしまっている、という状況のことです。

MIP は、IP アドレス / ネットマスクを伴うトンネルインターフェースと同じサブネット、あるいはレイヤー 3 (L3) セキュリティゾーンに向かうインターフェースの IP アドレス / ネットマスクと同じサブネットに対して設定できます。MIP はトンネルゾーンやセキュリティゾーンに向かうインターフェースごとに設定するものですが、その定義は Global ゾーンに保存されます。

注： ただし Untrust ゾーンのインターフェースに対して定義する場合は例外です。この場合、Untrust ゾーンのインターフェース IP アドレスと異なるサブネットに MIP を定義できます。ただし、Untrust ゾーンインターフェースを指す外部ルーターに適切なルートを追加して、受信トラフィックが MIP に到達できるようにしなければなりません。さらに、セキュリティデバイスに静的ルートを定義して、MIP とそれをホスト するインターフェースを対応づける必要があります。

図 33: マップ IP アドレス



注： セキュリティデバイスの機種によっては、インターフェースと同じアドレスを MIP として割り当てることもできますが、DIP プールから取得して割り当てることはできません。

アドレスどうしをマップするほか、サブネットとサブネットの関係でマッピングを定義することも可能です。この場合、マップ IP 側および元の IP 側の両方のサブネットに対して、同じネットマスクが適用されます。

MIP と Global ゾーン

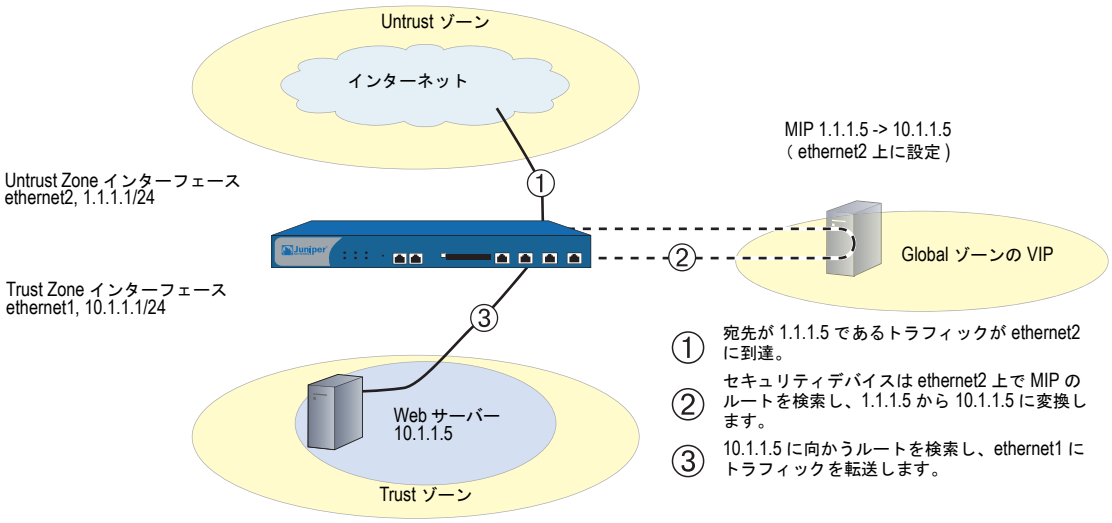
インターフェースに MIP を設定すると、それがどのゾーンに属するインターフェースであっても、Global ゾーンのアドレス帳に MIP が登録されます。すなわち、Global ゾーンのアドレス帳には、インターフェースが属するゾーンとは無関係に、すべての MIP が登録されるのです。2 つのゾーン間のトラフィックに関するポリシーでは、この MIP アドレスを宛先アドレスとして使えます。また、グローバルポリシーを定義する場合にも、やはり宛先アドレスとして使うことができます（グローバルポリシーについては、**2**-164 ページの「グローバルポリシー」を参照してください。）セキュリティデバイスは MIP を Global ゾーンに保存しますが、MIP を参照するポリシーでは、宛先ゾーンとして、Global ゾーンでも、MIP が指すアドレスが属するゾーンでも指定できます。

例 : Untrust ゾーンインターフェース上の MIP

この例では、ethernet1 を Trust ゾーンにバインドし、IP アドレスとして 10.1.1.1/24 を割り当てます。また、ethernet2 を Untrust ゾーンにバインドし、1.1.1.1/24 という IP アドレスを割り当てます。次に、Untrust ゾーンに属する 1.1.1.5 向けの HTTP トラフィックを、Trust ゾーンの 10.1.1.5 が割り当てられた Web サーバーに向ける MIP を設定します。次に、Untrust ゾーンに属する 1.1.1.5 向けの HTTP トラフィックを、Trust ゾーンの 10.1.1.5 が割り当てられた Web サーバーに向ける MIP を設定します。最後に、Untrust ゾーンの任意のアドレスから、Trust ゾーンに属する MIP (したがって MIP が指すアドレスを持つホスト) への HTTP トラフィックを許可するポリシーを定義します。セキュリティゾーンはすべて trust-vr ルーティングドメインにあります。

注 : MIP もそれが指すホストも、アドレス帳に載っていなくても構いません。

図 34: Untrust ゾーンインターフェース上の MIP



WebUI

1. **インターフェース**

   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように選択してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. **MIP**

   Network > Interfaces > Edit (ethernet2) > MIP > New: 次のように入力してから **OK** をクリックします。

   Mapped IP: 1.1.1.5
   Netmask: 255.255.255.255
   Host IP Address: 10.1.1.5
   Host Virtual Router Name: trust-vr

3. **ポリシー**

   Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), Any
   Destination Address:
   Address Book Entry: (**選択**), MIP(1.1.1.5)
   Service: HTTP
   Action: Permit

CLI

1. **インターフェース**

   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet2 zone untrust
   set interface ethernet2 ip 1.1.1.1/24

2. **MIP**

   set interface ethernet2 mip 1.1.1.5 host 10.1.1.5 netmask 255.255.255.255 vrouter trust-vr

---

注 : MIP の場合、特に指定しなければ netmask は 32 ビット (255.255.255.255) となり、単一のホストを表します。ある範囲のアドレスに対して MIP を定義することも可能です。たとえば次のような CLI で、クラス C サブネット内のアドレス 10.1.10.129 ～ 10.1.10.254 に対し、MIP として 1.1.1.5 を定義することができます。**set interface** *interface* **mip 1.1.1.5 host 10.1.10.128 netmask 255.255.255.128**. ただしこの範囲には、インターフェースアドレスやルーターアドレスは含まれません。

仮想ルーターは、特に指定しなければ trust-vr となります。したがって、仮想ルーターが trust-vr であったり、MIP のネットマスクが 32 ビットであったりする場合、明示的に指定する必要はありません。この設定例では、WebUI による設定と対称性を持たせるため、これらの引数は含まれています。

---

3. **ポリシー**

   set policy from untrust to trust any mip(1.1.1.5) http permit
   save

例 : 別のゾーンから MIP に到達するトラフィック

MIP を設定したのとは別のインターフェースを使って、別のゾーンからのトラフィックでも、MIP に到達できるようにすることができます。そのためには、他のそれぞれのゾーンにあるルーターにルートを設定して、対応するインターフェースの IP アドレスに宛てた内向きトラフィックが、MIP に到達できるようにする必要があります。

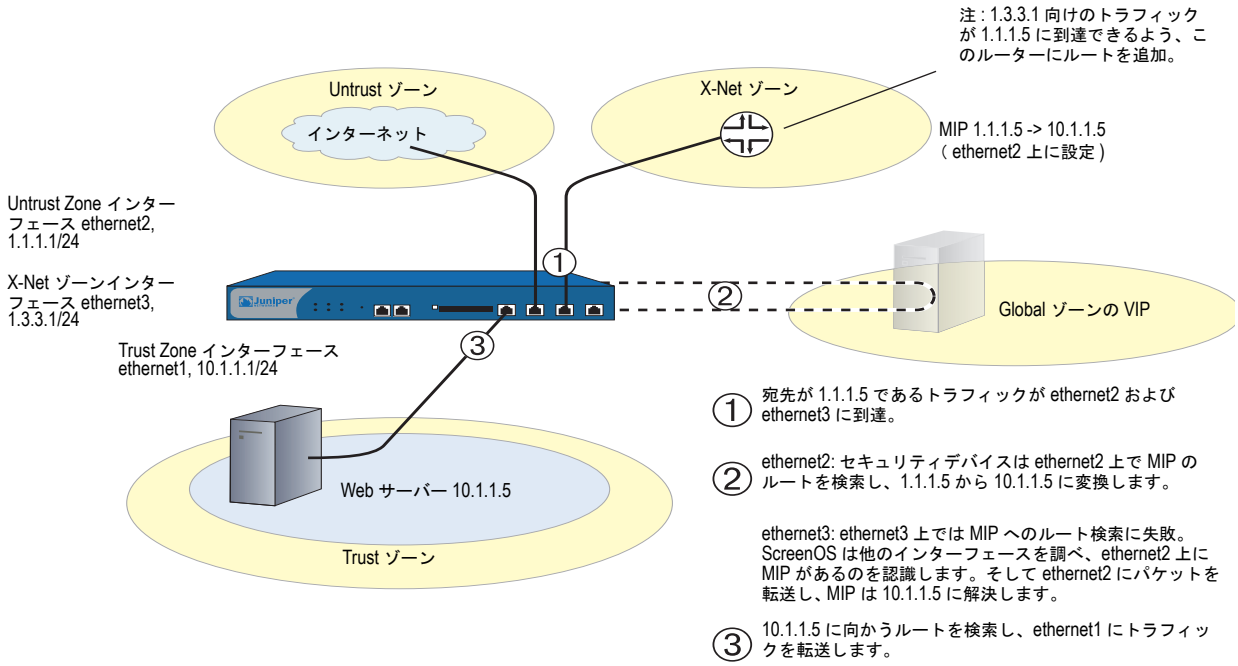
注 : MIP が、それを設定したインターフェースと同じサブネット上にある場合は、別のインターフェース経由で MIP に到達するトラフィック用のルートを、セキュリティデバイスに追加する必要はありません。逆に MIP がそのインターフェースの IP アドレスとは別のサブネット上にある場合 (これが起こりうるのは Untrust ゾーンのインターフェースにある MIP のみ) は、セキュリティデバイスのルーティングテーブルに静的ルートを追加する必要があります。静的ルートの追加には、**set vrouter** *name_str* **route** *ip_addr* **interface** *interface* というコマンドを使うか、または WebUI で同等の操作を行います。ここで *name_str* は、指定されたインターフェースが属する仮想ルーター、*interface* は MIP を設定するインターフェースを表します。

この例では、MIP (1.1.1.5) を Untrust ゾーン (ethernet2、1.1.1.1/24) のインターフェース上で設定し、Trust ゾーン (10.1.1.5) の Web サーバーにマップされるようにします。Trust ゾーンに向かうインターフェースは ethernet1 で、その IP アドレスは 10.1.1.1/24 です。

X-Net という名前でセキュリティゾーンを作成し、インターフェース ethernet3 をバインドして、そこに IP アドレス 1.3.3.1/24 を割り当てます。1.1.1.5 というアドレスを定義して、X-Net ゾーンの任意のアドレスから Untrust ゾーンにある MIP への HTTP トラフィックを許可するポリシーで使います。また、Untrust ゾーンから Trust ゾーンへの HTTP トラフィックを通過させるポリシーも設定します。セキュリティゾーンはすべて trust-vr ルーティングドメインにあります。

注 : X-Net ゾーン上のルーターに、1.1.1.5 (MIP) 宛のトラフィックを 1.3.3.1 (ethernet3 の IP アドレス) に向けるルートを追加する必要があります。

図 35: 別のゾーンから MIP に到達するトラフィック



WebUI

1. **インターフェースとゾーン**

   Network > Interfaces > Edit (ethernet1): 次のように入力してから **OK** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように選択してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet2): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

   Network > Zones > New: 次のように入力してから **OK** をクリックします。

   Zone Name: X-Net
   Virtual Router Name: untrust-vr
   Zone Type: Layer 3

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: X-Net
   IP Address/Netmask: 1.3.3.1/24

2. Address

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: 1.1.1.5
IP Address/Domain Name:
IP/Netmask: (選択)、1.1.1.5/32
Zone: Untrust

3. MIP

Network > Interfaces > Edit (ethernet2) > MIP > New: 次のように入力してから **OK** をクリックします。

Mapped IP: 1.1.1.5
Netmask: 255.255.255.255
Host IP Address: 10.1.1.5
Host Virtual Router Name: trust-vr

4. ポリシー

Policies > (From: X-Net, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), 1.1.1.5
Service: HTTP
Action: Permit

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), MIP(1.1.1.5)
Service: HTTP
Action: Permit

CLI

1. インターフェースとゾーン

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet2 zone untrust
set interface ethernet2 ip 1.1.1.1/24
set zone name X-Net
set interface ethernet3 zone X-Net
set interface ethernet3 ip 1.3.3.1/24
```

2. Address

```
set address untrust “1.1.1.5” 1.1.1.5/32
```

3. MIP

```
set interface ethernet2 mip 1.1.1.5 host 10.1.1.5 netmask 255.255.255.255
    vrouter trust-vr
```

注： 特に指定しなければ、MIP のネットマスクは 32 ビット (255.255.255.255)、仮想ルーターは trust-vr となります。したがって、コマンドで明示的に指定する必要はありません。この設定例では、WebUI による設定と対称性を持たせるため、引数に含まれています。

4. **ポリシー**

```
set policy from X-Net to untrust any “1.1.1.5” http permit
set policy from untrust to trust any mip(1.1.1.5) http permit
save
```

例 : MIP をトンネルインターフェースに追加

この例では、Trust ゾーンのネットワークの IP アドレス空間は 10.1.1.0/24、トンネルインターフェース 「 tunnel.8 」の IP アドレスは 10.20.3.1 とします。Trust ゾーンのネットワーク上にあるサーバーの物理 IP アドレスは 10.1.1.25 です。リモートサイトの Trust ゾーンのネットワークは、アドレス空間が重複しているとします。この場合、当該リモートサイトから VPN トンネル経由でローカルサーバーにアクセスできるようにするため、tunnel.8 インターフェースと同じサブネット上に MIP を設定します。MIP アドレスは 10.20.3.25/32 です (トンネルインターフェースを使う場合の、より完全な MIP 設定例については **5**-137 ページの「アドレスがオーバーラップする VPN サイト」を参照)。

WebUI

Network > Interfaces > Edit (tunnel.8) > MIP > New: 次のように入力してから **OK** をクリックします。

```
Mapped IP: 10.20.3.25
Netmask: 255.255.255.255
Host IP Address: 10.1.1.25
Host Virtual Router Name: trust-vr
```

CLI

```
set interface tunnel.8 mip 10.20.3.25 host 10.1.1.25 netmask 255.255.255.255
    vrouter trust-vr
save
```

注： 特に指定しなければ、MIP のネットマスクは 32 ビット (255.255.255.255)、仮想ルーターは trust-vr となります。したがって、コマンドで明示的に指定する必要はありません。この設定例では、WebUI による設定と対称性を持たせるため、引数に含まれています。

リモートサイトの管理者が Untrust ゾーンのアドレス帳にサーバーのアドレスを追加する際は、その物理 IP アドレス (10.1.1.25) ではなく、MIP (10.20.3.25) を指定する必要があります。

また、VPN 経由でサーバーに向かう外向きパケットに対しては、(DIP を使う) ポリシーベースの NAT-src を適用します。こうしておけば、ローカルサイトの管理者が Untrust ゾーンのアドレスを追加しても、ローカル Trust ゾーンのアドレスと衝突することはありません。逆に NAT-src を適用しないと、内向きパケットに適用するポリシーのソースアドレスが、Trust ゾーン内のアドレスと区別できなくなってしまいます。

MIP を Untrust ゾーンとして扱うインターフェース

IPv4 のアドレス資源が枯渇に向かっているので、ISP は顧客に対し、1 ～ 2 個程度の IP アドレスしか割り当てようとしない傾向があります。Untrust ゾーンに向かうインターフェース (NAT モードの Trust ゾーン向けインターフェース) の IP アドレスが 1 つしかない場合は、Untrust ゾーンインターフェースの IP アドレスを MIP (マップド IP) として使い、内部サーバーやホスト、あるいは VPN や L2TP トンネルの終点への内向きアクセスができるようにします。

MIP には、あるアドレス宛のトラフィックを別のアドレス宛にマップする働きがあります。したがって、Untrust ゾーンインターフェース IP アドレスを MIP として使えば、Untrust ゾーンインターフェースを使うインバウンドトラフィックをすべて、所定の内部アドレス宛にマップすることができます。Untrust インターフェース上の MIP により、VPN や L2TP トンネルの終点にマップされた場合、デバイスは自動的に、IKE パケットや L2TP パケットをトンネル終点に転送します。ただし Untrust インターフェース上に VPN や L2TP トンネルが設定されている場合を除きます。

Untrust ゾーンインターフェース IP アドレスを MIP として使い、宛先アドレスがその MIP、サービスタイプが HTTP であるようなポリシーを設定したとします。この場合、当該インターフェース経由で、WebUI 画面からセキュリティデバイスの Web 管理をすることはできなくなってしまいます。これはそのアドレスへのすべてのインバウンド HTTP トラフィックが、内部サーバーまたはホストにマップされているからです。ただし Web 管理用のポート番号を変更すれば WebUI を使用して、Untrust ゾーンを経由してデバイスを管理することができます。Web 管理ポート番号を変更する手順は次のとおりです。

1. Admin > Web: HTTP ポートフィールドに、登録されたポート番号 (1024 から 65,535) を入力します。次に、**Apply** をクリックします。

2. 次回以降、NetScreen デバイスを管理するために Untrust ゾーンインターフェースに接続する際は、IP アドレスの後にポート番号を追加して、たとえば http://209.157.66.170:5000 のように指定します。

例 : Untrust ゾーンインターフェース上の MIP

この例では、Untrust ゾーンインターフェース (ethernet3、1.1.1.1/24) の IP アドレスを、Web サーバーの MIP として設定します。この Web サーバーは、実際には Trust ゾーンにあり、IP アドレスは 10.1.1.5 です。ethernet3 インターフェース経由で、WebUI から NetScreen デバイスを管理できるようにするため、ポート番号を 8080 に変更します。次に、Untrust ゾーンから Trust ゾーンの MIP (したがって MIP が指すアドレスを持つホスト) 宛の HTTP サービスを許可するポリシーを設定します。ポート番号は HTTP のデフォルト値である 80 番になります。

WebUI

1. インターフェース

Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24

次のように入力してから **OK** をクリックします。

NAT: (選択)

注： デフォルトでは、Trust ゾーンにバインドされたどのインターフェースも NAT モードになっています。そのため、Trust ゾーンにバインドされたインターフェースではこのオプションはすでに有効にしています。

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

2. HTTP ポート

Configuration > Admin > Management: HTTP Port フィールドに **8080** と入力し、**Apply** をクリックします。

(HTTP 接続はできなくなります。)

3. 再度接続する

ブラウザーの URL アドレスフィールドには IP アドレスが入力されていますが、その後にポート番号 8080 を追加し、接続し直してください (現在、untrust インターフェースを介してデバイスを管理している場合には、**http://1.1.1.1:8080** と入力します。)

4. MIP

Network > Interface > Edit (ethernet3) > MIP > New: 次のように入力してから **OK** をクリックします。

Mapped IP: 1.1.1.1
Netmask: 255.255.255.255
Host IP Address: 10.1.1.5
Host Virtual Router Name: trust-vr

注： Untrust ゾーンインターフェース IP アドレスを MIP として使う場合のネットマスクは 32 ビットです。

5. Route

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

6. ポリシー

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), MIP(1.1.1.1)
Service: HTTP
Action: Permit

CLI

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **HTTP ポート**
   set admin port 8080

3. **MIP**
   set interface ethernet3 mip 1.1.1.1 host 10.1.1.5 netmask 255.255.255.255
   vrouter trust-vr

注 : 特に指定しなければ、MIP のネットマスクは 32 ビット (255.255.255.255)、仮想ルーターは trust-vr となります。したがって、コマンドで明示的に指定する必要はありません。この設定例では、WebUI による設定と対称性を持たせるため、引数に含まれています。

---

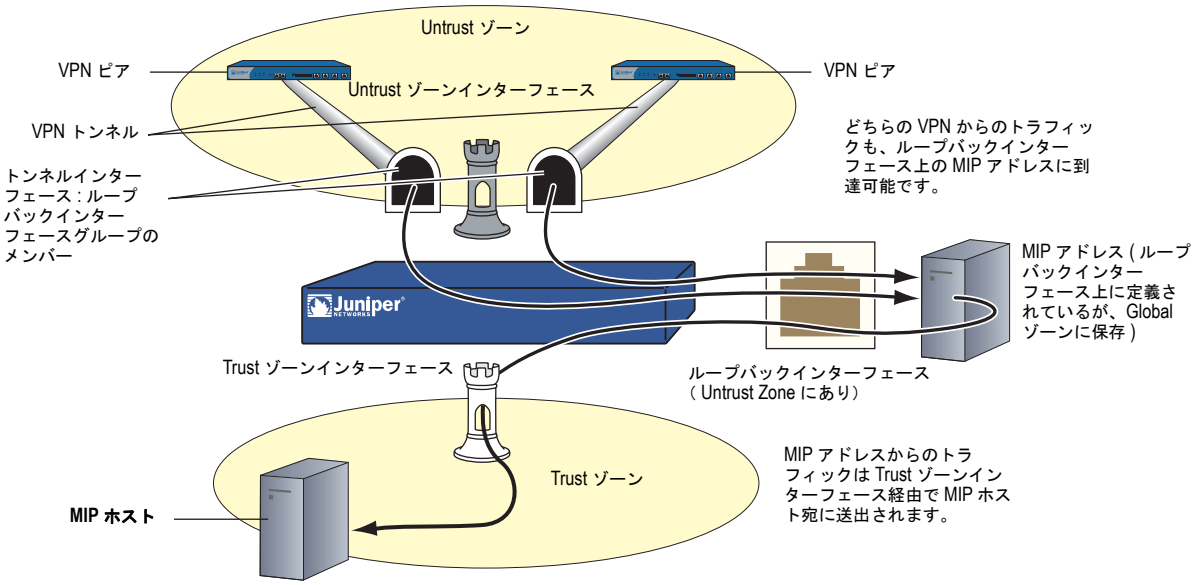
4. **Route**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

5. **ポリシー**
   set policy from untrust to trust any mip(1.1.1.1) http permit
   save

MIP とループバックインターフェース

ループバックインターフェース上に MIP を定義すると、インターフェースグループから MIP にアクセスできるようになります。その主な目的は、単一の MIP アドレスを使って、複数の VPN トンネルのうち 1 つを経由してホストにアクセスできるようにすることです。また、適当なトンネルを経由して、MIP ホストからリモートサイト宛のトラフィックを送出することも可能です。

図 36: ループバックインターフェース上の MIP



ループバックインターフェースは、MIP アドレスという資源の「置き場所」であると考えるとよいでしょう。「 loopback.*id_num* 」という名前のループバックインターフェース (ここで *id_num* は、デバイスの各インターフェースを一意に識別できるインデックス番号) を設定し、インターフェースに IP アドレスを割り当てます (**2**-58 ページの「ループバックインターフェース」を参照。) 次に、他のインターフェースからもループバックインターフェース上の MIP を使えるよう、ループバックグループのメンバーとして、他の各インターフェースも追加します。

ループバックインターフェースおよびそのメンバーインターフェースは、同じゾーン内の、別の IP サブネットに属するものでなければなりません。どのようなインターフェースでも、IP アドレスさえあれば、ループバックグループのメンバーにすることができます。ループバックインターフェースと、そのメンバーインターフェースの両方に対して MIP を設定した場合は、ループバックインターフェースに対する設定の方が優先します。ループバックインターフェースを、別のループバックグループのメンバーにすることはできません。

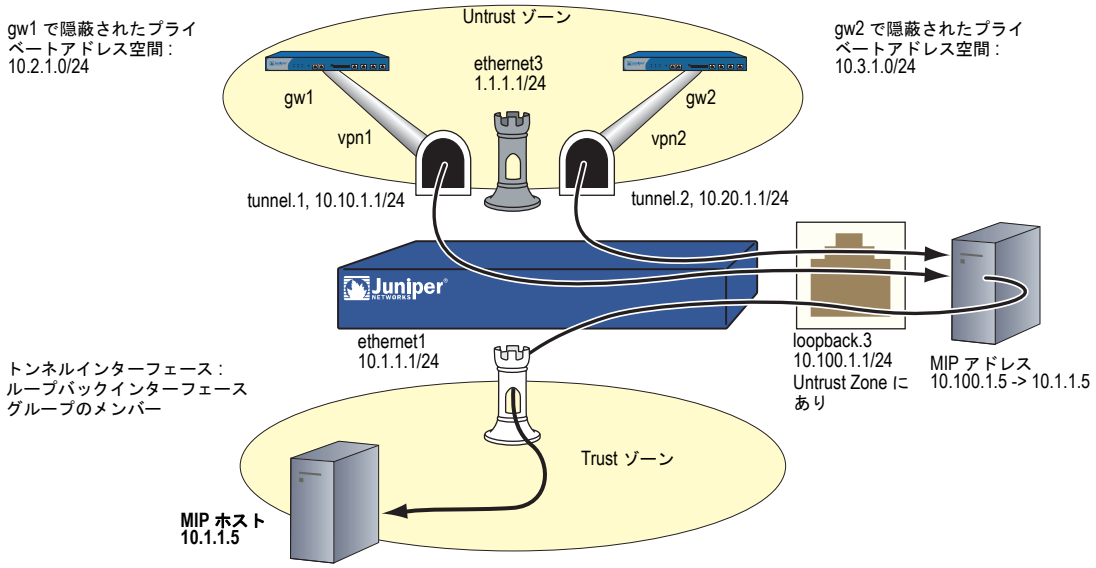
例 : 2 つのトンネルインターフェースに対する MIP

この例では次の 2 つのインターフェースを設定します。

- ethernet1 、Trust ゾーン、10.1.1.1/24
- ethernet3 、Untrust ゾーン、1.1.1.1/24
- tunnel.1 、Untrust ゾーン、10.10.1.1/24、vpn1 にバインド
- tunnel.2 、Untrust ゾーン、10.20.1.1/24、vpn2 にバインド
- loopback.3 、Untrust ゾーン、10.100.1.1/24

トンネルインターフェースは loopback.3 インターフェースグループのメンバーです。loopback.3 インターフェースには MIP アドレス 10.100.1.5 が含まれます。これは Trust ゾーン上のホスト 10.1.1.5 にマップするものです。

図 37: 2 つのトンネルインターフェースに対する MIP



10.100.1.5 宛のパケットが VPN トンネル経由で tunnel.1 に到達すると、セキュリティデバイスは、ループバックインターフェース loopback.3 上の MIP を検索します。見つかれば、元の宛先 IP アドレス (10.100.1.5) をホスト IP アドレス (10.1.1.5) に変換し、ethernet1 経由で MIP ホストにパケットを転送します。10.100.1.5 向けのトラフィックは、tunnel.2 の先にある VPN トンネル経由で届くこともあります。この場合もやはりセキュリティデバイスは、loopback.3 上の MIP を検索し、宛先 IP アドレスを 10.100.1.5 から 10.1.1.5 に変換して、パケットを MIP ホストに転送します。

このほか、必要に応じて、アドレス、VPN トンネル、ルート、ポリシーも定義します。セキュリティゾーンはすべて trust-vr ルーティングドメインにあります。

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24

   次のように入力してから **OK** をクリックします。

   NAT: (選択)

注 : デフォルトでは、Trust ゾーンにバインドされたどのインターフェースも NAT モードになっています。そのため、Trust ゾーンにバインドされたインターフェースではこのオプションはすでに有効にしています。

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Loopback IF: 次のように入力してから **OK** をクリックします。

Interface Name: loopback.3
Zone: Untrust (trust-vr)
IP Address/Netmask: 10.100.1.1/24

Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Fixed IP: (選択)
IP Address/Netmask: 10.10.1.1/24

Member of Loopback Group ドロップダウンリストから **loopback.3** を選択し、**OK** をクリックします。

Network > Interfaces > New Tunnel IF: 以下を入力して **Apply** をクリックします。

Tunnel Interface Name: tunnel.2
Zone (VR): Untrust (trust-vr)
Fixed IP: (選択)
IP Address/Netmask: 10.20.1.1/24

Member of Loopback Group ドロップダウンリストから **loopback.3** を選択し、**OK** をクリックします。

2. MIP

Network > Interfaces > Edit (loopback.3) > MIP > New: 次のように入力してから **OK** をクリックします。

Mapped IP: 10.100.1.5
Netmask: 255.255.255.255
Host IP Address: 10.1.1.5
Host Virtual Router Name: trust-vr

3. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: local_lan
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.0/24
Zone: Trust

Policy > Policy Elements > Addresses > New: 次のように入力してから **OK** をクリックします。

Address Name: peer-1
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.2.1.0/24
Zone: Untrust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: peer-2
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.3.1.0/24
Zone: Untrust

4. VPN

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (**選択**)
Gateway Name: gw1
Type: Static IP: (**選択**), Address/Hostname: 2.2.2.2
Preshared Key: device1
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to Tunnel Interface: (**選択する**), tunnel.1
Proxy-ID: (**選択**)
Local IP / Netmask: 0.0.0.0/0
Remote IP / Netmask: 0.0.0.0/0
Service: ANY

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn2
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (**選択**)
Gateway Name: gw2
Type: Static IP: (**選択**), Address/Hostname: 3.3.3.3
Preshared Key: device2
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Bind to Tunnel Interface: (**選択**), tunnel.2
Proxy-ID: (**選択**)
Local IP / Netmask: 0.0.0.0/0
Remote IP / Netmask: 0.0.0.0/0
Service: ANY

5. **ルート**
   Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 10.2.1.0/24
   Gateway: (選択)
   Interface: tunnel.1
   Gateway IP Address: 0.0.0.0

   Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 10.3.1.0/24
   Gateway: (選択)
   Interface: tunnel.2
   Gateway IP Address: 0.0.0.0

   Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選択)
   Interface: ethernet3
   Gateway IP Address: 1.1.1.250

6. **ポリシー**
   Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), peer-1
   Destination Address:
   Address Book Entry: (選択), MIP(10.100.1.5)
   Service: ANY
   Action: Permit

   Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), peer-2
   Destination Address:
   Address Book Entry: (選択), MIP(10.100.1.5)
   Service: ANY
   Action: Permit

   Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), local_lan
   Destination Address:
   Address Book Entry: (選択), Any
   Service: ANY
   Action: Permit

CLI

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface loopback.3 zone trust
set interface loopback.3 ip 10.100.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.10.1.1/24
set interface tunnel.1 loopback-group loopback.3
set interface tunnel.2 zone untrust
set interface tunnel.2 ip 10.20.1.1/24
set interface tunnel.2 loopback-group loopback.3
```

2. MIP

```
set interface loopback.3 mip 10.100.1.5 host 10.1.1.5 netmask
    255.255.255.255 vrouter trust-vr
```

注 : 特に指定しなければ、MIP のネットマスクは 32 ビット (255.255.255.255)、仮想ルーターは trust-vr となります。したがって、コマンドで明示的に指定する必要はありません。この設定例では、WebUI による設定と対称性を持たせるため、引数に含まれています。

---

3. アドレス

```
set address trust local_lan 10.1.1.0/24
set address untrust peer-1 10.2.1.0/24
set address untrust peer-2 10.3.1.0/24
```

4. VPN

```
set ike gateway gw1 address 2.2.2.2 outgoing-interface ethernet3 preshare
    device1 sec-level compatible
set vpn vpn1 gateway gw1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set ike gateway gw2 address 3.3.3.3 outgoing-interface ethernet3 preshare
    device2 sec-level compatible
set vpn vpn2 gateway gw2 sec-level compatible
set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

5. ルート

```
set vrouter trust-vr route 10.2.1.0/24 interface tunnel.1
set vrouter trust-vr route 10.3.1.0/24 interface tunnel.2
set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

6. ポリシー

```
set policy top from untrust to trust peer-1 mip(10.100.1.5) any permit
set policy top from untrust to trust peer-2 mip(10.100.1.5) any permit
set policy from trust to untrust local_lan any any permit
save
```

MIP グルーピング

MIP をインターフェースに割り当てると、宛先アドレスに使用するために IP アドレスの範囲が確保され、インターフェースを通過するパケット用に使われます。MIP をポリシーに使用することができ、それによりアドレスはパケットを受信するインターフェースに認識され、また出力パケットを送信するインターフェースのために使用できます。

しかしながら、単一ポリシーの複数の MIP を呼び出す必要が生じる状況もあります。例えば、単一のアドレス範囲では、特定のネットワークトポロジーにおいて、多くの宛先ホストまたはゲートウェイがあり、アドレスを充分提供できない場合があります。このような場合は *MIP グルーピング* を行う必要があり、これにより *マルチセルポリシー* を設計することができます。このようなポリシーでは、可能性のあるソースアドレスとして、複数のアドレス範囲を呼び出します。

例 : マルチセルポリシーにおける MIP グルーピング

次の例では、異なる 2 つの MIP アドレス定義を使用するポリシーを作成します (1.1.1.3 と 1.1.1.4)。

注 : この例では、作成したポリシーのポリシー ID が 104 だとします。

WebUI

Network > Interfaces > Edit > MIP (List)

Policies > New

CLI

```
set interface ethernet1/2 mip 1.1.1.3 host 2.2.2.2
set interface ethernet1/2 mip 1.1.1.4 host 3.3.3.3
set policy from untrust to trust any mip(1.1.1.3) any permit
set policy id 104
(policy:104)-> set dst-address mip(1.1.1.4)
(policy:104)-> exit
get policy id 104
```

注 : この例での最後の CLI コマンドを実行してから、次の表示を探して、確認します。

```
2 destinations: “MIP(1.1.1.3)”, “MIP(1.1.1.4)”
```

仮想 IP アドレス

仮想 IP (VIP) アドレスには、ある IP アドレスに届いたトラフィックを、TCP セグメントヘッダーや UDP データグラムヘッダー中の宛先ポート番号にもとづいて、別のアドレスにマップする働きがあります。たとえば、

- 1.1.1.3:80 向け (詳しくいうと IP アドレスが 1.1.1.4、ポート番号が 80) の HTTP パケットを、10.1.1.10 の Web サーバー宛にマップ。
- 1.1.1.3:21 向けの FTP パケットを、10.1.1.20 の FTP サーバー宛にマップ。
- 1.1.1.3:25 向けの SMTP パケットを、10.1.1.30 のメールサーバー宛にマップ。

いずれの場合も、元々の宛先 IP アドレスは同じです。セキュリティデバイスは、宛先ポート番号によって転送先ホストを振り分けます。

図 38: Virtual IP Address (仮想 IP アドレス)

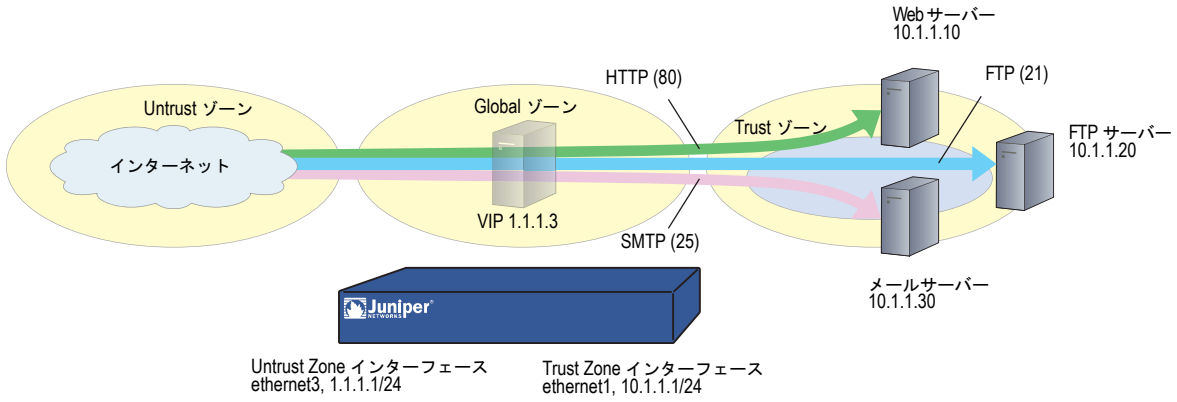


表 2: 仮想 IP 転送テーブル

Untrust ゾーンのインターフェース IP	Global ゾーンの VIP	ポート	転送	Trust ゾーンのホスト IP
1.1.1.1/24	1.1.1.3	80 (HTTP)		10.1.1.10
1.1.1.1/24	1.1.1.3	21 (FTP)		10.1.1.20
1.1.1.1/24	1.1.1.3	25 (SMTP)		10.1.1.30

セキュリティデバイスは、宛先が VIP であるトラフィックを受け取ると、その VIP に対応するアドレスのホストに転送します。ただし、VIP ホストがアウトバウンドトラフィックを発信した場合、事前に ingress インターフェース上に NAT か、またはホストから発信されるトラフィックに適用するポリシーに NAT-src が設定されていれば、セキュリティデバイスは元のソース IP アドレスを別のアドレスに変換します。そうでない場合は、VIP ホストを起点とするトラフィック上では ソース IP アドレスを変換しません。

仮想 IP の定義には次のような情報が必要です。

- VIP の IP アドレスは、Untrust ゾーンのインターフェースと同じサブネットになければならず、また、セキュリティデバイスによっては、そのインターフェースと同じアドレスでも構いません。

セキュリティデバイスの機種によっては、Untrust ゾーンのインターフェースが、DHCP または PPPoE 経由で、動的に IP アドレスを取得できます。このような状況において VIP を利用したい場合は、WebUI (Network > Interfaces > Edit （ Untrust ゾーンのインターフェースの場合） > VIP を使用して、以下のどちらかを行います。

- 複数の VIP に対応したデバイスで、Untrust ゾーンインターフェースと同じ IP アドレスを VIP に割り当てた場合、他の「普通に設定した」VIP は使えなくなります。
- 逆に、普通に設定した VIP がある場合は、それを削除しない限り、Untrust ゾーンインターフェースと同じ IP アドレスの VIP は設定できません。

- 要求を処理するサーバーの IP アドレス
- VIP から所定のホストの IP アドレスに転送したいサービスのタイプ

注 : VIP を設定できるインターフェースは Untrust ゾーンに限ります。

VIP に特有の留意事項

- 1 台のホストで複数のサーバープロセスを稼動している場合、「よく知られているサービス」に対する仮想ポート番号を設定できます。たとえば同じホスト上で FTP サーバーを 2 つ動かし、一方に 21 番、もう一方に 2121 番を割り当てる、という具合です。2 つめの FTP サーバーにアクセスするためには、仮想ポート番号をあらかじめ知っていて、パケットヘッダーにその番号を設定しなければなりません。
- 定義済みサービスばかりでなく、ユーザー定義のサービスについてもマッピングは可能です。
- ソースおよび宛先ポート番号が同じであっても、トランスポートが違えば、1 つの VIP でカスタムサービスを区別できます。
- カスタムサービスで使う宛先ポート番号は、1,024 ～ 65,535 だけではなく、1 ～ 65,535 の範囲から選べます。
- 1 つの VIP で、複数のポートを使うカスタムサービスにも対応できます。デフォルトでは、VIP で単一ポートサービスを使用することができます。VIP で、複数ポートサービスを使用できるようにするには、まず CLI コマンド **set vip multi-port** を発行し、それからセキュリティデバイスをリセットします。(83 ページの「例 : カスタムサービス、複数のポートを使うサービスに対応した VIP」を参照してください。)
- セキュリティデバイスが VIP トラフィックをマップするホストは、trust-vr から到達可能でなければなりません。trust-vr 以外のルーティングドメインにある場合は、到達するためのルートを定義してください。

VIP と Global ゾーン

Untrust ゾーンのインターフェースに VIP を設定すると、Global ゾーンのアドレス帳にその情報が登録されます。どのゾーンに属するインターフェースの VIP も、すべて Global ゾーンのアドレス帳で管理することになるのです。2 つのゾーン間のトラフィックに関するポリシーでは、この VIP アドレスを宛先アドレスとして使えます。また、グローバル ポリシーを定義する場合にも、やはり宛先アドレスとして使うことができます

例 : 仮想 IP サーバーの設定

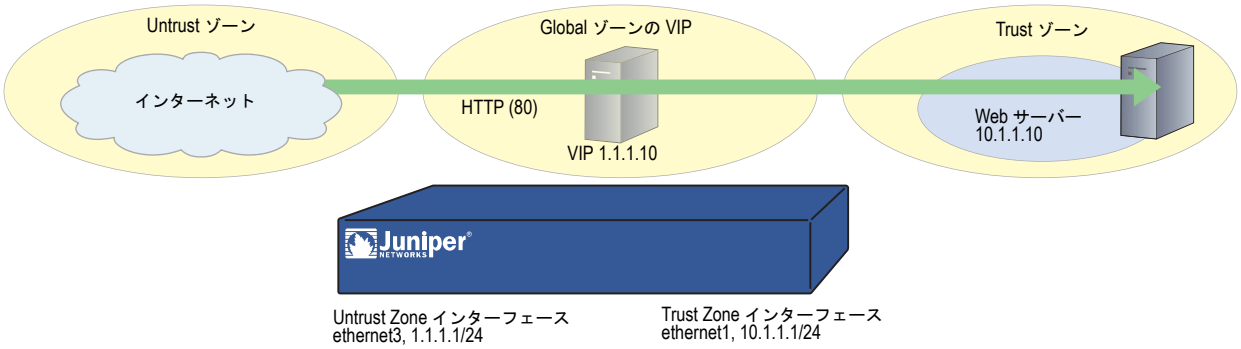
この例では、ethernet1 を Trust ゾーンにバインドし、IP アドレスとして 10.1.1.1/24 を割り当てます。また、ethernet3 を Untrust ゾーンにバインドし、1.1.1.1/24 という IP アドレスを割り当てます。

次に、1.1.1.10 に、インバウンド HTTP トラフィックを 10.1.1.10 の Web サーバーに転送する VIP を設定し、Untrust ゾーンから Trust ゾーンに属する VIP (したがって VIP が指すアドレスを持つホスト) へのトラフィックを許可するポリシーを定義します。

VIP は Untrust ゾーンインターフェース (1.1.1.0/24) と同じサブネットに属するので、Untrust ゾーンからのトラフィックが VIP に到達できるよう、ルートを定義する必要はありません。また、VIP によるトラフィックの転送先ホストについて、アドレス帳に登録する必要もありません。セキュリティゾーンはすべて trust-vr ルーティングドメインにあります。

注 : Untrust ゾーン以外のセキュリティゾーンからの HTTP トラフィックが VIP に到達できるようにしたい場合は、他のゾーンのルーターで 1.1.1.10 へのルートを設定して、当該ゾーンに向かうインターフェースを指すようにする必要があります。たとえば、ethernet2 がユーザー定義のゾーンに向かうインターフェースであり、当該ゾーンのルーターで、1.1.1.10 宛のトラフィックを ethernet2 に転送するよう設定済みであるとします。ルーターがトラフィックを ethernet2 に転送すると、セキュリティデバイスの転送機能が働き、ethernet3 上の VIP を見つけます。これによると 10.1.1.10 にマップすることになっているので、Trust ゾーンの ethernet1 に宛てて転送することになります。このしくみは、65 ページの「例 : 別のゾーンから MIP に到達するトラフィック」に解説したものと同様です。ソースのゾーンから Trust ゾーンの VIP に向けた HTTP トラフィックを許可するポリシーも設定しなければなりません。

図 39: 仮想 IP サーバー



WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24
   次のように選択してから **OK** をクリックします。
   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. **VIP**
   Network > Interfaces > Edit (ethernet3) > VIP: 次のように入力してから **Add** をクリックします。

   Virtual IP Address: 1.1.1.10

   Network > Interfaces > Edit (ethernet3) > VIP > New VIP Service: 次のように入力してから **OK** をクリックします。

   Virtual IP: 1.1.1.10
   Virtual Port: 80
   Map to Service: HTTP (80)
   Map to IP: 10.1.1.10

3. **ポリシー**
   Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), ANY
   Destination Address:
   Address Book Entry: (選択), VIP(1.1.1.10)
   Service: HTTP
   Action: Permit

CLI

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet2 ip 1.1.1.1/24

2. **VIP**
   set interface ethernet3 vip 1.1.1.10 80 http 10.1.1.10

3. **ポリシー**
   set policy from untrust to trust any vip(1.1.1.10) http permit
   save

例 : VIP 設定の編集

この例では、上述の例で構築した仮想 IP サーバーの設定を変更します。Web サーバーへのアクセスを制限するため、HTTP トラフィック用の仮想ポート番号を、デフォルト値の 80 番から 2211 番に変更します。これにより、2211 というポート番号を知らなければ、Web サーバーにアクセスできなくなります。

WebUI

Network > Interfaces > Edit (ethernet3) > VIP > Edit （ 1.1.1.10 に関する VIP サービス設定セクション ）: 次のように入力してから **OK** をクリックします。

Virtual Port: 2211

CLI

```
unset interface ethernet3 vip 1.1.1.10 port 80
set interface ethernet3 vip 1.1.1.10 2211 http 10.1.1.10
save
```

例 : VIP 設定の削除

この例では、先に作成、変更した VIP 設定を削除します。VIP の削除に先立ち、これに関連するポリシーをすべて削除しておかなければなりません。81 ページの「例 : 仮想 IP サーバーの設定」で作成したポリシーの ID 番号は 5 です。

WebUI

Policies > (From: Untrust, To: Trust) > Go: ID 番号 5 番のポリシーに対応する **Remove** をクリックします。

Network > Interfaces > Edit (ethernet3) > VIP: 1.1.1.10 に関する VIP 設定セクションの **Remove** をクリックします。

CLI

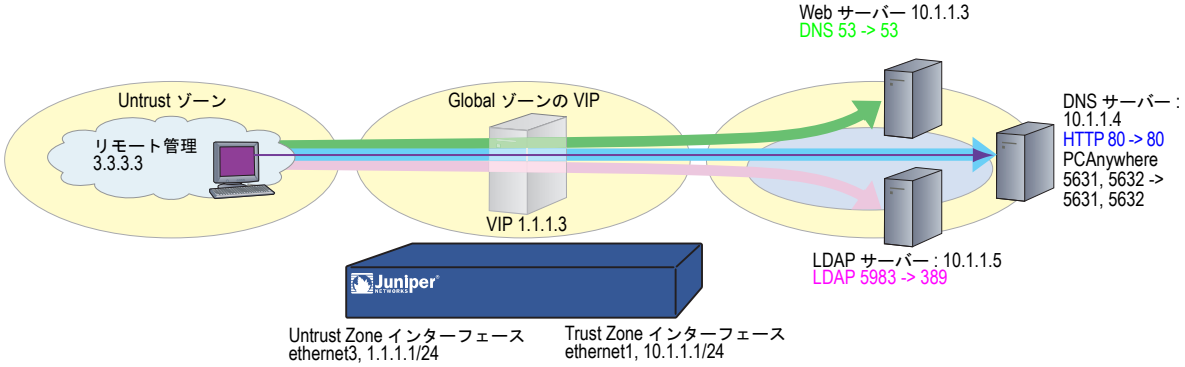
```
unset policy id 5
unset interface ethernet3 vip 1.1.1.10
save
```

例 : カスタムサービス、複数のポートを使うサービスに対応した VIP

この例では、次のように各サービスを各内部アドレスに転送するよう、1.1.1.3 で VIP を設定します。

サービス	トランスポート	仮想ポート番号	実際のポート番号	ホスト IP アドレス
DNS	TCP, UDP	53	53	10.1.1.3
HTTP	TCP	80	80	10.1.1.4
PCAnywhere	TCP, UDP	5631, 5632	5631, 5632	10.1.1.4
LDAP	TCP, UDP	5983	389	10.1.1.5

図 40: カスタムサービス、複数のポートを使うサービスに対応した VIP



VIP は、DNS の検索要求を 10.1.1.3 の DNS サーバーに、HTTP トラフィックを 10.1.1.4 の Web サーバーに、認証要求を 10.1.1.5 の LDAP サーバーで動作するデータベースにそれぞれ転送します。HTTP、DNS、PCAnywhere については、仮想ポート番号は実際のポート番号と同じです。LDAP の場合は、LDAP 認証トラフィックのセキュリティを少しでも向上するため、5983 番という仮想ポート番号を使います。

HTTP サーバーをリモート管理するため、カスタムサービスを定義し、PCAnywhere と名付けます。これは複数のポートを使うサービスで、データの送信や監視には TCP の 5631 番ポート、状態確認には UDP の 5632 番ポートを使います。

さらに、リモート管理のアドレスとして 3.3.3.3 を Untrust ゾーンのアドレス帳に登録し、Untrust ゾーンから Trust ゾーンに向かうトラフィックのうち、VIP を使うものに関するポリシーを定義します。セキュリティゾーンはすべて trust-vr ルーティングドメインにあります。

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 10.1.1.1/24

   次のように選択してから **OK** をクリックします。

   Interface Mode: NAT

   Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   Static IP: (ある場合は選択する)
   IP Address/Netmask: 1.1.1.1/24

2. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: **リモート管理**
IP Address/Domain Name:
IP/Netmask: (**選択**), 3.3.3.3/32
Zone: Untrust

3. 顧客サービス

Policy > Policy Elements > Services > Custom > New: 次のように入力してから **OK** をクリックします。

Service Name: PCAnywhere
No 1:
Transport protocol: TCP
Source Port Low: 0
Source Port High: 65535
Destination Port Low: 5631
Destination Port High: 5631
No 2:
Transport protocol: UDP
Source Port Low: 0
Source Port High: 65535
Destination Port Low: 5632
Destination Port High: 5632

4. VIP アドレス、サービス

注 : 複数のポートを使うサービスに VIP が対応できるよう、あらかじめ CLI コマンド **set vip multi-port** を実行し、設定を保存した上でデバイスを再起動してください。

Network > Interfaces > Edit (ethernet3) > VIP: click here to configure: Virtual IP Address フィールドに **1.1.1.3** と入力し **Add** をクリックします。

> New VIP Service: 次のように入力してから **OK** をクリックします。

Virtual IP: 1.1.1.3
Virtual Port: 53
Map to Service: DNS
Map to IP: 10.1.1.3

> New VIP Service: 次のように入力してから **OK** をクリックします。

Virtual IP: 1.1.1.3
Virtual Port: 80
Map to Service: HTTP
Map to IP: 10.1.1.4

> New VIP Service: 次のように入力してから **OK** をクリックします。

Virtual IP: 1.1.1.3
Virtual Port: 5631
Map to Service: PCAnywhere
Map to IP: 10.1.1.4

注： 複数のポートを使うサービスの場合、最小の仮想ポート番号を指定します。

> New VIP Service: 次のように入力してから **OK** をクリックします。

Virtual IP: 1.1.1.3
Virtual Port: 5983
Map to Service: LDAP
Map to IP: 10.1.1.5

注： 標準以外のポート番号を使うと、セキュリティを多少改善できます。標準ポート番号を使ったサービスが稼動していないか総当り的に調べるという、よくある攻撃を回避できるからです。

5. ポリシー

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), VIP(1.1.1.3)
Service: DNS
Action: Permit

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), VIP(1.1.1.3)
Service: HTTP
Action: Permit

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), VIP(1.1.1.3)
Service: LDAP
Action: Permit

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Remote Admin
Destination Address:
Address Book Entry: (選択), VIP(1.1.1.3)
Service: PCAnywhere
Action: Permit

CLI

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **[Address]**
   set address untrust “Remote Admin” 3.3.3.3/32

3. **顧客サービス**
   set service pcanywhere protocol udp src-port 0-65535 dst-port 5631-5631
   set service pcanywhere + tcp src-port 0-65535 dst-port 5632-5632

4. **VIP アドレス、サービス**
   set vip multi-port
   save
   reset
   System reset, are you sure? y/[n]
   set interface ethernet3 vip 1.1.1.3 53 dns 10.1.1.3
   set interface ethernet3 vip 1.1.1.3 + 80 http 10.1.1.4
   set interface ethernet3 vip 1.1.1.3 + 5631 pcanywhere 10.1.1.4
   set interface ethernet3 vip 1.1.1.3 + 5983 ldap 10.1.1.5

注 : 複数のポートを使うサービスの場合、最小の仮想ポート番号を指定します。

5. **ポリシー**
   set policy from untrust to trust any vip(1.1.1.3) dns permit
   set policy from untrust to trust any vip(1.1.1.3) http permit
   set policy from untrust to trust any vip(1.1.1.3) ldap permit
   set policy from untrust to trust “Remote Admin” vip(1.1.1.3) pcanywhere permit
   save

索引

C

CLI 、vip マルチポートを設定 80

D

DIP プール
- NAT-Src 1
- アドレスに関する留意点 14
- サイズ 14

I

IP アドレス、仮想 79

M

MIP 61
- Global ゾーン 62
- Untrust ゾーンとして扱うインターフェース 69–71
- アドレス範囲 64
- グルーピング、マルチセルポリシー 78
- 他のゾーンから到達可能 65
- 定義 6
- 両方向の変換 6

MIP 作成
- アドレス 63
- ゾーンインターフェース上に 63
- トンネルインターフェース上に 68

MIP 、デフォルト MIP
- 仮想ルーター 64
- ネットマスク 64

N

NAT
- NAT-src と NAT-dst 49–60
- 定義 1

NAT-dst 28–60
- MIP や VIP との同時使用 4
- アドレスシフティング 5
- 一方向の変換 7, 10
- パケットフロー 29–31
- ポートマッピング 4, 28, 46
- ルートに関する留意点 29, 32–34

NAT-dst, 、アドレス
- 1 対多の変換 38
- シフティング 28, 43
- 所定の範囲の IP アドレスを特定の IP アドレスに変換 10, 40
- 範囲 4
- 範囲から範囲 10, 43

NAT-dst 、単一 IP
- ポートマッピング 9
- ポートマッピングなし 9

NAT-dst, 、アドレス
- 1 対 1 の変換 35

NAT-Src 1, 13–25
- egress インターフェース 23–25
- インターフェースベース 2
- 固定ポートナンバー 14

NAT-src 、DIP プール 1
- PAT あり 7, 14–17
- アドレスシフトで変換 8
- 固定ポートナンバー 8

NAT-src 、アドレス
- シフティング 19–23
- シフティング、範囲に関する留意点 20

NAT-src 、変換
- 一方向 7, 10
- ポートアドレス 2

P

PAT 14

V

VIP
- グローバルゾーン 81
- 構成 81
- 削除 83
- 他のゾーンから到達可能 81
- 定義 6
- 必要な情報 79
- 編集 83

VIP サービス
- カスタムおよび複数のポート 83–87
- カスタム、低いポートナンバー 80

あ
アドレス変換
NAT, NAT-dst および NAT-src を参照

い
インターフェース
MIP....62
VIP....79

か
仮想 IP
VIP を参照

く
グローバルゾーン....81

せ
セキュリティデバイス....9

そ
ゾーン、グローバル....81

ね
ネットマスク、MIP デフォルト、MIP....64

は
パケットフロー、NAT-Dst....29–31

ほ
ポート
番号....86
マッピング....4, 28
ポリシーベースの NAT
NAT-dst と NAT-src を参照

ま
マップド IP
MIP を参照

概念と用例
ScreenOS リファレンス ガイド

第 9 部 :
ユーザー認証

リリース 6.0.0、改訂 02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

品番 : 530-017775-01-JP, 改訂 02

Copyright Notice

Copyright © 2007 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

目次

本編について vii

ドキュメントの規則 viii
Web ユーザーインターフェースの規則 viii
コマンドラインインターフェースの規則 viii
ネーミング規則および文字タイプ ix
説明図の規則 x
技術ドキュメントおよびテクニカルサポート xi

第 1 章 認証 1

ユーザー認証タイプ 1
管理ユーザー 2
複数タイプユーザー 3
グループ式 4
例 : グループ式 (AND) 5
例 : グループ式 (OR) 7
例 : グループ式 (NOT) 8
バナーのカスタマイズ 9
例 : WebAuth バナーのカスタマイズ 9
ログインバナー 10
例 : ログインバナーの作成 10

第 2 章 認証サーバー 11

認証サーバータイプ 12
ローカルデータベース 13
例 : ローカルデータベースタイムアウト 14
外部認証サーバー 15
認証サーバーオブジェクトプロパティ 16
認証サーバータイプ 17
リモート認証ダイヤルインユーザーサービス 17
RADIUS 認証サーバーオブジェクトプロパティ 18
サポートされるユーザータイプと機能 18
RADIUS ディクショナリーファイル 19
認証および XAuth ユーザーにサポートされている RADIUS 拡張機能 22
SecurID 25
SecurID 認証サーバーオブジェクトプロパティ 26
サポートされるユーザータイプと機能 26
軽量ディレクトリアクセスプロトコル 27
LDAP 認証サーバーオブジェクトプロパティ 28
サポートされるユーザータイプと機能 28
TACACS+ (Terminal Access Control Access Control System Plus) 28
TACACS+ サーバーオブジェクトプロパティ 30
管理認証の優先 30

認証サーバーオブジェクトの定義 31
例 : RADIUS 認証サーバー 31
例 : SecurID 認証サーバー 33
例 : LDAP 認証サーバー 35
例 : TACACS+ 認証サーバー 36
デフォルト認証サーバーの定義 37
例 : デフォルト認証サーバーの変更 37

第 3 章 インフラネットの認証 39

統合型アクセス管理ソリューション 40
ファイアウォールとインフラネットコントローラの連携 41
インフラネット認証用の構成 42

第 4 章 認証ユーザー 43

ポリシーで認証ユーザーを参照する 44
ランタイム認証 44
事前ポリシーチェック認証 (WebAuth) 45
ポリシーでの認証ユーザーグループの参照 46
例 : ランタイム認証 (ローカルユーザー) 47
例 : ランタイム認証 (ローカルユーザーグループ) 48
例 : ランタイム認証 (外部ユーザー) 49
例 : ランタイム認証 (外部ユーザーグループ) 51
例 : 複数グループのローカル認証ユーザー 53
例 : WebAuth (ローカルユーザーグループ) 55
例 : WebAuth (外部ユーザーグループ) 57
例 : WebAuth + SSL のみ (外部ユーザーグループ) 59

第 5 章 IKE、XAuth、および L2TP ユーザー 63

IKE ユーザーとユーザーグループ 63
例 : IKE ユーザーの定義 64
例 : IKE ユーザーグループの作成 65
ゲートウェイの IKE ユーザーを参照 66
XAuth ユーザーとユーザーグループ 66
IKE モードのイベントロギング 67
IKE ネゴシエーションの XAuth ユーザー 68
例 : XAuth 認証 (ローカルユーザー) 70
例 : XAuth 認証 (外部ユーザー) 72
XAuth クライアント 81
例 : XAuth クライアントとしてのセキュリティデバイス 81
L2TP ユーザーとユーザーグループ 82
例 : ローカルおよび外部 L2TP 認証サーバー 82

第 6 章 ワイヤレスおよびイーサネットインターフェース用の拡張認証 87

概要 88
サポートされている EAP のタイプ 88
802.1X 認証を使用可能または使用不可能にする 89
イーサネットインターフェース 89
ワイヤレスインターフェース 89
802.1X 設定の構成 90
802.1X ポート制御の構成 90
802.1X 制御モードの構成 91
同時ユーザーの最大数の設定 91

802.1X 設定の構成（続き）
再認証期間の設定 92
EAP 再送信を使用可能にする 92
EAP 再送信回数の構成 93
EAP 再送信期間の構成 93
サイレント（沈黙）期間の構成 93
認証サーバーオプションの構成 94
認証サーバーの指定 94
イーサネットインターフェース 94
アカウントタイプの設定 95
ゾーン確認を使用可能にする 95
802.1X 情報の表示 96
802.1X グローバル構成情報の表示 96
インターフェースの 802.1X 情報の表示 96
802.1X 統計の表示 97
802.1X セッション統計の表示 97
802.1X セッション詳細の表示 98
設定例 98
直接接続しているクライアントと RADIUS サーバーを持った
セキュリティデバイスの構成 98
クライアントとセキュリティデバイスの間にハブを持ったセ
キュリティデバイスの構成 99
ワイヤレスインターフェースを持った認証サーバーの構成 101

索引 ..... IX-I

本編について

*第9 部 : ユーザー認証*では、ScreenOS における異なるユーザータイプの認証方法について説明します。ユーザー認証について紹介し、ユーザープロファイルを保存できる 2 つの場所（内部データベースおよび外部認証サーバー）を説明した後は、認証、IKE、XAuth、L2TP ユーザーおよびユーザーグループの認証の構成例を多数示します。ログインバナーの変更、複数タイプユーザーの作成 (IKE/XAuth ユーザーなど)、認証を適用するポリシーのグループ表現の使用方法など、その他のユーザー認証アスペクトについても説明します。

本編の章は、以下のようになります。

- 第 1 章「認証」では、ScreenOS がサポートする様々な認証方法とその用途について説明します。
- 第 2 章「認証サーバー」では、外部認証サーバーとなる可能性のある RADIUS、SecurID、TACACS + 、LDAP の 4 種類のうちのいずれか 1 つあるいは内部データベースを使用するオプションについて説明し、さらにそれぞれと連動させるためのセキュリティデバイスの構成方法について説明します。
- 第 3 章「インフラネットの認証」では、統合型アクセス制御（UAC）ソリューションで、セキュリティデバイスが配備される方法を詳説します。Juniper Networks UAC は、企業インフラネットを横断したアプリケーションおよびサービスの配布を、安全、確実に行います。
- 第 4 章「認証ユーザー」では、認証ユーザーのプロファイルを定義する方法と、ローカルまたは RADIUS 認証サーバーのどちらかに格納されているユーザーグループに認証ユーザーを追加する方法を説明しています。
- 第 5 章「IKE、XAuth、および L2TP ユーザー」では、IKE ユーザー、XAuth ユーザー、および L2TP ユーザーを定義する方法について説明しています。XAuth セクションではセキュリティデバイスを XAuth サーバーとして使用する方法を中心に説明していますが、サブセクションで高性能なセキュリティデバイスを XAuth クライアントとして動作させるための構成方法についても説明します。
- 第 6 章「ワイヤレスおよびイーサネットインターフェース用の拡張認証」、では、Ethernet およびワイヤレスインターフェースの認証を行う、拡張認証プロトコルで利用可能なオプションを説明します。

ドキュメントの規則

このドキュメントは、次のセクションで説明されている規則を使用しています。

- viii ページの「Web ユーザーインターフェースの規則」
- viii ページの「コマンドラインインターフェースの規則」
- ix ページの「ネーミング規則および文字タイプ」
- x ページの「説明図の規則」

Web ユーザーインターフェースの規則

WebUI（Web ユーザーインターフェース）では、各作業の操作指示は、操作手順と構成設定値に分かれています。構成設定を入力できる WebUI ページを開くには、画面の左側にあるナビゲーション ツリーのメニュー項目をクリックして、そのページに移動します。先へ進むと、ナビゲーション パスが画面の上部に表示されます。各ページは角括弧で分離されています。

WebUI のパスおよびアドレスを定義するためのパラメータは、以下のとおりです。

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.2.2.5/32
Zone: Untrust

構成設定のオンラインヘルプを開くには、画面の左上にある疑問符（?）をクリックします。

ナビゲーションツリーにも、Help > Config Guide 構成ページがあり、セキュリティポリシーおよび IPSec （インターネットプロトコルセキュリティ）の構成に役立ちます。ドロップダウンメニューからオプションを選択して、そのページの指示に従います。構成設定のオンラインヘルプを開くには、左上にある **?** 文字をクリックします。

コマンドラインインターフェースの規則

次の規則は、例とテキストにおいて、コマンドラインインターフェース（CLI）コマンドの構文を示すために使用されます。

例においては、次のように使用されます。

- 角括弧 [ ] 内にあるものはすべてオプションです。
- 中括弧 { } 内にあるものはすべて必須です。
- 選択肢が複数ある場合、各選択肢はパイプ (|) で区切られています。例えば、次のように表示されます。

```
set interface { ethernet1 | ethernet2 | ethernet3 } manage
```

- 変数は*斜体*で表示されます。

  set admin user *name1* password *xyz*

テキストにおいては、コマンドは**太字**で、変数は*斜体*で表示されます。

注： キーワード入力時には、単語を間違いなく識別できる数の文字を入力すれば十分です。**set admin user wheezer j12fmt54** というコマンドを入力する際には、**set adm u whee j12fmt54** と入力するだけで十分です。ただし、本編に記載されたコマンドはすべて本来の形式で記載されています。

ネーミング規則および文字タイプ

ScreenOS はオブジェクトの名前 (アドレス、管理ユーザー、認証サーバー、IKE ゲートウェイ、仮想システム、VPN トンネルおよびゾーンなど、ScreenOS 構成に定義されているもの) に関して、次の規則に従います。

- 名前文字列に 1 つまたは複数のスペースが含まれる場合、文字列全体を二重引用符で囲む必要があります。例 :

  set address trust “local LAN” 10.1.1.0/24

- 二重引用符で囲まれた文字列の先頭または末尾のスペースを取り除きます。たとえば、**「 local LAN 」**は**「local LAN」**となります。

- 連続した複数のスペースは、一つのスペースとして扱われます。

- CLI キーワードの多くはケースセンシティブではありませんが、名前文字列はケースセンシティブです。たとえば、**「local LAN」**は**「local lan」**とは異なります。

ScreenOS は、次の文字タイプをサポートします。

- 1 バイト文字セット (SBCS) およびマルチバイト文字セット (MBCS)。SBCS の例に、ASCII、欧州言語、およびヘブライ語があります。2 バイト文字セット (DBCS) とも呼ばれる MBCS の例に、中国語、韓国語、および日本語があります。

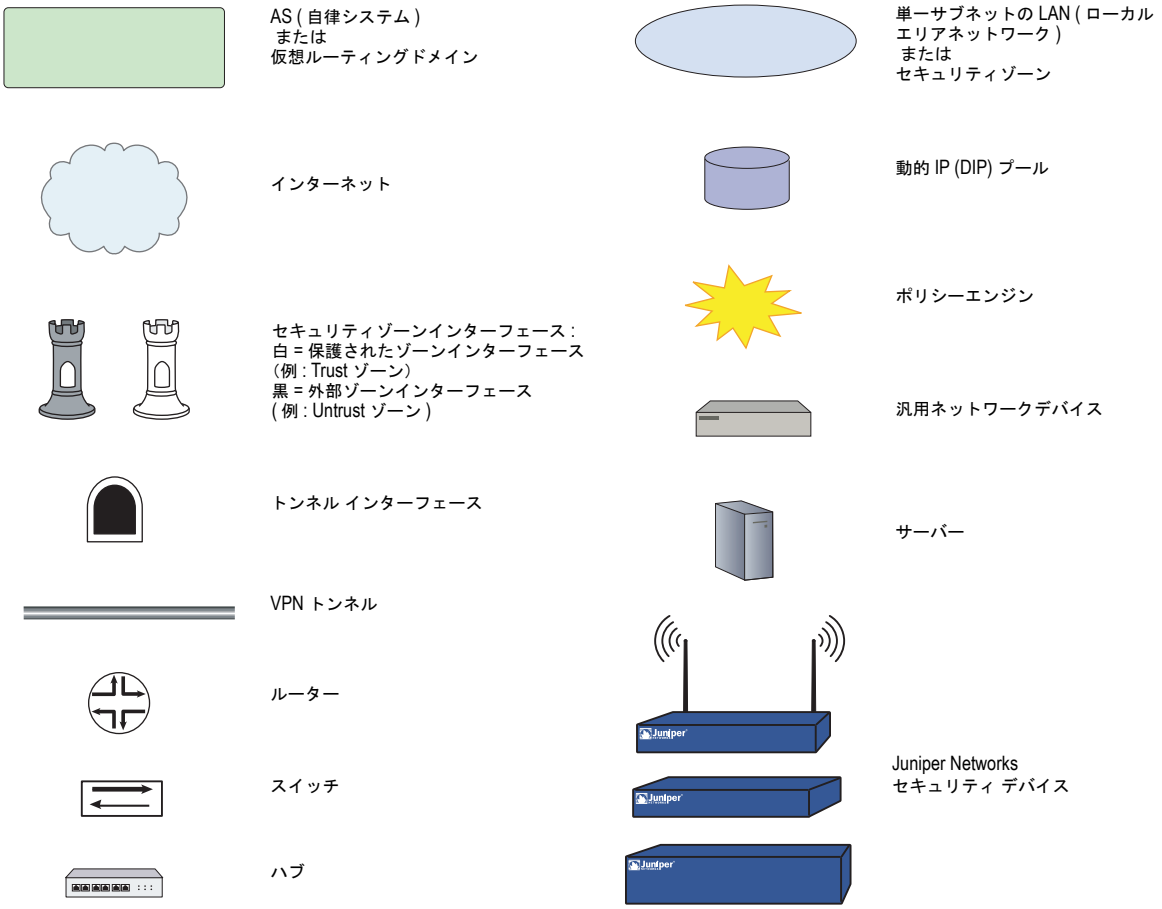
- ASCII 文字の 32（16 進数の 0x20）から 255（0xff)。ただし二重引用符 (“) は、スペースを含む名前文字列の先頭と末尾を示す特殊な意味をもつため、例外とします。

注： コンソール接続では、SBCS のみがサポートされます。ご利用のブラウザがサポートする文字セットに応じて、WebUI は SBCS および MBCS の両方をサポートします。

説明図の規則

次の図は、本編を通して説明図に使用されている画像の基本的なものです。

図 1: 説明図の画像



技術ドキュメントおよびテクニカルサポート

Juniper Networks 製品のいずれかの技術ドキュメントを入手するには、www.juniper.net/techpubs/ をご覧になってください。

テクニカルサポートについては、http://www.juniper.net/customers/support/ にある Case Manager を使って事例サポートを開くか、1-888-314-JTAC (米国内) か 1-408-745-9500 (その他の国) までお問い合わせください。

本書に間違いや欠落があった場合は、techpubs-comments@juniper.net までお知らせください。

第 1 章
認証

さまざまな種類のネットワークユーザーが利用できる認証タイプについての概要を紹介しましたので、本章では、管理ユーザー認証に関する簡単なセクションを取り扱います。また、異なるユーザータイプの組み合わせ、グループ式の利用、HTTP、FTP、L2TP、Telnet、XAuth ログインプロンプトで表示されるバナーのカスタマイズ方法についても説明します。最終のセクションでは、大きな 4 キロバイトのバナーを作成する方法を説明します。このバナーは、個々に定義された管理アクセスバナーおよびファイアウォール認証バナーよりも優先的に使用されます。本章のセクションは、以下のようになります。

- 1 ページの「ユーザー認証タイプ」
- 2 ページの「管理ユーザー」
- 3 ページの「複数タイプユーザー」
- 4 ページの「グループ式」
- 9 ページの「バナーのカスタマイズ」
- 10 ページの「ログインバナー」

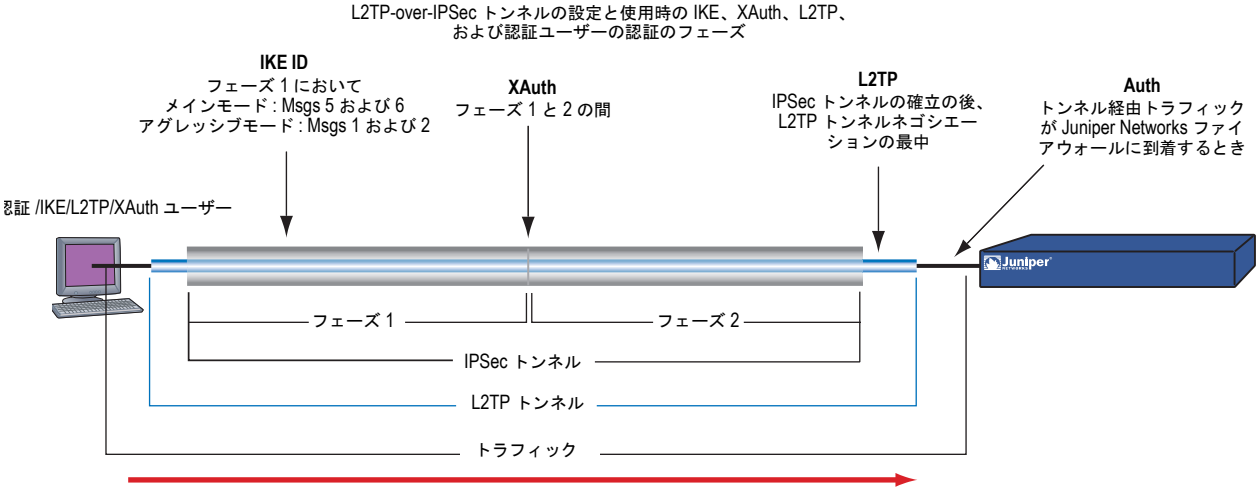
ユーザー認証タイプ

以下の章は、作成できる異なったタイプのユーザーおよびユーザーグループの説明と、ポリシー、IKE ゲートウェイ、および L2TP トンネルの構成時の使用方法を説明します。

- 43 ページの「認証ユーザー」
- 63 ページの「IKE ユーザーとユーザーグループ」
- 66 ページの「XAuth ユーザーとユーザーグループ」
- 82 ページの「L2TP ユーザーとユーザーグループ」

セキュリティデバイスは、各種のユーザーを接続プロセスの各フェーズで認証します。IKE 、XAuth 、L2TP および認証ユーザー認証技術は、L2TP-over-IPSec VPN トンネル作成中の異なる時間で生じます。2 ページの図 1 を参照してください。

図 1: L2TP-over-IPSec VPN トンネル中の認証



注 : XAuth と L2TP の両方ともがユーザー認証とアドレス割り当てを行うため、めったに一緒に使われることはありません。この 2 つは、VPN トンネルの作成時にどのようにそれぞれのタイプの認証が行われるかを示す目的でここでは一緒に示されています。

管理ユーザー

管理ユーザーはセキュリティデバイスの管理者です。管理ユーザーには 5 種類あります。

- ルート管理者
- ルートレベル読取 / 書込管理者
- ルートレベル読取専用管理者
- Vsys 管理者
- Vsys 読込専用管理

注 : 各タイプの管理ユーザーの権限と管理ユーザーの作成、変更、削除に関する情報は、3-1 ページの「管理」を参照してください。

セキュリティデバイスのルートユーザーのプロファイルは、ローカルデータベースに保存される必要がありますが、vsys ユーザーと読取 / 書込および読取専用権限を持ったルートレベルの管理ユーザーはローカルデータベースまたは外部認証サーバーに保存することができます。

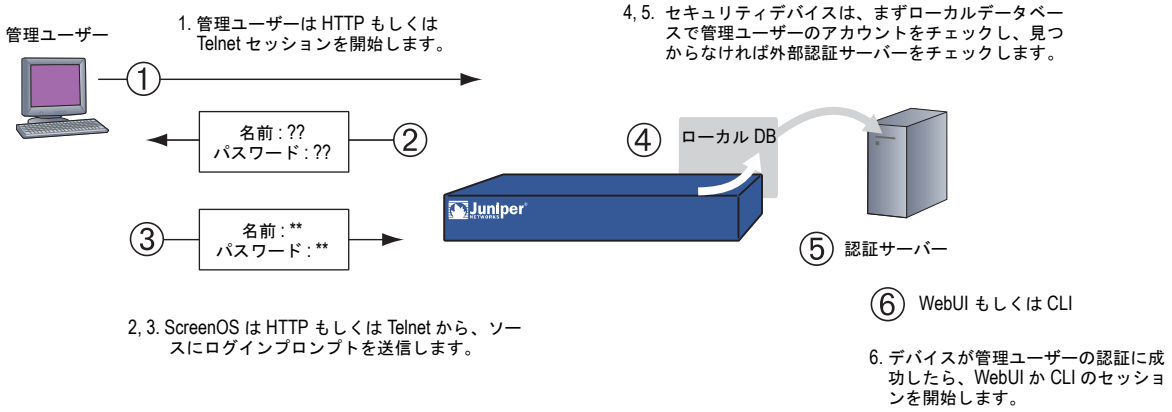
外部 RADIUS 認証サーバーに管理ユーザーアカウントを保存して、RADIUS ディクショナリーファイルを認証サーバーにロードした場合、サーバーで定義した管理権限を検索するよう選択できます。また、その認証サーバーに保存されたすべての管理ユーザーにグローバルで適用する権限レベルを指定するオプションもあります。読取 / 書込、または読取専用権限を指定することができます。管理ユー

ザーを外部 SecurID か LDAP 認証サーバーまたは RADIUS ディクショナリーファイルがない RADIUS サーバーに保存した場合、認証サーバーで管理ユーザーの権限を定義できません。したがって、セキュリティデバイスで権限レベルを割り当てる必要があります。

セキュリティデバイス上で設定される場合 :	そして RADIUS サーバーに RADIUS ディクショナリーファイルがロードされている場合には :	および SecurID、LDAP、または RADIUS ディクショナリーファイルがロードされていない RADIUS サーバーの場合には :
RADIUS サーバーから権限を得ます	適正な権限を割り当てる	ルートレベルもしくは vsys レベルの管理ログインが失敗する
外部管理者に読取 / 書込権限を割り当てる	ルートレベルもしくは vsys レベルの読取 / 書込権限を割り当てる	ルートレベル読取専用権限を割り当てる Vsys 管理者ログインが失敗する
外部管理者に読取専用権限を割り当てる	ルートレベルもしくは vsys レベルの読取専用権限を割り当てる	ルートレベル読取専用権限を割り当てる Vsys 管理者ログインが失敗する

図 2 は管理認証手順を示します。

図 2: 管理認証手順



複数タイプユーザー

認証、IKE、L2TP、XAuth ユーザーを組み合わせて、ローカルデータベースに保存する以下の組み合わせを作成することができます。

- 認証 / IKE ユーザー
- 認証 / IKE/XAuth ユーザー
- 認証 /L2TP ユーザー
- IKE/XAuth ユーザー
- 認証 /IKE/L2TP ユーザー
- L2TP/XAuth ユーザー
- IKE/L2TP ユーザー

- IKE/L2TP/XAuth ユーザー
- 認証 /XAuth ユーザー
- 認証 /IKE/L2TP/XAuth ユーザー

複数タイプユーザーアカウントをローカルデータベースで定義するときには、上記のすべての組み合わせを作成することはできますが、その前に以下の要件を考慮してください。

- IKE ユーザータイプとその他のいずれかのユーザータイプとを組み合わせる場合では、スケールのポテンシャルを制限します。IKE ユーザーアカウントは、ローカルデータベースに保存する必要があります。認証 /IKE、IKE/L2TP、および IKE/XAuth ユーザーアカウントを作成して、ユーザーの数がローカルデータベースの要領をオーバーするまで増えた場合には、それらのアカウントを外部認証サーバーに移転することはできません。IKE ユーザーアカウントを他のタイプのアカウントと分けておけば、非 IKE ユーザーアカウントを必要に応じて、外部認証サーバーに移動する柔軟性を持つことができます。
- L2TP および XAuth が同じサービスを提供する場合: リモートユーザー認証および IP、DNS サーバー、および WINS サーバーアドレス割り当て。L2TP-over-IPSec トンネルで L2TP と XAuth を併用することは推奨されません。2 つのプロトコルは同じ目的を達成するだけでなく、L2TP アドレス割り当ては、フェーズ 2 IKE ネゴシエーションが完了して L2TP ネゴシエーションが始まると XAuth アドレス割り当てを上書きしてしまいます。
- 認証 /L2TP と認証 /XAuth を組み合わせて、複数タイプユーザーアカウントをローカルデータベースに作成した場合、両方のログインで同じユーザー名とパスワードが使われなければなりません。

  単一の複数タイプユーザーアカウントを作成する方が便利ではありますが、ユーザータイプを 2 つの単一アカウントに分けることでセキュリティを強化することができます。たとえば、認証ユーザーアカウントは、外部 認証サーバーに、XAuth ユーザーアカウントはローカルデータベースに保存できます。そして、異なるログインユーザー名とパスワードをそれぞれのアカウントに割り当て、XAuth ユーザーを IKE ゲートウェイ構成で、認証ユーザーをポリシー構成で参照できます。ダイアルアップ VPN ユーザーは、場合によっては 2 つのまったく異なるユーザー名とパスワードで 2 回自身を認証する必要があります。

グループ式

グループ式は、ポリシーで、認証への要求を条件付にするために使用できるステートメントです。グループ式を使用すると、ユーザー、ユーザーグループ、他のグループ式を認証の代わり ("a" OR "b")、もしくは認証の要求事項 ("a" AND "b") として組み合わせることができるようになります。グループ式を、ユーザー、ユーザーグループ、もしくは別のグループ式を除外するために使用することができます（ NOT "c" ）。

注： セキュリティデバイスではグループ式を定義し (そして、ローカルデータベースに保存し) ますが、グループ式で参照するユーザーやユーザーグループは外部 RADIUS サーバーに保存されなければなりません。RADIUS サーバーは、ユーザーが複数のユーザーグループに所属することを許可します。ローカルデータベースサーバーでは許可されません。

グループ式は、OR、AND および NOT の 3 つのオペレーターを使用します。OR、AND、および NOT が関連する式内のオブジェクトは、認証ユーザー、認証ユーザーグループ、もしくは前もって定義されたグループ式などです。表 1 はオブジェクト、グループ式および例をリストします。

表 1: グループ式の例

オブジェクト	式	例
ユーザー	OR	ポリシーではユーザーに *a* OR *b* と指定し、ユーザーが *a* or *b* の条件と一致した場合、セキュリティデバイスが認証します。
	AND	グループ式における AND の使用にあたっては、2 つの式オブジェクトのうち最低 1 つがユーザーグループかグループ式であることが必要になります。（ユーザーが同時にユーザー *a* AND ユーザー *b* であることを要求するのは非合理です。）ポリシーの認証アスペクトが、ユーザーが同時に *a* AND *b* のグループのメンバーであることを要求している場合には、セキュリティデバイスは両方の条件が満足された場合のみ、ユーザーを認証します。
	NOT	ポリシーではユーザーがユーザー *c* (NOT *c*) 以外であることを指定し、セキュリティデバイスはユーザーが *c* でない限り、認証します。
ユーザーグループ	OR	ポリシーではユーザーが「グループ *a* OR グループ *b* 」であることを指定し、セキュリティデバイスはユーザーがどちらかのグループに属していると認証します。
	AND	ポリシーではユーザーが「グループ *a* AND グループ *b* 」であることを指定し、セキュリティデバイスはユーザーが両方のグループに属していると認証します。
	NOT	ポリシーではユーザーがグループ C 以外 (NOT 田 i) のグループに属していることを指定し、セキュリティデバイスはユーザーがそのグループに属していない限り、ユーザーを認証します。
グループ式	OR	ポリシーでは、ユーザーが「グループ式 *a* OR グループ式 *b* 」に適合することを指定し、セキュリティデバイスはどちらかのグループ式に適合した場合にユーザーを認証します。
	AND	ポリシーでは、ユーザーが「グループ式 *a* AND グループ式 *b* 」に適合することを指定し、セキュリティデバイスは両方のグループ式に適合した場合にのみユーザーを認証します。
	NOT	ポリシーでは、ユーザーがグループ式 *c* に適合しないこと（NOT *c*）を指定し、セキュリティデバイスは、ユーザーがグループ式に適合しない場合にのみ認証します。

例 : グループ式 (AND)

この例では、「 sales AND marketing 」を表現するグループ式「 s + m 」を作成します。認証ユーザーグループ 「sales」と「marketing」を前もって、「radius1」という名前の外部 RADIUS 認証サーバーに作成してあり、それらにユーザーを指定してあります （外部 RADIUS 認証サーバーを構成する事例は、31 ページの「例 : RADIUS 認証サーバー」を参照してください。）そして、認証コンポーネントが、両方のユーザーグループのユーザーに「 project1 」(10.1.1.70) という名前のサーバーの中の機密事項をアクセスできるように、イントラゾーンポリシーでグループ式を使用します。

注： イントラゾーンポリシーが正しく機能するためには、ソースと宛先アドレスは同じゾーンに到達する複数のインターフェースを介してセキュリティデバイスに接続した異なるサブネットになければなりません。2 つのアドレスの間でトラフィックをルートできるルーティングデバイスはセキュリティデバイス以外にあってはなりません。イントラゾーンポリシーの詳細については、**2**-161 ページの「ポリシー」を参照してください。

WebUI

1. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: project1
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 10.1.1.70/32
   Zone: Trust

2. **グループ式**
   Policy > Policy Elements > Group Expressions > New: 次のように入力してから **OK** をクリックします。

   Group Expression: s+m
   AND: (**選択**), sales AND marketing

3. **ポリシー**
   Policy > Policies > (From: Trust, To: Trust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), Any
   Destination Address:
   Address Book Entry: (**選択**), project1
   Service: ANY
   Action: Permit
   Position at Top: (**選択**)

   > Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

   Authentication: (**選択**)
   Auth Server: (**選択**)
   Use: radius1
   Group Expression: (**選択**), External Group Expression - s+m

CLI

1. **アドレス**
   set address trust project1 10.1.1.70/32

2. **グループ式**
   set group-expression s+m sales and marketing

3. **ポリシー**
   set policy top from trust to trust any project1 any permit auth server radius1
   group-expression s+m
   save

例 : グループ式 (OR)

この例では、“amy OR basil” を表現するグループ式 殿 /bî を作成します。すでに、「 radius1 」という名前の外部 RADIUS 認証サーバーに、認証ユーザーアカウント「 amy 」および「 basil 」が作成されています。（外部 RADIUS 認証サーバーを構成する事例は、31 ページの「例 : RADIUS 認証サーバー」を参照してください。）そして、Trust ゾーンから DMZ へのポリシーにそのグループ式を使用します。ポリシーの認証構成要素は、210.1.1.70 にある「 web1 」という名前の Web サーバーにアクセスするには、ユーザーが amy もしくは basil であることを要求します。

WebUI

1. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: web1
IP Address/Domain Name
IP/Netmask: (選択), 210.1.1.70/32
Zone: DMZ

2. グループ式

Policy > Policy Elements > Group Expressions > New: 次のように入力してから **OK** をクリックします。

Group Expression: a/b
OR: (選択), amy OR basil

3. ポリシー

Policy > Policies > (From: Trust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), web1
Service: ANY
Action: Permit
Position at Top: (選択)

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Authentication: (選択)
Auth Server: (選択)
Use: radius1
Group Expression: (選択), External Group Expression - a/b

CLI

1. アドレス

```
set address trust project1 210.1.1.70/32
```

2. グループ式

```
set group-expression a/b amy or basil
```

3. ポリシー

```
set policy top from trust to dmz any web1 any permit auth server radius1
    group-expression a/b
save
```

例：グループ式 (NOT)

この例では、「 NOT temp 」を表現するグループ式「 -temp 」を作成します。すでに、「 radius1 」という名前の外部 RADIUS 認証サーバーにローカル認証ユーザーアカウント「 temp 」が作成されています。（外部 RADIUS 認証サーバーを構成する事例は、31 ページの「例 : RADIUS 認証サーバー」を参照してください。）そして、そのグループ式をすべてのフルタイムの社員のインターネットアクセスを許可するが、契約社員は許可しない Trust ゾーンから Untrust ゾーンへのポリシーに使用します。このポリシーの認証コンポーネントは、Untrust ゾーンへのアクセスを拒否されているのユーザー「 temp 」を除く、Trust ゾーンの全員に認証を要求します。

WebUI

1. **グループ式**
   Policy > Policy Elements > Group Expressions > New: 次のように入力してから **OK** をクリックします。

   Group Expression: -temp
   OR: (**選択**), NOT temp

2. **ポリシー**
   Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), Any
   Destination Address:
   Address Book Entry: (**選択**), Any
   Service: HTTP
   Action: Permit
   Position at Top: (**選択**)

   > Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

   Authentication: (**選択**)
   Auth Server: (**選択**)
   Use: Local
   Group Expression: (**選択**), External Group Expression - -temp

CLI

1. **グループ式**
   set group-expression -temp not temp

2. **ポリシー**
   set policy top from trust to untrust any any any permit auth server radius1
   group-expression -temp
   save

バナーのカスタマイズ

バナーとはログインのタイプにより、モニターのさまざまな場所に表示されるメッセージのことです。

- セキュリティデバイスに管理ユーザーが接続する場合には、Telnet もしくはコンソールディスプレイの上部

注 : Telnet またはコンソールバナーの下に、バナー行を追加することができます。Telnet のバナーとコンソールのバナーが異なっても、Telnet とコンソールのログインディスプレイの 2 行目のバナー行は同じままとなります。2 次バナーを作成するには、以下のコマンドを入力してください。**set admin auth banner secondary** *string* 。

- 認証ユーザーが WebAuth アドレスへのログオンに成功した後の、Web ブラウザー上部
- 認証ユーザーへの成功メッセージ、および失敗メッセージは、Telnet、FTP、もしくは HTTP ログインプロンプトの前後

コンソールログイン以外のすべてのバナーは、すでにデフォルトメッセージが決められています。セキュリティデバイスを使用するネットワーク環境によりふさわしいバナーのメッセージをカスタマイズすることができます。

例 : WebAuth バナーのカスタマイズ

この例では、ブラウザーに表示されるメッセージを変更して、認証ユーザーが WebAuth を通じてログオンに成功した後、認証に成功したことを伝えします。新しいメッセージは「 Authentication approved 」(認証が認可されました) です。

WebUI

Configuration > Admin > Banners > WebAuth: Success Banner フィールドに、**Authentication approved** と入力し、**Apply** をクリックします。

CLI

```
set webauth banner success "Authentication approved"
save
```

ログインバナー

ログインバナーのサイズは、4 キロバイトまで拡大できます。これにより、管理者および認証済みユーザーが、セキュリティデバイスおよびデバイスの背後の保護されたリソースにログインする前に表示される、使用条件のステートメントを表示するスペースができます。ログインバナーは、セキュリティデバイスで作成しそこに格納するクリアテキスト ASCII ファイルです。ファイル名は **usrterms.txt** としなければなりません。システムの再起動により、このバナーが有効になります。バナーファイルが 4 キロバイトより大きければ、セキュリティデバイスはそのファイルを受け付けません。CLI と WebUI によって入力された既存のバナーを使用し続けます。

有効になると、このログインバナーは、ルートシステムとすべての仮想システム（vsys）によって大域的に使用されます。vsys 間または vsys 内では、異なったバナーを使用したりカスタマイズしたりできません。ログインバナーは、個々に定義された管理アクセスバナーおよびファイアウォール認証バナーより優先的に使用されます。ユーザー名とパスワードを入力したら、ユーザーは **Login** ボタンをクリックします。**Enter** キーを押しても、デバイスにログインできません。

例：ログインバナーの作成

SCP ユーティリティを使用して、セキュリティデバイスにバナーファイルを安全にコピーします。次のコマンドを使って、ユーザー名 **netscreen** の管理者は、バナーファイル **my_large_banner.txt** を IP アドレス 1.1.1.2 にあるセキュリティデバイスにコピーします。バナーファイルは、セキュリティデバイスに **usrterms.txt** という名前で保存する必要があります。

```
linux:~#scp my_large_banner.txt netscreen@1.1.1.2:usrterms.txt
```

新しいバナーを有効にするには、デバイスを再起動します。バナーファイルを変更するには、新しいファイルを作成し、既存のファイルを新しいファイルで上書きします。

バナーを削除するには、セキュリティデバイスで次のコマンドを発行します。

```
device-> delete file usrterms.txt
```

デバイスを再起動した後、ログインバナー機能が無効になります。

第 2 章

認証サーバー

この章では、すべてのセキュリティデバイスに組み込まれたローカルデータベース、そして RADIUS、SecurID、および LDP 認証サーバーなどの、各種の認証サーバーを検証します。本章のセクションは、以下のようになります。

- 12 ページの「認証サーバータイプ」
- 13 ページの「ローカルデータベース」
- 15 ページの「外部認証サーバー」
- 17 ページの「認証サーバータイプ」
  - 17 ページの「リモート認証ダイヤルインユーザーサービス」
  - 25 ページの「SecurID」
  - 27 ページの「軽量ディレクトリアクセスプロトコル」
  - 28 ページの「TACACS+ (Terminal Access Control Access Control System Plus)」
- 30 ページの「管理認証の優先」
- 31 ページの「認証サーバーオブジェクトの定義」
- 37 ページの「デフォルト認証サーバーの定義」

認証サーバータイプ

セキュリティデバイスを構成して、ローカルデータベースや 1 つもしくは複数の認証サーバーに以下のタイプのユーザーの識別を確認させることができます。

- 認証
- IKE
- L2TP
- XAuth
- Admin
- 802.1x

注： IKE ユーザーアカウントは、ローカルデータベースに保存する必要があります。L2TP と XAuth リモート設定の割り当てと管理権限割り当てをサポートしている唯一の外部サーバーは RADIUS です。

セキュリティデバイスは、ローカルデータベースに加えて、外部の RADIUS、SecurID 、LADP、および TACACS+ サーバーをサポートします。それぞれの認証サーバーを使って、認証ユーザー、L2TP ユーザー、XAuth ユーザー、および管理ユーザーを認証することができます。ScreenOS は、認証ユーザーの代替認証スキームである、WebAuth もサポートします。WebAuth の例は、59 ページの「例 : WebAuth + SSL のみ (外部ユーザーグループ)」を参照してください。認証ユーザーアカウントタイプを含むいずれの認証サーバーも、デフォルトの WebAuth 認証サーバーになることができます。表 2 はサポートされているサーバータイプと認証機能をリストしています。

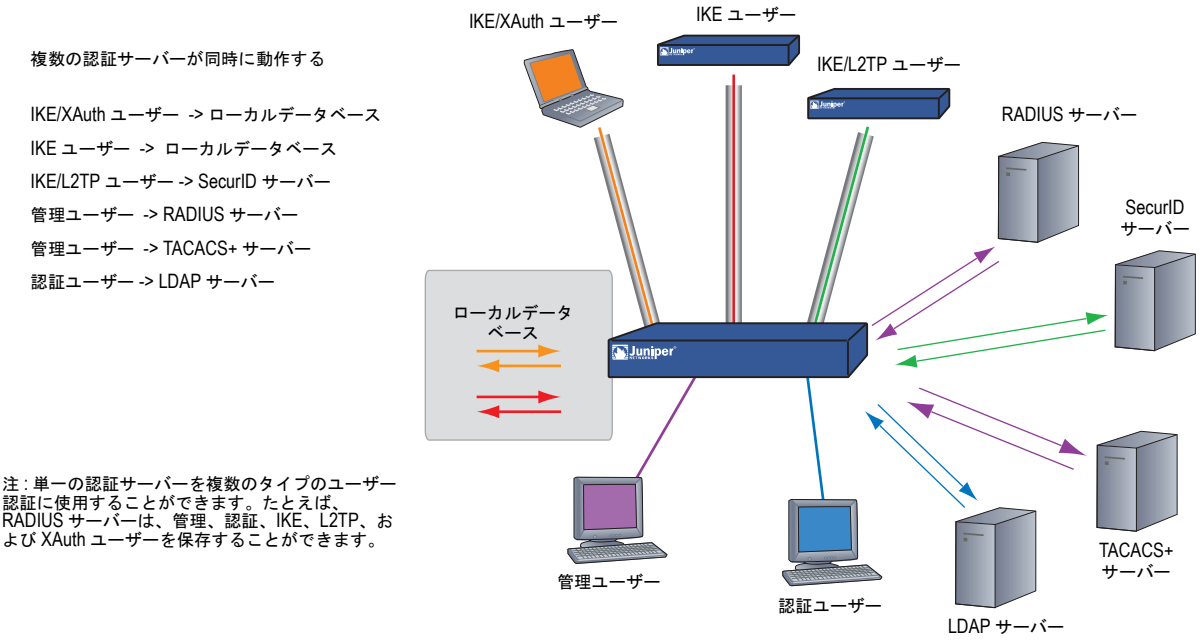
表 2: 認証サーバータイプ、ユーザータイプおよび機能

	サポートされるユーザータイプと機能									
			L2TP ユーザー		XAuth ユーザー		管理ユーザー			
サーバータイプ	認証ユーザー	IKE ユーザー	認証	リモート設定	認証	リモート設定	認証	権限	ユーザーグループ	グループ式
Local	X	X	X	X	X	X	X	X	X	
RADIUS	X		X	X	X	X	X	X	X	X
SecurID	X		X		X		X			
LDAP	X		X		X		X			
TACACS+							X	X		

ほとんどの Juniper Networks セキュリティデバイスでは、システムあたり最大 10 個の 1 次認証サーバー (ルートシステムおよび仮想システム) を任意のタイプの組み合わせで同時に使用することができます。この合計数には、ローカルデータベースが含まれますが、バックアップ認証サーバーは含まれません。RADIUS もしくは LDAP サーバーは、2 つのバックアップサーバーを、そして SecurID

サーバーは 1 つのバックアップサーバーをサポートします。したがって、たとえばローカルデータベースと、それぞれに 2 つずつのバックアップサーバーを割り当てた 9 個の異なる 1 次 RADIUS サーバーを使用するケースもあります。図 3 を参照してください。

図 3: 認証サーバーのタイプ

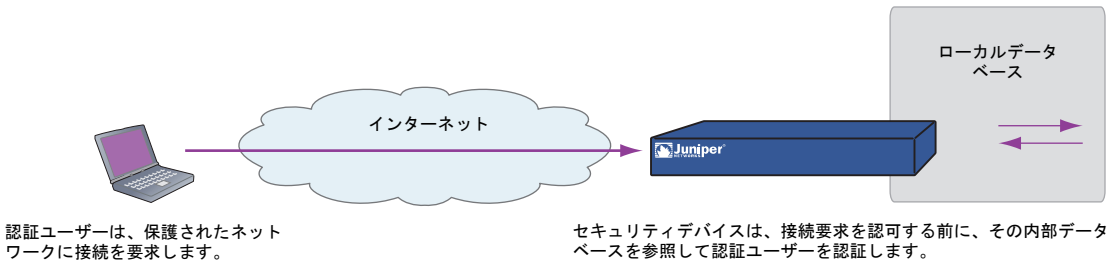


以下のセクションでは、ローカルデータベースと認証サーバーに関して詳しい説明をします。

ローカルデータベース

すべての Juniper Networks セキュリティデバイスは、認証のために組み込みユーザーデータベースをサポートします。セキュリティデバイスでユーザーを定義する場合には、セキュリティデバイスはユーザー名およびパスワードをそのローカルデータベースに入力します。図 4 を参照してください。

図 4: ローカル認証



ローカルデータベースは、以下のタイプのユーザーと認証機能をサポートします。

- ユーザー
  - 認証
  - IKE
  - L2TP
  - XAuth
  - Admin
  - 802.1x
- 認証機能 :
  - 管理権限
  - WebAuth
  - ユーザーグループ
  - グループ式

注 : セキュリティデバイスでグループ式を定義しますが、ユーザーやユーザーグループは外部 RADIUS 認証サーバーに保存されなければなりません。グループ式に関するより詳細な情報は、4 ページの「グループ式」を参照してください。

ローカルデータベースは、すべての認証タイプでデフォルトの認証サーバーです。ユーザーやユーザーグループを WebUI や CLI を介して追加する方法は、43 ページの「認証ユーザー」、および 63 ページの「IKE、XAuth、および L2TP ユーザー」を参照してください。

例 : ローカルデータベースタイムアウト

デフォルトでは、管理および認証ユーザーに対するローカルデータベース認証タイムアウトは 10 分になっています。この例では、それを管理ユーザーではタイムアウトをなしにして、認証ユーザーでは 30 分後にタイムアウトするように変更します。

WebUI

Configuration > Admin > Management: Enable Web Management Idle Timeout チェックボックスをクリアにし、**Apply** をクリックします。

Configuration > Auth > Servers > Edit (Local): Timeout フィールドに **30** と入力して、**Apply** をクリックします。

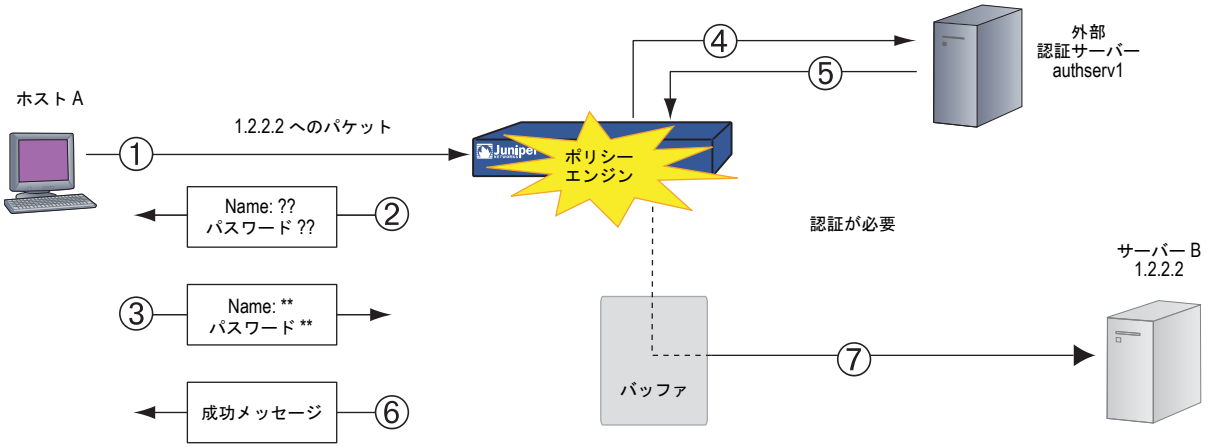
CLI

```
set admin auth timeout 0
set auth-server Local timeout 30
save
```

外部認証サーバー

セキュリティデバイスは 1 つもしくは複数の外部認証サーバーや、ユーザーアカウントを保存する *auth servers* に接続することができます。セキュリティデバイスが認証確認を必要とする接続要求を受け取ると、ポリシー、L2TP トンネル構成もしくは、IKE ゲートウェイ構成により指定された外部認証サーバーから、認証チェックを要求します。セキュリティデバイスは認証を要求しているユーザーと認証を許可している認証ユーザーとの間のリレーの役割を果たします。図 5 は外部認証サーバーが認証に成功するまでのステップを示します。

図 5: 外部認証サーバー



1. ホスト A は、FTP、HTTP、もしくは Telnet TCP SYN パケットを 1.2.2.2 に送信します。
2. セキュリティデバイスは、パケットを代行受信して、それに対応するポリシーが authserv1 による認証を必要とすることを確認し、パケットをバッファに入れて、ユーザーにユーザー名とパスワードの入力のプロンプトを出します。
3. ユーザーは、ユーザー名とパスワードを入力します。
4. セキュリティデバイスは、ログイン情報を authserv1 に中継します。
5. Authserv1 は、セキュリティデバイスに認証成功を通知します。
6. セキュリティデバイスは、認証ユーザーにログインが成功したことを通知します。
7. セキュリティデバイスは、その後パケットをバッファから宛先の 1.2.2.2 に送信します。

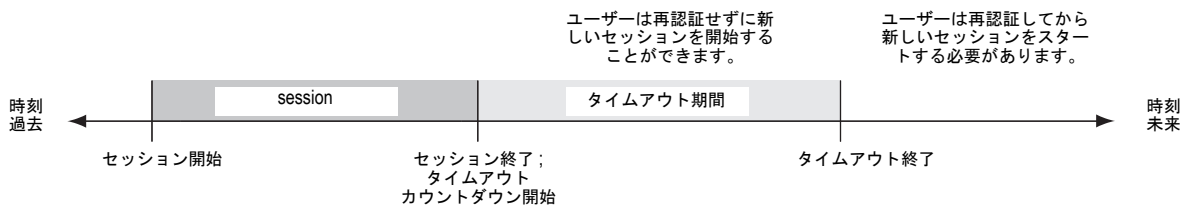
認証サーバーオブジェクトプロパティ

セキュリティデバイスは、各認証サーバーをポリシー、IKE ゲートウェイ、L2TP サーバーから参照できるオブジェクトとして扱います。表 3 で説明するプロパティは、認証サーバーオブジェクトを定義し、識別します。

表 3: 認証サーバーオブジェクトプロパティ

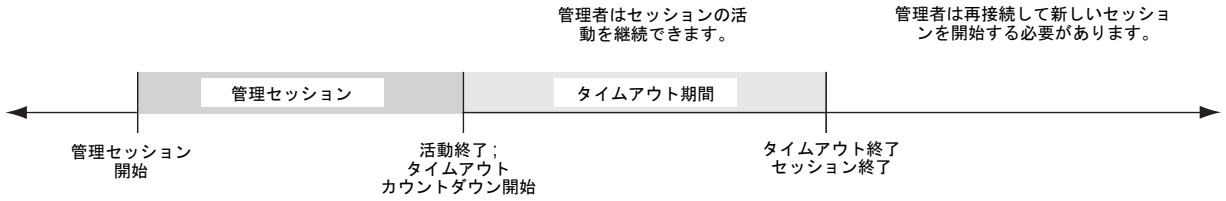
プロパティ	説明	
Object name	authserv1 などの名前文字列。事前に定義されている唯一の認証サーバーはローカルです。	
ID number	ID 番号を自分で設定するか、セキュリティデバイスに自動的に設定することを許可することができます。ID 番号を自分で設定するときには、未使用のものを選択する必要があります。	
Type	RADIUS、SecurID、LDAP、TACACS+	
Server name	サーバーの IP アドレスまたはドメイン名。	
Backup1	1 次バックアップサーバーの IP アドレスまたはドメイン名。	
Backup2	2 次バックアップサーバーの IP アドレスまたはドメイン名。	
Account Type	Auth、L2TP、802.1x、XAuth のユーザーのタイプの 1 つ以上、または Admin だけ。	
Timeout value	タイムアウト値は、認証ユーザーに対するものか、管理ユーザーに対するものかで、意味が異なります。	
	認証ユーザー	タイムアウトカウントダウンは、最初の認証済みセッションが完了してから開始します。カウントダウンがタイムアウトしきい値に達する前に、ユーザーが新しいセッションを開始した場合、タイムアウトのカウントダウンはリセットされます。デフォルトのタイムアウト値は 10 分で、最大値は 255 分です。タイムアウト機能を無効にするには、タイムアウト値を 0 に設定します。図 6 を参照してください。
	管理ユーザー	アイドルタイムの長さがタイムアウトしきい値に達した場合、セキュリティデバイスは管理セッションを終了させます。セキュリティデバイスの管理を継続するためには、管理者はデバイスを再接続して自身を再認証する必要があります。デフォルトのタイムアウト値は 10 分で、最大値は 1000 分です。タイムアウト機能を無効にするには、タイムアウト値を 0 に設定します。図 7 を参照してください。
Forced Timeout	強制タイムアウトは、アイドルタイムアウトとは異なり、ユーザーがアイドル状態であるかどうかには関係なく、認証済みユーザーのアクセスが終了してから絶対的なタイムアウトを考慮します。そのユーザーの認証テーブルエントリ、および認証テーブルエントリに関連付けられた全セッションが削除されます。デフォルトは 0（無効）、範囲は 0 ～ 10000（6.9 日）です。	

図 6: 認証サーバーオブジェクトプロパティ



注 : ユーザー認証タイムアウトは、セッションアイドルタイムアウトとは異なります。あらかじめ定義された時間内に活動がない場合には、セキュリティデバイスは自動的にセッションをセッションテーブルから削除します。

図 7: 管理タイムアウトプロパティー



すべてのサーバーオブジェクトに適用される前記のプロパティに加えて、各サーバーのみに適用されるいくつかのプロパティがあります。これらについては「認証サーバータイプ」に説明しています。

認証サーバータイプ

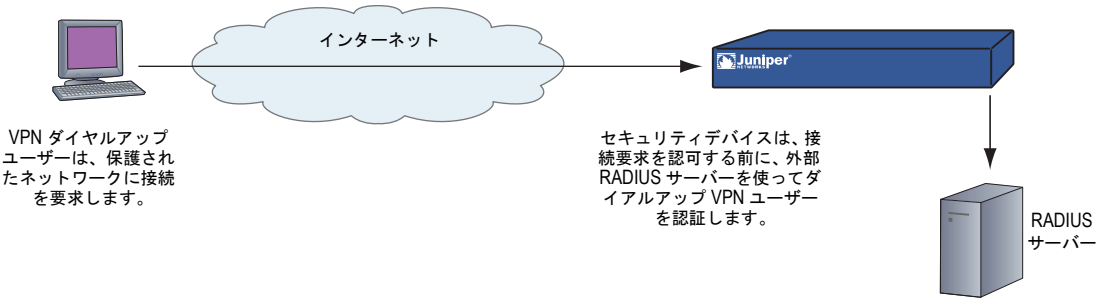
内部データベースに加えて、セキュリティデバイスは次の 4 種類の外部認証サーバーをサポートします。

- リモート認証ダイヤルインユーザーサービス RADIUS
- SecurID
- 軽量ディレクトリアクセスプロトコル LDAP
- TACACS + Terminal Access Controller Access Control System Plus

リモート認証ダイヤルインユーザーサービス

RADIUS (リモート認証ダイヤルインユーザーサービス) は、最大数万ユーザーをサポートできる認証サーバーのプロトコルです。

図 8: RADIUS の外部認証サーバーとしての使用



RADIUS クライアント (この場合は、セキュリティデバイス) は、一連のクライアントとサーバーの通信を通じてユーザーを認証します。基本的には、RADIUS は、ログオンするユーザーに、ユーザー名とパスワードを入力するように要求します。その後、それらの値をデータベースの値と照合して、ユーザーがいったん認証されるとクライアントはユーザーに適正なネットワークサービスへのアクセスを提供します。

セキュリティを RADIUS に対応して構成するには、RADIUS サーバーの IP アドレスを指定して RADIUS サーバーで定義したものと同じ共有秘密値を定義します。共有秘密値は、RADIUS サーバーがセキュリティと RADIUS デバイスの間のトラフィックを暗号化する鍵を生成するために使用するパスワードです。

RADIUS 認証サーバーオブジェクトプロパティ

16 ページの「認証サーバーオブジェクトプロパティ」に記載される汎用認証サーバープロパティに加えて、RADIUS サーバーでは表 4 に示すプロパティも利用できます。

表 4: RADIUS 認証サーバーオブジェクトプロパティ

プロパティ	説明
Shared Secret	セキュリティデバイスと RADIUS サーバーの間で共有される秘密値 (パスワード)。デバイスは、この秘密値を使って RADIUS サーバーに送信するユーザーのパスワードを暗号化します。
RADIUS Port	セキュリティデバイスが認証要求を送信する RADIUS サーバーのポート番号。デフォルトのポート番号は 1645 です。
RADIUS Retry Timeout	前の要求が応答を引き出さない場合に、別の認証要求を RADIUS サーバーに送信するまでのセキュリティデバイスの待ち時間を秒数で示したもの。デフォルトは 10 秒です。

サポートされるユーザータイプと機能

RADIUS サーバーは以下のタイプのユーザーと認証機能をサポートします。

- 認証ユーザー
- L2TP ユーザー (認証およびリモート設定)
- 管理ユーザー (認証および権限割り当て)
- ユーザーグループ
- XAuth ユーザー (認証およびリモート設定)

  XAuth モジュールは、表 5 で示す RADIUS サーバーから取得した Session-timeout および Idle-timeout 属性をサポートします。

表 5: XAuth 属性サポート

属性	説明
Session-timeout	Session-timeout 属性が 0 でない値である場合、タイムアウト値に到達すると、フェーズ 1/ フェーズ 2 セキュリティアソシエーション SA および XAuth は両方とも終了します。
Idle-timeout	0 でない値である場合、Idle-timeout 属性はローカルフェーズ 2 SA アイドル時間構成およびメンバー SA ホールド時間に優先されます。 Idle-timeout 値が 0 である場合、ローカルフェーズ 2 SA アイドル時間およびメンバー SA ホールド時間が使用されます。
XAuth Accounting Start	ユーザーが正しく認証された後、XAuth Accounting start が外部 RADIUS サーバーへ送信されます。
XAuth Accounting Stop	XAuth 接続がダウンになると、XAuth Accounting stop 外部 RADIUS サーバーへ送信されます。フェーズ 1/ フェーズ 2 SA と XAuth の接続はすべて、以下の条件で終了します。 ■ RADIUS サーバーの Session-timeout 属性に到達した ■ RADIUS サーバーの Session-timeout 属性が構成されていない 代わりに、XAuth セッション寿命が使用されます。 ■ すべてのフェーズ 2 SA で、RADIUS サーバーの Idle-timeout 属性に到達した ■ クライアント切断が、デッドピア検出 DPD またはハートビートによって検出された ■ RADIUS サーバーが Idle-timeout 属性を提供していないので、ローカルに構成されたフェーズ 2 SA アイドル時間またはメンバー SA ホールド時間に到達した

RADIUS サーバーは、IKE ユーザーを除くローカルデータベースがサポートするすべてのユーザータイプと機能をサポートできます。4 種類の外部認証サーバーでは、RADIUS だけが現時点において、そのような広範囲のサポートを行っています。RADIUS サーバーが、管理権限、ユーザーグループ、リモート L2TP および XAuth IP アドレス、DNS および WINS サーバーアドレス割り当てなどの、ScreenOS に特化した属性をサポートするためには、これらの属性を定義する RADIUS ディクショナリーファイルをロードする必要があります。

注 : ScreenOS は、IP アドレス割り当てに、標準 RADIUS 属性を使用します。IP アドレス割り当てに、RADIUS のみを使用したい場合には、ScreenOS のベンダー固有属性 (VSA) をロードする必要はありません。

RADIUS ディクショナリーファイル

ディクショナリーファイルは、RADIUS サーバーにロードできる VSA (ベンダー固有属性) を定義します。VSA の値を定義すると、ScreenOS はユーザーがセキュリティデバイスにログオンしたときに、それらを検索することができます。ScreenOS VSA は、管理権限、ユーザーグループ、リモート L2TP および XAuth IP アドレス、DNS および WINS サーバーアドレス割り当てを含みます。RADIUS ディクショナリーファイルには、Cisco RADIUS サーバー用と Funk Software RADIUS サーバー用の 2 種類があります。Microsoft RADIUS サーバーを使用している場合には、ディクショナリーファイルはありません。*Bi-Directional Remote VPN using XAuth and Firewall Authentication with Microsoft Internet Authentication Service (IAS)* で概説したように構成します。このドキュメントは、http://kb.juniper.net/kb/documents/public/kbdocs/ns10382/ns10382.pdf からダウンロードできます。

それぞれの RADIUS ディクショナリーファイルは、表 6 に示す特定情報を含みます。

表 6: RADIUS ディクショナリーファイルの内容

フィールド	説明
Vendor ID	ScreenOS ベンダー ID VID (VID もしくは IETF 番号) は、3224 です。VID は、特定の属性に対して特定のベンダーを識別します。RADIUS サーバーのタイプによっては、各属性の項目に VID を入力するように要求するものもあれば、一度入力したらグローバルに適用してくれるものもあります。さらに詳細な情報は、RADIUS サーバー資料を参照してください。
Attribute Name	属性名は、NS-Admin-Privilege、NS-User-Group、NS-Primary-DNS-Server など、個々の ScreenOS 特有の属性を表します。
Attribute Number	属性番号は、個々のベンダー特有の属性を特定します。ScreenOS 特有の属性番号は、2 つの範囲に包含されます。 ■ ScreenOS: 1 - 199 ■ Global PRO: 200 以上 たとえば、ユーザーグループの ScreenOS 属性番号は 3 です。ユーザーグループの Global PRO 属性番号は 200 です。
Attribute Type	属性タイプは、属性データ (もしくは値) が表示される、文字列、IP アドレス、整数などの書式を特定します。

RADIUS サーバーは、RADIUS ディクショナリーファイルをロードすると、上記の情報を自動的に受け取ります。新しいデータエントリを作成するには、手動で、属性タイプに示される書式で値を入力する必要があります。たとえば、読取 / 書込管理者の項目は以下のように表示されます。

VID	Attribute Name	Attribute Number	Attribute Type	値
3224	NS-Admin-Privileges	1	data = int4 (ie, integer)	2 (2 = all privileges)

ディクショナリーファイルをダウンロードするには、
http://www.juniper.net/customers/csc/research/netscreen_kb/downloads、/dictionary/funk_radius.zip
または
http://www.juniper.net/customers/csc/research/netscreen_kb/downloads/dictionary/cisco_radius.zip

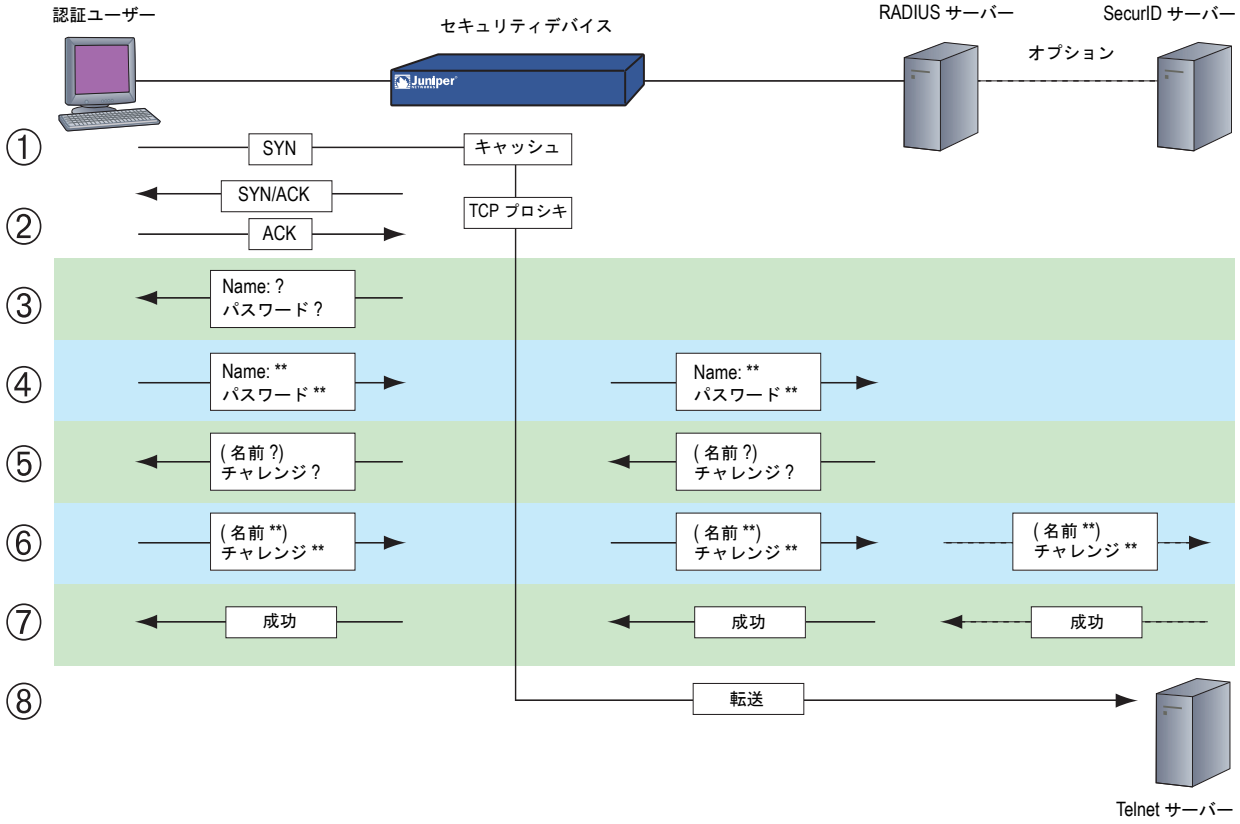
にアクセスし、ログインして、ファイルをローカルファイルに保存してください。

注 : Funk Steel Belted RADIUS の新しいバージョンでは、すでに RADIUS ファイアウォール辞書ファイルを RADIUS サーバーにロードしています。

RADIUS アクセスチャレンジ

Juniper Networks セキュリティデバイスは、認証ユーザーが Telnet を通じてログオンしようとするとき、外部 RADIUS サーバーからアクセスチャレンジパケットを処理することができます。アクセスチャレンジは、ユーザー名とパスワードの承認後、ログインプロセスに追加の条件を示します。認証ユーザーがログインプロンプトに正しいユーザー名とパスワードで応答した後で、RADIUS サーバーはセキュリティデバイスにアクセスチャレンジを送信し、それが次にユーザーに転送されます。ユーザーが応答すると、セキュリティデバイスはユーザー応答と共に新しいアクセス要求を RADIUS サーバーに送信します。ユーザーの応答が適切な場合、認証プロセスは成功します。図 9 は telnet を介してサーバーに送信したい認証ユーザーが必要なステップをリストしています。

図 9: RADIUS アクセスチャレンジの順序



1. 認証サーバーは SYN パケットを送信して、Telnet サーバーに Telnet セッションの TCP 接続を開始します。

2. セキュリティデバイスはパケットを代行受信し、ポリシーリストをチェックして、このセッションがユーザー認証を必要とするかを判断します。セキュリティデバイスは SYN パケットをキャッシュして、TCP 3 方向ハンドシェイクをユーザーにプロキシします。

3. セキュリティはユーザーにユーザー名とパスワードでログインするように求めます。

4. 認証ユーザーは自分のユーザー名とパスワードを入力し、セキュリティデバイスに送信します。セキュリティデバイスは次に、RADIUS サーバーにログイン情報を使用してアクセス要求を送信します。
5. 情報が正しい場合、RADIUS サーバーはセキュリティデバイスに、チャレンジに対してユーザーに応答を指示するプロンプトを表示する応答メッセージと共にアクセスチャレンジを送信します。(アクセスチャレンジは、ユーザー名をもう一度指定する認証をオプションで指示できます。2 番目のユーザー名は、最初と同じもの、または別のものである場合があります。セキュリティデバイスはこの後で、応答メッセージ属性の内容を含む別のログインプロンプトをユーザーに送信します。
6. 認証ユーザーは自分のチャレンジ応答（オプションでユーザー名）を入力し、セキュリティデバイスに送信します。セキュリティデバイスは次に、ユーザーのチャレンジ応答と共に、RADIUS サーバーへの 2 番目のアクセス要求を送信します。

   RADIUS サーバーは別の認証サーバーを経由してチャレンジ応答を認証する必要があります。たとえば、SecureID サーバーがトークンコードを認証しなければならない場合、RADIUS サーバーは別の認証サーバーにアクセス要求を送信します。
7. RADIUS サーバーがチャレンジ応答を別のサーバーに転送する場合、そのサーバーはアクセス承認を送信します。または、RADIUS サーバー自体がチャレンジ応答を承認する場合、RADIUS サーバーはアクセス承認メッセージをセキュリティデバイスに送信します。セキュリティデバイスは、ログインが正常に行われたことを認証ユーザーに通知します。
8. セキュリティデバイスは最初の SYN パケットを元の宛先に送信します。元の宛先とは、Telnet サーバーです。

注： ScreenOS はこのリリースの時点で、L2TP のアクセスチャレンジはサポートしていません。

認証および XAuth ユーザーにサポートされている RADIUS 拡張機能

ScreenOS は、次の属性を持った認証および拡張認証 XAuth モジュールを通して RADIUS 拡張機能をサポートします。

- 23 ページの「NS アクセスサービスタイプ」
- 23 ページの「フレーム化プールおよびフレーム化 IP アドレス」
- 24 ページの「アカウントセッション ID」
- 24 ページの「コーリングステーション ID」
- 24 ページの「コールドステーション ID」
- 24 ページの「互換性 RFC-2138」
- 24 ページの「ユーザー名」
- 24 ページの「セパレータ」
- 25 ページの「フェールオーバー」

NS アクセスサービスタイプ

NS-Access-Service-Type 属性は、サービスタイプに関する情報を提供します。セキュリティデバイスは、ユーザーによって要求されるサービスのタイプを示す各アクセス要求にこの属性を追加します。この属性はデフォルトで有効になっています。

RADIUS モジュールは、Telnet、FTP または HTTP 認証モジュールから要求を受信すると、WEB-AUTH (2) に値を設定します。RADIUS モジュールは、XAuth モジュールから要求を受信すると、VPN-IPSEC (3) に値を設定します。

デバイスは、アクセス要求メッセージに *ns-access-service-type* および値を含めています。RADIUS サーバーは、要求しているユーザーにサービスへのアクセスを許可すると判断した場合、アクセス承認メッセージを送信します。サービスタイプが要求ユーザーに適用可能でない場合、RADIUS サーバーはアクセス拒否メッセージを送信します。

RADIUS サーバーは、アクセス応答メッセージには *ns-access-service-type* 属性を含めません。

フレーム化プールおよびフレーム化 IP アドレス

RADIUS サーバーは、アクセス承認メッセージに **framed-pool** 属性を含めます。Framed-Pool 属性が含まれていると、デバイスは、このプールからのユーザーに IP アドレスを割り付けます。ただし、デバイスは、アクセス要求メッセージで Framed-Pool 属性を送信しません。

表 7 は、デバイスがどのように framed-pool および framed-ip-address 属性を処理するかを示しています。RADIUS 拡張機能には、仮想システム（VSYS）レベルでアドレスプールを処理する機能も含んでいます。

表 7: サポートされる属性

サポートされる属性	解決
Framed-Pool 属性および Framed-IP-Address 属性は両方ともアクセス承認メッセージに含まれる。	Framed-Pool 属性は、Framed-IP-Address value が 0xFFFFFFFE (255.255.255.254) である場合を除き、RADIUS サーバーによって必ず無視されます。この場合、デバイスは RADIUS サーバーが送信した Framed-Pool 属性からアドレスを割り付けます。
Framed-Pool 属性および Framed-IP-Address 属性が両方ともアクセス承認メッセージに含まれない。	デバイスは、エンドユーザーに IP アドレスを割り当てません。
Framed-IP-Address 属性はアクセス承認メッセージに含まれ、0xFFFFFFFE (255.255.255.254) という値を持っている。 Framed-Pool 属性はない。	デバイスは、その VSYS に構成されているデフォルトの IP アドレスプールから IP アドレスを割り付けます。
Framed-Pool 属性で送信されたプールは構成されていない、またはプールに IP アドレスがない。	次のエラーメッセージが生成され、ネゴシエーションは終了します。 ■ Login failed: IP pool needed but not configured. ■ Login failed: No more IP address available in IP pool. 両方のシナリオで、クライアントは次のメッセージを受信します。 No more IP address available in IP pool

アカウントセッション ID

acct-session-id はそれぞれのアカウンティングセッションを一意的に識別します。XAuth ユーザーがデバイスに接続するたびに、デバイスはユーザーを認証し、新しい acct-session-id を確立します。これがアカウンティングセッションを識別するために使われます。アカウンティングセッションはデバイスが RADIUS サーバーに Accounting-Start メッセージを送信したときから、Accounting-Stop メッセージを送るまでの時間です。ユーザーを識別するために、それぞれの RADIUS アクセスまたは RADIUS 要求メッセージには calling-station-id が含まれること（下記に説明）があります。

acct-session-id length *number* は account-session-id の長さバイト単位です。この値のデフォルトの長さは 11 バイトです。数字の設定は、デフォルトの長さに問題があるかもしれないいくつかの RADIUS サーバーのためにあります。acct-session-id の長さは 6 バイト以上 10 バイト以下の間で設定できます。デフォルトの設定に戻すには、次のコマンドを実行します。

unset auth-server *name_str* **radius attribute acct-session-id** *number*

コーリングステーション ID

calling-station-id 属性はコールの発信元を識別します。例えば、この値はコールの発信元であるユーザーの電話番号かもしれません。

コールドステーション ID

called-station-id 属性はコールの宛先または受信先を識別します。例えば、この値はコールの発信元であるユーザーの電話番号かもしれません。

互換性 RFC-2138

compatibility rfc-2138 属性は RADIUS アカウンティングを RFC 2865 ではなく、RFC 2138 を遵守するようにします。RFC 2865 （最新の基準）と RFC 2138 が相反する操作の場合、コマンドは RFC 2865 ではなく RFC 2138 に従って作動します。行動が追加型の場合、コマンドは RFC 2865 と RFC 2138 の両方に互換性があります。

ユーザー名

username は特定の認証サーバーのドメイン名または文字を抽出するユーザー名の一部を指定します。ユーザー名が認証中に取り扱っているドメイン名を、認証サーバーのドメイン名として指定します。

セパレータ

デバイスは抽出が行われる箇所を識別するために、セパレータ文字を使用します。抽出作業は、指定した文字（その文字自体を含めて）の、それぞれのインスタンスの右側にある文字をすべて削除します。一番右にあるセパレータ文字から始めます。セパレータコマンドの例は以下のとおりです。

set auth-server *name_str* **username separator** *string* **number** *number*

場所 :

- *name_str* は認証サーバーの名前です。
- *string* は文字のセパレータです。
- *number* は文字抽出を行う文字セパレータインスタンスの数です。

指定したセパレータ文字の数（*数*）がユーザー名の実際のセパレータ文字の数より大きい場合、コマンドは一番最後のセパレータ文字で抽出をやめます。

注 : デバイスは抽出を行う前に、ドメイン名マッチングを行います。

フェールオーバー

fail-over 属性は、認証に失敗してから、デバイスがバックアップ認証サーバーを使って認証を再度試みるまでの時間復元時間を秒で指定します。

1 次サーバーに送信した認証要求が失敗すると、デバイスはバックアップサーバーで試みます。バックアップサーバーでの認証に成功し、復元時間が過ぎたら、デバイスは次の認証要求をバックアップサーバーに送信します。さもなければ、1 次サーバーへの要求を再開します。指定できる範囲は 0 秒（使用不可）から 86400 秒です。

フェールオーバーおよび復元時間のコマンドは次のとおりです。

set auth-server *name_str* **fail-over revert-interval** *number*

場所 :

- *name_str* は認証サーバーの名前です。
- *number* は時間の長さです秒。

注 : これは RADIUS および LDAP サーバーのみに適用されます。

SecurID

SecurID は、固定パスワードの代わりに、2 つの要因を組み合わせて動的に変化するパスワードを生成します。SecureID は、*authenticator* と呼ばれ（図 10）、毎分変化する *トークンコード*と呼ばれるランダムに生成される数字文字列を LCD ウィンドウで表示するクレジットカードサイズのデバイスを発行します。ユーザーは、PIN (個別識別番号) も持っています。ユーザーがログオンするときには、ユーザー名と PIN および現状のトークンコードを入力します。

図 10: SecurID トークン



Authenticator は、RSA のみが知っているアルゴリズムを起動させ LCD に表示される値を生成します。認証されるべきユーザーが PIN とカードに表示された番号を入力すると、ACE サーバーは同じアルゴリズムを起動させ、データベースにある値と受信した値を照合させます。照合すれば、認証は成功です。

セキュリティデバイスと RSA SecurID ACE サーバーの関係は、セキュリティデバイスと RADIUS サーバーの関係に似ています。それは、セキュリティデバイスがクライアントとなり、認証要求の認可のため外部サーバーに転送し、ユーザー・サーバー間のログイン情報を中継するという点でです。SecurID が RADIUS と異なる点は、ユーザーの「パスワード」が、常に変化するトークンコードに関連していることです。

SecurID 認証サーバーオブジェクトプロパティ

16 ページの「認証サーバーオブジェクトプロパティ」に記載される汎用認証サーバープロパティに加えて、SecurID サーバーでは表 8 に示すプロパティも利用できます。

表 8: SecurID 認証サーバーオブジェクトプロパティ

プロパティ	説明
Authentication Port	セキュリティデバイスが認証要求を送信する SecurID ACE サーバーのポート番号。デフォルトのポート番号は 5500 です。
Encryption Type	セキュリティデバイスと SecurID ACE サーバー間の通信の暗号化に使用されるアルゴリズム、SDI もしくは DES 。
Client Retries	SecurID クライアントセキュリティデバイスが、試みを中断するまでに SecurID ACE サーバーと通信を確立しようとした回数。
Client Timeout	セキュリティデバイスが認証リトライの間に待つ秒数。
Use Duress	異なった PIN 番号の使用を禁止もしくは許可するオプション。オプションが使用可能になり、ユーザーが以前に認識された拘束 PIN 番号を入力すると、セキュリティデバイスは、信号を SecurID ACE サーバーに送り、ユーザーが拘束中に自身の意思に反してログインを行っていることを伝えます。SecurID ACE サーバーは、今回限りでアクセスを許可した後、ユーザーが SecurID 管理者と連絡をとるまではこれ以上のログインのトライを受け付けません。拘束モードは、SecurID ACE サーバーがこのオプションをサポートしている場合のみ提供されます。

サポートされるユーザータイプと機能

SecurID ACE サーバーは、以下のタイプのユーザーと認証機能をサポートします。

- 認証ユーザー
- L2TP ユーザー (ユーザー認証。L2TP ユーザーはセキュリティバイスからデフォルト L2TP 設定を受け取ります)
- XAuth ユーザー (ユーザー認証; リモート設定割り当てのサポートはありません)
- 管理ユーザー (ユーザー認証; 管理ユーザーは読取専用のデフォルト権限割り当てを受け取ります)

現時点では、SecurID ACE サーバーは、L2TP もしくは XAuth リモート設定か ScreenOS 管理権限を割り当てることはできませんが、認証目的で、SecurID サーバーで L2TP、XAuth および管理ユーザーアカウントを保存することはできます。また、ScreenOS は、SecurID と併用する場合には、ユーザーグループサポートを提供しません。

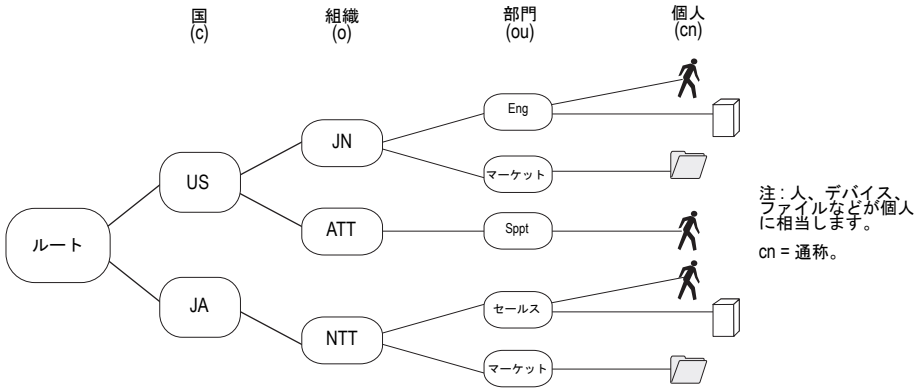
軽量ディレクトリアクセスプロトコル

LDAP (軽量ディレクトリアクセスプロトコル) は、1996 年にミシガン大学で開発されたディレクトリサーバーの基準です。LDAP は、枝分かれする木と似た階層構造で情報を整理、アクセスするプロトコルです。その目的としては 2 つあります。

- ネットワーク上で、組織、個人、ファイルなどのリソースを見つける
- ディレクトリサーバーによって制御されるネットワークへの接続をトライするユーザーの認証を支援する

基本的な LDAP の構造は、国、組織、部門、個人の順に枝分かれします。この他に「州」や「郡」などの中間的レベルもあります。図 11 は LDAP の枝分かれした組織構造の例を示します。

図 11: LDAP 階層型構造



注 : LDAP に関する情報は、RFC 1777 の *Lightweight Directory Access Protocol* を参照してください。

セキュリティデバイスを、軽量ディレクトリアクセスプロトコル (LDAP) サーバーとリンクするように構成することができます。このサーバーは、各ユーザーを個別に識別するために、LDAP 階層構文を使用します。

LDAP 認証サーバーオブジェクトプロパティ

16 ページの「認証サーバーオブジェクトプロパティ」に記載される汎用認証サーバープロパティに加えて、LDAP サーバーでは表 9 に示すプロパティも利用できます。

表 9: LDAP 認証サーバーオブジェクトプロパティ

プロパティ	説明
LDAP Server Port	セキュリティデバイスが認証要求を送信する LDAP サーバーのポート番号。デフォルトのポート番号は 389 です。 **注 :** セキュリティデバイスの LDAP ポート番号を変更する場合は、LDAP サーバーでも変更してください。
Common Name Identifier	LDAP サーバーに入った個人を識別するために、LDAP サーバーが使用する識別子。たとえば、「 uid 」項目は「ユーザー ID 」を意味し、「 cn 」は「通称名」を意味します。
Distinguished Name (dn)	共通識別子を使用する前に、LDA サーバーが特定のエントリを検索するために使用するパス。(たとえば、c = us;o = juniper では、「 c 」は「国」を示し、「 o 」は、「組織」を表します)

サポートされるユーザータイプと機能

LDAP サーバーは、以下のタイプのユーザーと認証機能をサポートします。

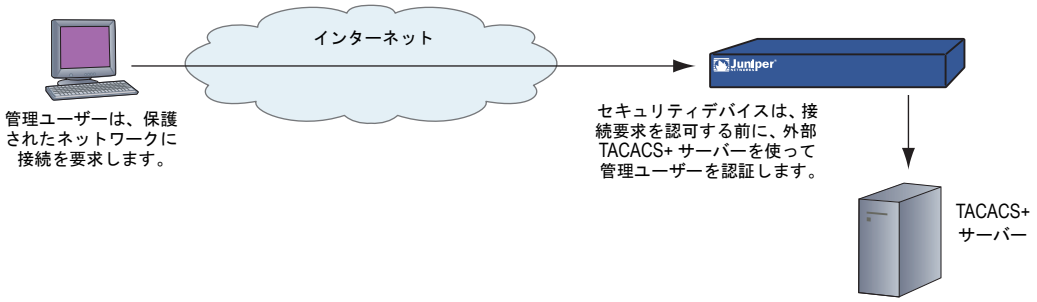
- 認証ユーザー
- L2TP ユーザー (ユーザー認証。L2TP ユーザーはセキュリティバイスからデフォルト L2TP 設定を受け取ります)
- XAuth ユーザー (ユーザー認証; リモート設定割り当てのサポートはありません)
- 管理ユーザー (ユーザー認証; 管理ユーザーは読取専用のデフォルト権限割り当てを受け取ります)

現時点では、LDAP サーバーは L2TP、XAuth、および管理ユーザーアカウントを認証目的で保存することはできますが、L2TP や XAuth リモート設定もしくは ScreenOS 管理権限を割り当てすることはできません。また、ScreenOS は、LDAP と併用する場合には、ユーザーグループサポートを提供しません。

TACACS+ (Terminal Access Control Access Control System Plus)

TACACS + (Terminal Access Controller Access Control System Plus) はユーザーの集中評価を提供するセキュリティアプリケーションです。TACACS + サービスは通常、UNIX または Windows NT のワークステーションで実行される TACACS + デーモン上で、データベースに維持されます。

図 12: TACACS+ サーバーへの認証



TACACS + クライアント (この場合は、セキュリティデバイス) は、一連のクライアントとサーバーの通信を通じてユーザーを認証します。基本的には、TACACS + は、ログオンするユーザーに、ユーザー名とパスワードを入力するように要求します。その後、それらの値をデータベースの値と照合して、ユーザーがいったん認証されるとクライアントはユーザーに適正なネットワークサービスへのアクセスを提供します。

セキュリティを TACACS + に対応して構成するには、TACACS + サーバーの IP アドレスを指定して TACACS + サーバーで定義したものと同じ共有秘密値を定義します。共有秘密値は、TACACS + サーバーがセキュリティと TACACS + デバイスの間のトラフィックを暗号化する鍵を生成するために使用するパスワードです。

TACACS + は、個別のモジュール式の認証、許可および課金機能を提供します。ScreenOS での TACACS + サポートにより、TACACS + サーバーは、独立して以下のように認証と許可を提供できます。

- 認証と許可

  TACACS + は認証と許可の機能を分離しています。リモート認証は管理ユーザーについてだけサポートされます。認証された管理者は、特権レベルおよび vsys を割り当てられます。ScreenOS はユーザーレベル許可のみをサポートします。

- 2 台までの TACACS + サーバーを構成

  1 次 TACACS + サーバーが到着可能でない場合、バックアップ TACACS + サーバーに問い合わせます。詳細については、30 ページの「管理認証の優先」を参照してください。

TACACS+ サーバーオブジェクトプロパティ

16 ページの「認証サーバーオブジェクトプロパティ」に記載される汎用認証サーバープロパティに加えて、TACACS+ サーバーでは表 10 に示すプロパティも利用できます。

表 10: TACACS+ サーバーオブジェクトプロパティ

プロパティ	説明
Shared Secret	セキュリティデバイスと TACACS+ サーバーの間で共有される秘密値 (パスワード)。デバイスは、この秘密値を使って TACACS+ サーバーに送信するユーザーのパスワードを暗号化します。
TACACS+ Port	セキュリティデバイスが認証要求を送信する TACACS+ サーバーのポート番号。デフォルトのポート番号は 49 です。
TACACS+ Retry Timeout	前の要求が応答を引き出さない場合に、別の認証要求を TACACS+ サーバーに送信するまでのセキュリティデバイスの待ち時間を秒数で示したもの。デフォルトは 3 秒です。
Client Retries	TACACS+ クライアントセキュリティデバイスが、試みを中断するまでに TACACS+ サーバーと通信を確立しようとした回数。
Client Timeout	セキュリティデバイスが認証リトライの間に待つ秒数。
Encryption	TACACS+ は、クライアントとサーバーのやりとりの全ペイロードを暗号化します。

管理認証の優先

ScreenOS では、ローカルおよびリモート認証サービスについて認証プロセスを優先できます。管理者は、認証サービスを問い合わせるシーケンスおよび最初の試行が失敗した場合に講ずるべき処置を定義します。

- 認証サービスの優先

  ローカルデータベース上のリモート認証サーバーでの認証により高い優先順位を設定します。ルート権限を持つ管理者は、管理者認証サービスが試みられる認証サービス（ローカルまたはリモート）のシーケンスを定義できます。ルートの管理者は、認証サービスの 1 つを 1 次に設定します。もう一方は自動的に 2 次サービスになります。

- フォールバック活動の定義

  1 次認証サービスが失敗した場合、2 次サービスで認証するデフォルトか、バイパスするか、いずれかにデバイスを構成できます。上記のアクションは、ルート権限を持つ管理者とルート権限を持たない管理者では異なって定義されます。

- 外部で認証された管理者の受け入れ

  リモート認証サーバーによって認証されたルート権限を持つ管理者を受け入れるかどうか、セキュリティデバイスを構成します。

- デフォルトの認証

  リモート認証が失敗し、ローカル認証が無効になっている場合、デバイスはルート権限を持つ管理者がローカルに認証されることを可能にします。このフォールバック手順はシリアルコンソールに限定されます。

認証サーバーオブジェクトの定義

ポリシー、IKE ゲートウェイ、および L2TP トンネルで、外部認証サーバー を参照する前に、まず認証サーバーオブジェクトを定義する必要があります。以下の例では、RADIUS サーバー、SecurID サーバー、LDAP サーバー、および TACACS+ サーバーに、認証サーバーオブジェクトを定義する方法を示します。

例 : RADIUS 認証サーバー

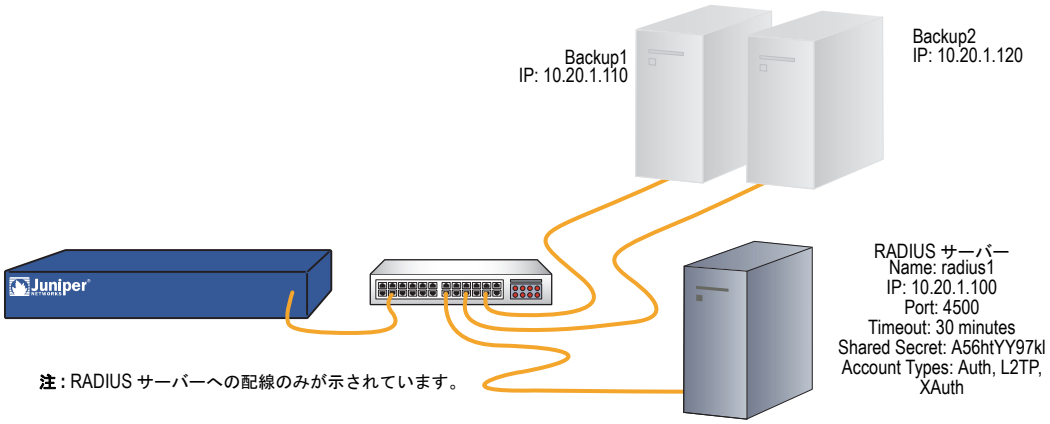
以下の例では、RADIUS サーバーの認証サーバーオブジェクトを定義します。認証、L2TP、および XAuth のような、ユーザーアカウントタイプを指定します。RADIUS サーバーには、「 radius1 」という名前をつけて、セキュリティデバイスが自動的に割り当てる ID 番号を受け入れるようにします。IP アドレス、10.20.1.100 を入力して、ポート番号をデフォルト (1645) から 4500 に変更します。共有秘密値は「 A56htYY97kl 」と定義します。また、IP アドレスがそれぞれ 10.20.1.110 と 10.20.1.120 の 2 つのバックアップサーバーを割り当てます。

認証アイドルタイムアウト値をデフォルト 10 分から 30 分に変更し、RADIUS 再試行タイムアウトを 3 秒から 4 秒に変更します。しかし、この設定では、(1 つのキーストロークが 30 分ごとに送られている限り) セッションが理論上は無期限に開いたままになるので、強制タイムアウトを 60 分に設定して、セッションの合計時間を制限します。この設定では、ユーザーの認証テーブルエントリが削除された 1 時間後に、その認証テーブルエントリに関連付けられたセッションはすべて削除されます。ユーザーは再認証が必要になります。

また、RADIUS ディクショナリーファイルを RADIUS サーバーにロードして、以下のベンダー固有属性 (VSA) の検索をサポートするようにします。ユーザーグループ、管理権限、リモート L2TP および XAuth 設定。

図 13 では、セキュリティデバイスは、認証、L2TP、XAuth 認証要求を 10.20.1.100 の 1 次 RADIUS サーバー “radius1” に送信します。セキュリティデバイスが、1 次 RADIUS サーバーとのネットワーク接続を失うと、認証要求を 10.20.1.110 の backup1 に転送します。セキュリティデバイスが backup1 に到達できない場合には、認証要求を 10.20.3.120 の backup2 に転送します。

図 13: RADIUS バックアップ例



WebUI

Configuration > Auth > Auth Servers > New: 次のように入力してから **OK** をクリックします。

Name: radius1
IP/Domain Name: 10.20.1.100
Backup1: 10.20.1.110
Backup2: 10.20.1.120
Timeout: 30
Forced Timeout: 60
Account Type: Auth, L2TP, XAuth
RADIUS: (選択)
RADIUS Port: 4500
Retry Timeout: 4 (秒)
Shared Secret: A56htYY97kl

RADIUS サーバーに RADIUS ディクショナリーファイルをロードします。

注 : 詳細については、19 ページの「RADIUS ディクショナリーファイル」を参照してください。RADIUS サーバーにディクショナリーファイルをロードする方法は、使用されるサーバーの資料を参照してください。

CLI

```
set auth-server radius1 type radius
set auth-server radius1 account-type auth l2tp XAuth
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 forced-timeout 60
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500
set auth-server radius1 radius timeout 4
set auth-server radius1 radius secret A56htYY97kl
save
```

注 : アカウントタイプを入力する順番は重要です。たとえば、まず **set auth-server radius1 account-type l2tp** と入力すると、それに続く選択肢は **XAuth** のみで、**l2tp** の後に **auth** を入力することはできません。アルファベット順ですので、正しい順番を覚えるのは簡単です。

ポート番号を変更することで、デフォルトの RADIUS ポート番号 (1645) を狙う攻撃の可能性を軽減することができます。

RADIUS サーバーに RADIUS ディクショナリーファイルをロードします。

注 : 詳細については、19 ページの「RADIUS ディクショナリーファイル」を参照してください。RADIUS サーバーにディクショナリーファイルをロードする方法は、使用されるサーバーの資料を参照してください。

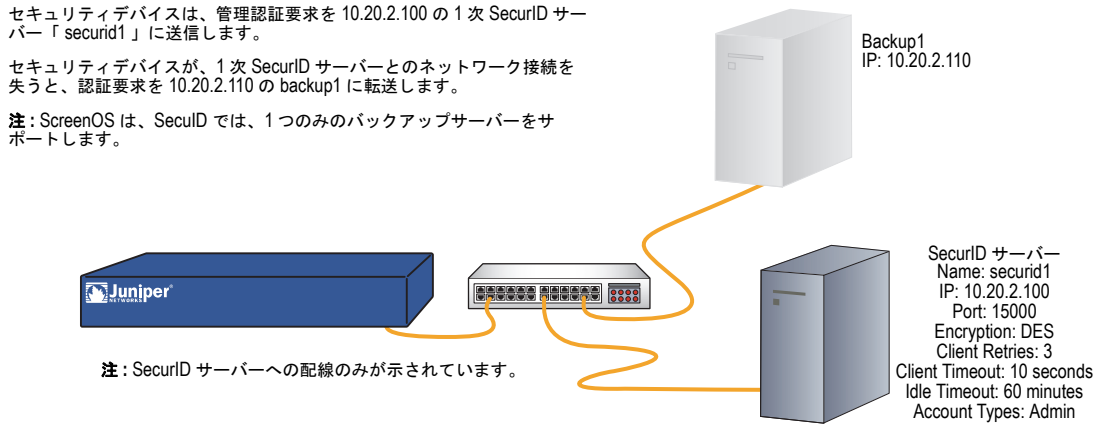
例 : SecurID 認証サーバー

以下の例では、SecurID ACE サーバーの認証サーバーオブジェクトを構成します。ユーザーアカウントタイプを管理と指定します。サーバーには、「 securid1 」という名前をつけて、セキュリティデバイスが自動的に割り当てる ID 番号を受け入れるようにします。1 次サーバーの IP アドレス、10.20.2.100 とバックアップサーバーの IP アドレスを入力します。10.20.2.110. ポート番号をデフォルト (5500) から 15000 に変更します。セキュリティデバイスと SecurID ACE サーバーは、DES 暗号を使用して、認証情報を保護します。リトライは 3 回まで許可され、クライアントタイムアウト値は 10 秒です。アイドルタイムアウト値は、デフォルト（ 10 分）から 60 分に変更します。**Use Duress** 設定は使用不能になります。図 14 を参照してください。

注 : クライアントタイムアウト値は、SecurID クライアントセキュリティデバイス) が認証リトライの間に待つ秒数です。

アイドルタイムアウト値は、セキュリティデバイスが活動していない管理セッションを自動的に終了させるまでのアイドルタイムの分数です (管理ユーザーやその他のユーザータイムに適用されるタイムアウト値の比較情報は、16 ページの「認証サーバーオブジェクトプロパティ」を参照してください。

図 14: SecurID バックアップ例



WebUI

Configuration > Auth > Auth Servers > New: 次のように入力してから **OK** をクリックします。

Name: securid1
IP/Domain Name: 10.20.2.100
Backup1: 10.20.2.110
Timeout: 60
Account Type: admin
SecurID: (選択)
Client Retries: 3
Client Timeout: 10 seconds
Authentication Port: 15000
Encryption Type: DES
User Duress: No

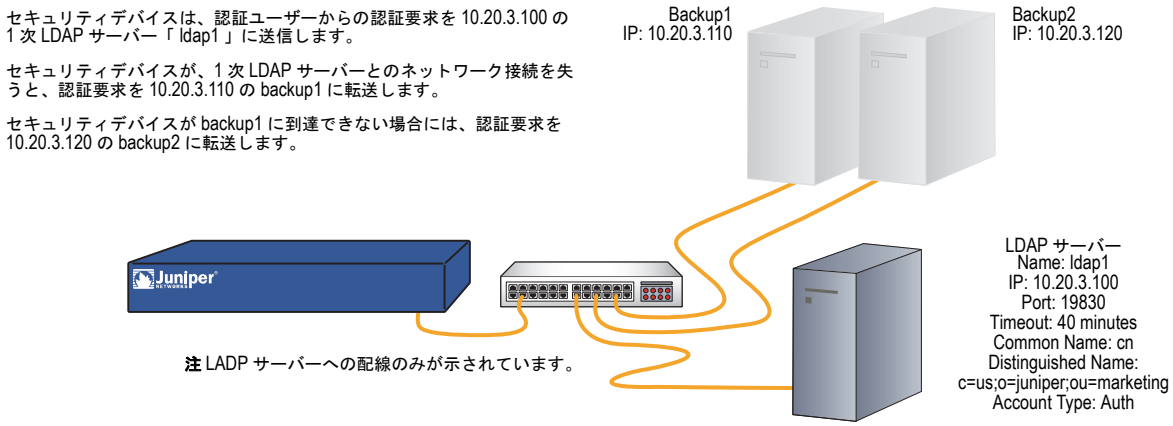
CLI

```
set auth-server securid1 type securid
set auth-server securid1 server-name 10.20.2.100
set auth-server securid1 backup1 10.20.2.110
set auth-server securid1 timeout 60
set auth-server securid1 account-type admin
set auth-server securid1 securid retries 3
set auth-server securid1 securid timeout 10
set auth-server securid1 securid auth-port 15000
set auth-server securid1 securid encr 1
set auth-server securid1 securid duress 0
save
```

例 : LDAP 認証サーバー

以下の例では、LDAP サーバーの認証サーバーオブジェクトを構成します。ユーザーアカウントタイプを **auth** と指定します。LDAP サーバーには、「 ldap1 」という名前をつけて、セキュリティデバイスが自動的に割り当てる ID 番号を受け入れるようにします。IP アドレス、10.20.3.100 を入力して、ポート番号をデフォルト 389 から 19830 に変更します。アイドルタイムアウト値は、デフォルト（10 分）から 40 分に変更します。また、IP アドレスがそれぞれ 10.20.3.110 と 10.20.3.120 の 2 つのバックアップサーバーを割り当てます。LDAP の通称識別子は **cn** で、識別名は、**c = us;o = juniper;ou = marketing** です。図 15 を参照してください。

図 15: LDAP バックアップ例



WebUI

Configuration > Auth > Auth Servers > New: 次のように入力してから **OK** をクリックします。

Name: ldap1
IP/Domain Name: 10.20.3.100
Backup1: 10.20.3.110
Backup2: 10.20.3.120
Timeout: 40
Account Type: Auth
LDAP: (選択)
LDAP Port: 4500
Common Name Identifier: cn
Distinguished Name (dn): c=us;o=juniper;ou=marketing

CLI

```
set auth-server ldap1 type ldap
set auth-server ldap1 account-type auth
set auth-server ldap1 server-name 10.20.3.100
set auth-server ldap1 backup1 10.20.3.110
set auth-server ldap1 backup2 10.20.3.120
set auth-server ldap1 timeout 40
set auth-server ldap1 ldap port 15000
set auth-server ldap1 ldap cn cn
set auth-server ldap1 ldap dn c=us;o=juniper;ou=marketing
save
```

例 : TACACS+ 認証サーバー

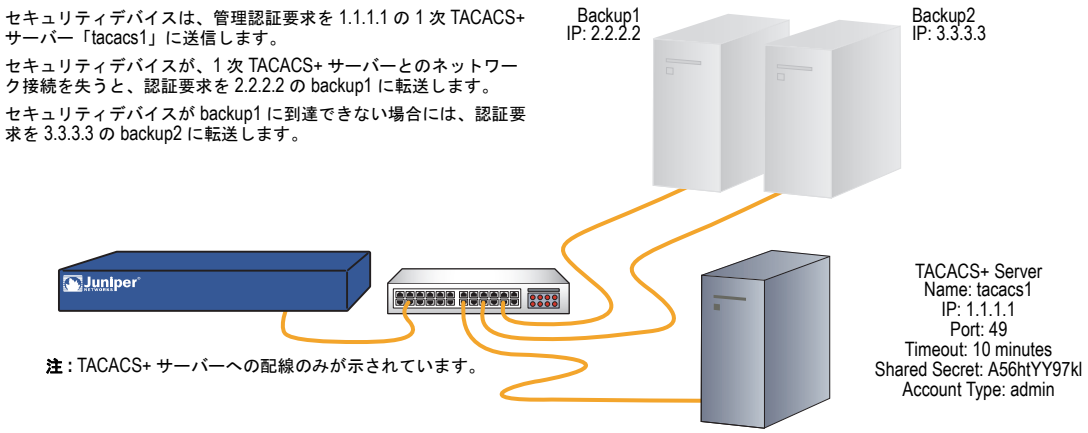
以下の例では、TACACS + サーバーの認証サーバーオブジェクトを定義します。TACACS + サーバーには、「tacacs1」という名前をつけて、セキュリティデバイスが自動的に割り当てる ID 番号を受け入れるようにします。IP アドレスに 1.1.1.1 を入力します。共有シークレットを 鄭 56htYY97klî を定義します。また、IP アドレスがそれぞれ 2.2.2.2 および 3.3.3.3 の 2 つのバックアップサーバーを割り当てます。

デバイス上で構成した TACACS + 機能が利用可能になる前に、TACACS + サーバーにアクセスし構成しなければなりません。

認証アイドルタイムアウト値をデフォルト（10 分）から 30 分に変更し、TACACS + 再試行タイムアウトを 3 秒から 4 秒に変更します。しかし、この設定では、（1 つのキーストロークが 30 分ごとに送られている限り）セッションが理論上は無期限に開いたままになるので、強制タイムアウトを 60 分に設定して、セッションの合計時間を制限します。この設定では、ユーザーの認証テーブルエントリが削除された 1 時間後に、その認証テーブルエントリに関連付けられたセッションはすべて削除されます。ユーザーは再認証が必要になります。

図 16 で、セキュリティデバイスは、管理認証要求を 1.1.1.1 の 1 次 TACACS + サーバー「tacacs1」に送信します。セキュリティデバイスが、1 次 TACACS + サーバーとのネットワーク接続を失うと、認証要求を 2.2.2.2 の backup1 に転送します。セキュリティデバイスが backup1 に到達できない場合には、認証要求を 3.3.3.3 の backup2 に転送します。

図 16: TACACS+ バックアップ例



WebUI

Configuration > Auth > Auth Servers > New: 次のように入力してから **OK** をクリックします。

Name: tacacs1
IP/Domain Name: 1.1.1.1
Backup1: 2.2.2.2
Backup2: 3.3.3.3
Timeout: 10
Forced Timeout: 60
Account Type: admin
TACACS: (選択)
TACACS Port: 49
Retry Timeout: 4 (seconds)
Shared Secret: A56htYY97kl

CLI

```
set auth-server tacacs1 type tacacs
set auth-server tacacs1 account-type auth l2tp XAuth
set auth-server tacacs1 server-name 1.1.1.1
set auth-server tacacs1 backup1 2.2.2.2
set auth-server tacacs1 backup2 3.3.3.3
set auth-server tacacs1 forced-timeout 60
set auth-server tacacs1 timeout 10
set auth-server tacacs1 tacacs port 49
set auth-server tacacs1 tacacs timeout 4
set auth-server tacacs1 tacacs secret A56htYY97kl
set admin auth server tacacs1
save
```

注 : ポート番号を変更することで、デフォルトの TACACS ポート番号 (49) を狙う攻撃の可能性を軽減することができます。

デフォルト認証サーバーの定義

デフォルトによって、ローカルデータベースは、すべてのユーザータイプでデフォルト認証サーバーになっています。外部認証サーバーを以下の 1 つか複数のユーザータイプのデフォルト認証サーバーと指定することができます。

- Admin
- Auth
- L2TP
- XAuth
- 802.1x

そして、デフォルト認証サーバーをポリシー、L2TP トンネル、もしくは IKE ゲートウェイで認証を構成するときに、特定のユーザータイプに使用したい場合には、構成ごとに毎回認証サーバーを指定する必要はありません。セキュリティデバイスは、以前にデフォルトとして指定している適正な認証サーバーを参照します。

例 : デフォルト認証サーバーの変更

この例では、前記の例で作成した RADIUS、SecurID、および LDAP 認証サーバーオブジェクトを使用します :

- radius1 (31 ページの「例 : RADIUS 認証サーバー」を参照)
- securid1 (33 ページの「例 : SecurID 認証サーバー」を参照)
- ldap1 (35 ページの「例 : LDAP 認証サーバー」を参照)

その後、ローカルデータベース、radius1、securid1、および ldap1 を以下のユーザータイプのデフォルトサーバーとして割り当てます。

- Local: XAuth ユーザーのデフォルト認証サーバー
- radius1: L2TP ユーザーのデフォルト認証サーバー
- securid1: 管理ユーザーのデフォルト認証サーバー
- ldap1: 認証ユーザーのデフォルト認証サーバー

注： デフォルトでは、ローカルデータベースは、すべてのユーザータイプでデフォルト認証サーバーになっています。したがって、すでに外部認証サーバーを XAuth ユーザーのデフォルトサーバーとして割り当てていない限り、そのような構成を行う必要はありません。

WebUI

VPNs > AutoKey Advanced > XAuth Settings: Default Authentication Server ドロップダウンリストから、**Local** を選択して、**Apply** をクリックします。

VPNs > L2TP > Default Settings: Default Authentication Server ドロップダウンリストから、**radius1** を選択して、**Apply** をクリックします。

Configuration > Admin > Administrators: Admin Auth Server ドロップダウンリストから、**Local/securid1** を選択して、**Apply** をクリックします。

Configuration > Auth > Firewall: Default Authentication Server ドロップダウンリストから、**ldap1** を選択して、**Apply** をクリックします。

CLI

```
set XAuth default auth server Local
set l2tp default auth server radius1
set admin auth server securid1
set auth default auth server ldap1
save
```

注： デフォルトでは、ローカルデータベースは、すべてのユーザータイプでデフォルト認証サーバーになっています。したがって、すでに外部認証サーバーを XAuth ユーザーのデフォルトサーバーとして割り当てていない限り、そのような構成を行う必要はありません。

第 3 章

インフラネットの認証

本章では、統合型アクセス管理（UAC）ソリューションで、セキュリティデバイスが配備される様子を説明します。Juniper Networks 統合型アクセス管理 ソリューションは、企業インフラネットを横断したアプリケーションおよびサービスの配布を、安全かつ確実に行います。UAC ソリューションとは、ネットワーク、アプリケーションおよび端点のインテリジェンスの調整、ネットワークアプリケーションをサポートするのに必要な制御の提供、ネットワーク使用の管理、および脅威の低減を行う、IP ベースのエンタープライズインフラストラクチャです。

統合型アクセス管理（UAC）ソリューションの構成および実装に関する詳細については、*Unified Access Control Administration Guide* を参照してください。

本章のセクションは、以下のようになります。

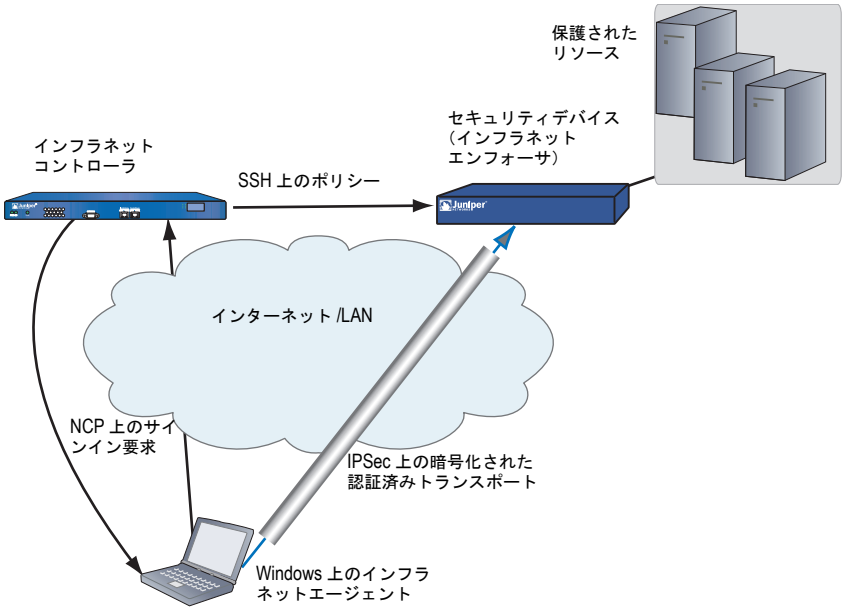
- 40 ページの「統合型アクセス管理ソリューション」
- 41 ページの「ファイアウォールとインフラネットコントローラの連携」
- 42 ページの「インフラネット認証用の構成」

統合型アクセス管理ソリューション

統合型アクセス管理 の実装では、セキュリティデバイスは インフラネットコントローラ と連携して、ポリシーを実施します。*インターフェースエンフォーサ*とも呼ばれるセキュリティデバイスが、図 17 で示すように、保護したいサーバーおよびリソースの前に実装されます。

統合型アクセス管理ソリューション、インフラネットコントローラの詳細については、*Unified Access Control Administration Guide* を参照してください。

図 17: インフラネット認証用のセキュリティデバイスの実装



セキュリティデバイスとインフラネットコントローラは、連携して、認定されたエンドユーザーが保護されたリソースにのみアクセスできるように、細分化された端点のセキュリティとファイアウォールサービスを提供します。

たとえば、*従業員*用の保護されたリソースへの完全なアクセスや、*契約者*用の制限されたアクセスなど、アクセスのレベルを定義する役割を持つようにインフラネットコントローラを構成できます。また、端点が、あるセキュリティ要件を満たす必要があり、満たさない場合は、保護されたリソースへのアクセスを拒否する、インフラネットコントローラのポリシーも作成できます。たとえば、ウィルス撃退アプリケーションの最小限のバージョンを使用し、かつ最新のアンチウイルスの定義を持つことを、端点に要求できます。端点がセキュリティ要件を満たさない場合、端点が要件を満たすようにする方法をユーザーに指示するページを表示できます。

セキュリティデバイスは、役割と端点セキュリティの遵守に基づいて、リソースへのアクセスを許可または拒否します。セキュリティデバイスは、NetScreen アドレス変更通知（NACN）プロトコルを使用する SSH 接続上のインフラネットコントローラと接続されます。2 つのデバイス間の接続を構成するには、*Unified Access Control Administration Guide* を参照してください。

ファイアウォールとインフラネットコントローラの連携

このセクションは、通信を確立し、セキュリティポリシーを実行するため、ファイアウォール（Juniper Networks セキュリティデバイス）とインフラネットコントローラが連携する様子を説明します。

1. 起動時に、セキュリティデバイスは、NACN プロトコルを使用して、SSL 接続上のインフラネットコントローラと連絡をとります。

   セキュリティデバイスが、8 台までのインフラネットコントローラと連携するように構成できます。セキュリティデバイスは、1 度に 1 つのインフラネットコントローラとしか通信しません。他のインフラネットコントローラは、インフラネットコントローラクラスタ内のフェールオーバーに使用されます。セキュリティデバイスが最初のインフラネットコントローラに接続できない場合、接続できるまで、構成リストの次のコントローラとの接続を試みます。セキュリティデバイスで構成されたインフラネットコントローラはすべて、同じインフラネットコントローラクラスタのメンバである必要があります。

2. セキュリティデバイスがインフラネットコントローラとの NACN 接続を確立した後、インフラネットコントローラはセキュリティデバイスとの SSH 接続を開始します。インフラネットコントローラは、ポリシーとユーザー認証情報をセキュリティデバイスへプッシュするため、この SSH 接続を使用します。

3. インフラネットコントローラがユーザーを認証し、ユーザーのコンピュータが端点のセキュリティポリシーに準拠していることを確認する場合は常に、インフラネットコントローラは、セキュリティデバイスへユーザー認証情報をプッシュします。この情報は、各認証済みユーザーの*認証テーブル*エントリを含んでいます。

   認証テーブルエントリは、ユーザーの役割とソース IP アドレスから構成されます。IKE ゲートウエイ、VPN およびトンネルインフラネット認証ポリシーによって、ユーザーの端点は、ネットワークトラフィックを保護するセキュリティデバイスと IPSec トンネルを確立できます。

4. セキュリティデバイスは、インフラネット認証ポリシーと合致するユーザーからのトラフィックを検知すると、ユーザーの保護されたリソースへのアクセスを許可するかどうかを判断するため、保護されたリソースに適用するアクセスポリシーおよびユーザーの認証テーブルエントリを使用します。

   アクションの許可および拒否に加えて、インフラネットコントローラポリシーでは、DI、IDP、AV、ロギング、Web フィルタリング、およびアンチスパムのような追加のアクション項目をインフラネットコントローラにバインドできます。これらのアクションにインフラネットコントローラを構成する前に、関連するアクション項目に対するファイアウォールポリシーを構成し、インフラネット認証用にデバイスをセットアップしなければなりません。

   インフラネットコントローラポリシーは、ファイアウォールポリシーの特定の機能をオンまたはオフできます。たとえば、AV アクションがインフラネットコントローラアクセスポリシー（Resource policies > ScreenOS オプション）に対して定義されている場合、ファイアウォールはユーザーのトラフィックにウィルスがないか解析しますが、DI、IDP、ロギング、Web フィルタリング、またはアンチスパムは実行しません。

5. 必要に応じて、インフラネットコントローラは、セキュリティデバイスにコマンドを送信し、ポリシーや認証テーブルエントリを削除したり、保護されたリソースへのアクセスを拒否します。たとえば、ユーザーのコンピュータが、端点のセキュリティポリシーに準拠しなくなったときやインフラネットコントローラとの接続が失われたとき、ユーザーの役割の構成を変更したとき、またはネットワーク上のウイルスなどのセキュリティの問題に対応して、インフラネットコントローラ上の全ユーザーアカウントを使用不可能にするときなどに、この状況が発生する場合があります。

詳細については、*Unified Access Control Administration Guide* を参照してください。

インフラネット認証用の構成

インフラネット認証用にセキュリティデバイスを構成するのに必要なタスクは、次のとおりです。

- セキュリティデバイスをルート（route）または透過モードにセットアップする
- インターフェースをセキュリティゾーンにバインドする
- 認証局サーバー設定を構成する
- インフラネットコントローラインスタンスをルートモードで作成する
- インフラネットコントローラインスタンスの構成を表示する
- ソースの IP ベースのポリシーを設定する
- インフラネットエンフォーサでポリシーを設定する
- セキュリティデバイスでキャプティブポータルを構成する

上のタスクを実行するには、ルートアクセスを持っていなければなりません。各タスクの構成方法の詳細については、*Unified Access Control Administration Guide* を参照してください。

第 4 章

認証ユーザー

認証ユーザー（または *auth user* ）は、ファイアウォールを越えた接続を行うときに、認証のためにユーザー名とパスワードを提供しなければならないネットワークユーザーです。認証ユーザーアカウントは、ローカルデータベースか、外部 RADIUS、SecurID、もしくは LDAP サーバーに保存できます。

複数の認証ユーザーアカウントをひとまとめにして、認証ユーザーグループを作成し、ローカルデータベースまたは RADIUS サーバーに保存することができます。1 つの認証ユーザーアカウントは、ローカルデータベースまたは RADIUS サーバーの最大 4 個のユーザーグループに入れることができます。RADIUS サーバーで外部ユーザーグループを作成するときは、セキュリティデバイスでまったく同じ（ただしメンバーのいない）ユーザーグループを作成する必要があります。たとえば、「 rs1 」という名前の RADIUS サーバー上に「 au_grp1 」という名前の認証ユーザーグループを定義して、メンバー 10 名をそのグループに参加させる場合は、セキュリティデバイスで、やはり「 au_grp1 」という名前のユーザーグループを定義して、外部ユーザーグループとしての識別させます。しかし、メンバーの追加は行わないようにする必要があります。ポリシーで、外部ユーザーグループ「 au_grp1 」と、認証サーバー「 rs1 」を参照して、ポリシーにトラフィックを照合することにより認証チェックを開始させた場合には、セキュリティデバイスは、指定された RADIUS サーバーを適正に検索することができます。本章のセクションは、以下のようになります。

- 44 ページの「ポリシーで認証ユーザーを参照する」
  - 44 ページの「ランタイム認証」
  - 45 ページの「事前ポリシーチェック認証 (WebAuth)」
- 46 ページの「ポリシーでの認証ユーザーグループの参照」
  - 47 ページの「例 : ランタイム認証 (ローカルユーザー)」
  - 48 ページの「例 : ランタイム認証 (ローカルユーザーグループ)」
  - 49 ページの「例 : ランタイム認証 (外部ユーザー)」
  - 51 ページの「例 : ランタイム認証 (外部ユーザーグループ)」
  - 53 ページの「例 : 複数グループのローカル認証ユーザー」
  - 55 ページの「例 : WebAuth (ローカルユーザーグループ)」
  - 57 ページの「例 : WebAuth (外部ユーザーグループ)」
  - 59 ページの「例 : WebAuth + SSL のみ (外部ユーザーグループ)」

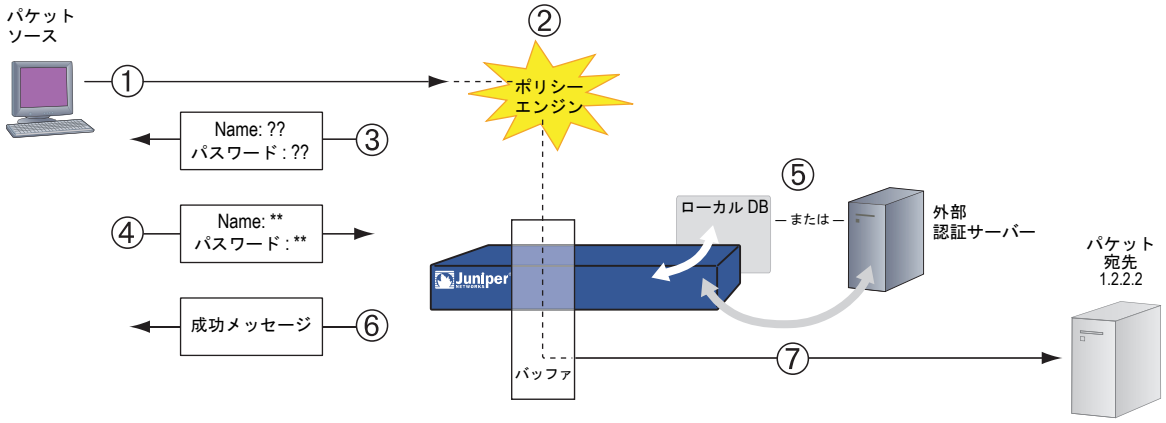
ポリシーで認証ユーザーを参照する

認証ユーザーを定義すると、ユーザーに 2 つの認証スキームのどちらかで自身を認証することを要求するポリシーを作成することができます。最初のスキームは、認証を要求するポリシーと照合する FTP、HTTP、もしくは Telnet トラフィックがセキュリティデバイスに到達するときにユーザーを認証します。2 つめのスキームでは、ユーザーはユーザー認証を要求するポリシーが適用されるトラフィック (FTP、HTTP、もしくは Telnet 以外のものならどれでも) を送信する前に自身を認証します。

ランタイム認証

ユーザーが、認証を要求するポリシーが適用される HTTP、FTP、もしくは Telnet 接続要求を起動しようとする場合には、セキュリティデバイスは、要求を代行受信して、ユーザーに名前とパスワードを入力するプロンプトが出されます (**2**-172 ページの「ユーザー認証」を参照)。許可を与える前に、セキュリティデバイスはユーザー名とパスワードをローカルデータベースか外部認証サーバーに保存されたものと照合します。図 18 を参照してください。

図 18: ユーザーのポリシールックアップ

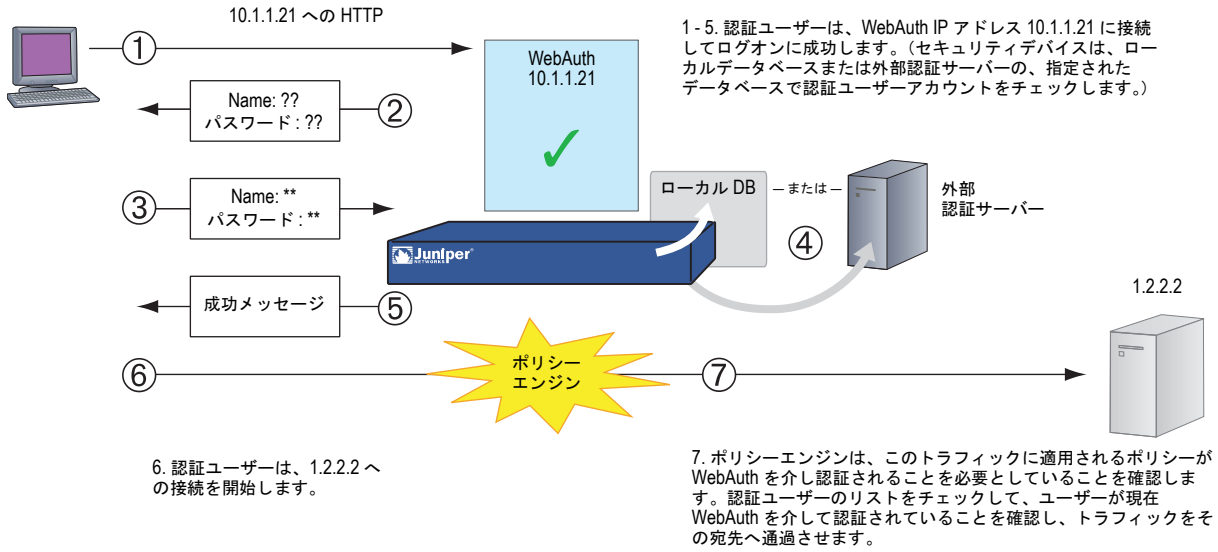


1. 認証ユーザーは、1.2.2.2 に FTP、HTTP、もしくは Telnet パケットを送信します。
2. セキュリティデバイスはパケットを代行受信して、ポリシーがローカルデータベースまたは外部認証サーバーによる認証を要求していることを確認し、パケットをバッファに入れます。
3. セキュリティデバイスは、FTP、HTTP、もしくは Telnet を介して、ユーザーにログイン情報を入力するプロンプトを出します。
4. ユーザーは、ユーザー名とパスワードを入力します。
5. セキュリティデバイスは、ポリシー指定されているように、ローカルデータベースで認証ユーザーアカウントをチェックするか、ログイン情報を外部認証サーバーに送信します。
6. 適正な照合があれば（もしくは、外部認証サーバーから適正な照合が通知されると) セキュリティデバイスは、ユーザーにログインが成功したことを通知します。
7. セキュリティデバイスは、パケットをバッファから宛先の 1.2.2.2 に送信します。

事前ポリシーチェック認証 (WebAuth)

意図された宛先にトラフィックを送信する前に、認証ユーザーはセキュリティデバイスの WebAuth 機能のホストである IP アドレスに HTTP セッションを開始し、自身を認証します。セキュリティデバイスがユーザーを認証すると、ユーザーは WebAuth を介して認証されることを要求するポリシーで許可される宛先にトラフィックを送信することができます。図 19 を参照してください。

図 19: WebAuth 例



WebAuth に関する詳細情報 :

- デフォルトの WebAuth サーバーをローカルサーバーのままにするか、外部認証サーバーにその役目を持たせるようにするか、選択することができます。WebAuth 認証サーバーとなるための主な条件は、認証サーバーが認証ユーザーアカウントタイプをもたなければならないということです。
- WebAuth アドレスは、それをホストするために使用するインターフェースと同じサブネットになければなりません。たとえば、認証ユーザーに、IP アドレス 1.1.1.1/24 を持つ ethernet3 を介して WebAuth に接続してもらいたい場合には、WebAuth に、1.1.1.0/24 サブネットの IP アドレスを割り当てます。
- WebAuth アドレスは、任意の物理インターフェース、サブインターフェースもしくは VSI (仮想セキュリティインターフェース) の IP アドレスと同じサブネットにおくことができます (各種のインターフェースの情報に関しては、2-35 ページの「インターフェース」を参照してください。
- 透過モードで WebAuth を使用したい場合には、WebAuth アドレスを VLAN1 IP アドレスと同じサブネットにおくことができます。
- WebAuth アドレスは複数のインターフェースにおくことができます。
- 同じセキュリティゾーンに複数のインターフェースが関連付けられている場合は、WebAuth アドレスを 1 つのインターフェースのサブネットにおくと、異なったインターフェースを使用して同じゾーンから来るトラフィックも到達することができます。

- セキュリティデバイスが特定のソース IP アドレスでユーザーを認証した場合、WebAuth 経由の認証を必要とするポリシーで指定されているように、その後、同じアドレスのその他のユーザーからのトラフィックを許可します。ユーザーがすべてのオリジナルソースアドレスを 1 つの変換アドレスに変更する NAT デバイスからトラフィックを発信する場合に該当します。
- デバイスに指示して、WebAuth のセッションとして SSL (HTTPS) 接続のみを受け入れることができます。

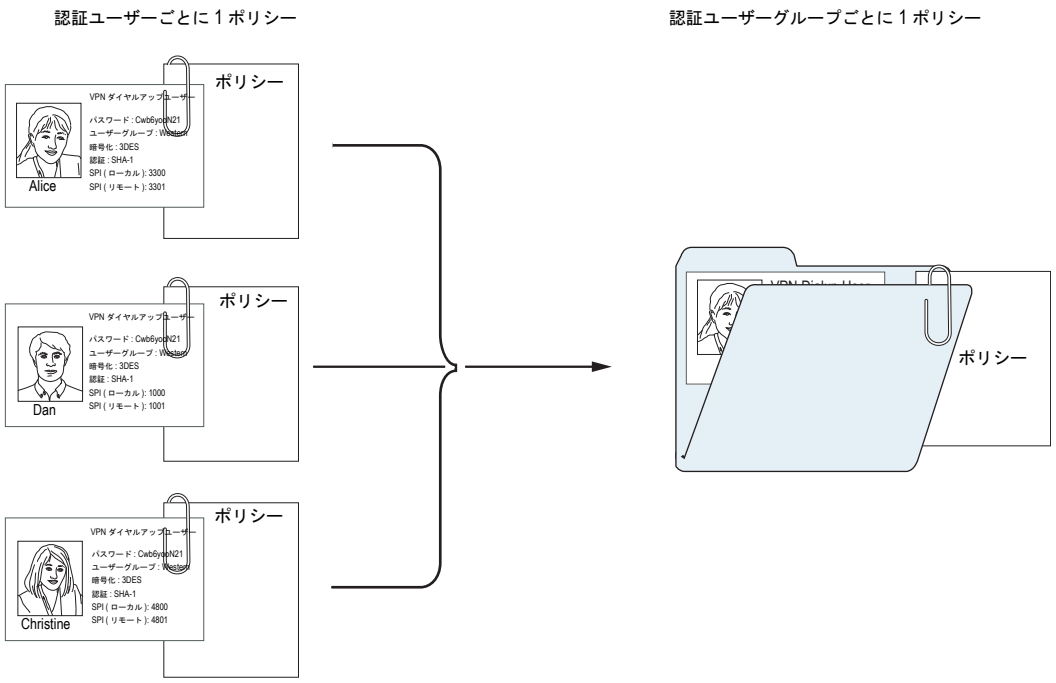
ポリシーでの認証ユーザーグループの参照

複数の認証ユーザーを管理するには、認証ユーザーグループを作成してローカルセキュリティデバイスまたは外部 RADIUS サーバーに保存します。

注： RADIUS サーバーのグループのユーザーを保存する場合、セキュリティデバイスにメンバーが入っていない外部ユーザー グループを作成し、RADIUS サーバーで作成したユーザーグループの名前に対応する名前を付けます。

各ユーザーを個別に管理するのではなく、ユーザーをグループとしてまとめ、グループに対して行う変更が各グループメンバーに伝達されるようにできます。1 つの認証ユーザーは、ローカルデータベースまたは RADIUS サーバーの最大 4 個のユーザーグループのメンバーであることができます。複数グループに属する認証ユーザーは、ユーザーがメンバーとして属する各グループに対して定義されたリソースにアクセスの許可を受けるために、ユーザー名とパスワードを一度だけ指定することが要求されます。図 20 を参照してください。

図 20: 認証ユーザーグループ



例 : ランタイム認証 (ローカルユーザー)

この例では、louis という名前のローカル認証ユーザーを、パスワード iDa84rNk、Trust ゾーンアドレス帳の “host1” という名前がついたアドレスで定義します。その後、2 つの出力ポリシーを構成します : 1 つはすべてのアウトバウンドトラフィックを拒否し、もう 1 つは host1 から louis に自分を認証するように要求します (Louis は、すべてのアウトバウンドトラフィックを host1 から発信する必要があります)。セキュリティデバイスは、それ以外のすべてのアドレス、および host1 からの非認証トラフィックを拒否します。

WebUI

1. ローカル認証ユーザーとアドレス

Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

User Name: louis
Status: Enable
Authentication User: (選択)
User Password: Da84rNk
Confirm Password: iDa84rNk

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: host1
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.4/32
Zone: Trust

2. ポリシー

Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), Any
Service: ANY
Action: Deny

Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), host1
Destination Address:
Address Book Entry: (選択), Any
Service: ANY
Action: Permit
Position at Top: (選択)

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Authentication: (選択)
Auth Server: (選択)
Use: Local
User: (選択), Local Auth User - louis

CLI

1. **ローカルユーザーとアドレス**
   set user louis password iDa84rNk
   set address trust host1 10.1.1.4/32

注： デフォルトでは、パスワードを割り当てたユーザーは認証ユーザーとみなされます。

2. **ポリシー**
   set policy from trust to untrust any any any deny
   set policy top from trust to untrust host1 any any permit auth user louis
   save

例：ランタイム認証 (ローカルユーザーグループ)

この例では、auth_grp1 という名前のローカルユーザーグループを定義します。あらかじめ作成した認証ユーザー (louis と lara) をグループに追加します。それから、auth_grp1 を参照するポリシーを構成します。ポリシーは、auth_grp1 に FTP-GET および FTP-PUT 権限と、DMZ ゾーンの「ftp1」(IP アドレス 1.2.2.3/32) という名前の FTP サーバーにアクセスできる Trust ゾーンのアドレス名「auth_grp1」(IP アドレス 10.1.8.0/24) を与えます。

注： ローカルデータベースにユーザーグループを作成するときには、そのユーザータイプはユーザーを追加するまでは未定義のままになります。その時点では、ユーザーグループは追加したユーザーの 1 つ 1 つか複数のタイプになります。IKE、L2TP、および XAuth ユーザータイプを追加することによって、複数タイプユーザーグループを作成することができます。管理ユーザーは、その他のユーザータイプと組み合わせることはできません。

WebUI

1. **ローカルユーザーグループとメンバー**
   Objects > Users > Local Groups > New: Group Name フィールドに **auth_grp1** と入力して、以下を行い、**OK** をクリックします。

   louis を選択して、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

   lara を選択して、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: auth_grp1
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 10.1.8.0/24
   Zone: Trust

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: ftp1
IP Address/Domain Name:
IP/Netmask: (選択), 1.2.2.3/32
Zone: DMZ

3. ポリシー

Policy > Policies > (From: Trust; To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), auth_grp1
Destination Address:
Address Book Entry: (選択), ftp1
Service: FTP
Action: Permit
Position at Top: (選択)

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Authentication: (選択)
Auth Server: (選択)
Use: Local
User Group: (選択), Local Auth Group - auth_grp1

CLI

1. ローカルユーザーグループとメンバー

```
set user-group auth_grp1 location local
set user-group auth_grp1 user louis
set user-group auth_grp1 user lara
```

2. アドレス

```
set address trust auth_grp1 10.1.8.0/24
set address dmz ftp1 1.2.2.3/32
```

3. ポリシー

```
set policy top from trust to dmz auth_grp1 ftp1 ftp permit auth user-group
    auth_grp1
save
```

例 : ランタイム認証 (外部ユーザー)

この例では、以下の属性を持つ「 x_srv1 」という名前の LDAP 認証サーバーを定義します。

- Account type: auth
- IP address: 10.1.1.100
- Backup1 IP address: 10.1.1.110
- Backup2 IP address: 10.1.1.120

- Authentication timeout: 60 分
- LDAP port number: 14500
- Common name identifier: cn
- Destinguished name: c = us;o = netscreen

パスワード eTcS114u を持つ認証ユーザーの「 euclid 」を外部認証サーバーにロードします。そして、外部ユーザー euclid のために認証サーバー x_srv1 の認証を要求する出力ポリシーを構成します。

WebUI

1. **認証サーバー**
   Configuration > Auth > Auth Servers > New: 次のように入力してから **OK** をクリックします。

   Name: x_srv1
   IP/Domain Name: 10.1.1.100
   Backup1: 10.1.1.110
   Backup2: 10.1.1.120
   Timeout: 60
   Account Type: Auth
   LDAP: (**選択**)
   LDAP Port: 14500
   Common Name Identifier: cn
   Distinguished Name (dn): c=us;o=netscreen

2. **外部ユーザー**
   外部 LDAP 認証サーバー x_serv1 でパスワード eTcS114u をもつ認証ユーザー 「euclid」を定義します。

3. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: euc_host
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 10.1.1.20/32
   Zone: Trust

4. **ポリシー**
   Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), Any
   Destination Address:
   Address Book Entry: (**選択**), Any
   Service: ANY
   Action: Permit
   Position at Top: (**選択**)

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

```
Authentication: ( 選択 )
Auth Server: ( 選択 )
   Use: x_srv1
User: ( 選択 ), External User
External User: euclid
```

CLI

1. **認証サーバー**
   ```
   set auth-server x_srv1
   set auth-server x_srv1 type ldap
   set auth-server x_srv1 account-type auth
   set auth-server x_srv1 server-name 10.1.1.100
   set auth-server x_srv1 backup1 10.1.1.110
   set auth-server x_srv1 backup2 10.1.1.120
   set auth-server x_srv1 timeout 60
   set auth-server x_srv1 ldap port 14500
   set auth-server x_srv1 ldap cn cn
   set auth-server x_srv1 ldap dn c=us;o=netscreen
   ```
2. **外部ユーザー**
   外部 LDAP 認証サーバー x_serv1 でパスワード eTcS1l4u をもつ認証ユーザー 「euclid」を定義します。
3. **アドレス**
   ```
   set address trust euc_host 10.1.1.20/32
   ```
4. **ポリシー**
   ```
   set policy top from trust to untrust euc_host any any auth server x_srv1 user euclid
   save
   ```

例 : ランタイム認証 (外部ユーザーグループ)

この例では、「 radius1 」という名前の外部 RADIUS 認証サーバーを構成して、「 auth_grp2 」という名前の外部認証ユーザーグループを定義します。外部認証ユーザーグループ auth_grp2 は 2 箇所で定義します。

1. 外部 RADIUS 認証サーバー「 radius1 」
2. セキュリティデバイス

注 : RADIUS 認証サーバー構成は、31 ページの「例 : RADIUS 認証サーバー」とほとんど同じですが、ユーザーアカウントタイプに「auth」のみを指定することが異なります。

認証ユーザーグループ「 auth_grp2 」を RADIUS サーバー上のみで認証ユーザーを入れ、セキュリティデバイスのグループには入れないようにしま。このグループのメンバーは、IP アドレス 10.1.1.80 にあるサーバーに排他的にアクセスする必要がある複数の会計士です。サーバーのアドレス帳入力を作成して、アドレスに「midas」という名前をつけます。そして、両方とも Trust ゾーンにある auth_grp2 から midas への認証トラフィックのみを許可するゾーン内ポリシーを構成します (ゾーン内ポリシーに関する詳細な情報は、**2**-161 ページの「ポリシー」を参照してください)。

RADIUS サーバー

1. RADIUS サーバーに RADIUS ディクショナリーファイルをロードします。

注： RADIUS ディクショナリーファイルに関する詳細については、19 ページの「RADIUS ディクショナリーファイル」を参照してください。RADIUS サーバーにディクショナリーファイルをロードする方法は、RADIUS サーバーの資料を参照してください。

Microsoft IAS RADIUS サーバーを使用している場合には、ディクショナリーファイルはありません。代わりに、サーバーで正しいベンダー固有属性 (VSA) を定義します。

---

2. RADIUS サーバーで認証アカウントユーザーを定義した後、ScreenOS ユーザーグループ VSA を使用してユーザーグループ「 auth_grp2 」を作成し、グループに追加したい認証ユーザーアカウントに適用します。

WebUI

1. 認証サーバー

Configuration > Auth > Auth Servers > New: 次のように入力してから **OK** をクリックします。

Name: radius1
IP/Domain Name: 10.20.1.100
Backup1: 10.20.1.110
Backup2: 10.20.1.120
Timeout: 30
Account Type: Auth
RADIUS: (選択)
RADIUS Port: 4500
Shared Secret: A56htYY97kl

2. 外部ユーザーグループ

Objects > Users > External Groups > New: 次のように入力してから **OK** をクリックします。

Group Name: auth_grp2
Group Type: Auth

3. アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: midas
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.80/32
Zone: Trust

4. ポリシー

Policy > Policies > (From: Trust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), midas
Service: ANY

Action: Permit
Position at Top: (選択)

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Authentication: (選択)
Auth Server: (選択)
Use: radius1
User Group: (選択), External Auth Group - auth_grp2

CLI

1. **認証サーバー**
   set auth-server radius1 type radius
   set auth-server radius1 account-type auth
   set auth-server radius1 server-name 10.20.1.100
   set auth-server radius1 backup1 10.20.1.110
   set auth-server radius1 backup2 10.20.1.120
   set auth-server radius1 timeout 30
   set auth-server radius1 radius port 4500
   set auth-server radius1 radius secret A56htYY97kl
2. **外部ユーザーグループ**
   set user-group auth_grp2 location external
   set user-group auth_grp2 type auth
3. **アドレス**
   set address trust midas 10.1.1.80/32
4. **ポリシー**
   set policy top from trust to trust any midas any permit auth server radius1 user-group auth_grp2
   save

例 : 複数グループのローカル認証ユーザー

この例では、Mary という名前のローカルユーザーを定義します。Mary は 2 つのサーバーへのアクセスを必要とするセールスマネージャです。サーバー A はセールスマン用のもので（sales_reps グループ）、サーバー B はマネージャ用のものです (sales_mgrs グループ)。両方へのアクセスを許可するために、Mary を 2 つのユーザーグループに追加します。次に、各グループに 1 つずつ、2 つのポリシーを作成します。

注 : この例では、ほかのグループ メンバーの構成が表示されません。

WebUI

1. **ローカルユーザー**
   Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

   User Name: mary
   Status: Enable
   Authentication User: (選択)
   User Password: iFa8rBd
   Confirm Password: iFa8rBd

2. **ローカルユーザーグループとメンバー**
   Objects > Users > Local Groups > New: Group Name フィールドに **sales_mgrs** と入力して、以下を行い、**OK** をクリックします。

   mary を選択して、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

   Objects > Users > Local Groups > New: Group Name フィールドに **sales_reps** と入力して、以下を行い、**OK** をクリックします。

   mary を選択して、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

3. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: sales
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 10.1.8.0/24
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: server_a
   IP Address/Domain Name:
   IP/Netmask: (**選択**)、1.1.1.5/32
   Zone: Untrust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: server_b
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 1.1.1.6/32
   Zone: Untrust

4. **ポリシー**
   Policy > Policies > (From: Trust; To: Untrust) > New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (**選択**), sales
   Destination Address:
   Address Book Entry: (**選択**), server_a
   Service: FTP
   Action: Permit
   Position at Top: (**選択**)

   > Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

   Authentication: (**選択**)
   Auth Server: (**選択**)
   Use: Local
   User Group: (**選択**), Local Auth Group - sales_reps

Policy > Policies > (From: Trust; To: Untrust) > New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**), sales
Destination Address:
Address Book Entry: (**選択**), server_b
Service: FTP
Action: Permit
Position at Top: (**選択**)

> Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

Authentication: (**選択**)
Auth Server: (**選択**)
Use: Local
User Group: (**選択**), Local Auth Group - sales_mgrs

CLI

1. **ローカルユーザー**
   set user mary password iFa8rBd
2. **ローカルユーザーグループとメンバー**
   set user-group sales_mgrs location local
   set user-group sales_mgrs user mary
   set user-group sales_reps location local
   set user-group sales_reps user mary
3. **アドレス**
   set address trust sales 10.1.8.0/24
   set address untrust server_a 1.1.1.5/32
   set address untrust server_b 1.1.1.6/32
4. **ポリシー**
   set policy top from trust to untrust sales server_a ftp permit auth user-group sales_reps
   set policy top from trust to untrust sales server_b ftp permit auth user-group sales_mgrs
   save

例 : WebAuth (ローカルユーザーグループ)

この例では、ユーザーにインターネットでアウトバウンドトラフィックを発信する前に、WebAuth 方式であらかじめ自身を認証するように要求します。セキュリティデバイスのローカルデータベースで「 auth_grp3 」という名前のユーザーグループを作成します。Trust ゾーンの全員に認証ユーザーアカウントを作成し、auth_grp3 に追加します。

Trust ゾーンインターフェースは、ethernet1 を使用して IP アドレス 10.1.1.1/24 を持っています。WebAuth IP アドレスとして 10.1.1.50 を割り当てて、デフォルト WebAuth サーバーとしてローカルデータベースを使用します。そのため、ユーザーがインターネットにトラフィックを発信する前には、まず 10.1.1.50 に HTTP 接続を確立して、ユーザー名とパスワードでログオンします。セキュリティデバイスはユーザー名とパスワードを自身のデータベースと照合して、認証

要求を認可もしくは拒否します。要求が認可されると、認証されたユーザーは、30 分以内にインターネットにトラフィックを発信できます。初回のセッションを終了した後、セキュリティデバイスがユーザーに自身を再認証するように要求するまでに、別のセッションを発信する猶予が 30 分あります。

WebUI

1. **WebAuth**

   Configuration > Auth > WebAuth: WebAuth サーバードロップダウンリストから、**Local** を選択して、**Apply** をクリックします。

   Network > Interfaces > Edit (ethernet1): **WebAuth** を選択して、WebAuth IP フィールドに **10.1.1.50** と入力します。

   Configuration > Auth > Auth Servers > Edit (Local): Timeout フィールドに **30** と入力して、**Apply** をクリックします。

2. **ユーザーグループ**

   Objects > Users > Local Groups > New: Group Name フィールドに **auth_grp3** と入力して、以下を行い、**OK** をクリックします。

   user name を選択して、**< <** ボタンを使用して、Available Members 列から Group Members 列に移動します。

   選択手順を繰り返してグループが完成するまで認証ユーザーを追加します。

3. **ポリシー**

   Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   　　Address Book Entry: (**選択**), Any
   Destination Address:
   　　Address Book Entry: (**選択**), Any
   Service: ANY
   Action: Permit

   > Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

   Authentication: (**選択**)
   WebAuth: (**選択**)
   User Group: (**選択**), Local Auth Group - auth_grp3

CLI

1. **WebAuth**

```
set webauth server Local
set interface ethernet1 webauth-ip 10.1.1.50
set interface ethernet1 webauth
set auth-server Local timeout 30
```

2. **ユーザーグループ**

```
set user-group auth_grp3 location local
```

注 : セキュリティデバイスは、追加したメンバーのタイプからローカルユーザーグループタイプを判断します。auth_grp3 を認証ユーザーグループにするには、グループに認証ユーザーを追加します。

以下のコマンドを使って作成したばかりのユーザーグループに認証ユーザーを追加します。

set user-group auth_grp3 user *name_str*

3. ポリシー

```
set policy top from trust to untrust any any any permit webauth user-group
    auth_grp3
save
```

例 : WebAuth (外部ユーザーグループ)

WebAuth は、ファイアウォールを越えてトラフィックを発信する前にユーザーをあらかじめ認証する方法です。この例では、すべての出力トラフィックで WebAuth 方式での認証を要求するポリシーを作成します。

RADIUS サーバー「 radius1 」とセキュリティデバイスで「 auth_grp4 」という名前の認証ユーザーグループを作成します。RADIUS サーバーで、Trust ゾーンの全員にユーザーアカウントを作成し、auth_grp4 に追加します。

注 : ここで使われる RADIUS 認証サーバー構成は、31 ページの「例 : RADIUS 認証サーバー」とほとんど同じですが、ユーザーアカウントタイプに「auth」のみを指定するところが異なります。

Trust ゾーンインターフェースは ethernet1 を使用し、IP アドレス 10.1.1.1/24 を持っています。WebAuth IP アドレスとして 10.1.1.50 を割り当て、外部 RADIUS 認証サーバー「 radius1 」をデフォルト WebAuth サーバーとして使用します。そのため、ユーザーがインターネットにトラフィックを発信する前には、まず 10.1.1.50 に HTTP 接続を確立して、ユーザー名とパスワードでログオンします。セキュリティデバイスは、すべての WebAuth ユーザー認証要求と応答を「 radius1 」とログオンしようとしているユーザーの間で中継します。

RADIUS サーバー

1. RADIUS サーバーに RADIUS ディクショナリーファイルをロードします。

注 : RADIUS ディクショナリーファイルに関する詳細については、19 ページの「RADIUS ディクショナリーファイル」を参照してください。RADIUS サーバーにディクショナリーファイルをロードする方法は、RADIUS サーバーの資料を参照してください。

2. 認証サーバー「 radius1 」にユーザーグループ「 auth_grp4 」を入力し、認証ユーザーアカウントを入れます。

WebUI

1. **認証サーバー**
   Configuration > Auth > Auth Servers > New: 次のように入力してから **OK** をクリックします。

   Name: radius1
   IP/Domain Name: 10.20.1.100
   Backup1: 10.20.1.110
   Backup2: 10.20.1.120
   Timeout: 30
   Account Type: Auth
   RADIUS: (選択)
   RADIUS Port: 4500
   Shared Secret: A56htYY97k

2. **WebAuth**
   Configuration > Auth > WebAuth: WebAuth Server ドロップダウンリストから、**radius1** を選択して、**Apply** をクリックします。

   Network > Interfaces > Edit (ethernet1): **WebAuth** を選択して、WebAuth IP フィールドに **10.10.1.50** と入力し、**OK** をクリックします。

3. **ユーザーグループ**
   Objects > Users > External Groups > New: 次のように入力してから **OK** をクリックします。

   Group Name: auth_grp4
   Group Type: Auth

4. **ポリシー**
   Policy > Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Any
   Destination Address:
   Address Book Entry: (選択), Any
   Service: ANY
   Action: Permit

   > Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

   Authentication: (選択)
   WebAuth: (選択)
   User Group: (選択), External Auth Group - auth_grp4

CLI

1. **Auth-Server**

```
set auth-server radius1 type radius
set auth-server radius1 account-type auth
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
```

```
set auth-server radius1 radius port 4500
set auth-server radius1 radius secret A56htYY97kl
```

2. **WebAuth**

```
set webauth server radius1
set interface ethernet1 webauth-ip 10.1.1.50
set interface ethernet1 webauth
```

3. **ユーザーグループ**

```
set user-group auth_grp4 location external
set user-group auth_grp4 type auth
```

4. **ポリシー**

```
set policy top from trust to untrust any any any permit webauth user-group
    auth_grp4
save
```

例 : WebAuth + SSL のみ (外部ユーザーグループ)

この例では WebAuth をセキュアソケットレイヤ (SSL) テクノロジーと組み合わせ、ログインする際にユーザーが送信するユーザー名とパスワードの安全を確保します。WebAuth は WebUI を介してセキュリティデバイスへの管理トラフィックの管理の安全を確保するために使用する証明書と同じものを使用します。(SSL に関する詳細は、3-5 ページの「セキュアソケットレイヤー」を参照してください。)

外部認証サーバー＋ SSL を使用した WebAuth の構成には、次の手順が含まれます。

- 外部 RADIUS 認証サーバー「 radius1 」を定義して「 auth_grp5 」という名の認証ユーザーグループを、RADIUS サーバーとセキュリティデバイスの両方に作成します。RADIUS サーバーでは、Untrust ゾーンの認証ユーザー全員にユーザーアカウントを作成し、auth_grp5 に追加します。

注 : 「auth」のみをユーザーアカウントタイプとして指定すること以外、ここで使われる RADIUS サーバー設定は、31 ページの「例 : RADIUS 認証サーバー」とほとんど同じものです。

- Untrust　ゾーンインターフェースは、ethernet3 を使用し、IP アドレス 1.1.1.1/24 を持ちます。WebAuth IP アドレスとして、1.1.1.50 を割り当て、デバイスが WebAuth 認証要求に SSL 接続のみを受け入れるよう指示し、外部 RADIUS 認証サーバー「radius1」を、デフォルト WebAuth サーバーとして定義します。
- 以下の SSL 設定を指定します。
  - セキュリティデバイスに前もってロードしている証明書の IDX 番号 (この例では、1)
  - DES_SHA-1 暗号
  - SSL ポート番号 2020
- そして、Untrust ゾーンから Trust ゾーンへのすべてのトラフィックに WebAuth + SSL 方式を介して認証を要求する入力ポリシーを構成します。

注： デジタル証明書を入手しロードする方法に関する情報は、5-19 ページの「公開鍵暗号化」を参照してください。

そのため、ユーザーが内部ネットワークにトラフィックを発信する前には、まず https://1.1.1.50:2020 に HTTP 接続を確立して、ユーザー名とパスワードでログオンする必要があります。セキュリティデバイスは、すべての WebAuth ユーザー認証要求と応答を「 radius1 」とログオンしようとしているユーザーの間で中継します。

RADIUS サーバー

1. RADIUS サーバーに RADIUS ディクショナリーファイルをロードします。

注： NetScreen ディクショナリーファイルに関する詳細については、19 ページの「RADIUS ディクショナリーファイル」を参照してください。RADIUS サーバーにディクショナリーファイルをロードする方法は、RADIUS サーバーの資料を参照してください。

2. 認証サーバー「 radius1 」にユーザーグループ「 auth_grp5 」を入力し、認証ユーザーアカウントを入れます。

WebUI

1. 認証サーバー

Configuration > Auth > Auth Servers > New: 次のように入力してから **OK** をクリックします。

Name: radius1
IP/Domain Name: 10.20.1.100
Backup1: 10.20.1.110
Backup2: 10.20.1.120
Timeout: 30
Account Type: Auth
RADIUS: (選択)
RADIUS Port: 4500
Shared Secret: A56htYY97k

2. WebAuth

Configuration > Auth > WebAuth: WebAuth Server ドロップダウンリストから、**radius1** を選択して、**Apply** をクリックします。

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

WebAuth: (選択)
IP: 1.1.1.50
SSL Only: (選択)

3. SSL

Configuration > Admin > Management: 次のように入力してから **OK** をクリックします。

HTTPS (SSL) Port: 2020
Certificate: (あらかじめロードした証明書を選択)
Cipher: DES_SHA-1

4. **ユーザーグループ**
   Objects > Users > External Groups > New: 次のように入力してから **OK** をクリックします。

   Group Name: auth_grp5
   Group Type: Auth

5. **ポリシー**
   Policy > Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Any
   Destination Address:
   Address Book Entry: (選択), Any
   Service: ANY
   Action: Permit

   > Advanced: 以下を入力して、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

   Authentication: (選択)
   WebAuth: (選択)
   User Group: (選択), External Auth Group - auth_grp5

CLI

1. **認証サーバー**

```
set auth-server radius1 type radius
set auth-server radius1 account-type auth
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500
set auth-server radius1 radius secret A56htYY97kl
```

   RADIUS サーバーに RADIUS ディクショナリーファイルをロードします。

注 : RADIUS ディクショナリーファイルに関する詳細については、19 ページの「RADIUS ディクショナリーファイル」を参照してください。RADIUS サーバーにディクショナリーファイルをロードする方法は、RADIUS サーバーの資料を参照してください。

---

2. **WebAuth**

```
set webauth server radius1
set interface ethernet3 webauth-ip 1.1.1.50
set interface ethernet3 webauth ssl-only
```

3. **SSL**

```
set ssl port 2020
set ssl cert 1
set ssl encrypt des sha-1
set ssl enable
```

4. **ユーザーグループ**
   set user-group auth_grp5 location external
   set user-group auth_grp5 type auth

5. **ポリシー**
   set policy top from untrust to trust any any any permit webauth user-group
   auth_grp5
   save

第 5 章

IKE、XAuth、および L2TP ユーザー

本章では、3 種類のトンネリングプロトコルに関連するユーザー ー IKE (Internet Key Exchange) ユーザー、XAuth ユーザー、L2TP (Layer 2 Transport Protocol) ユーザーについて説明します。本章のセクションは、以下のようになります。

- 63 ページの「IKE ユーザーとユーザーグループ」
- 66 ページの「XAuth ユーザーとユーザーグループ」
  - 68 ページの「IKE ネゴシエーションの XAuth ユーザー」
  - 81 ページの「XAuth クライアント」
- 82 ページの「L2TP ユーザーとユーザーグループ」

注 : IKE および L2TP の概念と構成例については、*第 5 部: 仮想プライベート ネットワーク* を参照してください。

IKE ユーザーとユーザーグループ

IKE ユーザーは、動的に割り当てられた IP アドレスを持つリモート VPN ユーザーです。ユーザー、実際にはユーザーのデバイスは、セキュリティデバイスとのフェーズ 1 ネゴシエーションの間に、IKE ID と一緒に証明書もしくは事前共有鍵を送って自身を認証します。

IKE ID は、E メールアドレス、IP アドレス、ドメイン名、もしくは ASN1-DN であることがあります。セキュリティデバイスは、ユーザーが以下のいずれかを送信した場合には IKE ユーザーを認証します。

- 識別名 (DN) フィールドもしくは、SubAltName フィールドに 1 つか複数の値が示される**証明書**は、セキュリティデバイスで構成されたユーザーの IKE ID と同一です。
- **事前共有鍵**と **IKE ID** およびセキュリティデバイスは、受信した IKE ID と、セキュリティデバイスに保存された事前共有鍵シード値から同一の事前共有鍵を生成することができます。

注： 抽象構文記法、v. 1 、distinguished name (ASN1-DN) フォーマットを使用した IKE ID の例は、
CN = joe,OU = it,O = juniper,L = sunnyvale,ST = ca,C = us,E = joe@juniper.net です。

AutoKey IKE ゲートウェイ構成の IKE ユーザーもしくはユーザーグループを参照します。類似したゲートウェイとトンネル構成を必要とする IKE ユーザーをグループにまとめることによって、各 IKE ユーザーに、1 つのゲートウェイとトンネルを定義するかわりに、そのグループ (およびそのゲートウェイを参照する 1 つの VPN トンネル) を参照する 1 つのゲートウェイを定義するだけになります。

すべてのホストに別のユーザーアカウントを作成することが非実用的であることはよくあります。そのような場合、グループ IKE ID ユーザーと呼ばれる、1 人のメンバーだけをもつ IKE ユーザーグループを作成することができます。そのユーザーの IKE ID は、ダイアルアップ IKE ユーザーの IKE ID 定義になくてはならない値のセットを含みます。リモートダイアルアップ IKE ユーザーの IKE ID がグループ IKE ID ユーザーの IKE ID と適合すれば、ScreenOS はそのリモートユーザーを認証します。詳細については、**5**-182 ページの「グループ IKE ID」を参照してください。

注： IKE ユーザーと IKE ユーザーグループアカウントは、ローカルデータベースにのみ保存できます。

例 : IKE ユーザーの定義

この例では、それぞれ異なったタイプの IKE ID を持つ 4 人の IKE ユーザー、Amy、Basil、Clara、および Desmond を定義します。

- Amy - E メールアドレス (ユーザー完全修飾ドメイン名もしくは U-FQDN): my@juniper.net
- Basil - IP アドレス : 3.3.1.1
- Clara - 完全修飾ドメイン名 (FQDN): www.juniper.net
- Desmond - ASN1-DN 文字列 :
  CN = des,OU = art,O = juniper,L = sunnyvale,ST = ca,C = us,E = des@juniper.net

WebUI

Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

User Name: Amy
Status: Enable
IKE User: (**選択**)
Simple Identity: (**選択**)
IKE ID Type: AUTO
IKE Identity: amy@juniper.net

Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

User Name: Basil
Status: Enable

IKE User: (選択)
Simple Identity: (選択)
IKE ID Type: AUTO
IKE Identity: 3.3.1.1

Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

User Name: Clara
Status: Enable
IKE User: (選択)
Simple Identity: (選択)
IKE ID Type: AUTO
IKE Identity: www.juniper.net

Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

User Name: Desmond
Status: Enable
IKE User: (選択)
Use Distinguished Name for ID: (選択)
CN: des
OU: art
Organization: juniper
Location: sunnyvale
State: ca
Country: us
E-mail: des@juniper.net

CLI

```
set user Amy ike-id u-fqdn amy@juniper.net
set user Basil ike-id ip 3.3.1.1
set user Clara ike-id fqdn www.juniper.net
set user Desmond ike-id wildcard
    CN=des,OU=art,O=juniper,L=sunnyvale,ST=ca,C=us,E=des@juniper.net
save
```

例 : IKE ユーザーグループの作成

この例では、ike_grp1 という名前のユーザーグループを作成します。IKE ユーザーの Amy を追加すると IKE ユーザーグループになります。次の 64 ページの「例 : IKE ユーザーの定義」で定義した 3 人の IKE ユーザーを追加します。

WebUI

Objects > Users > Local Groups > New: Group Name フィールドに **ike_grp1** と入力して、以下を行い、**OK** をクリックします。

Amy を選択して、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

Basil を選択して、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

Clara を選択して、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

Desmond を選択して、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

CLI

```
set user-group ike_grp1 location local
set user-group ike_grp1 user amy
set user-group ike_grp1 user basil
set user-group ike_grp1 user clara
set user-group ike_grp1 user desmond
save
```

ゲートウェイの IKE ユーザーを参照

IKE ユーザーや IKE ユーザーグループを定義した後、リモート IKE ゲートウェイがダイアルアップユーザーまたはダイアルアップユーザーグループであるときは、IKE ゲートウェイ構成で参照できます。

ゲートウェイ構成での IKE ユーザーを参照は、以下の例を参照してください。

- 5-159 ページの「ポリシーベース ダイヤルアップ VPN、AutoKey IKE」
- 5-187 ページの「グループ IKE ID（証明書）の作成」
- 5-182 ページの「証明書付きグループ IKE ID」

XAuth ユーザーとユーザーグループ

XAuth プロトコルは 2 つの要素から構成されています。リモート VPN ユーザー認証 (ユーザー名とパスワード) および TCP/IP アドレス割り当て（ IP アドレス、ネットマスク、DNS サーバー、WINS サーバー割り当て）です。ScreenOS は、いずれのコンポーネントも、個別もしくは両方のコンポーネントの適用をサポートします。

注 : 割り当てられるネットマスクは常に、255.255.255.255 で、変更できません。

XAuth ユーザーまたはユーザーグループは、AutoKey IKE VPN トンネルを経由してセキュリティデバイスに接続し、オプションで TCP/IP 設定をセキュリティデバイスから受信するときに、自分自身が認証する 1 人または複数のリモートユーザーです。IKE ユーザーの認証が実際には VPN ゲートウェイまたはクライアントの認証であるのとは対照的に、XAuth ユーザーの認証は、ユーザー自身の認証です。XAuth ユーザーは、自分自身のみが知っている情報、たとえば、ユーザー名やパスワードを入力する必要があります。

ScreenOS-Remote クライアントは、VPN トラフィックを送信するときに、仮想アダプタを作成するために受けとる TCP/IP 設定を使用する一方、VPN 以外のトラフィックの場合は ISP またはネットワーク管理者により指定された TCP/IP ネットワークアダプタ設定を使用します。既知の IP アドレスをリモートユーザーに割り当てることで、特定のトンネルインターフェースを介してそれらのアドレスへのセキュリティデバイス上でのルートを定義できます。そして、セキュリティデバイスは、戻るルーティングがデフォルトゲートウェイを介してではなく、VPN トンネルを通って、リモートユーザーの IP アドレスに到達することを保証できます。アドレス割り当ては、ダウンストリームファイアウォールがポリシー作成時にこれらのアドレスを参照することを可能にします。IP アドレスが XAuth 寿命が設定された個々の XAuth ユーザーに関連付けられる時間の長さをコントロールできます。

注 : 仮想アダプタは、セキュリティデバイスが VPN トンネル接続の間にリモートユーザーに割り当てる TCP/IP 設定（ IP アドレス、DNS サーバーアドレス、WINS サーバーアドレス）です。ScreenOS-Remote クライアントのみ、仮想アダプタ機能をサポートします。Juniper Networks セキュリティプラットフォームはサポートしません。

ScreenOS は、XAuth の以下の特性をサポートします。

- ローカル XAuth ユーザーおよび外部 XAuth ユーザーの認証
- RADIUS 認証サーバーに保存された場合の、XAuth ユーザーグループおよび外部 XAuth ユーザーグループの認証
- RADIUS 認証サーバーに保存されたローカル XAuth ユーザーおよび外部 XAuth ユーザーへの IP アドレスプールからの IP、DNS サーバー、および WINS サーバーアドレス割り当て

  セキュリティデバイスで、外部 RADIUS サーバーに保存されたデフォルト XAuth 設定を使用するように構成するためには、以下のいずれかの手順を実行します。

  - WebUI: VPN > AutoKey Advanced > XAuth Settings ページで、**Query Client Settings on Default Server** を選択します。
  - CLI: **set XAuth default auth server** *name_str* **query-config** コマンドを入力します。

  セキュリティデバイスは、外部 RADIUS サーバーに保存されたゲートウェイ特有の XAuth 設定も使用できます。特定の IKE ゲートウェイを構成するときは、以下のいずれかの手順を行います。

  - WebUI: VPNs > AutoKey Advanced > Gateway > New > Advanced ページで、External Authentication ドロップダウンリストから、RADIUS の名前を選択し、**Query Remote Setting** を選択します。
  - CLI: **set ike gateway** *name_str* **XAuth server** *name_str* **query-config** コマンドを入力します。
- アドレス割り当てのない認証のみ、認証のないアドレス割り当てのみ (**set ike gateway** *name_str* **XAuth bypass-auth**)、および認証とアドレス割り当ての組み合わせ

IKE モードのイベントロギング

リモートユーザーがインターネット鍵交換（IKE）によってネットワークにアクセスすると、ScreenOS は XAuth でユーザーを認証します。ScreenOS はトラフィックログにイベントの詳細を記録します。ログの詳細には次が含まれます。

- ゲートウェイの IP アドレス
- ユーザー名
- セッション再試行の回数
- ローカルの IP プールまたは RADIUS サーバーから割り当てられたクライアントの IP アドレス

トラフィックログの表示に関する詳細については、*第 3 部 : 管理*を参照してください。

IKE ネゴシエーションの XAuth ユーザー

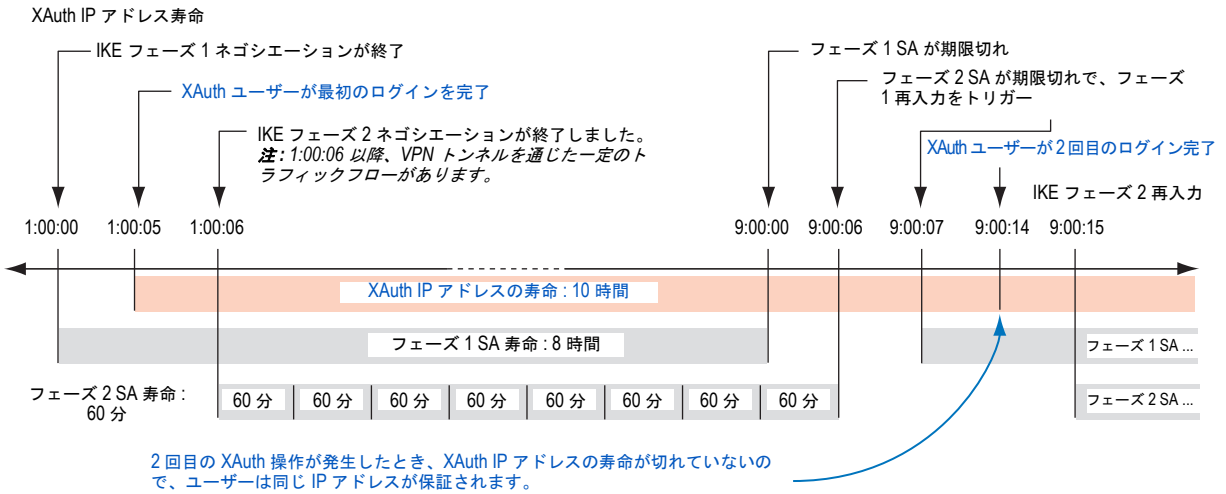
ScreenOS は、XAuth バージョン 6 (v6) をサポートします。フェーズ 1 IKE ネゴシエーションの双方の参加者が XAuth v6 をサポートすることを確認するために、双方は最初の 2 つのフェーズ 1 メッセージで、互いに以下のベンダー ID を送信します。0x09002689DFD6B712。ベンダー ID 番号は、XAuth 1 インターネット草稿、draft-beaulieu-ike-XAuth-02.txt で指定されています。

フェーズ 1 ネゴシエーションが完了したら、セキュリティデバイスはリモートサイトの XAuth ユーザーにログインプロンプトを送信します。XAuth ユーザーが正しいユーザー名とパスワードでログオンに成功したら、セキュリティデバイスはユーザーに IP アドレス、32 ビットネットマスク、DNS サーバーアドレス、WINS サーバーアドレス設定を割り当てて、双方はフェーズ 2 ネゴシエーションに移ります。

XAuth ユーザーは、ログインプロセスを完了するのに 60 秒間かかります。最初のログインが失敗すると、XAuth ユーザーは最大 4 回まで再試行をし、各試行ごとに 60 秒間かけることができます。ユーザーが 5 回連続失敗した場合、セキュリティデバイスはログインプロンプトを表示しなくなり、セッションを終了します。

XAuth で割り当てられた IP アドレスは、XAuth アドレス寿命で指定される期間内に、ユーザーに属します。IP アドレスは XAuth ユーザーにこれより長く属している場合があり、それはフェーズ 1 およびフェーズ 2 セキュリティアソシエーション (SA) 再入力によります。図 21 はフェーズ 1 およびフェーズ 2 再入力操作および XAuth IP アドレス寿命の関係を示します。

図 21: フェーズ 1 およびフェーズ 2 再入力操作および XAuth IP アドレス寿命



1. フェーズ 1 SA は 8 時間の寿命に設定され、最初の 8 時間が経過すると期限切れになります。

2. フェーズ 2 SA 寿命は 60 分に設定されます。XAuth ユーザーが自分のユーザー名とパスワードを入力する間、最初の IKE ネゴシエーション中に 5 秒の遅延があるため、8 回目の フェーズ 2 SA は、フェーズ 1 ネゴシエーションが完了した後で 8 時間 6 秒 (XAuth ログインのための 5 秒 + フェーズ 2 ネゴシエーションのための 1 秒) 経過した時点で期限切れになります。

3. アクティブな VPN トラフィックがあるため、8 回目のフェーズ 2 SA の期限切れにより、6 秒前に期限切れとなった フェーズ 1 SA が再入力されます。つまり、フェーズ 1 IKE ネゴシエーション (または「再ネゴシエーション」) が発生します。

4. フェーズ 1 IKE の再ネゴシエーションが完了した後で、セキュリティデバイスは XAuth ユーザーにもう一度ログインするようにプロンプトします。

注 : 最初のログインの後で再びログインするのを避けるには、VPN トンネルの待機時間を CLI コマンド ***set vpn*** *name* **gateway** *name* **idletime** *number (分)* を使って 0 以外に構成してください。フェーズ 1 IKE 再ネゴシエーションの完了時に VPN 活動がある場合、セキュリティデバイスは XAuth ユーザーに再びログインするようにプロンプトしません。このオプションを指定すると、ユーザーは中断なしで大きなファイルをダウンロードしたり、ストリーミングメディアを送受信したり、Web カンファレンスに参加することができるようになります。

---

5. XAuth アドレス寿命 (10 時間) がフェーズ 1 SA 寿命を超えるため、ユーザーは次のフェーズ 1 再入力が行われた後で別のアドレスを取得する可能性がある場合でも、同じ IP アドレスを維持します。

   XAuth アドレス寿命がフェーズ 1 SA 寿命よりも短かった場合、セキュリティデバイスはユーザーに別の IP アドレスを割り当て、そのアドレスは前もって割り当てられたアドレスと同じであるか、同じでない場合があります。

注 : ユーザーが常に同じ IP アドレスを割り当てられることが重要であれば、ユーザー構成でアドレスを指定することができます。この場合セキュリティデバイスは、IP プールからランダムに割り当てる代わりに、このアドレスを割り当てます。そのアドレスが、IP プールに入っていると、別ユーザーに割り当てられてしまい、必要なときに使用できなくなるため、IP プールに入れてはならないことを留意してください。

アドレス寿命を変更するには、以下のいずれかを実行します。

- (WebUI) VPNs > AutoKey Advanced > XAuth Settings: Reserve Private IP for XAuth User フィールドに数字 (分) を入力し、**Apply** をクリックします。
- (CLI) `set XAuth lifetime` *`number`*

効果的にアドレス寿命機能を使用不可にするには、許可される最小値である 1 を入力します。

例 : XAuth 認証 (ローカルユーザー)

この例では、x1 という名前のローカルデータベースにパスワード aGgb80L0ws を持つ XAuth ユーザーを定義し ます。

そして、このユーザーをリモート IKE ゲートウェイの IP 2.2.2.2 のピアへの構成で参照します。リモートゲートウェイには「 gw1 」という名前をつけて、Main mode とフェーズ 1 のプロポーザル pre-g2-3des-sha を指定して、事前共有鍵 juniper1 を使用します。VPN 1 トンネルに「vpn1」という名前をつけて、フェーズ 2 ネゴシエーションにプロポーザル「Compatible」セットを指定します。Untrust ゾーンインターフェース ethernet3 を出力インターフェースとして選択します。

WebUI

1. **XAuth ユーザー**
   Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

   User Name: x1
   Status: Enable
   XAuth User: (**選択**)
   User Password: iDa84rNk
   Confirm Password: iDa84rNk

2. **VPN**
   VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

   Gateway Name: gw1
   Security Level: Custom
   Remote Gateway Type:
   Static IP Address: (**選択**), Address/Hostname: 2.2.2.2
   Preshared Key: juniper1
   Outgoing Interface: ethernet3

   > Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

   Security Level: Custom: (**選択**)
   Phase 1 Proposal: pre-g2-3des-sha
   Mode (Initiator): Main (ID **保護**)
   XAuth Server: (**選択**)
   Local Authentication: (**選択**)
   User: (**選択**), x1

   VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

   VPN Name: vpn1
   Security Level: Compatible
   Remote Gateway Tunnel: gw1

CLI

1. **XAuth ユーザー**

```
set user x1 password aGgb80L0ws
set user x1 type XAuth
unset user x1 type auth
```

注 : CLI コマンド **set user** *name_str* **password** *pswd_str* は、認証ユーザーを作成します。XAuth のみのユーザーを作成するには、ユーザーを XAuth ユーザーとして定義してから (**set user** *name_str* type **XAuth**)、認証ユーザー定義を削除する必要があります (**unset user** *name_str* **type auth**)。

2. VPN

```
set ike gate gw1 ip 2.2.2.2 main outgoing-interface ethernet3 preshare juniper1
    proposal pre-g2-3des-sha
set ike gateway gw1 XAuth server Local user x1
set vpn vpn1 gateway gw1 sec-level compatible
save
```

例 : XAuth 認証 (ローカルユーザーグループ)

この例では、ローカルデータベースに xa-grp1 という名前のユーザーグループを作成し、70 ページの「例 : XAuth 認証 (ローカルユーザー)」で作成した XAuth ユーザーの「x1」を追加します。そのユーザーをグループに追加すると、自動的に XAuth ユーザーグループになります。

そして、このグループをリモート IKE ゲートウェイの IP 2.2.2.2 のピアへの構成で参照します。リモートゲートウェイには「gw1 」という名前をつけて、Main mode とフェーズ 1 のプロポーザル pre-g2-3des-sha を指定して、事前共有鍵「 juniper1 」を使用します。VPN トンネルに「vpn2」という名前をつけて、フェーズ 2 ネゴシエーションにプロポーザル「Compatible」セットを指定します。Untrust ゾーンインターフェース ethernet3 を出力インターフェースとして選択します。

WebUI

1. XAuth ユーザーグループ

Objects > Users > Local Groups > New: Group Name フィールドに **xa-grp1** と入力して、以下を行い、**OK** をクリックします。

x1 を選択して、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

2. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: gw2
Security Level: Custom
Remote Gateway Type:
Static IP Address: (選択), Address/Hostname: 2.2.2.2
Preshared Key: juniper2
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Phase 1 Proposal: pre-g2-3des-sha
Mode (Initiator): Main (ID 保護)
XAuth Server: (選択)
Local Authentication: (選択)
User Group: (選択), xa-grp1

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn2
Security Level: Compatible
Remote Gateway Tunnel:
Predefined: (選択), gw2

CLI

1. **XAuth ユーザーグループ**
   set user-group xa-grp1 location local
   set user-group xa-grp1 user x1

2. **VPN**
   set ike gate gw2 ip 2.2.2.2 main outgoing-interface ethernet3 preshare juniper2 proposal pre-g2-3des-sha
   set ike gateway gw2 XAuth server Local user-group xa-grp1
   set vpn vpn2 gateway gw2 sec-level compatible
   save

例 : XAuth 認証 (外部ユーザー)

この例では、外部 SecurID 認証サーバーで、以前にロードした iNWw10bd01 というパスワードを持つ「 xa-1 」という名前の XAuth ユーザーを参照します。この例は、33 ページの「例 : SecurID 認証サーバー」とほぼ同じである SecurID 認証サーバーの構成を使用しますが、ここではアカウントタイプを XAuth と定義することが異なります。

XAuth ユーザー xa-1 をリモート IKE ゲートウェイの IP 2.2.2.2 のピアへの構成で参照します。リモートゲートウェイには「 gw3 」という名前をつけて、Main mode とフェーズ 1 のプロポーザル pre-g2-3des-sha を指定して、事前共有鍵「 juniper3 」を使用します。VPN 1 トンネルに「 vpn3 」という名前をつけて、フェーズ 2 ネゴシエーションにプロポーザル g2-esp-3des-sha を指定します。Untrust ゾーンインターフェース ethernet3 を出力インターフェースとして選択します。

WebUI

1. **外部 SecurID 認証サーバー**
   Configuration > Auth > Auth Servers > New: 次のように入力してから **OK** をクリックします。

   Name: securid1
   IP/Domain Name: 10.20.2.100
   Backup1: 10.20.2.110
   Timeout: 60
   Account Type: XAuth
   SecurID: (選択)
   Client Retries: 3
   Client Timeout: 10 seconds
   Authentication Port: 15000
   Encryption Type: DES
   User Duress: No

2. **XAuth ユーザー**
   外部 SecurID 認証サーバー securid1 で、パスワード iNWw10bd01 を持つ認証ユーザー「 xa-1 」を定義します。

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: gw3
Security Level: Custom
Remote Gateway Type:
Static IP Address: (選択), Address/Hostname: 2.2.2.2
Preshared Key: juniper3
Outgoing Interface: ethernet3

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Phase 1 Proposal: pre-g2-3des-sha
Mode (Initiator): Main (ID 保護)
XAuth Server: (選択)
External Authentication: (選択), securid1
User: (選択)
Name: xa-1

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn3
Security Level: Compatible
Remote Gateway Tunnel:
Predefined: (選択), gw3

CLI

1. 外部 SecurID 認証サーバー

```
set auth-server securid1 type securid
set auth-server securid1 server-name 10.20.2.100
set auth-server securid1 backup1 10.20.2.110
set auth-server securid1 timeout 60
set auth-server securid1 account-type XAuth
set auth-server securid1 securid retries 3
set auth-server securid1 securid timeout 10
set auth-server securid1 securid auth-port 15000
set auth-server securid1 securid encr 1
set auth-server securid1 securid duress 0
```

2. XAuth ユーザー

外部 SecurID 認証サーバー securid1 で、パスワード iNWw10bd01 を持つ認証ユーザー「 xa-1 」を定義します。

3. VPN

```
set ike gate gw3 ip 2.2.2.2 main outgoing-interface ethernet3 preshare juniper3
    proposal pre-g2-3des-sha
set ike gateway gw3 XAuth server securid1 user xa-1
set vpn vpn3 gateway gw3 sec-level compatible
save
```

例 : XAuth 認証 (外部ユーザーグループ)

この例では、「 radius1 」という名前の外部 RADIUS 認証サーバーを構成して、「 xa_grp2 」という名前の外部認証ユーザーグループを定義します。外部 XAuth ユーザーグループ xa-grp2 は 2 箇所で定義します。

1. 外部 RADIUS 認証サーバー「 radius1 」

2. セキュリティデバイス

注 : RADIUS 認証サーバー構成は、31 ページの「例 : RADIUS 認証サーバー」とほとんど同じですが、ユーザーアカウントタイプに「XAuth」のみを指定することが異なります。

XAuth ユーザーグループ「 xa-grp2 」を RADIUS サーバー上のみで XAuth ユーザーを入れ、セキュリティデバイスのグループには入れないようにします。このグループのメンバーは、リモートサイトの小売業者で、企業 LAN の FTP サーバーへのアクセスを必要とします。IP アドレスが 10.2.2.0/24 のリモートサイトの項目を Untrust ゾーンアドレス帳に追加して、`reseller1` という名前をつけます。また、IP アドレス 10.1.1.5/32 を持った FTP サーバー「rsl-srv1」のアドレスを Trust ゾーンアドレス帳に入力します。

2.2.2.2 への VPN トンネルを、ユーザーグループ xa-grp2 の XAuth ユーザーを認証するように構成します。リモートゲートウェイには「 gw4 」という名前をつけて、Main mode とフェーズ 1 のプロポーザル pre-g2-3des-sha を指定して、事前共有鍵「 juniper4 」を使用します。VPN トンネルに「vpn4」という名前をつけて、フェーズ 2 ネゴシエーションにプロポーザル「Compatible」セットを指定します。Untrust ゾーンインターフェース ethernet3 を出力インターフェースとして選択します。

最後に Untrust ゾーンの reseller1 からの FTP トラフィックを vpn4 を介して、Trust ゾーンの rs1-svr1 に送信することを許可するポリシーを作成します。

RADIUS サーバー

1. RADIUS サーバーに RADIUS ディクショナリーファイルをロードします。

注 : RADIUS ディクショナリーファイルに関する詳細については、19 ページの「RADIUS ディクショナリーファイル」を参照してください。RADIUS サーバーにディクショナリーファイルをロードする方法は、RADIUS サーバーの資料を参照してください。

---

2. 外部認証サーバー「 radius1 」に認証ユーザーグループ「 xa-grp2 」を入力し、XAuth ユーザーアカウントを入れます。

WebUI

1. **認証サーバー**

   Configuration > Auth > Auth Servers > New: 次のように入力してから **OK** をクリックします。

   Name: radius1
   IP/Domain Name: 10.20.1.100
   Backup1: 10.20.1.110
   Backup2: 10.20.1.120
   Timeout: 30
   Account Type: XAuth
   RADIUS: (選択)
   RADIUS Port: 4500
   Shared Secret: A56htYY97kl

2. **外部ユーザーグループ**

   Objects > Users > External Groups > New: 次のように入力してから **OK** をクリックします。

   Group Name: xa-grp2
   Group Type: XAuth

3. **アドレス**

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: reseller1
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.2.2.0/24
   Zone: Untrust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: rsl-svr1
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.5/32
   Zone: Trust

4. **VPN**

   VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

   Gateway Name: gw4
   Security Level: Custom
   Remote Gateway Type:
   Static IP Address: (選択), Address/Hostname: 2.2.2.2
   Preshared Key: juniper4
   Outgoing Interface: ethernet3

   > Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

   Phase 1 Proposal: pre-g2-3des-sha
   Mode (Initiator): Main (ID 保護)
   XAuth Server: (選択)
   External Authentication: (選択), securid1
   User Group: (選択)
   Name: xa-grp2

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: vpn4
Security Level: Compatible
Remote Gateway:
Predefined: (選択), gw4

5. ポリシー

Policy > Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), reseller1
Destination Address:
Address Book Entry: (選択), rsl-svr1
Service: FTP-Get
Action: Tunnel
Tunnel VPN: vpn4
Modify matching bidirectional VPN policy: (オフ)
Position at Top: (選択)

CLI

1. 認証サーバー

```
set auth-server radius1 type radius
set auth-server radius1 account-type XAuth
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500
set auth-server radius1 radius secret A56htYY97kl
```

2. 外部ユーザーグループ

```
set user-group xa-grp2 location external
set user-group xa-grp2 type XAuth
```

3. アドレス

```
set address untrust reseller1 10.2.2.0/24
set address trust rsl-svr1 10.1.1.5/32
```

4. VPN

```
set ike gate gw4 ip 2.2.2.2 main outgoing-interface ethernet3 preshare juniper4
    proposal pre-g2-3des-sha
set ike gateway gw4 XAuth server radius1 user-group xa-grp2
set vpn vpn4 gateway gw4 sec-level compatible
```

5. ポリシー

```
set policy top from untrust to trust reseller1 rsl-svr1 ftp-get tunnel vpn vpn4
save
```

例 : XAuth 認証およびアドレス割り当て (ローカルユーザーグループ)

この例では、ローカルデータベースに保存された IKE/XAuth ユーザーの認証と、IP、DNS サーバーおよび WINS サーバー IP アドレス割り当ての両方を設定します。

注 : また、XAuth ユーザーの認証とアドレス割り当てに、外部 RADIUS 認証サーバーを使うこともできます。外部 SecurID か、LDAP 認証サーバーは、XAuth 認証のみ (アドレス割り当てには使えません) に使用することができます。IKE ユーザー認証には、ローカルデータベースのみが使えます。

IKE/XAuth ユーザーがセキュリティデバイスに、ダイアルアップ VPN 接続を行うと、セキュリティデバイスは、フェーズ 1 ネゴシエーションの間に、IKE ID と RSA 証明書を使用して IKE ユーザー（クライアントデバイス）を認証します。セキュリティデバイスは、その後 XAuth ユーザー（デバイスを使用している個人のこと）をユーザー名とパスワードを使用して認証し、フェーズ 1 とフェーズ 2 ネゴシエーションの間に、IP 、DNS サーバーおよび WINS サーバー IP アドレスを割り当てます。

ローカルユーザーグループ ixa-grp1 を作成します。そして、「 ixa-u1 」(パスワード : ccF1m84s) と 「ixa-u2 」(パスワード : C113g1tw) の 2 つの IKE/XAuth 認証ユーザーを定義してグループに追加し、それによってグループタイプを IKE/XAuth と定義します (他の IKE/XAuth ユーザーの追加はこの例では示されていません)。

アドレスが 10.2.2.1 から 10.2.2.100 の範囲の xa-pool1 いう名前の DIP プールを作成します。セキュリティデバイスが XAuth ユーザーに IP アドレスを割り当てるときには、このプールのアドレスを使います。

注 : DIP プールは、ルーティングやアドレス割り当ての重複の問題を避けるために、XAuth ユーザーがトラフィックを誘導するゾーンのアドレススペースとは異なったアドレススペースになければなりません。

以下の XAuth デフォルト設定を構成します。

- XAuth アドレスタイムアウトを 480 分に設定します。
- デフォルト認証サーバーとしてローカルデータベースを選択します。
- セキュリティデバイスがチャレンジ（暗号鍵）を、自分のログイン名とパスワードを暗号化する鍵として使うリモートクライアントに送信することができる、CHAP (チャレンジハンドシェイク式認証プロトコル) を使用可能にします。
- xa-pool1 をデフォルト DIP プールとして選択します。
- 1 次および 2 次 DNS サーバー IP アドレスをそれぞれ 10.1.1.150 と 10.1.1.151 と定義します。
- 1 次および 2 次 WINS サーバー IP アドレスをそれぞれ 10.1.1.160 と 10.1.1.161 と定義します。

ユーザーグループ ixa-grp1 を参照し、デフォルト XAuth 認証サーバー設定を使用する「 ixa-gw1 」という名前の IKE ゲートウェイを構成します。そして、「ixa-tun1」という名前の VPN トンネルと ixa-grp1 から Trust ゾーン (IP アドレス 10.1.1.0/24) へ VPN トンネル ixa-tun1 を介してトラフィックを許可するポリシーを構成します。

WebUI

1. IKE/XAuth ユーザーとユーザーグループ

Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

User Name: ixa-u1
Status: Enable
IKE User: (選択)
Simple Identity: (選択)
IKE ID Type: AUTO
IKE Identity: u1@juniper.net
XAuth User: (選択)
User Password: ccF1m84s
Confirm Password: ccF1m84s

Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

User Name: ixa-u2
Status: Enable
IKE User: (選択)
Simple Identity: (選択)
IKE ID Type: AUTO
IKE Identity: u2@juniper.net
XAuth User: (選択)
User Password: C113g1tw
Confirm Password: C113g1tw

Objects > Users > Local Groups > New: Group Name フィールドに **ixa-grp1** と入力して、以下を行い、**OK** をクリックします。

ixa-u1 を選択して、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

ixa-u2 を選択して、< < ボタンを使用して、Available Members 列から Group Members 列に移動します。

2. IP プール

Objects > IP Pools > New: 次のように入力してから **OK** をクリックします。

IP Pool Name: xa-pool1
Start IP: 10.2.2.1
End IP: 10.2.2.100

3. **デフォルト XAuth 認証サーバー**
   VPNs > AutoKey Advanced > XAuth Settings: 以下を入力して **Apply** をクリックします。

   Reserve Private IP for XAuth User: 480 Minutes
   Default Authentication Server: Local
   Query Client Settings on Default Server: (**オフ**)
   CHAP: (**選択**)
   IP Pool Name: xa-pool1
   DNS Primary Server IP: 10.1.1.150
   DNS Secondary Server IP: 10.1.1.151
   WINS Primary Server IP: 10.1.1.160
   WINS Secondary Server IP: 10.1.1.161

4. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: Trust_zone
   IP Address/Domain Name:
   IP/Netmask: (**選択**), 10.1.1.0/24
   Zone: Trust

5. **VPN**
   VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

   Gateway Name: ixa-gw1
   Security Level: Custom
   Remote Gateway Type:
   Dialup User Group: (**選択**)
   Group: ixa-grp1

   > Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

   Phase 1 Proposal: rsa-g2-3des-sha
   Mode (Initiator): Aggressive
   Outgoing Interface: ethernet3
   XAuth Server: (**選択**)
   User Default: (**選択**)
   User Group: (**選択**), xa-grp1

   VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

   VPN Name: ixa-vpn1
   Security Level: Compatible
   Remote Gateway:
   Predefined: (**選択**), ixa-grp1

6. **ポリシー**
   Policy > Policies > (From: Untrust; To: Trust) New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), Dial-Up VPN
   Destination Address:
   Address Book Entry: (選択), Trust_zone
   Service: ANY
   Action: Tunnel
   Tunnel VPN: ixa-vpn1
   Modify matching bidirectional VPN policy: (オフ)
   Position at Top: (選択)

CLI

1. **IKE/XAuth ユーザーとユーザーグループ**
   set user-group ixa-grp1 location local
   set user ixa-u1 type ike XAuth
   set user ixa-u1 ike-id u-fqdn u1@ns.com
   set user ixa-u1 password ccF1m84s
   unset user ixa-u1 type auth
   set user ixa-u2 type ike XAuth
   set user ixa-u2 ike-id u-fqdn u2@juniper.net
   set user ixa-u2 password C113g1tw
   unset user ixa-u2 type auth

2. **IP プール**
   set ippool xa-pool1 10.2.2.1 10.2.2.100

3. **デフォルト XAuth 認証サーバー**
   set XAuth lifetime 480
   set XAuth default auth server Local chap
   set XAuth default ippool xa-pool1
   set XAuth default dns1 10.1.1.150
   set XAuth default dns2 10.1.1.151
   set XAuth default wins1 10.1.1.160
   set XAuth default wins2 10.1.1.161

4. **アドレス**
   set address trust Trust_zone 10.1.1.0/24

5. **VPN**
   set ike gateway ixa-gw1 dialup ixa-grp1 aggressive outgoing-interface ethernet3 proposal rsa-g2-3des-sha
   set ike gateway ixa-gw1 XAuth server Local user-group ixa-grp1
   set vpn ixa-vpn1 gateway ixa-gw1 sec-level compatible

6. **ポリシー**
   set policy top from untrust to trust “Dial-Up VPN” Trust_zone any tunnel vpn ixa-vpn1
   save

XAuth クライアント

XAuth クライアントは、AutoKey IKE VPN トンネルを介して XAuth サーバーに接続するリモートユーザーまたはデバイスです。セキュリティデバイスは、リモート XAuth サーバーからの認証要求に応答して XAuth クライアントとして機能することが可能です。フェーズ 1 ネゴシエーションが完了したら、リモート XAuth サーバーは、セキュリティデバイスにログインプロンプトを送信します。XAuth クライアントとして動作するセキュリティデバイスが正しいユーザー名およびパスワードで正常にログインする場合、フェーズ 2 ネゴシエーションが開始されます。

XAuth クライアントとしてセキュリティデバイス構成するには以下を指定します。

- IKE ゲートウェイ名
- XAuth ユーザー名およびパスワード

以下のタイプの XAuth 認証を構成できます。

- **Any** — CHAP (チャレンジハンドシェイク式認証プロトコル) またはPAP (パスワード認証プロトコル) のいずれかを許可します。
- **CHAP** — CHAP のみを許可します。

例 : XAuth クライアントとしてのセキュリティデバイス

この例では、まずリモート IKE ゲートウェイ *gw1* を IP アドレス 2.2.2.2 で構成します。標準セキュリティレベルを指定し、事前共有鍵 *juniper1* を使用します。次に IKE ゲートウェイ用に、ユーザー名 *beluga9*、パスワード *1234567* で XAuth クライアントを構成します。さらにクライアント用に CHAP 認証を要求します。

WebUI

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: gw1
Security Level: Standard (選択)
Remote Gateway Type:
Static IP Address: (選択), Address/Hostname: 2.2.2.2
Preshared Key: juniper1
Outgoing Interface: Untrust

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

XAuth Client: (選択)
User Name: beluga9
Password: 1234567
Allowed Authentication Type: (選択), CHAP Only

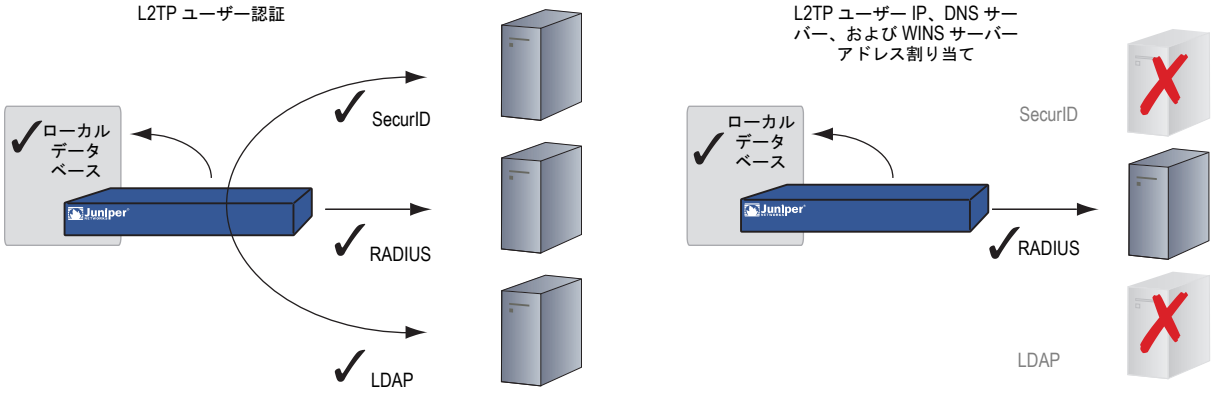
CLI

```
set ike gateway gw1 ip 2.2.2.2 Main outgoing-interface untrust preshare juniper1
    sec-level standard
set ike gateway gw1 XAuth client chap username beluga9 password 1234567
save
```

L2TP ユーザーとユーザーグループ

L2TP (レイヤー 2 トンネリングプロトコル) は、リモートユーザーを認証して、IP、DNS サーバーおよび WINS サーバーアドレスを割り当てる手段を提供します。ローカルデータベース、または外部認証サーバーが L2TP ユーザーを認証するようにセキュリティデバイスを構成することができます。IP、DNS サーバーおよび WINS サーバーアドレス割り当てを行うには、セキュリティデバイスをローカルデータベース、または RADIUS サーバー（RADIUS ディクショナリーファイルがロードされる、19 ページの「RADIUS ディクショナリーファイル」を参照）を使用するよう設定します。図 22 を参照してください。

図 22: ユーザーを L2TP で認証する



L2TP の 2 つのアスペクトにたいしてそれぞれ異なる認証サーバーの組み合わせを使用することもできます。たとえば、L2TP ユーザーの認証には SecurID サーバーを使い、アドレス割り当てはローカルデータベースから行うことができます。以下の例は、L2TP の両方のコンポーネントを扱う 2 つの認証サーバーのアプリケーションの例を示します。別の例と、L2TP の詳細な紹介は 5-205 ページの「レイヤー 2 トンネリングプロトコル」を参照してください。

例 : ローカルおよび外部 L2TP 認証サーバー

この例では、L2TP ユーザーを認証するために、外部 SecurID 認証サーバーを設定し、IP、DNS サーバーおよび WINS サーバーアドレスを割り当てるためにローカルサーバーを使用します。

外部 SecurID 認証サーバーは securid1 です。33 ページの「例 : SecurID 認証サーバー」とほぼ同じですが、アカウントタイプが L2TP であることが異なります。SecurID 認証サーバーパラメータは以下のとおりです。

- Name: securid1
- IP Address: 10.20.2.100
- Backup1 IP Address: 10.20.2.110
- Port: 15000
- Client Retries: 3
- Client Timeout: 10 seconds

- Idle Timeout: 60 minutes
- Account Type: L2TP
- Encryption: DES

L2TP デフォルト設定は以下のとおりです。

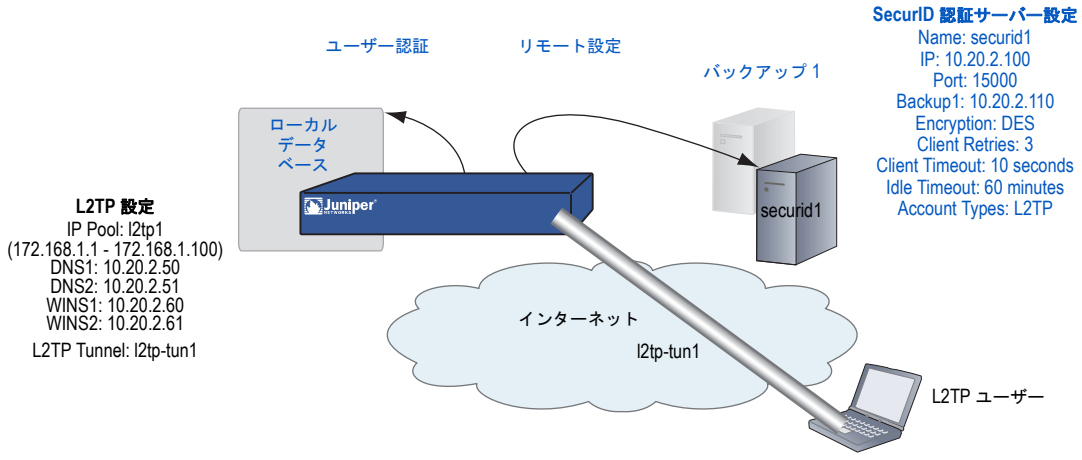
- IP Pool: l2tp1 (172.168.1.1 - 172.168.1.100)
- DNS 1 次サーバー IP: 10.20.2.50
- DNS 2 次サーバー IP: 10.20.2.51
- PPP 認証 : CHAP
- WINS 1 次サーバー IP: 10.20.2.60
- WINS 2 次サーバー IP: 10.20.2.61

セキュリティデバイスを上記の設定で構成した後、認証に securid1 を参照して、アドレス割り当てにデフォルト設定を使用する「 l2tp-tun1 」という名前の L2TP トンネルを作成します。

また上記のように SecurID サーバーを設定し、L2TP ユーザーを入れます。図 23 は L2TP 設定、SecurID 認証サーバー設定およびネットワークの設定を示します。

注 : L2TP のみの構成は安全とは言えません。L2TP トンネルにセキュリティを加えるためには、5-218 ページの「L2TP-over-IPSec を構成する」で行われるように、透過モードの IPSec トンネルと組み合わせることが推奨されます。

図 23: ローカルおよび外部 L2TP 認証サーバー



WebUI

1. 認証サーバー

Configuration > Auth > Auth Servers > New: 次のように入力してから **OK** をクリックします。

Name: securid1
IP/Domain Name: 10.20.2.100
Backup1: 10.20.2.110
Timeout: 60
Account Type: L2TP
SecurID: (選択)
Client Retries: 3
Client Timeout: 10 seconds
Authentication Port: 15000
Encryption Type: DES
Use Duress: No

2. IP プール

Objects > IP Pools > New: 次のように入力してから **OK** をクリックします。

IP Pool Name: l2tp1
Start IP: 172.168.1.1
End IP: 172.168.1.100

3. L2TP デフォルト設定

VPNs > L2TP > Default Settings: 以下を入力して **Apply** をクリックします。

Default Authentication Server: Local
IP Pool Name: l2tp1
PPP Authentication: CHAP
DNS Primary Server IP: 10.20.2.50
DNS Secondary Server IP: 10.20.2.51
WINS Primary Server IP: 10.20.2.60
WINS Secondary Server IP: 10.20.2.61

4. L2TP トンネル

VPNs > L2TP > Tunnel > New: 次のように入力してから **OK** をクリックします。

Name: l2tp-tun1
Use Custom Settings: (選択)
Authentication Server: securid1
Query Remote Settings: (オフ)
Dialup User: (選択), Allow Any

CLI

1. 認証サーバー

```
set auth-server securid1 type securid
set auth-server securid1 server-name 10.20.2.100
set auth-server securid1 backup1 10.20.2.110
set auth-server securid1 timeout 60
set auth-server securid1 account-type l2tp
set auth-server securid1 securid retries 3
set auth-server securid1 securid timeout 10
set auth-server securid1 securid auth-port 15000
set auth-server securid1 securid encr 1
set auth-server securid1 securid duress 0
```

2. **IP プール**
   set ippool l2tp1 172.168.1.1 172.168.1.100

3. **L2TP デフォルト設定**
   set l2tp default auth server Local
   set l2tp default ippool l2tp1
   set l2tp default ppp-auth chap
   set l2tp dns1 10.20.2.50
   set l2tp dns1 10.20.2.51
   set l2tp wins1 10.20.2.60
   set l2tp wins2 10.20.2.61

4. **L2TP トンネル**
   set l2tp l2tp-tun1
   set l2tp l2tp-tun1 auth server securid1
   save

第 6 章

ワイヤレスおよびイーサネットインターフェース用の拡張認証

本章では、イーサネットおよびワイヤレスインターフェースの認証を行う、拡張認証プロトコル（EAP）で利用可能なオプションおよびプロトコルの使用例を説明します。本章のセクションは、以下のようになります。

- 88 ページの「概要」
- 88 ページの「サポートされている EAP のタイプ」
- 89 ページの「802.1X 認証を使用可能または使用不可能にする」
- 90 ページの「802.1X 設定の構成」
- 94 ページの「認証サーバーオプションの構成」
- 96 ページの「802.1X 情報の表示」
- 98 ページの「設定例」
  - 98 ページの「直接接続しているクライアントと RADIUS サーバーを持ったセキュリティデバイスの構成」
  - 99 ページの「クライアントとセキュリティデバイスの間にハブを持ったセキュリティデバイスの構成」
  - 101 ページの「ワイヤレスインターフェースを持った認証サーバーの構成」

概要

EAP は、複数の認証方法をサポートする認証フレームワークです。EAP は通常、レイヤー 3 アドレス指定がなくても、ポイントツーポイントプロトコル（PPP）あるいは IEEE 802 のように、データリンク層上で直接動作します。

IEEE 802.1X は、ポートベースのアクセスポリシー制御用に使用され、IKEv2 は、認証のオプションとしてそれを使用します。EAP は、透過またはルート（ネットワークアドレス変換が有効または無効）モードに構成された、セキュリティデバイスで機能します。NetScreen 冗長プロトコル（NSRP）は、高い可用性を備えたネットワークで EAP をサポートします。ログメッセージと SNMP サポートも利用可能です。

802.1X のサポートは、全プラットフォームで利用可能です。

EAP は、レイヤー 2 で動作する PPP の認証部分として機能します。申請者すなわちクライアントが、適切な信任状を送信し、認証サーバー（通常は RADIUS サーバー）がユーザーレベル権限を定義した後、EAP は、クライアントを認証します。EAP を使用すると、認証情報はすべて、セキュリティデバイスを通過します（これは、EAP 認証の通過方式と呼ばれます）。ユーザー情報はすべて認証サーバーに格納されます。

ベンダー固有属性（VSA）をサポートする認証に RADIUS サーバーを使用する場合、クライアントがメンバであるゾーンを確認する、ゾーン確認機能を使用できます。

サポートされている EAP のタイプ

図 11 に示す EAP タイプがサポートされています。

表 11: EAP タイプ

タイプ	説明
EAP-TLS（トランスポートレイヤーセキュリティ）	EAP の最も一般的な派生形であり、ほとんどの RADIUS サーバーがサポートします。EAP-TLS は、ユーザーとサーバーの認証、および動的なセッション鍵生成に、証明書を使用します。
EAP-TTLS（トンネル化トランスポートレイヤーセキュリティ）	認証に必要なのは、サーバー側の証明書および有効なユーザー名とパスワードだけです。Steel-Belted RADIUS は TTLS をサポートします。
EAP-PEAP（保護 EAP）	EAP-TLS の機能の不足を補い、管理の複雑さを低減するため設計されました。必要なのは、サーバー側の証明書および有効なユーザー名とパスワードだけです。鍵交換、セッション再開、フラグメント化および再アセンブリをサポートします。Steel-Belted RADIUS および Microsoft IAS は、保護 EAP をサポートします。
EAP-MD5（メッセージダイジェストアルゴリズム 5）	MD5 ハッシュを確認するため、チャレンジと応答のプロセスを使用するアルゴリズム。

802.1X 認証を使用可能または使用不可能にする

デフォルトでは、802.X 認証は無効です。WebUI または CLI を使用して、イーサネットおよびワイヤレスインターフェースのための 802.1X 認証を使用可能にできます。イーサネットインターフェースで 802.1 X 認証を使用可能にするには、インターフェースの構成を変更します。SSID を作成、構成し、それをワイヤレスインターフェースにバインドすると、ワイヤレスインターフェースで 802.1X が自動的に使用可能になります。

イーサネットインターフェース

ethernet1 インターフェースで 802.1X を使用可能にするには、次の手順の 1 つを使用します。

WebUI

Network > Interfaces > List > Edit (ethernet1) > 802.1X: **Enable** をクリックします。

CLI

ethernet1 インターフェースで 802.1X を使用可能にするには、以下のコマンドを入力します。

```
set interface ethernet1 dot1x
```

ethernet1 インターフェースで 802.1X を使用不可能にするには、以下のコマンドを入力します。

```
unset interface ethernet1 dot1x
```

ワイヤレスインターフェース

ワイヤレスインターフェースで 802.1X を使用可能にするには、次の手順の 1 つを使用します。次の手順は、認証方式に WPA、暗号化方式に TKIP を使用して、**hr** という名前の SSID を作成します。認証サーバー、は **radius1** という名前の、定義済みの RADIUS サーバーです。SSID は、次にワイヤレスインターフェース 0/1 にバインドされます。

WebUI

Wireless > SSID > Click **New**. 次のように入力してから **OK** をクリックします。

SSID Name: hr
WPA Based Authentication and Encryption Methods: **WPA、TKIP** を選択します。
Auth Server: **radius1** を選択します。
Wireless Interface Binding: **wireless0/1** を選択します。

セキュリティデバイスによっては、ページのトップにある Activate Changes ボタンをクリックして、または Wireless > Activate Changes を選択して、変更を有効にする必要があります。

ワイヤレスインターフェースで 802.1X を使用不可能にするには、Wireless Interface Binding リストで **none** を選択します。

CLI

ワイヤレスインターフェースで 802.1X を使用可能にするには、SSID を作成、構成し、それをワイヤレスインターフェースにバインドします。

```
set ssid name hr
set ssid hr authentication wpa encryption tkip auth-server radius1
set ssid hr interface wireless0/1
```

ワイヤレスインターフェースで 802.1X を使用不可能にするには、以下のコマンドの 1 つを入力して、SSID をインターフェースからアンバインドします。

```
unset ssid hr interface
```

トランシーバーが 2 台あるセキュリティデバイスについては、以下のコマンドを入力しても、インターフェースをトランシーバーからアンバインドできます。

```
unset interface wireless0/1 wlan
```

また、認証サーバーの使用を必要としない SSID の認証方式を変更して、ワイヤレスインターフェースで 802.1X を使用不可能にできます。**set interface** *wireless_interface* **shutdown** コマンドで、ワイヤレスインターフェースを使用不可能にしても、802.1X は使用不可能になります。

802.1X 設定の構成

イーサネットインターフェースについては、オプションで 802.1X 設定を構成できます。ワイヤレスインターフェースについては、これらの設定は変更できず、表 12 に示すデフォルト値が使用されます。

表 12: 802.1X 設定

オプション	デフォルト値	代替値
Port control	auto	force-unauthorized
Control mode	virtual	インターフェース
Maximum user	16 (イーサネット); 128 (ワイヤレス)	1-256
Reauthentication period	3600	0 -86400
Retransmission	enable	disable
Retransmission count	3	1-16
Retransmission period	3	1-120
Silent period	5	0-3600

802.1X ポート制御の構成

イーサネットインターフェースが 802.1X 認証試行を処理する方法を構成できます。デフォルトでは、ポート状態は **auto** であり、802.1X 認証は正常に進行できます。**force-unauthorized** オプションの使用により、トラフィックをすべてブロックし、クライアントによる認証試行をすべて無視するように、イーサネットインターフェースを設定できます。また、インターフェースについて 802.1X を使用不可能にすることにより、クライアントによる試行をすべて認証するようにもインターフェースを構成できます（これは、force-authorized 状態とも呼ばれます）。

次の例では、ethernet1 インターフェースに対して port-control 状態を force-unauthorized に設定します。これにより、インターフェースは全トラフィックをブロックし、クライアントの認証試行を無視するよう指定されます。

WebUI

Network > Interfaces > List > Edit (Ethernet1) > 802.1X: 以下を入力して **Apply** をクリックします。

Port Control: **Force-unauthorized** を選択します。

CLI

```
set interface ethernet1 dot1x port-control force-unauthorized
```

802.1X 制御モードの構成

次のモードの 1 つを指定すると、インターフェースに接続されたデバイスで MAC アドレスベースの認証を実行するかどうか指定できます。

- Interface: インターフェースに接続されたデバイスの MAC アドレスは認証されません。1 つのトラステッドデバイスがインターフェースに接続されている場合だけ、このオプションを使用します。
- Virtual: インターフェースに接続されたデバイスの MAC アドレスは認証されます。無許可の MAC アドレスを持つデバイスからのパケットはドロップされます。このモードは、インターフェースのデフォルト設定です。ワイヤレスインターフェースは、virtual（仮想）モードだけを使用します。

次の例では、ethernet1 インターフェースの制御モードを interface に設定します。

WebUI

Network > Interfaces > List > Edit (Ethernet1) > 802.1X: 以下を入力して **Apply** をクリックします。

Control Mode: Interface

CLI

```
set interface ethernet1 dot1x control-mode interface
```

同時ユーザーの最大数の設定

インターフェースが virtual 制御モードにあるとき、セキュリティデバイスは、設定された同時ユーザー数までを許可します。デフォルトでは、セキュリティデバイスは、イーサネットインターフェースでは 16 人の同時ユーザーを、ワイヤレスインターフェースでは 128 人のユーザーを受け付けます。有効な値の範囲は 1 ～ 256 です。制御モードを interface モードに設定している場合、同時ユーザーの最大値を設定できません。

次の例では、ethernet1 インターフェースの同時ユーザーの最大数を 24 に設定します。

WebUI

Network > Interfaces > List > Edit (Ethernet1) > 802.1X: 以下を入力して **Apply** をクリックします。

Maximum User: 24

CLI

set interface ethernet1 dot1x max-user 24

再認証期間の設定

デフォルトでは、802.1 申請者（クライアント）の再認証は、セキュリティデバイスで可能になっています。セキュリティデバイスは、3600 秒（1 時間）後にクライアントの再認証を試みます。

イーサネットインターフェースについては、0 ～ 86400 秒（24 時間）までの再認証期間を設定できます。再認証期間を使用不可能にするには、期間を 0 に設定します。ワイヤレスインターフェースについては、再認証期間をデフォルト値から変更できません。RADIUS サーバーが、デフォルト値以外の再認証期間を提供している場合、セキュリティデバイスは、RADIUS が割り当てた値を使用できます。

次の例では、ethernet1 インターフェースの再認証期間を 7200 秒（2 時間）に設定します。

WebUI

Network > Interfaces > List > Edit (Ethernet1) > 802.1X: 以下を入力して **Apply** をクリックします。

Re-Authentication Period: 7200

CLI

set interface ethernet1 dot1x reauth-period 7200

再認証期間をデフォルト値に設定するには、**unset interface** *interface_name* **dot1x reauth-period** コマンドを使用します。

EAP 再送信を使用可能にする

クライアントが応答しない場合の、クライアントへの EAP 要求の再送信を使用可能にできます。デフォルトでは再送信が有効になっています。オプションで、再送信される EAP 要求の最大数と、再送信の間隔を設定できます。再送信の最大数に到達すると、クライアントの認証されたセッションが終了し、認証が失敗します。

次の例では、ethernet1 インターフェースに対して EAP 要求の再送信を使用可能にします。

WebUI

Network > Interfaces > List > Edit (Ethernet1) > 802.1X: 802.1X Enable チェックボックスを選択して、**Apply** をクリックします。

CLI

set interface ethernet1 dot1x retry

EAP 再送信回数の構成

デフォルトでは、セキュリティデバイスは最高 3 つの EAP 要求を送信します。EAP 要求の数を 1 ～ 16 までに構成できます。

次の例では、EAP 要求送信の数を 8 に設定します。

WebUI

Network > Interfaces > List > Edit (Ethernet1) > 802.1X: 以下を入力して **Apply** をクリックします。

Re-Transmission Count: 8

CLI

送信される再送信パケットの数を構成するには、次のコマンドを使用します。

```
set interface ethernet1 dot1x retry count 8
```

EAP 再送信期間の構成

デフォルトでは、EAP 再送信の間隔は 3 秒です。1 ～ 120 秒まで設定できます。

次の例では、EAP 再送信間の間隔を 5 に設定します。

WebUI

Network > Interfaces > List > Edit (Ethernet1) > 802.1X: 以下を入力して **Apply** をクリックします。

Re-Transmission Count: 5

CLI

```
set interface ethernet1 dot1x retry period 5
```

サイレント（沈黙）期間の構成

サイレント（沈黙) 期間とは、認証が失敗した後、セキュリティデバイスが沈黙している期間のことです。サイレント期間には、セキュリティデバイスは、クライアント認証の要求を開始したり、それに応答したりしません。

デフォルトでは、認証が失敗すると、セキュリティデバイスは 5 秒間沈黙し、認証再送回数は 0 にリセットされます。

サイレント期間は 0 ～ 3600 秒（1 時間) までの値です。サイレント期間に 0 を指定すれば、再試行が失敗した後、802.1X 認証状態は無認証のままです。

次の例では、ethernet1 インターフェースのサイレント期間を 30 秒に設定します。

WebUI

Network > Interfaces > List > Edit (Ethernet1) > 802.1X: 以下を入力して **Apply** をクリックします。

Silent Period: 30

CLI

```
set interface ethernet1 dot1x silent-period 30
```

認証サーバーオプションの構成

ネットワークの認証サーバーを構成し、それらを定義したら、これらのサーバーの 1 つをインターフェース用の認証サーバーとして指定できます。また、次の認証サーバーオプションを設定できます。

- アカウントタイプ（802.1X クライアント）
- ゾーン確認

認証サーバーの指定

特定のインターフェースの認証サーバーとして、定義済みのサーバーを使用できます。

イーサネットインターフェース

イーサネットインターフェースでは、インターフェース構成の変更により、認証サーバーを指定します。次の例では、ethernet1 インターフェース用の認証サーバーとして、既存の **radius1** サーバーを指定します。

WebUI

Network > Interfaces > List > Edit (Ethernet1) > 802.1X: Server Name リストから認証サーバーを選択し、**Apply** をクリックします。

CLI

```
set interface ethernet1 dot1x auth-server radius1
```

ワイヤレスインターフェース

ワイヤレスインターフェースでは、SSID 構成の変更により、認証サーバーを指定します。次の例では、**hr** という名前の SSID を変更し、既存の **radius1** サーバーを wireless0/1 インターフェースの認証サーバーに指定します。

Wireless > SSID > Edit (hr SSID): **New** をクリックします。セキュリティデバイスによっては、次の 1 つを選択し、**OK** をクリックします。

WEP Based Authentication and Encryption Methods: WEP **暗号化 : Open、WEP Encryption** を選択し、Auth Server **リストから radius1 を選択します。**
802.1X Based Authentication and Encryption Methods: **802.1X** を選択し、Auth Server **リストから radius1 を選択します。**

CLI

```
set ssid hr authentication wpa encryption auto auth-server radius1
```

WebUI を使用して、認証サーバー情報を構成するには、Auth Servers ページに移動します。

Configuration > Auth > Auth Servers: 適用可能なオプション値を入力または選択し、**Apply** をクリックします。

アカウントタイプの設定

認証サーバーを定義または変更すると、802.1X クライアントを受け付ける認証サーバーを指定できます。

WebUI

認証サーバーが 802.1X クライアントを受け入れるように指定するには、次の手順を使用します。

Configuration > Auth > Auth Servers > New (既存のサーバーでは Edit): Account Type 領域に関連する情報をすべて入力し、802.1X チェックボックスを選択して、**Apply** をクリックします。

CLI

radius1 という名前の既存のサーバーが、802.1X クライアントを受け入れるように指定するには、次の手順を使用します。

```
set auth-server radius1 account_type 802.1x
```

ゾーン確認を使用可能にする

RADIUS サーバーがベンダー固有属性（VSA) 拡張をサポートしている場合、ゾーン確認を使用可能にできます。この機能は、ユーザーがメンバであるゾーンおよびポートで設定されているゾーンを確認します。ポートで設定されたゾーンが、ユーザーがメンバであるゾーンの場合だけ、認証が許可されます。

お使いの辞書ファイルに、文字列属性タイプとして Zone_Verification という属性名を追加します。ベンダー ID は 3224 であり、属性番号は 10 です。

WebUI

ゾーン確認を使用可能にするには、次の手順を使用します。

Configuration > Auth > Auth Servers > New (既存のサーバーでは Edit): 関連する情報をすべて入力し、**RADIUS** を選択します。次に、Zone Verification の Enabled チェックボックスを選択して、**Apply** をクリックします。

CLI

radius1 という名前の RADIUS サーバーのゾーン確認を使用可能にするには、次のコマンドを入力します。

```
set auth-server radius1 radius zone-verification
```

802.1X 情報の表示

CLI で 802.1X 構成に関する詳細情報を表示できます。WebUI を使用すると、表示できない 802.1X 情報があります。

802.1X グローバル構成情報の表示

グローバルな 802.1X 構成情報を表示するには、次のコマンドを入力します。

get dot1x

このコマンドは、各イーサネットおよびワイヤレスインターフェースの次の情報を表示します。

- 802.1X 状況 : 使用可能または使用不可
- Mode: virtual (仮想) または interface (インターフェース)
- 許容されるユーザー最大数からのユーザー数
- 再認証が必要になるまでの秒数
- ポート制御モード状況

次は **get dot1x** コマンドのサンプル出力です。

```
------------------------------------------------------------------------------
Name            IEEE802.1x  Mode        User    re-auth     Status
  Ethernet1     Enabled     virtual     1/64    3600s       Auto
  Ethernet2     Disabled    virtual     0/64    3600s       Auto
  Ethernet3     Enabled     interface   --      1200s       F-U
  Ethernet3.1   Enabled     virtual     0/64    3600s       Auto
  Ethernet4     Enabled     virtual     0/16    3600s       Auto
------------------------------------------------------------------------------
```

インターフェースの 802.1X 情報の表示

特定のインターフェースの 802.1X 構成とユーザー情報を表示するには、次のコマンドを入力します。

get interface *interface_name* dot1x

次はサンプル出力です。

```
IEEE 802.1x enabled
port-control: auto, mode: virtual
user 1/max 64  auth-server: test-radius
reauth enable   period 1200s
silent enable   period 300s
to-supplicant retry enable   count 3   period 10s
------------------------------------------------------------------
User 0003e40220b1, session id 1, authorized
Total 1 user shown
  ------------------------------------------------------------------
```

802.1X 統計の表示

特定のインターフェースの 802.1X 統計を取得するには、WebUI または CLI を使用します。

WebUI

Network > 802.1X > Statistic: ページのトップのリストからインターフェースを選択します。

CLI

ethernet0/2 インターフェースの 802.1X 統計を表示するには、次のコマンドを入力します。

```
get interface ethernet0/2 dot1x statistics
```

次はサンプル出力です。

```
Interface Ethernet0/2:
------------------------------------------------------------------------------
Interface ethernet1 802.1x statistics:
in eapol               0 | out eapol              0 | in start          0
in logoff              0 | in resp/id             0 | in resp           0
out req/id             0 | out req                0 | in invalid         0
in len error           0 |

Interface ethernet1 802.1x diagnostics:
while connecting:
enters                 0 | eap logoffs            0 |

while authenticating:
enters                 0 | auth success           0 | auth timeouts     0
auth fail              0 | auth reauth            0 | auth start          0
auth logoff            0 |
```

802.1X セッション統計の表示

802.1X セッション統計を表示するには、次のコマンドを入力します。

get dot1x session

次はサンプル出力です。

```
Alloc 2/max 1024, alloc failed 0
Id 1/ vsys 0, flag 00000000, re-auth 3105s, ethernet1, 0003e40220c2, authorized
Id 2/ vsys 0, flag 00000000, re-auth 430s, ethernet3.1, 0003e40220b1,
fail-silent
Total 2 session shown
```

802.1X セッション詳細の表示

特定の 802.1X セッションの詳細情報を表示するには、次のコマンドを入力します。

```
get dot1x session id session_id
```

次はサンプル出力です。

```
Id 1, flag 00000000, vsys id 0(Root)
Interface ethernet1(vsd 0), supp-mac 0003e40220c2, status authorized
Re-auth timeout 3105s, type eap-md5
  As radius_test, zone-verification on
  Retry 0, as retry 0
  ------------------------------------------------------------------------
  statistics:
in octets           0 | out octets              0 | in frames         0
out frames          0
  ------------------------------------------------------------------------
```

設定例

このセクションには、以下の 3 つの例があります。

- 98 ページの「直接接続しているクライアントと RADIUS サーバーを持ったセキュリティデバイスの構成」
- 99 ページの「クライアントとセキュリティデバイスの間にハブを持ったセキュリティデバイスの構成」
- 101 ページの「ワイヤレスインターフェースを持った認証サーバーの構成」

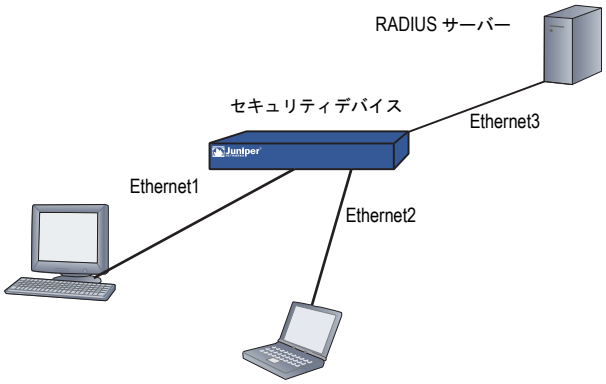
直接接続しているクライアントと RADIUS サーバーを持ったセキュリティデバイスの構成

図 24 に示されたように、このネットワークシナリオには、次のパラメータでセキュリティデバイスと直接接続されている 2 つのクライアントがあります。

- Ethernet1 インターフェースに直接接続されたクライアント。
- Ethernet2 インターフェースに直接接続されたクライアント。
- 10.1.40.3/24 の IP アドレスを持った Trust ゾーン にバインドされた Ethernet3 インターフェース。
- 802.1X でユーザーを認証する Ethernet3 インターフェースに接続された radius1（10.1.1.200) という名前の RADIUS サーバー。認証ポートとしてポート 1812 を、秘密として mysecret を使用します。

直接接続している 2 つのクライアントだけが、Ethernet1 と Ethernet2 というインターフェースに接続されているデバイスなので、制御モードは **interface** に構成されます。

図 24: 直接接続しているクライアントと RADIUS サーバーを持ったセキュリティデバイス




```
set interface ethernet1 dot1x
set interface ethernet2 dot1x
set interface ethernet1 dot1x control-mode interface
set interface ethernet2 dot1x control-mode interface

set interface ethernet3 zone trust
set interface ethernet3 ip 10.1.1.10/24

set auth-server radius1 account-type 802.1x
set auth-server radius1 type radius
set auth-server radius1 radius port 1812
set auth-server radius1 radius secret mysecret
set auth-server radius1 server-name 10.1.1.200

set interface ethernet1 dot1x auth-server radius1
set interface ethernet2 dot1x auth-server radius1
```

クライアントとセキュリティデバイスの間にハブを持ったセキュリティデバイスの構成

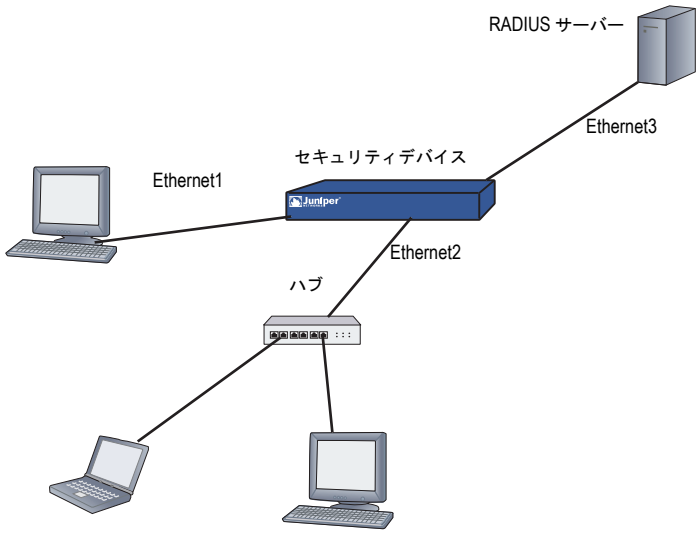
図 25 に示されたように、次のシナリオは、セキュリティデバイスに接続された付属のクライアントと、セキュリティデバイスに直接接続されたクライアントを持ったハブを使用します。

注 : 802.1X 機能は、セキュリティデバイスとクライアントの間にあるスイッチではサポートされません。セキュリティデバイスにスイッチを接続している場合、スイッチが接続されているインターフェースで 802.1X を使用不可能にすることを推奨します。

このシナリオは次のパラメータを使用します。

- Ethernet2 インターフェースに接続されたハブ（制御モード **virtual**）。
- Ethernet1 インターフェースに接続されたクライアント（制御モード **interface**）。
- 10.1.40.3/24 の IP アドレスを持った Trust ゾーン にバインドされた Ethernet3 インターフェース。
- 802.1X でユーザーを認証する Ethernet3 インターフェースに接続された radius1（10.1.1.200) という名前の RADIUS サーバー。認証ポートとしてポート 1812 を、秘密として mysecret を使用。

図 25: クライアントとセキュリティデバイスの間にハブを持ったセキュリティデバイス




```
set interface ethernet1 dot1x
set interface ethernet2 dot1x
set interface ethernet1 dot1x control-mode interface
set interface ethernet2 dot1x control-mode virtual

set interface ethernet3 zone trust
set interface ethernet3 ip 10.1.1.10/24

set auth-server radius1 account-type 802.1x
set auth-server radius1 type radius
set auth-server radius1 radius port 1812
set auth-server radius1 radius secret mysecret
set auth-server radius1 server-name 10.1.1.200

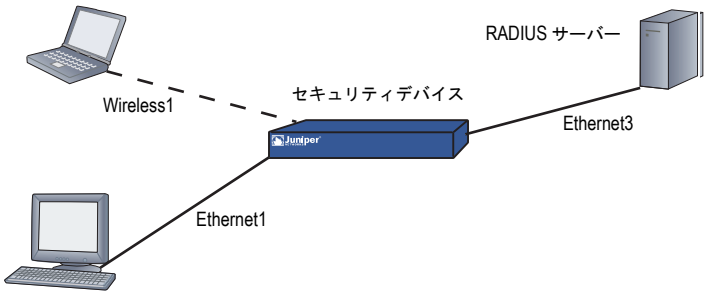
set interface ethernet1 dot1x auth-server radius1
set interface ethernet2 dot1x auth-server radius1
```

ワイヤレスインターフェースを持った認証サーバーの構成

図 26 に示されたように、次のシナリオには、ワイヤレスクライアントにサービスを提供するワイヤレスインターフェースと、セキュリティデバイスに次のパラメータで直接接続されているクライアントを持ったセキュリティデバイスがあります。

- ワイヤレスインターフェースに接続されたワイヤレスクライアント。
- Ethernet1 インターフェースに接続されたクライアント（制御モード **interface**）。
- 10.1.40.3/24 の IP アドレスを持った Trust ゾーン にバインドされた Ethernet3 インターフェース。
- 802.1X でユーザーを認証する Ethernet3 インターフェースに接続された radius1（10.1.1.200) という名前の RADIUS サーバー。認証ポートとしてポート 1812 を、秘密として mysecret を使用します。
- engineering という名前の SSID。WPA 認証、AES あるいは TKIP 暗号化を使用。認証サーバーとして radius1 を指定し、ワイヤレスインターフェースにバインドされている。

図 26: ワイヤレスインターフェースを持った認証サーバーの構成




```
set interface ethernet1 dot1x
set interface ethernet1 dot1x control-mode interface

set interface ethernet3 zone trust
set interface ethernet3 ip 10.1.1.10/24

set auth-server radius1 account-type 802.1x
set auth-server radius1 type radius
set auth-server radius1 radius port 1812
set auth-server radius1 radius secret mysecret
set auth-server radius1 server-name 10.1.1.200

set interface ethernet1 dot1x auth-server radius1

set ssid name engineering
set ssid engineering authentication wpa encryption auto auth-server radius1
set ssid engineering interface wireless0/1
```

索引

B

bypass-auth 67

C

CHAP 77

I

IKE ユーザー 63–66
- IKE ID 63, 77
- グループ 63, 64
- グループ、定義グループ、定義 65
- サーバーサポート 12
- 定義 64
- 他のユーザータイプ 4

L

L2TP
- アドレス割り当て 82
- 外部認証サーバー 82
- ユーザー認証 82
- ローカルデータベース 82

L2TP ユーザー 82
- XAuth と共に 4
- サーバーサポート 12

LDAP 27–28
- 構造 27
- サーバーポート 28
- 識別名 28
- 通称名識別子 28
- ユーザータイプサポート 28

M

mode config 67

R

RADIUS 17–20
- オブジェクトのプロパティ 18
- 共有秘密値 18
- 再試行タイムアウト 18
- ディクショナリーファイル 2, 19
- 認証サーバーオブジェクト 31
- ポート 18

RFC 1777、*Lightweight Directory Access Protocol* 27

S

ScreenOS
- RADIUS ベンダー ID 20

SecurID 25
- ACE サーバー 26
- Authentication Port 26
- authenticator 25
- Use Duress オプション 26
- 暗号化のタイプ 26
- トークンコード 25
- 認証サーバーオブジェクト 33
- ユーザータイプサポート 26

SecurID クライアント
- リトライ 26

SecurID クライアント SecurID
- タイムアウト 26

SSL
- WebAuth + SSL 59

T

TACACS+
- Client Retries 30
- Client Timeout 30
- オブジェクトのプロパティ 30
- 共有秘密値 30
- 再試行タイムアウト 30
- 認証サーバーオブジェクト 36
- ポート 30

V

VPN 待機時間 69

VSA 19

VSA 属性タイプ 20

W

WebAuth 12, 45
- SSL 59
- 外部ユーザーグループ 57
- 事前ポリシー認証 45
- ユーザーグループ、ローカル 55

X

XAuth
bypass-auth....67
TCP/IP 割り当て....68
VPN 待機時間....69
外部....72
外部 XAuth....72
仮想アダプタ....66
クエリーリモート設定....67
クライアントとしての ScreenOS....81
クライアント認証....81
定義....66
ユーザー認証....72
XAuth アドレス
IP アドレス寿命....68–69
タイムアウト....68
認証....77
割り当て....66
XAuth ユーザー....??–80
L2TP と共に....4
サーバーサポート....12
認証....66
ローカルグループ....71
ローカル認証....70
....66–??
XAuth、外部
ユーザーグループ認証....74
認証サーバー
XAuth クエリー....67

あ

アイドルセッションタイムアウト....17
アドレス
L2TP 割り当て....82
XAuth ユーザーの IP 寿命....68
アドレス、XAuth
割り当て....66
アドレス、XAuth アドレス、XAuth
タイムアウト....68
暗号化、SecurID....26

い

インフラネットエンフォーサ
概要....40
接続ポリシー、構成....40
インフラネットエンフォーサの接続ポリシー、構成.
40
インフラネットコントローラ
アクション....41
概要....40
リソースポリシー....41
インフラネット認証....42

か

仮想アダプタ....66
管理ユーザー....2
RADIUS の権限....3
サーバーサポート....12
タイムアウト....16
認証の優先....30

く

グループ式....4–8
オペレータ....5
サーバーサポート....12
ユーザー....5

け

軽量ディレクトリアクセスプロトコル
LDAP を参照

さ

サーバー、認証
認証サーバーを参照

し

識別名....28

せ

セッションアイドルタイムアウト....17

た

タイムアウト
管理ユーザー....16
認証ユーザー....16

つ

通称名....28

て

ディクショナリーファイル、RADIUS....2
データベース、ローカル....13–14

と

統合型アクセス制御ソリューション
概要....vii, 39
トークンコード....25

に

認証
優先....30

認証サーバー 11–38
external 15
ID 番号 16
LDAP 27–28
SecurID 25
SecurID、定義 33
アイドルタイムアウト 16
アドレス 16
最大数 12
種類 16
定義 31–38
デフォルト 37, 38
認証サーバーを参照
認証プロセス 15
バックアップ 16
認証サーバー、RADIUS 17–20
ユーザータイプサポート 18
認証サーバー、RADIUS 認証サーバー、RADIUS
定義 31
認証サーバー、TACACS +
定義 36
認証サーバー、オブジェクト
プロパティ 16
認証サーバー、オブジェクト認証、サーバー、オブジェクト
名前 16
認証テーブルエントリ 41
認証ユーザー 43–62
admin 2
IKE 12, 63
L2TP 82
WebAuth 12
XAuth 66
グループ 43, 46
サーバーサポート 12
手動鍵 12
タイプおよびアプリケーション 1–4
タイムアウト 16
認証ユーザーを参照
複数タイプ 3
ポリシー内 44
ユーザータイプ 12
ローカルデータベース 13–14
ログイン、異なる 4
認証ユーザー、WebAuth 45
SSL 59
ユーザーグループ、外部 57
ユーザーグループ、ローカル 55
認証ユーザー、認証
事前ポリシー 45
認証サーバー 12
ポイント 1
認証ユーザー、ランタイム
認証 44
ユーザーグループ、外部 51
ユーザーグループ、ローカル 48
ユーザー、外部 49
ローカル、ユーザー 47
認証ユーザー、ランタイム認証ユーザー、ランタイム
認証プロセス 44

は

バナー 9

ふ

フォールバック
プロパティの割り当て 30
プロトコル、CHAP 77
プロパティの割り当て 30

へ

ベンダー ID、VSA ベンダー ID、VSA 20
ベンダー固有属性 19

ゆ

ユーザー
admin 2
IKE
IKE ユーザーを参照
L2TP 82–85
WebAuth 12
XAuth 66–80
管理、タイムアウト 16
グループ、サーバーサポート 12
複数タイプ 3
ユーザー、IKE
IKE ユーザーを参照
ユーザー、認証
認証ユーザーを参照

ら

ランタイム認証 44

り

リモート認証ダイヤルインユーザーサービス
RADIUS を参照

ろ

ローカルデータベース
IKE ユーザー 64
タイムアウト 14
ユーザータイプサポート 14

概念と用例
ScreenOS リファレンス ガイド

第 10 部 :
仮想 システム

リリース 6.0.0、改訂 02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

品番 : 530-017776-01-JP, 改訂 02

Copyright Notice

Copyright © 2007 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

目次

本編について v

ドキュメントの規則 v
Web ユーザーインターフェースの規則 v
コマンドラインインターフェースの規則 vi
ネーミング規則および文字タイプ vi
説明図の規則 viii
技術ドキュメンおよびテクニカルサポート ix

第 1 章 仮想システム 1

概要 2
Vsys オブジェクト 4
Vsys オブジェクトと管理者の作成 4
Vsys にデフォルト仮想ルーターを設定する 6
ゾーンを共有仮想ルーターにバインドする 6
Vsys 管理者としてログイン 7
仮想システムプロファイル 9
Vsys セッションカウンタ 10
Vsys セッション情報 10
高可用性ペアにおける動作 10
Vsys プロファイルの作成 10
リソース限度の設定 11
Vsys プロファイル割り当てによるセッション限度の追加 12
セッションの変更設定 13
セッション限度到達アラームの変更設定 13
Vsys プロファイルの削除 14
Vsys 設定値の表示 14
変更設定の表示 14
プロファイルの表示 15
セッションの統計情報の表示 17
CPU リソースの共有と分割 17
CPU ウェイトの構成 18
公平モードのパケットフロー 19
公平モードから共有モードへの移行 20
CPU 限度機能を使用可能にする 20
CPU 使用率の測定 20
共有から公平モードへ移行 CPU 使用率しきい値の設定 23
共有モードに戻る方法を構成 25
ルート Vsys 固定 CPU ウェイトの設定 26
Vsys と仮想プライベートネットワーク 27
セキュリティアソシエーションの表示 27
IKE クッキーの表示 28

ポリシー スケジューリング 29
ポリシースケジューラの作成 29
ポリシースケジュールをポリシーにバインド 30
ポリシースケジュールの表示 30
ポリシースケジュールの削除 30

第 2 章 VLAN ベースのトラフィック分類 31

概要 31
VLAN 32
VLANs with Vsys 33
レイヤー 2 仮想システムの構成 34
例 1: 1 ポートを構成 35
例 2: それぞれが個別の Untrust ゾーンを持つ 2 つの 4 ポート統合の構成 39
例 3: 1 つの Untrusted ゾーンを共有する 2 つの 4 ポート統合の構成 45
サブインターフェースと VLAN タグの定義 51
仮想システム間の通信 54
VLAN の再タグ付け 57
例 : 58

第 3 章 トラフィックの振り分け 61

概要 61
トラフィックの振り分け 61
通過トラフィックの振り分け 62
専用および共有インターフェース 67
専用インターフェース 67
共有インターフェース 67
物理インターフェースのインポートとエクスポート 69
物理インターフェースを仮想システムにインポートする 69
物理インターフェースを仮想システムからエクスポートする 70

第 4 章 IP ベースのトラフィック分類 71

概要 71
ルートシステムに IP 範囲を指定する 72
IP ベースのトラフィック分類を設定する 73

索引 ..... IX-I

本編について

第 10 部: 仮想 システム では、仮想システム、専用 / 共有インターフェース、VLAN ベースおよび IP ベースのトラフィック分類について解説します。

本編の章は、以下のようになります。

- 第 1 章「仮想システム」では、仮想システムとプロファイル、オブジェクト、管理タスクについて解説します。
- 第 2 章「VLAN ベースのトラフィック分類」、は仮想システムの VLAN ベーストラフィック分類を説明します。
- 第 3 章「トラフィックの振り分け」、は ScreenOS がトラフィックを振り分ける方法を説明します。
- 第 4 章「IP ベースのトラフィック分類」、は仮想システムの IP ベーストラフィック分類を説明します。

ドキュメントの規則

このドキュメントは、次のセクションで説明されている規則を使用しています。

- v ページの「Web ユーザーインターフェースの規則」
- vi ページの「コマンドラインインターフェースの規則」
- vi ページの「ネーミング規則および文字タイプ」
- viii ページの「説明図の規則」

Web ユーザーインターフェースの規則

WebUI（Web ユーザーインターフェース）では、各作業の操作指示は、操作手順と構成設定値に分かれています。構成設定を入力できる WebUI ページを開くには、画面の左側にあるナビゲーション ツリーのメニュー項目をクリックして、そのページに移動します。先へ進むと、ナビゲーション パスが画面の上部に表示されます。各ページは角括弧で分離されています。

WebUI のパスおよびアドレスを定義するためのパラメータは、以下のとおりです。

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

```
Address Name: addr_1
IP Address/Domain Name:
    IP/Netmask: ( 選択 ), 10.2.2.5/32
Zone: Untrust
```

構成設定のオンライン ヘルプを開くには、画面の左上にある疑問符（?）をクリックします。

ナビゲーションツリーにも、Help > Config Guide 構成ページがあり、セキュリティポリシーおよび IPSec （インターネットプロトコルセキュリティ）の構成に役立ちます。ドロップダウンメニューからオプションを選択して、そのページの指示に従います。構成設定のオンラインヘルプを開くには、左上にある **?** 文字をクリックします。

コマンドラインインターフェースの規則

次の規則は、例とテキストにおいて、コマンドラインインターフェース（CLI）コマンドの構文を示すために使用されます。

例においては、次のように使用されます。

- 角括弧 [ ] 内にあるものはすべてオプションです。
- 中括弧 { } 内にあるものはすべて必須です。
- 選択肢が複数ある場合、各選択肢はパイプ (|) で区切られています。例えば、次のように表示されます。

  set interface { ethernet1 | ethernet2 | ethernet3 } manage

- 変数は*斜体*で表示されます。

  set admin user *name1* password *xyz*

In text, commands are in **boldface** type and variables are in *italic* type.

注： キーワード入力時には、単語を間違いなく識別できる数の文字を入力すれば十分です。**set admin user wheezer j12fmt54** というコマンドを入力する際には、**set adm u whee j12fmt54** と入力するだけで十分です。ただし、本編に記載されたコマンドはすべて本来の形式で記載されています。

ネーミング規則および文字タイプ

ScreenOS はオブジェクトの名前 (アドレス、管理ユーザー、認証サーバー、IKE ゲートウェイ、仮想システム、VPN トンネルおよびゾーンなど、ScreenOS 構成に定義されているもの) に関して、次の規則に従います。

- 名前文字列に 1 つまたは複数のスペースが含まれる場合、文字列全体を二重引用符で囲む必要があります。例えば

  set address trust “local LAN” 10.1.1.0/24

- 二重引用符で囲まれた文字列の先頭または末尾のスペースを取り除きます。たとえば、「 **local LAN** 」は「**local LAN**」となります。
- 連続した複数のスペースは、一つのスペースとして扱われます。
- CLI キーワードの多くはケースセンシティブではありませんが、名前文字列はケースセンシティブです。たとえば、「**local LAN**」は「**local lan**」とは異なります。

ScreenOS は、次の文字タイプをサポートします。

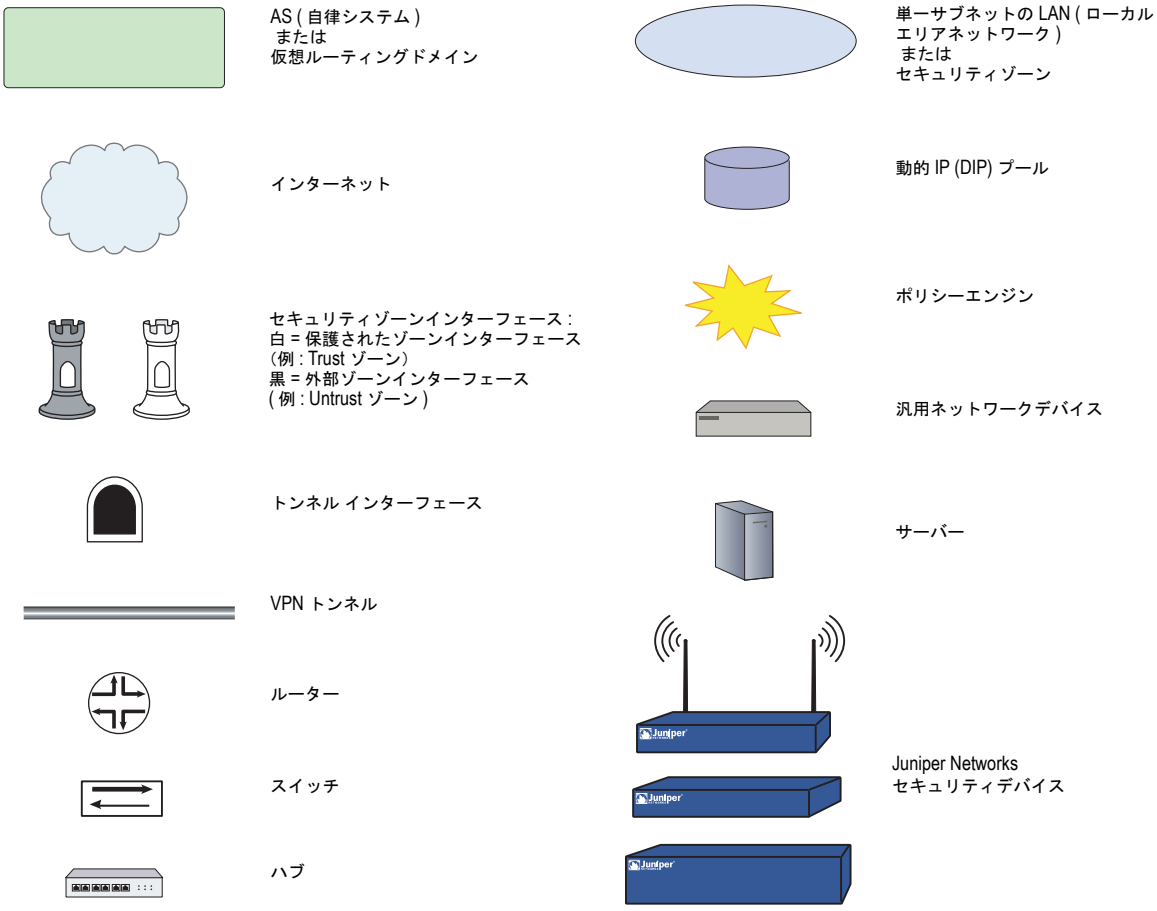
- 1 バイト文字セット (SBCS) およびマルチバイト文字セット (MBCS)。SBCS の例に、ASCII、欧州言語、およびヘブライ語があります。2 バイト文字セット (DBCS) とも呼ばれる MBCS の例に、中国語、韓国語、および日本語があります。
- ASCII 文字の 32（16 進数の 0x20）から 255（0xff)。ただし二重引用符 (") は、スペースを含む名前文字列の先頭と末尾を示す特殊な意味をもつため、例外とします。

注 : コンソール接続では、SBCS のみがサポートされます。ご利用のブラウザがサポートする文字セットに応じて、WebUI は SBCS および MBCS の両方をサポートします。

説明図の規則

次の図は、本編を通して説明図に使用されている画像の基本的なものです。

図 1: 説明図の画像



技術ドキュメンおよびテクニカルサポート

Juniper Networks 製品のいずれかの技術ドキュメントを入手するには、www.juniper.net/techpubs/ をご覧になってください。

テクニカルサポートについては、http://www.juniper.net/customers/support/ にある Case Manager を使って事例サポートを開くか、1-888-314-JTAC (米国内) か 1-408-745-9500 (その他の国) までお問い合わせください。

本書に間違いや欠落があった場合は、techpubs-comments@juniper.net までお知らせください。

第 1 章

仮想システム

この章は仮想システム、オブジェクトおよび管理タスクを説明します。本章のセクションは、以下のようになります。

- 2 ページの「概要」
- 4 ページの「Vsys オブジェクト」
  - 4 ページの「Vsys オブジェクトと管理者の作成」
  - 6 ページの「Vsys にデフォルト仮想ルーターを設定する」
  - 6 ページの「ゾーンを共有仮想ルーターにバインドする」
- 7 ページの「Vsys 管理者としてログイン」
- 9 ページの「仮想システムプロファイル」
  - 10 ページの「Vsys プロファイルの作成」
  - 12 ページの「Vsys プロファイル割り当てによるセッション限度の追加」
  - 13 ページの「セッションの変更設定」
  - 13 ページの「セッション限度到達アラームの変更設定」
  - 14 ページの「Vsys プロファイルの削除」
  - 14 ページの「Vsys 設定値の表示」
- 17 ページの「CPU リソースの共有と分割」
  - 19 ページの「公平モードのパケットフロー」
  - 20 ページの「CPU 限度機能を使用可能にする」
  - 20 ページの「CPU 使用率の測定」
  - 23 ページの「共有から公平モードへ移行 CPU 使用率しきい値の設定」
  - 25 ページの「共有モードに戻る方法を構成」
  - 26 ページの「ルート Vsys 固定 CPU ウェイトの設定」

- 27 ページの「Vsys と仮想プライベートネットワーク」
  - 27 ページの「セキュリティアソシエーションの表示」
  - 28 ページの「IKE クッキーの表示」
- 29 ページの「ポリシー スケジューリング」
  - 29 ページの「ポリシースケジューラの作成」
  - 30 ページの「ポリシースケジュールをポリシーにバインド」
  - 30 ページの「ポリシースケジュールの表示」
  - 30 ページの「ポリシースケジュールの削除」

概要

Juniper Networks セキュリティセキュリティシステムを論理的に、複数の仮想システムに分割して、マルチテナントサービスを提供することができます。各仮想システム (vsys) は独立したセキュリティドメインであり、それぞれに管理者 (*仮想システム管理者 (Virtual system administrator)* あるいは略して *vsys admins*) を立てることができます。管理者は、アドレス帳、ユーザーリスト、カスタムサービス、VPN、ポリシーなどを設定して、独自のセキュリティドメインを構築できます。ただし、ルートレベル管理者のみが、ファイアウォールセキュリティオプションの設定、仮想システム管理者の作成、インターフェースやサブインターフェースの定義をすることができます。

注 : どのプラットフォームがこの機能をサポートするかについては、Juniper Networks セキュリティマーケティング文書を参照してください。

ScreenOS がサポートする管理者レベルについては **3**-33 ページの「管理レベル」を参照してください。

Juniper Networks 仮想システムには、2 種類のトラフィック分類をサポートします。一方だけを使用することも、並行して同時に使用することも可能です。

表 1 は、vsys がサポートできる Untrust および Trust セキュリティゾーンのインターフェースを示しています。

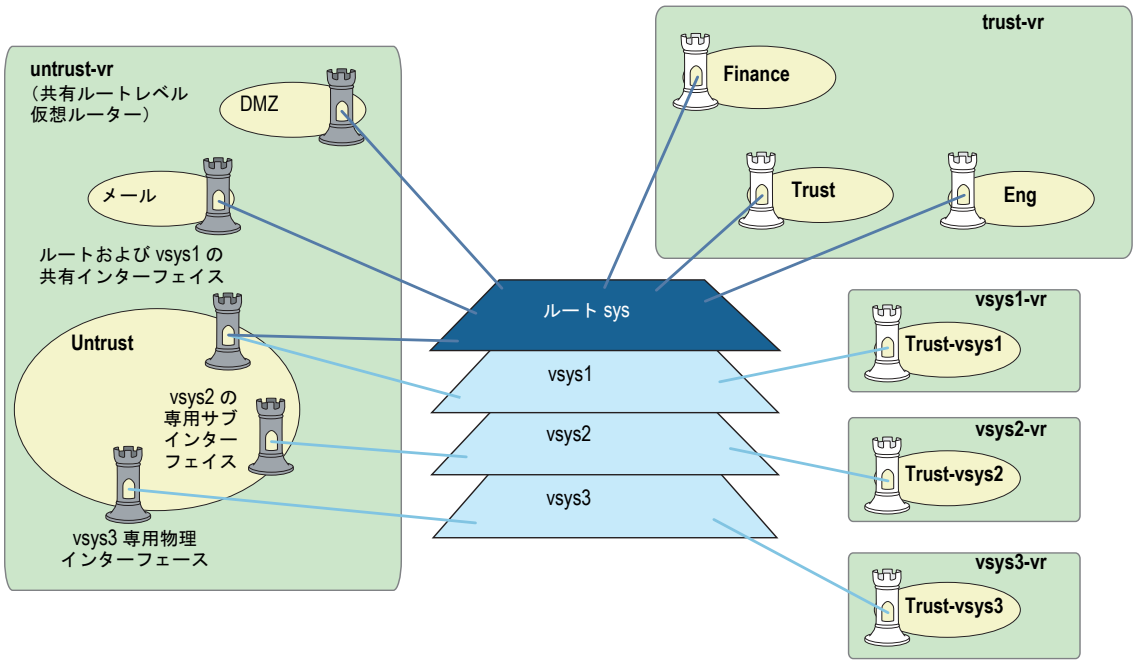
表 1: Vsys サポート

Untrust ゾーン用のインターフェースタイプ	Trust ゾーン用のインターフェースタイプ
専用物理インターフェース	専用物理インターフェース
サブインターフェース (インバウンドおよびアウトバウンドトラフィックの中継[1] 手段として VLAN タグ機能を備える)	サブインターフェース (VLAN タグ機能を備える)
ルートシステムとの共有インターフェース (物理インターフェース、サブインターフェース、冗長インターフェース、統合インターフェース)	ルートシステム (と IP ベーストラフィック分類[2]) との共有物理インターフェース

1. VLAN タグおよび中継 (トランク) について詳しくは、31 ページの「VLAN ベースのトラフィック分類」を参照してください。
2. IP ベースのトラフィック分類について詳しくは、71 ページの「IP ベースのトラフィック分類」を参照してください。

図 2 は、上記インターフェースタイプの 1 つ、2 つ、または 3 つのすべてを同時にセキュリティゾーンにバインドできることを示しています。さらに、同じタイプのインターフェースを複数バインドすることも可能です。

図 2: Vsys とのインターフェースおよびゾーンバインド



Vsys オブジェクト

ルート管理者、ルートレベル読取 / 書込管理者は、次の手順で vsys オブジェクトを作成できます。

- 仮想システムの定義
- (必要に応じ) vsys 管理者の定義 (複数でも可)。

注 : ルートレベル管理者は、読取 / 書込特権を持つ vsys 管理者、読取専用特権を持つ vsys 管理者を、vsys ごとに 1 人ずつ割り当てることができます。

- 仮想ルーターの選択。vsys ではこれを、Trust-*vsysname* ゾーン、Untrust-Tun-*vsysname* ゾーン、Global-*vsysname* ゾーンで使います。

Vsys オブジェクトを作成した後、それが機能するためには、ルートレベル管理者としてその他の設定を行う必要があります。サブインターフェースあるいはインターフェースを設定し、また場合によっては共有仮想ルーター、共有セキュリティゾーンを設定する必要があります。これらの設定は、vsys が VLAN ベースあるいは IP ベースのトラフィック分類、または両者の組み合わせをサポートするように意図されているかによります。これらの設定を行った後、ルートレベル管理者は仮想システムをログアウトし、定義されている場合は vsys 管理者にログインを許可し、アドレス、ユーザー、サービス、VPN、ルート、ポリシーの構成を始めます。

Vsys オブジェクトと管理者の作成

この例では、ルートレベル管理者として 3 つの vsys オブジェクトを作成します。vsys1、vsys2、vsys3 です。vsys1 の vsys 管理者として Alice を割り当て、パスワードを wIEaS1v1 とします。同様に、vsys2 の vsys 管理者は Bob、パスワードは pjF56Ms2 とします。vsys3 には vsys 管理者を作成しません。セキュリティデバイスが自動生成する管理者定義のままとします。具体的には、vsys 管理者名「 vsys_vsys3 」、パスワード「 vsys_vsys3 」となります。

注 : vsys 管理者のプロファイル（ユーザー名やパスワー）を設定できるのはルートレベル管理者だけです。セキュリティデバイスはユーザーが所属している vsys を判断するためにユーザーネームを使用するので、vsys 管理者はユーザーネームの変更はできません。しかしながら、vsys 管理者はパスワードを変更することが可能で、変更する必要があります。

vsys 名、管理者名、パスワードは、ケースセンシティブです。したがって、たとえば 「Vsys abc」と 「vsys ABC」と異なります。

vsys1 および vsys2 ではデフォルト仮想ルーターを使います。vsys3 では共有ルートレベル untrust-vr を選択します。

WebUI 上で vsys を作成した後も、ルートシステムにログインし続けることになります。新たに作成された vsys にログインするには、次のような操作が必要です。

Vsys > Configure > に列挙されている仮想システム名から選択して **Enter** をクリックします。

ログインした vsys に該当する WebUI ページが現れます。情報表示領域の上部には、vsys 名が「Vsys: *Name*」という形で表示されます。

CLI で vsys を作成した場合はただちに、ここで作成した vsys にログインした状態になります (作成済みの vsys にルートレベルからログインするには、**enter vsys** *name_str* というコマンドを使います)。vsys にログインしたら CLI コマンドプロンプトが変更されて、コマンドを発行しているシステム名が含まれるようになります。

WebUI

1. **Vsys1**

   Vsys > Configure > New: 次のように入力してから **OK** をクリックします。

   Vsys Name: vsys1
   Vsys Admin Name: Alice
   Vsys Admin New Password: wlEaS1v1
   Confirm New Password: wlEaS1v1
   Virtual Router:
   Create a default virtual router: (選択)

2. **Vsys2**

   Vsys > Configure > New: 次のように入力してから **OK** をクリックします。

   Vsys Name: vsys2
   Vsys Admin Name: Bob
   Vsys Admin New Password: pjF56Ms2
   Confirm New Password: pjF56Ms2
   Virtual Router:
   Create a default virtual router: (選択)

3. **Vsys3**

   Vsys > Configure > New: 次のように入力してから **OK** をクリックします。

   Vsys Name: vsys3
   Virtual Router:
   Select an existing virtual router: (選択), untrust-vr

CLI

1. **Vsys1**

```
device-> set vsys vsys1
device(vsys1)-> set admin name Alice
device(vsys1)-> set admin password wlEaS1v1
device(vsys1)-> save
device(vsys1)-> exit
```

注 : コマンドの実行後は、**save** コマンドを実行してから **exit** コマンドを実行してください。そうでないと変更した内容が保存されません。

2. **Vsys2**

```
device-> set vsys vsys2
device(vsys2)-> set admin name Bob
device(vsys2)-> set admin password pjF56Ms2
device(vsys2)-> save
device(vsys2)-> exit
```

3. **Vsys3**

```
device-> set vsys vsys3 vrouter share untrust-vr
device(vsys3)-> save
```

Vsys にデフォルト仮想ルーターを設定する

ルートレベル管理者が vsys オブジェクトを作成すると、自動的に次の仮想ルーターが使えるようになっています。

- すべての共有ルートレベル仮想ルーター (untrust-vr など)

  Vsys とルートシステムは、Untrust ゾーンばかりでなく、untrust-vr や、その他の仮想ルーター (ルートレベルで共有可能と定義したもの) も共有します。

- 自分自身の仮想ルーター

  Vsys レベル仮想ルーター名は、初期状態では *vsysname-vr* となっています。もちろん、もっと意味のある名前に変更することもできます。これは vsys ごとに用意される仮想ルーターで、初期状態では、Trust-*vsysname* ゾーンのルーティングテーブルを管理するようになっています。vsys レベル仮想ルーターはどれも共有できません。

Vsys のデフォルト仮想ルーターとして、共有仮想ルーターでも、vsys レベル仮想ルーターでも選択できます。デフォルトの仮想ルーターを変更するには、vsys を入力し、次の CLI コマンドを使用します。

set vrouter *name* **default-vrouter**

ルートレベル管理者は、すべての vsys ゾーンを untrust-vr ルーテイングドメインに置きたい場合 (たとえば Trust-*vsysname* ゾーンに向かうインターフェースがすべて Route モードである場合)、vsys レベルセキュリティゾーンバインディングを *vsysname*-vr から untrust-vr に変更することにより、vsysname-vr を使わずに済ますことができます。仮想システムの詳細については、**7**-15 ページの「ルーティング」を参照してください。

注 : 現行の ScreenOS は、仮想システムでユーザー定義の仮想ルーターが使えます。

ゾーンを共有仮想ルーターにバインドする

vsys (仮想システム) はそれぞれが独立したセキュリティドメインであり、ルートシステムとセキュリティゾーンを共有できるほか、独自のセキュリティゾーンを定義することもできます。ルートレベル管理者が vsys オブジェクトを作成すると、次のゾーンが自動的に引き継がれるか、作成されます。

- すべての共有ゾーン (ルートシステムから引き継がれる)
- 共有 Null ゾーン (ルートシステムから引き継がれた)
- Trust-*vsys_name* ゾーン
- Untrust-Tun-*vsys_name* ゾーン
- Global-*vsys_name* ゾーン

注 : 各ゾーンタイプについて詳しくは **2**-25 ページの「ゾーン」を参照してください。

Vsys ごとに、上記とは別にユーザー定義のセキュリティゾーンを使用することもできます。このゾーンを、ルートレベルで定義された共有仮想ルーターや、当該 vsys 専用の仮想ルーターにバインドできます。Vsys1 という名前のセキュリティゾーンを作成する手順を以下に示します。

WebUI

Vsys > Enter (vsys1)

Network > Zones > New: 次のように入力してから **OK** をクリックします。

Zone Name: (**ゾーン名を入力**)
Virtual Router Name: (**ドロップダウンリストから仮想ルーターを選択**)
Zone Type: Layer 3

CLI

```
device-> enter vsys vsys1
device(vsys1)-> set zone name name_str
device(vsys1)-> set zone vrouter vrouter
device(vsys1)-> save
```

Vsys やルートシステムに定義できるセキュリティゾーンの数には、デバイスレベルで設定可能なセキュリティゾーン数による制限しかありません。ルート管理者またはルートレベル読取 / 書込管理者は、セキュリティゾーンをすべて、特定の vsys に割り当てることも可能です。逆に、どの仮想システムもルートレベルセキュリティゾーンを共有し、ユーザー定義の vsys レベルゾーンを使わないのであれば、セキュリティゾーンをすべてルートレベルで使えることになります。

注 : デバイスレベルで設定可能なユーザー定義 (カスタム) セキュリティゾーンの総数は、ルートレベルのカスタムゾーン数 (ゾーンライセンスキーで定義) と、vsys ライセンスキーで許可されたカスタムゾーン数の和になります。

Vsys 管理者としてログイン

Vsys 管理者は vsys に直接ログインしますが、ルートレベル管理者はルートレベルから vsys に入ります。Vsys 管理者が vsys からログアウトすると、接続はただちに断たれます。ただしルートレベル管理者が vsys からログアウトすると、ルートシステムにログアウトします。

次の例は、vsys 管理者として、vsys にログオン、パスワードの変更、ログアウトの方法を示しています。

この例では、vsys 管理者が、自分に割り当てられたログイン名 **jsmith** およびパスワード **Pd50iH10** を入力して、vsys1 にログオンする様子を示します。さらに、パスワードを **I6Dls13guh** に変更し、ログアウトします。

注 : Vsys 管理者は自分のログイン名（ユーザー名）を変更することができません。ログイン名すべて固有で、セキュリティデバイスが適切な vsys へのログイン接続をルートするために使われます。

WebUI

1. **ログイン**
   ブラウザーの URL フィールドに、vsys1 の Untrust ゾーンインターフェース IP アドレスを入力します。

   Network Password ダイアログボックスが現れるので、以下を入力して **OK** をクリックします。

   User Name: jsmith
   Password: Pd50iH10

2. **パスワードの変更**
   Configuration > Admin > Administrators: 次のように入力してから **OK** をクリックします。

   Vsys Admin Old Password: Pd50iH10
   Vsys Admin New Password: I6Dls13guh
   Confirm New Password: I6Dls13guh

3. **ログアウト**
   メニューの一番下にある **Logout** をクリックします。

CLI

1. **ログイン**
   SCS (Secure Command Shell)、Telnet、HyperTerminal のいずれかを使い、セッションコマンドラインプロンプトから vsys1 の Untrust ゾーンインターフェース IP アドレスを入力します。

   次のユーザー名とパスワードでログインします。

   - User Name: jsmith
   - Password: Pd50iH10

2. **パスワードの変更**
   set admin password I6Dls13guh
   save

3. **ログアウト**
   exit

仮想システムプロファイル

ルートレベルユーザー（セキュリティデバイスの管理者）は、vsys ごとにセッション限度とリソース限度を使用可能、または使用不可にできます。ある vsys に対してセッション限度を構成しておくと、その vsys がセッション限度に到達または超過したとき、セキュリティデバイスはその セッション限度を実施して その vsys のパケットをドロップします。サービス数を超過する場合、たとえば vsys セッションの総数がシステムセッションの総数を超えることがある場合は、ある特定の vsys 用にセッション数を予約しておくことができます。セキュリティデバイスは、セッション限度によってドロップされるパケットを追跡します。

注 : 仮想システムを使用するには、vsys キーをインストールしてから、この機能を使用可能に設定する必要があります。これはデフォルトで無効になっています。

ScreenOS では、vsys に対してリソース限度を構成するには 次の 2 つの方法があります。

- プロファイルの割り当て
- コマンドによる設定変更

以下に、vsys ごとにリソースに最大限度と予約限度を定義できるリソースを示します。

- 動的 IP アドレス（DIP）
- マップ IP アドレス（MIP）
- ユーザー定義のサービスとグループ
- ポリシーとマルチキャストポリシー
- セッション
- ゾーンアドレス帳入力とグループは、ゾーン別、vsys 別の限度です。
- ユーザー定義セキュリティゾーン

注 : ScreenOS は、すべての仮想システムのアドレスとアドレスグループが含まれている共有ゾーンについて、ゾーンアドレス帳限度とゾーンアドレスグループ限度を実施します。共有ゾーンのアドレスまたはアドレス帳を vsys から見る場合、その vsys 内で構成されたアドレスまたはアドレス帳しかリストされません。共有ゾーン内のアドレスおよびアドレスグループ用に使用されるリソースは、その共有ゾーンが作成されたルートシステムに対して課金されます。

共有ゾーンのアドレスとアドレスグループは、予約できません。

CPU ウェイトを vsys プロファイルに含めることができます。これによって、特定の vsys に CPU 処理時間の一部を割り当てることができます。詳細については 18 ページの「CPU ウェイトの構成」を参照してください。

Vsys セッションカウンタ

セキュリティデバイスは vsys セッションを新規作成したときに、その vsys のセッションカウンタを 1 つ増やします。セッションが終了すると、カウンタを 1 つ減らします。

セキュリティデバイスは、アクティブ、非アクティブを問わず、また時間に関係なく vsys が保持したすべてのセッションをカウントします。

Vsys セッション情報

セキュリティデバイスは、セッション統計を vsys 別に記録します。セキュリティデバイス管理者（ルート管理者）は、すべての vsys のすべての収集統計情報とセッション情報を見ることができます。vsys 管理者は、管理者の vsys ドメインのセッションと統計情報だけを見ることができます。

高可用性ペアにおける動作

NetScreen 冗長プロトコル (NSRP) で構成された 2 つのデバイスがアクティブ - アクティブモードの場合、2 つのセッションが同時に作成されると、vsys は設定されているセッション限度より 1 つ多いセッションを保有するおそれがあります。

NSRP またはアクティブ - アクティブモードの詳細については、*第 11 部: 高可用性* を参照してください。

Vsys プロファイルの作成

Vsys プロファイルは、最大限度を保持する場所です。また、オーバーロードの場合、ScreenOS で vsys や仮想システムのグループを制御できる、特定の限度やセッションに限定したアラームしきい値も保持できます。Vsys クライアントのニーズを満たすようなサービスに対する階層化限度を設計できます。たとえばサービスをゴールド、シルバー、ブロンズに分けて、それぞれに異なるリソース最大値を割り当てることができます。

次の 2 種類のデフォルトプロファイルがあります。

- VsysDefaultProfile

  デフォルトでは、vsys の新規作成時に VsysDefaultProfile が適用されます。VsysDefaultProfile は、定義によって、すべてのリソースへのアクセスを許可しますが保証はしません。新規作成した vsys に別の vsys プロファイルを割り当てし直すことによって、リソースへのアクセスを制御することができます。この vsys プロファイルは編集できません。

- RootProfile

  デフォルトでは、ルート vsys は RootProfile を使用します。RootProfile に限度を定義すると、仮想システムが排他的に使用できる特定の静的リソースを予約することができます。

これらのデフォルト プロファイルのほかに、vsys プロファイルを 18 個まで作成できます。作成した 1 個のプロファイルに、1 つまたは複数の vsys を割り当てることができます。

リソース限度の設定

Vsys リソースのグローバル最大値は、セキュリティデバイスに依存します。最大限度および予約限度が明示的に設定されない限り、デバイスのデフォルト値が適用されます。Vsys を作成後、その限度値を表示するには、**get vsys** *vsys_name* コマンドを使用します。

リソースの最大限度および予約限度を設定するには、次の点に留意してください。

- 最大限度値は、デバイスに依存依存するグローバル最大値を超えることができません。**get vsys-profile global** コマンドを使って、グローバル最大値を確認してください。
- セッションを除くすべてのリソースについて、現在使用中のリソース数（実使用数）より小さい値を最大限度値に設定することはできません。実使用数を確認するには、**get vsys-profile global** コマンドを使用してください。

  セッションについては、使用中のセッション数より小さい値をセッション最大値に設定できます。そうしても現在のセッションはドロップされません。実使用セッション数が最大値を下回ると最大値が実施されますが、新しいセッションを作成することができなくなります。**get vsys session-limit** コマンドを使った場合、負の値の使用可能セッション数が表示されます。
- 予約値に、設定済みの最大値を超える値を設定できません。
- 合計割り当て使用数（すべての仮想システムの合計予約数または合計実使用数のいずれか大きい値）は、グローバル最大値を超えることはできません。

次の表に、3 つの仮想システム（vs1、vs2、および vs3）の合計割り当て使用数がどのように算出されるかを示します。

	vs1	vs2	vs3	Global
予約数（設定済みの値）	20	2	40	
実使用数	40	15	37	
割り当て数	40	15	40	95

割り当て数の計算では、v3 の実際の使用数が設定済み予約数より小さくても、予約数の方を使用していることに注目してください。グローバルの最大値は 95 です。

次の例では、以下の値で新しい vsys プロファイルを作成します。

- Name: gold
- CPU weight: 30 (デフォルトは 50)
- DIPs: maximum: 25, reserve: 5
- MIP (Mapped IP): maximum: 25
- Mpolicies: maximum: 5
- Policies: maximum: 50
- Session: maximum: 1200

WebUI

Vsys > Profile: New を選択し、名前と設定値を入力してから **OK** をクリックします。

CLI

```
set vsys-profile name gold cpu-weigh 30
set vsys-profile gold dips max 25 reserve 5
set vsys-profile gold mips max 25
set vsys-profile gold mpolicies max 5
set vsys-profile gold policies max 50
set vsys-profile gold sessions max 1200
save
```

Vsys プロファイル割り当てによるセッション限度の追加

WebUI または CLI で、vsys プロファイルにセッション限度を割り当てることができます。セッション限度を設定するには、次のパラメータの 1 つまたは複数を定義する必要があります。

- session max

  セッション最大値は、100 からセキュリティシステム全体の最大セッション数までの値です。デフォルト値は、セキュリティシステム全体の最大セッション数です（セッション限度が実施されていない状態と同然）。

- reserve

  サービスが超過する場合、予約数は、指定した vsys の予約セッション数または保証セッション数となります。予約数を指定できる範囲は、0 ～ vsys に割り当てる最大セッション数です。

- alarm

  アラームしきい値は、アラームを起動する最大限度率です。デフォルト値は、構成済み vsys のセッション限度の 100 % です。

次の例では、**gold** という名前の vsys プロファイルにセッション限度を設定します。限度値は次のとおりです。

- session max: 2500
- Reserve: 2000
- Alarm: 90（セッション最大値の 90 % に達したときにアラームが起動されます）

このプロファイルに割り当てる vsys は、セッションを一度に 2,500 個まで保有できます。セキュリティデバイス全体でサービス超過が生じると、vsys は 2,000 個のセッションしか保有できません。Vsys がセッション最大値の 90 % を消費した時点で、アラームが起動します。

WebUI

Vsys > Profile > Edit

CLI

set vsys-profile gold session max 2500 reserve 2000 alarm 90

作成した vsys プロファイルに *vsys1* という名前の vsys を割り当てるには、WebUI または CLI を使用します。

WebUI

Vsys > Configure > Edit

CLI

set vsys vsys1 vsys-profile name gold

セッションの変更設定

既存の vsys プロファイルに定義されているセッション限度、予約数、アラームしきい値は、vsys ごとに変更設定することができます。それには、vsys にログインして変更設定を行います。デフォルトでは、仮想システムに変更設定値は存在しません。

注 : ScreenOS は、セッション変更設定値を vsys プロファイルではなく vsys に関連付けます。

次の例では、セッション最大値を 2,500 から 3,500 に変更設定します。

WebUI

Vsys > Configure > Edit（*vsys*）

CLI

enter vsys vsys1
（vsys1）set override session-limit max 3500
（vsys1）save

セッション限度到達アラームの変更設定

セッション限度到達（SLR）アラームを設定できます。アラームは、SLR レベルに達したとき、または超えたときに起動します。vsys のセッション数が 10 秒間連続してアラームの起動レベルを下回ると、セキュリティデバイスはアラームを停止します。セキュリティデバイスは、アラームメッセージをログ記録します。

Vsys SLR アラームに簡易ネットワーク管理プロトコル（SNMP）トラップを設定することができます。SNMP の詳細については、*第 2 部 : 基本* を参照してください。

次の例では、vsys のセッション数がセッション限度の 80 % に達したときにアラームが起動するように定義します。元の「gold」プロファイルには、セッション限度の 90 % に達したときにアラームが起動するよう設定されています。

WebUI

Vsys > Configure > Edit（*vsys*）

CLI

```
enter vsys vsys1
    (vsys1) set override session-limit alarm 80
    (vsys1) save
```

Vsys プロファイルの削除

WebUI または CLI で、vsys プロファイルを削除することができます。Vsys プロファイルを削除する前に、このプロファイルを使用している vsys がいないことを確認します。ScreenOS は、使用中のプロファイルの削除を許しません。

削除しようとしているプロファイルが使用中であるというメッセージを受信した場合、別の vsys プロファイルを使用するように変更した後に、再び削除を行います。

次の例では、vsys プロファイル **gold** を削除します。

WebUI

Vsys > Profile: 削除する vsys プロファイルの右側の **Remove** をクリックします。

CLI

```
unset vsys-profile gold
```

Vsys 設定値の表示

セキュリティデバイスの管理者は、すべての仮想システムに関するセッション統計情報を見ることができます。しかし、vsys コンテキスト内では当該 vsys の統計しか見ることができません。

変更設定の表示

CLI で、vsys に設定されている変更設定値を表示するには、**get vsys** *vsys_name* コマンド、または **get vsys override** コマンドを入力します。Vsys コンテキストを入力し、**get override session-limit** コマンドを入力する方法もあります。

次に、**get vsys vsys2** の出力例を示します。

```
device-> get vsys vsys2

Total number of vsys: 2

Name            Id Profile  Interface           IP Address         Vlan vsd
vsys2            2 VsysDef~ N/A                 N/A                N/A
Vsys-limit        Maximum   Reserved  Actual-use
dips                  254          0           0
mips                  384          0           0
mpolicies             200          0           0
policies              512          0           0
sessions           250064          0           0
user-serv-grps        128          0           0
user-servs            512          0           0
user-zones            215          0           1
zone-addr-grps        512          0           0(Untrust)
```

```
zone-addrs          20000         4            4(Untrust)
cpu-weight             50         -            0
(* - The marked setting has been overridden.)
```

WebUI で変更設定値を表示することもできます。

次の例では、vsys コンテキスト内で、branch1 という名前の vsys の予約情報を表示します。

WebUI

Vsys > Profile > Edit

CLI

enter vsys branch1
    (branch1) get override session-limit
    (branch1) exit

プロファイルの表示

WebUI または CLI で、ルート管理者として各 vsys プロファイルを見ることができます。WebUI では、すべてのプロファイルまたは現在の使用状況サマリーを表示することはできません。CLI では、ルート管理者としてすべての vsys プロファイルと、実使用に関する統計情報が含まれているグローバル使用状況サマリーを表示することができます。CLI では vsys 管理者として vsys にログインし、vsys が使用している vsys プロファイルを見ることができます。

WebUI

Vsys > Profile: 表示するプロファイルを選択します。

CLI 1

device-> **get vsys-profile red**

```
vsys-profile-name  ref-cnt  vsys-limit       maximum   reserved   peak-use
-------------------------------------------------------------------------------
 red                     0   dips                 254        0        0
                             mips                 384        0        0
                             mpolicies            200        0        0
                             policies             512        0        0
                             sessions            3000      100        0
                             user-serv-grps       128        0        0
                             user-servs           512        0        0
                             user-zones           215        0        0
                             zone-addr-grps       512        0        0
                             zone-addrs         20000        4        0
                             cpu-weight = 44, 29% of total cpu-weight 150
                             session alarm level = 100%
-------------------------------------------------------------------------------
```

CLI 2

device-> **get vsys-profile red**

```
* indicates default vsys profile.
 vsys-profile-name  ref-cnt  vsys-limit       maximum   reserved   peak-use
-------------------------------------------------------------------------------
*VsysDefaultProfile      2   dips                 254        0        0
                             mips                 384        0        0
                             mpolicies            200        0        0
                             policies             512        0        0
                             sessions          250064        0        0
                             user-serv-grps       128        0        0
```

```
                            user-servs           512       0       0
                            user-zones           215       0
1(vsys2)
                            zone-addr-grps       512       0       0
                            zone-addrs         20000       4 4(vsys2/Unt~)
                            cpu-weight = 50, 33% of total cpu-weight 150
                            session alarm level = 100%
vsys-profile-name  ref-cnt  vsys-limit       maximum   reserved   peak-use
-------------------------------------------------------------------------
 RootProfile             1  dips                 254       0       0
                            mips                6144       0       0
                            mpolicies            200       0       0
                            policies           20000       0       0
                            sessions          250064       0       0
                            user-serv-grps       128       0       0
                            user-servs          2048       0       0
                            user-zones           215       0       0
                            zone-addr-grps       512       0
2(Root/Tru~)
                            zone-addrs         20000       0
7(Root/Tru~)
                            cpu-weight = 50, 33% of total cpu-weight 150
                            session alarm level = 100%
-------------------------------------------------------------------------
 red                     0  dips                 254       0       0
                            mips                 384       0       0
                            mpolicies            200       0       0
                            policies             512       0       0
                            sessions            3000     100       0
                            user-serv-grps       128       0       0
                            user-servs           512       0       0
                            user-zones           215       0       0
                            zone-addr-grps       512       0       0
                            zone-addrs         20000       4       0
                            cpu-weight = 44, 29% of total cpu-weight 150
                            session alarm level = 100%
-------------------------------------------------------------------------
global usage summary:       global-limit     maximum   allocated  actual
                                                          use      use
-------------------------------------------------------------------------
                            dips                65535       0       0
                            mips                 6145       0       0
                            mpolicies             200       0       0
                            policies            20000       0       0
                            sessions           250064       0       0
                            user-serv-grps        128       0       0
                            user-servs           2048       0       0
                            user-zones            215       1       1
                            zone-addr-grps        512       2       2
                            zone-addrs          20000      95      75
                                                      total cpu-weight = 150
```

注： Peak-use 値は、vsys プロファイルを使用しているすべての仮想システムのなかで最も高い値です。

セッションの統計情報の表示

セッションの統計情報を表示するには、vsys コンテキストを入力してから、**get session** コマンドを入力します。

WebUI

使用できません。

CLI

```
(vsys1)-> get session
vsys1: sw alloc 0/max 3500, alloc failed 0, mcast alloc 0
Total 0 sessions shown
(vsys1)->
```

CPU リソースの共有と分割

デフォルトでは、セキュリティシステム内ですべての仮想システムが同じ CPU リソースを共有します。このため、仮想システム（vsys）の 1 つが CPU リソースを独占するおそれがあります。

たとえば セキュリティシステム内の 20 個の仮想システムの 1 つが DOS 攻撃を受けてすべての CPU リソースを消費した場合、CPU は残る 19 個の仮想システムのどのトラフィックも処理することができなくなります。本質的に、20 個すべての仮想システムが DOS 攻撃を受けたのと同然の状態になります。CPU 限度機能としても知られている CPU 過重使用保護はこのような状況になるのを防ぐ機能です。

この機能を使用すると、「共有利用」に対する「公平利用」または「公平モード」としてセキュリティデバイスを構成することができます。より均等なリソ - ス処理分散化を可能にするには、公平モードへの切り換えを起動するフロー CPU 利用しきい値の割り当てを行うことができます。また、公平モードから共有モードに戻すこともできます。デフォルトでは、セキュリティデバイスは共有モードで動作します。

公平利用を実施するには、vsys に CPU ウェイトを割り当てます。ScreenOS は、セキュリティデバイス内のすべての仮想システムに相対的なこれらのウェイトを使って、ウェイトに相対的な時間を割り当てます。ScreenOS は、時間割り当てを 1 秒間隔で実施します。これは、vsys が自分に割り当てられた時間割り当てを 1 秒間超過せず、かつファイアウォールに過重負荷がかからない限り、vsys のパケットはドロップされないことを意味します。

注 : CPU 過重使用保護機能は、vsys プロファイルによって制約されるセッション限度値には依存しません。

システム管理者として、公平モードで vsys を通過する交通量を決定するため、vsys の CPU ウェイト（他の仮想システムに相対的）を設定します。

セキュリティシステムが公平モードで稼動中に予想されるバーストを識別し、各 vsys に適切な CPU ウェイトを選びバーストがセキュリティシステムを通過できるようにする必要があります。選択したウェイトによって有害なパケットドロップが起きる可能性がないことを、事前に検証することをお勧めします。

この機能を使ってルート vsys の CPU ウェイトを固定化することもできます。

CPU ウェイトの構成

CPU ウェイトは、各 vsys の CPU 時間割り当てを算出するために使用される非物理量です。時間割り当ての算出では、該当 vsys の CPU ウェイトだけでなく、セキュリティシステム内のすべての仮想システムの CPU ウェイトとが使用されます。

たとえば、次のような CPU ウェイトを持つ仮想システムを想定します。

- vsys1: 10
- vsys2: 20
- vsys3: 30
- vsys4: 40

CPU ウェイトの合計は 100 です。時間割り当ては、この合計値に対する vsys の比率である CPU ウェイト率に CPU リソースを乗算した結果の値であり、vsys が 1 秒間隔で使用可能な、使用可能 CPU リソースをパーセントで表す値です。仮想システムの時間割り当ては、次のようになります。

- 10/100: 10％
- 20/100: 20％
- 30/100: 30％
- 40/100: 40％

注： CPU ウェイトは静的リソースではありません。ScreenOS は、vsys の削除や追加が行われると CPU ウェイトを再計算します。

Vsys を作成すると、別の vsys プロファイルを指定しない限り自動的にデフォルトの vsys プロファイル（VsysDefaultProfile）が適用されます。デフォルトの vsys プロファイルには、CPU ウェイト 50 が構成されています。CPU ウェイトを変更することができます。それには、該当 vsys が使用している vsys プロファイルの CPU ウェイトを変更します。または、vsys にログインしてから **set override cpu-weight** コマンドを使って CPU ウェイトの変更設定を行います。

次の例では、**corp-profile** vsys プロファイルの CPU ウェイトを **40** に変更します。

WebUI

Vsys > CPU Limit: corp-profile vsys プロファイルに対して、**Edit** をクリックし、CPU Weight 項目に **40** と入力してから **OK** をクリックします。

CLI

set vsys-profile corp-profile cpu-weigh 40

公平モードのパケットフロー

過重使用保護機能が使用可能になっている場合、セキュリティデバイスに重負荷がかかると、ScreenOS はデバイスを公平モードに移行します。

公平モードの間、ScreenOS はパケットを次のように処理します。

1. システムはパケットにリソースを割り当て、タイムスタンプを作成します。
2. フロー CPU がパケットを処理します。
3. システムは、仮想システムを照合して、パケットについて課金すべきかかどうか、その仮想システムの時間割り当ての残量を判断します。残量が無くなっていれば、システムはパケットをドロップします。ScreenOS がどの vsys に課金すべきをかを判断する方法については、表 2 を参照してください。
4. システムは、パケットを処理し、処理に要した CPU 処理時間を現在時刻とステップ 1 のタイムスタンプから算出し、それを vsys の時間割り当て残量から差し引きます。

仮想システムの時間割り当ての全量が消費されると、システムは以降の vsys のすべてのパケットをドロップします。

表 2: 課金対象 Vsys の判断

ソース Vsys	宛先 Vsys	課金対象 Vsys
ルート	ルート	ルート
ルート	宛先 vsys	宛先 vsys
ソース vsys	ルート	ソース vsys
ソース vsys	宛先 vsys	ソース vsys

注 : このパケットドロップ（実施）は、公平モードでのみ行われます。

システムは、時間割り当てを 125 ミリ秒毎にリフレッシュします。

注 : CPU の過重使用保護は、フロー CPU がハードウェアからサポートを受けずに独力で実行します。この機能は、時間割り当てが残っている仮想システムのパケットを処理することに最善を尽くします。しかし、パケットについてどの vsys を課金すべきか判断するのに時間がかかるため、仮想システムが時間割り当て量を超過しない保証はありません。

時間割り当てを越えたためパケットをドロップするのにかかった時間も、該当 vsys に課金されます。過重なトラフィックを受信しているために継続的に時間割り当てを超過する場合、該当 vsys のどのパケットもシステムを通過できません。

公平モードから共有モードへの移行

ScreenOS は、ルート管理者がセキュリティデバイスをどのように構成するかに依存して次のように動作します。

- 管理者が明示的にセキュリティデバイスを共有モードに設定するまで、公平モードを維持します。
- 指定された時間限度が超過すると、共有モードに戻します。

予測フロー CPU 使用率が構成済みしきい値を下回ると、自動的に共有モードに戻します。

CPU 限度機能を使用可能にする

CLI で CPU 限度機能コマンドの多くを使用する前に、対象リソースの初期化と割り当てを行う必要があります。CLI で CPU 限度パラメータを構成した後に、機能を使用可能に設定する必要があります。

WebUI

Vsys > CPU Limit: **CPU Limit Enable** チェックボックスをオンにして **OK** をクリックします。

CLI

CPU 限度機能の対象となるリソースの初期化と割り当てを行うには、次のコマンドを入力します。

```
set cpu-limit
```

CPU 限度パラメータを構成した後に、次のコマンドを入力して機能を使用可能にします。

```
set cpu-limit enable
```

機能を無効にするには、次のコマンドを入力します。

```
unset cpu-limit enable
```

機能を無効にし、リソースの割り当てを解除するには、次のコマンドを入力します。

```
unset cpu-limit
```

CPU 使用率の測定

各セキュリティデバイスは、経過した CPU 周期数を測定します。セキュリティデバイス内の各 vsys の CPU ウェイトを使って、各 vsys にリソース割り当てを設定することができます。

セキュリティシステムの現在の CPU 使用率を判断するには、ルート管理者としてログインし、**get performance cpu-limit**、または **get vsys cpu-limit** コマンドを使用します。これらのコマンドは、各 vsys に設定されている CPU 時間割り当て比率として、vsys ごとの CPU 使用率を返します。

注 : これらのコマンドを使用する前に、**set cpu-limit enable** コマンドを使って CPU 限度機能を使用可能にする必要があります。このコマンドの詳細については、*ScreenOS CLI Reference Guide* を参照してください。

次の出力は、公平モードで動作しているセキュリティデバイスの合計 6 個の構成済み仮想システム（5 個の仮想システムとルート仮想システム）を示しています。

```
                                  CPU Quota %
Vsys Name     Wgt  Cfg %   1 min  5 min  15 min
Root           50   16.6      0      0       0
corp           50   16.6     99     99      99
v1             50   16.6      8     18      10
v2             50   16.6      8     18      10
v3             50   16.6      7     17       9
v4             50   16.6      7     17      13
```

この出力は、次の項目を表示します。

- Vsys Name
- Wgt - この vsys に設定されている CPU ウェイト
- Cfg % - この vsys に設定されている CPU リソース率
- 1 min - 過去 1 分間に vsys が使用した CPU 割り当て比率
- 5 min - 過去 5 分間に vsys が使用した CPU 割り当て比率
- 15 min - 過去 15 分間に vsys が使用した CPU 割り当て比率

この例では、構成済み仮想システムのうち、vsys corp は過去 1 分間、5 分間、15 分間に自分に割り当てられた CPU 時間のほぼ全量を使用しています。CPU リソースをまったく使用しなかった Root vsys を除いて、他の仮想システムは各自に割り当てられた CPU 時間のうち、過去 1 分間に 7 ～ 8 % 、5 分間に 17 ～ 18 % を使用しています。

Vsys の詳細なパケット情報を調べるには、**get performance cpu-limit detail vsys all** *vsys_name* コマンドを使用します。このコマンドは、指定した vsys に関する過去 60 秒および 60 分間の統計情報を返します。

この出力には、次のような情報が表示されます。

- 正常に通過したパケット数
- ドロップされたパケット数
- CPU 割り当て比率

```
device-> get performance cpu-limit detail vsys corp
vsys corp:
Last 60 seconds (paks passed,paks dropped by cpu limit/cpu quota %):
59:  916, 10550/78  58: 1206, 13796/99  57: 1252, 13751/99
56: 1255, 13747/99  55: 1302, 13700/99  54: 1308, 13694/99
53: 1337, 13666/99  52: 1232, 13770/99  51: 1222, 13780/99
50: 1263, 13740/99  49: 1322, 13680/99  48: 1311, 13691/99
47: 1334, 13668/99  46: 1317, 13686/99  45: 1319, 13683/99
```

```
44: 1322, 13680/99  43: 1333, 13670/99  42: 1323, 13679/99
41: 1337, 13665/99  40: 1333, 13670/99  39: 1331, 13671/99
38: 1325, 13678/99  37: 1318, 13685/99  36: 1319, 13683/99
35: 1318, 13685/99  34: 1333, 13668/99  33: 1355, 13647/99
32: 1346, 13656/99  31: 1360, 13642/99  30: 1360, 13643/99
29: 1351, 13651/99  28: 1346, 13656/99  27: 1357, 13646/99
26: 1339, 13663/99  25: 1337, 13665/99  24: 1356, 13646/99
23: 1329, 13674/99  22: 7190,  6961/99  21: 13164,     0/ -
20: 13219,     0/ -  19: 13765,     0/ -  18: 15136,     0/ -
17: 7730,     0/ -  16:  200,     0/ -  15:  200,     0/ -
14:  200,     0/ -  13:  200,     0/ -  12:  200,     0/ -
11:  200,     0/ -  10:  200,     0/ -   9:  200,     0/ -
 8:  200,     0/ -   7:  200,     0/ -   6:  200,     0/ -
 5:  200,     0/ -   4:  200,     0/ -   3:  200,     0/ 7
 2:  648,  5566/47   1: 1317, 13685/99   0: 1333, 13670/99

Last 60 minutes (paks passed,paks dropped by cpu limit):
59:   77968,  471526 58:   85666,  537590 57:   33921,  523433
56:   21110,  564548 55:   80572,  748114 54:   91814,  538566
53:   83932,  544342 52:   72268,  624337 51:    1339,  708070
50:   87790,  970630 49:   96317, 1084226 48:   68805,  267087
47:       0,       0 46:       0,       0 45:       0,       0
44:       0,       0 43:       0,       0 42:       0,       0
41:       1,       0 40:       0,       0 39:       0,       0
38:       0,       0 37:       0,       0 36:       0,       0
35:       0,       0 34:       0,       0 33:       0,       0
32:       0,       0 31:       0,       0 30:       0,       0
29:       0,       0 28:       0,       0 27:       0,       0
26:       0,       0 25:       0,       0 24:       0,       0
23:       0,       0 22:       0,       0 21:       1,       0
20:       0,       0 19:       0,       0 18:       0,       0
17:       0,       0 16:       0,       0 15:       0,       0
14:       0,       0 13:       0,       0 12:       0,       0
11:       0,       0 10:   90714,  679865  9:   86549, 1478569
 8:   88999, 1429512  7:  238258,  566208  6:  316219,  479793
 5:  477711,       0  4:  376981,       0  3:  439035,       0
 2:  395397,  735399  1:   87908,  743423  0:       0,       0
```

この出力は、過去 60 秒間の状況を示しています。corp vsys が 0 秒 ～ 2 秒、22 秒 ～ 59 秒において CPU 割り当て量を超え、平均して毎秒約 10,000 個以上のパケットがドロップされています。

たとえば過去 1 秒の時点で 1,317 パケットが通過し、CPU 割り当て量を超えたことにより 13,685 パケットがドロップされています。3 秒 ～ 16 秒まで、毎秒 200 個の corp vsys パケットが通過しています。セキュリティデバイスは共有モードに戻っています（共有モードのとき、ScreenOS は 「% CPU quota」覧に「-」を出力します)。22 秒の時点で、システムは再び公平モードに移っています。

ルート管理者として CPU 統計情報を表示するには、表示する詳細レベルによっていくつかの方法があります。表 3 を参照。

表 3: CPU 使用保護の Get コマンドオプション

コマンド	目的
get performance cpu-limit	すべての仮想システムについて、CPU ウェイト、対応する CPU 時間割り当て比率、および CPU 割り当て比率を返します。
get performance cpu-limit detail vsys *vsys_name*	指定された vsys について、過去 60 秒間、60 分間に収集した詳細な統計情報を返します。
get cpu-limit utilization	過去 60 秒間のフロー CPU 使用率、または予測フロー CPU 使用率を返します。 ■ ファイアウォールが共有モードで動作しているときに、表示される数値はフロー CPU 使用率です。 ■ ファイアウォールが公平モードのときは、表示される数値は予測フロー CPU 使用率です。 モードを共有から公平、公平、公平から共有へ切り換える自動しきい値を決定するのに使用されます。 数字の右側にあるアスタリスク文字（*）は、その時にデバイスが公平モードであったことを示します。 このコマンドで表示される使用率は、**get performance cpu** コマンドのものよりも 8 から 12 % 低くなります。これは、**get cpu-limit utilization** コマンドではいくつかのオーバヘッド値が含まれないためです。
get vsys cpu-limit	**get performance cpu-limit** コマンドと同じ出力を表示します。

共有から公平モードへ移行 CPU 使用率しきい値の設定

共有モード（デフォルト）から公平モードに移行し、他の仮想システムも CPU リソースが使えるよすにするため、セキュリティシステムを構成することができます。それには、次の操作を行います。設定値が適切で、その効果も確認できるまで、一部の手順を繰り返し実行する必要があります。

WebUI または CLI で、CPU 使用率しきい値を設定できます。WebUI の例では、コマンド選択肢を要約します。CLI の例では、完全な手順を示します。

注 : CPU 限度機能によって構成されるフロー CPU 使用率は、**get performance cpu** コマンドの出力とは異なる方法で計算されます。共有から公平モードへの移行しきい値を設定するには、次のいずれかの操作を行います。

WebUI

Vsys > CPU Limit: **CPU Limit Enable** チェックボックスをオンにして **OK** をクリックします。

Fair to Shared: セキュリティデバイスが共有モードに戻る方法を選択します。**automatic** を選択する場合、しきい値を入力します。**Fair Time**（デバイスが Fair mode を使うための明示的な秒数）を選択する場合は、希望する秒数を入力します。

Shared to Fair: しきい値を入力します。また、ホールドダウン時間（オプション）を入力します。

CLI

1. デバイスがトラフィックを処理中でないことを確認してください。

2. CPU 限度機能を初期化するには、次のコマンドを入力します。

   set cpu-limit

3. **shared-to-fair-threshold** 設定は、セキュリティデバイスが共有から公平モードへ移行するしきい値を表し、この値を上回ると移行が行われます。

   オプションでホールドダウン時間を設定することができます。これは、CPU 使用率が指定された共有から公平モード移行しきい値を上回り、セキュリティモードが公平モードに移行する最小時間です。

   shared-to-fair-threshold と **hold-down time**（オプション）を設定するには、しきい値（1 から 100 までの数字）とホールドダウン時間（0 から 1800 秒（30 分）までの値）を入力します。

   set cpu-limit shared-to-fair threshold *threshold* [hold-down-time *number*]

4. CPU 限度を使用可能にするには、次のコマンドを入力します。

   set cpu-limit enable

5. 現在のモード、および他の CPU 限度パラメータを確認するには、次のコマンドを入力します。

   get cpu-limit

   ```
   device-> get cpu-limit
   Current mode: shared
   Shared->fair: threshold 80%, hold down time 1
   Fair->shared: automatic, threshold 70%
   CPU limit: enabled
   ```

6. デバイスを共有モードに維持するレベルでトラフィックを送信します。

7. セキュリティシステムが共有モードに留まることを確認するには、次のコマンドを入力します。

   get cpu-limit utilization

   出力例 :

   ```
   device-> get cpu-limit utilization
   Last 60 seconds:
   59: 14   58: 14   57: 14   56: 14   55: 14   54: 14
   53: 14   52: 15   51: 14   50: 14   49: 14   48: 15
   47: 14   46: 15   45: 14   44: 15   43: 14   42: 15
   .... …出力が継続します …
   ```

   トラフィックの開始後、出力中にアスタリスクが表示される場合は、ファイアウォールが公平モードで、共有から公平モード移行しきい値が低すぎることを示します。次の手順で進めます。

   a. トラフィックを止めます。

   b. **set cpu-limit shared-to-fair threshold** *flow_threshold* コマンドで、共有から公平モード移行しきい値を上げます。

c. セキュリティシステムを共有モードに戻すには、次のように入力します。

exec cpu-limit mode shared

d. トラフィックを再開し、必要に応じて手順 7 を繰り返し実行します。

8. デバイスを公平モードに移行させるレベルまで、トラフィックを増加します。

9. セキュリティシステムが公平モードに移行したことを確認するには、次のコマンドを入力します。

get cpu-limit utilization

```
device-> get cpu-limit utilization
Last 60 seconds:
59: 96*  58: 94*  57: 96*  56: 96*  55: 96*  54: 82*
53: 20   52: 14   51: 15   50: 14   49: 15   48: 14
47: 14   46: 14   45: 14   44: 14   43: 14   42: 14
41: 15   40: 14   39: 15   38: 15   37: 15   36: 14
35: 15   34: 14   33: 14   32: 14   31: 15   30: 14
29: 14   28: 14   27: 15   26: 15   25: 15   24: 15
23: 91*  22: 96*  21: 97*  20: 96*  19: 97*  18: 96*
17: 97*  16: 96*  15: 98*  14: 96*  13: 98*  12: 96*
11: 98*  10: 96*   9: 97*   8: 96*   7: 97*   6: 96*
 5: 97*   4: 96*   3: 97*   2: 96*   1: 97*   0: 96*
(* - In Fair mode; projected CPU utilization displayed.)
```

トラフィックを増加したにもかかわらずシステムが公平モードに移行しない場合は、共有から公平モード移行しきい値が高すぎるためです。次の手順を実行します。

a. トラフィックを止めます。

b. **set cpu-limit shared-to-fair threshold** *flow_threshold* コマンドを入力して、共有から公平モード移行しきい値を下げます。

注 : **get cpu-limit utilization** コマンドをガイドとして使うことができます。

---

c. トラフィックを再開し、正しいしきい値を設定できるまで手順 9 を繰り返します。

共有モードに戻る方法を構成

共有から公平モード移行 CPU 使用率しきい値を設定後、共有モードへ自動移行、明示的期間の経過後に共有モードへ移行、または公平モードを維持するようにデバイスを構成できます。

- 共有モードへ自動移行するように構成するため、セキュリティデバイスは構成するしきい値を使用します。しきい値は予測フロー CPU 使用率で表され、この値を下回るとセキュリティデバイスが公平から共有モードへ移行します。ホールドダウン時間を設定することもできます。これは、フロー CPU 使用比率がフロー CPU 使用比率しきい値を上回らなければならない最小時間で表されます。

- 明示的期間を設定するには、セキュリティデバイスが公平時間設定値で公平モードを使用するように設定します。公平時間は 0 から 7200 秒までの範囲の数字です。

- 公平モードを維持するには、**never** 設定値を選択します。

次の例では、ルート管理者としてログインして、予測フロー CPU 使用率が指定しきい値を下回ったときセキュリティデバイスが自動的に共有モードに戻るように構成します。

この例では、公平から共有モードへ移行 CPU 使用率しきい値を初めて設定することを想定します。そのため、デバイスを希望通りに動作させることができる前に、手順を繰り返しいくつかの異なる設定値を試行する必要があります。確認のための手順も含まれています。CLI コマンドの例を示します。

注 : この手続きは、自動公平モードを使用可能にする場合にのみ必要です。

WebUI

Vsys > CPU Limit: CPU Limit Enable チェックボックスをオンにして、**OK** をクリックします。

Fair to Shared: **セキュリティデバイスが共有モードに戻る方法を選択します。Automatic を選択する場合、しきい値を入力します。**

CLI

1. セキュリティデバイスが公平モードを維持するレベルでトラフィックがセキュリティデバイスに到着することを確認します。
2. 自動公平モードしきい値を設定するには、次のコマンドを入力します。

   set cpu-limit fair-to-shared automatic threshold *number*

3. デバイスが共有モードへ移行するレベルになるまでトラフィック率を下げます。
4. ファイアウォールが共有モードに戻ることを確認するため、**get cpu-limit utilization** コマンドを入力します。
5. ファイアウォールがまだ公平モードのままである場合、より低い値を自動公平しきい値に適用してこの手順を繰り返します。

ルート Vsys 固定 CPU ウェイトの設定

ルート vsys の CPU 比率を明示的に指定するため、ルート vsys CPU ウェイトを計算できます。ただし、vsys の追加や削除を行うと、ルート vsys CPU ウェイトを再計算する必要があります。

正確なルート vsys CPU ウェイトを算出するには、その他すべての仮想システムの CPU ウェイトを設定する必要があります。次の式を用いて必要なルート vsys CPU ウェイトを計算します。

$$R = \frac{PW}{1 - P}$$

場所 :

- R は、ルート vsys CPU ウェイトです。
- P は、ルート vsys に適した CPU の比率で、

$$0 \leq P \leq 1$$

- W は、他のすべての仮想システムのウェイトの和です。

次の例では、4 個の仮想システムを 3 個の vsys プロファイルに分散し、CPU リソースの 30 % をルート vsys に割り当てます。

- Gold profile (CPU weight = 40): 1 vsys
- Silver profile (CPU weight = 30): 2 vsys
- RootProfile: 1 root vsys

ルート vsys（W）を除くすべての vsys の CPU ウェイトの和は 100 です。ルート v sys に割り当てる比率（P）は、30 % または .3 です。

前出の式を使用します。R = P*W/(1-P) = .3*100/.7 = 43

検証すると、ルート vsys の比率は 43/(100 + 43) で、約 30 % という結果が出ます。

今後 vsys を追加または削除することがあると、*W* の見直しと、ルート vsys CPU ウェイト *R* の再計算が必要です。

Vsys と仮想プライベートネットワーク

ルート vsys 管理者は、次のような仮想プライベートネットワーク（VPN）情報を見ることができます。

- すべての構成済み、またはアクティブのみのセキュリティアソシエーション（SA）
- インターネット鍵交換 (IKE) クッキー

読取書込み、読取専用特権を持つ vsys 管理者は、自分の vsys に関する情報のみを見ることができます。

次のセクションでは、この情報の詳細について、および情報を表示する方法を説明します。

セキュリティアソシエーションの表示

セキュリティデバイスのルート管理者は、**get sa** コマンドを使ってすべての仮想システムのセキュリティアソシエーション（SA）を表示することができます。このコマンドを発行すると、セキュリティデバイスに格納されている IPSec SA の総数（ルートシステムとすべての構成済み仮想システム）が抽出されます。

アクティブの SA のみを表示するには、**get sa active** コマンドを入力します。

WebUI から、SA を表示することもできます。

次の例では、システム管理者としてルート仮想システムとすべての仮想システムのすべての SA を見ることができます。

WebUI

VPNs > Monitor Status

CLI

get sa

Vsys 管理者で CLI を使用している場合は、**get sa** コマンドを入力して、vsys の SA を表示することができます。

アクティブの SA のみを表示するには、**get sa active** コマンドを入力します。

次の例では、clothing_store の vsys 管理者として vsys のアクティブ SA のみ表示します。

WebUI

VPNs > Monitor Status

CLI

```
enter vsys clothing_store
(clothing_store) get sa active
(clothing_store) exit
```

IKE クッキーの表示

IKE クッキーは、CLI からのみ表示できます。

セキュリティデバイスのシステム管理者として、システムのすべての IKE クッキー（ルートと vsys IKE クッキー）を見ることができます。CLI で、**get ike cookie** コマンドを入力します。

次の例では、システム管理者として IKE クッキーを表示します。

WebUI

使用できません。

CLI

get ike cookie

Vsys 管理者として、管理している vsy s の IKE クッキーを表示するには、vsys コンテキストを入力してから、**get ike cookie** コマンドを入力します。

次の例では、管理している *card_shop* vsys の IKE クッキーを表示します。

WebUI

使用できません。

CLI

```
enter vsys card_shop
(card_shop) get ike cookie
(card_shop) exit
```

ポリシー スケジューリング

Vsys コンテキスト内で、vsys 管理者は、ポリシーがアクティブなるタイムスロットを 1 回のみまたは反復するようにスケジュールすることができます。

新しいポリシーを作成すると、vsys 管理者はスケジューラを作成し、それを 1 つまたは複数の既存のポリシーにバインドすることができます。スケジューラがタイムアウトすると、セッションはエージアウトします。

このセクションでは、次の操作を説明します。

- 29 ページの「ポリシースケジューラの作成」
- 30 ページの「ポリシースケジュールをポリシーにバインド」
- 30 ページの「ポリシースケジュールの表示」
- 30 ページの「ポリシースケジュールの削除」

ポリシースケジューラの作成

Vsys 管理者として、1 回のみ、または反復してポリシーをアクティブするようにスケジュールすることができます。スケジューラに意味のある名前を付けて、開始時間と停止時間を設定することができます。コメントも添付することができます。

次の例では、月曜日から金曜日の 午前 8:00 〜 11:30 時、午後 1:00 〜 5:00 にのみサービスを繰り返し提供するようにスケジューラを構成します。スケジューラは時間制限を設定し、ポリシーはサービス制限を設定します。vsys コンテキストを入力し、構成を行います。

WebUI

Vsys > Configure > Enter

Objects > Schedules > **New** をクリックし、スケジュール用紙にデータを入力してから **OK** をクリックします。

CLI

```
device(hr)-> set scheduler restrictionM recurrent monday start 8:00 stop 11:30
    start 13:00 stop 17:00
device(hr)-> set scheduler restrictionTu recurrent tuesday start 8:00 stop 11:30
    start 13:00 stop 17:00
device(hr)-> set scheduler restrictionW recurrent wednesday start 8:00 stop 11:30
    start 13:00 stop 17:00
device(hr)-> set scheduler restrictionTh recurrent thursday start 8:00 stop 11:30
    start 13:00 stop 17:00
device(hr)-> set scheduler restrictionF recurrent friday start 8:00 stop 11:30 start
    13:00 stop 17:00
device(hr)-> save
```

ポリシースケジュールをポリシーにバインド

スケジューラは、ポリシーの作成時にポリシーに添付することができ、または後に WebUI でバインドすることができます。

この例では、Trust から Untrust まで新しいポリシーを作成し、ソースと宛先それぞれのアドレス帳入力を設定します。

WebUI

Vsys > Configure > Enter

Policies: ゾーンを選択し、**New** をクリックします。ポリシーを構成してから、**Advanced** をクリックします。ページの一番下で、ドロップダウンリストから Schedule を選択してから **OK** をクリックします。

CLI

```
device(hr)-> set policy id 1 from trust to untrust company any http deny schedule
    restrictionM
device(hr)-> set policy id 1 from trust to untrust company any http deny schedule
    restrictionTu
device(hr)-> set policy id 1 from trust to untrust company any http deny schedule
    restrictionW
device(hr)-> set policy id 1 from trust to untrust company any http deny schedule
    restrictionTh
device(hr)-> set policy id 1 from trust to untrust company any http deny schedule
    restrictionF
device(hr)-> save
```

ポリシースケジュールの表示

WebUI または CLI で 構成済みのスケジュールを表示できます。

WebUI

Vsys > Configure > Enter

Objects > Schedules

CLI

```
device(hr)-> get scheduler
```

ポリシースケジュールの削除

次の例では、ログインしている vsys 管理者として、**restrictionW** という名前のスケジュールを削除します。

WebUI

Vsys > Configure > Enter

Objects > Schedules: Click **Remove**.

CLI

```
device(hr)-> unset scheduler restrictionW
```

第 2 章

VLAN ベースのトラフィック分類

この章は仮想システムの VLAN ベーストラフィック分類を説明します。本章のセクションは、以下のようになります。

- 31 ページの「概要」
  - 32 ページの「VLAN」
  - 33 ページの「VLANs with Vsys」
- 34 ページの「レイヤー 2 仮想システムの構成」
- 51 ページの「サブインターフェースと VLAN タグの定義」
- 54 ページの「仮想システム間の通信」
- 57 ページの「VLAN の再タグ付け」

概要

VLAN ベースのトラフィック分類の場合、セキュリティデバイスは VLAN タグを参照して、各システムに向かうサブインターフェースにトラフィックを振り分けます。

デフォルトでは、vsys は、共有 Untrust ゾーンとその vsys 用の Trust ゾーンの 2 つのセキュリティゾーンを有します。各 vsys は Untrust ゾーンインターフェースを、ルートシステムと他の仮想システムと共有できます。vsys には、Untrust ゾーンに向かう、自分自身のサブインターフェースや (ルートシステムからインポートした) 専用物理インターフェースがあります。

注 : ScreenOS は、IEEE 802.1Q VLAN 規格に準拠する VLAN に対応しています。

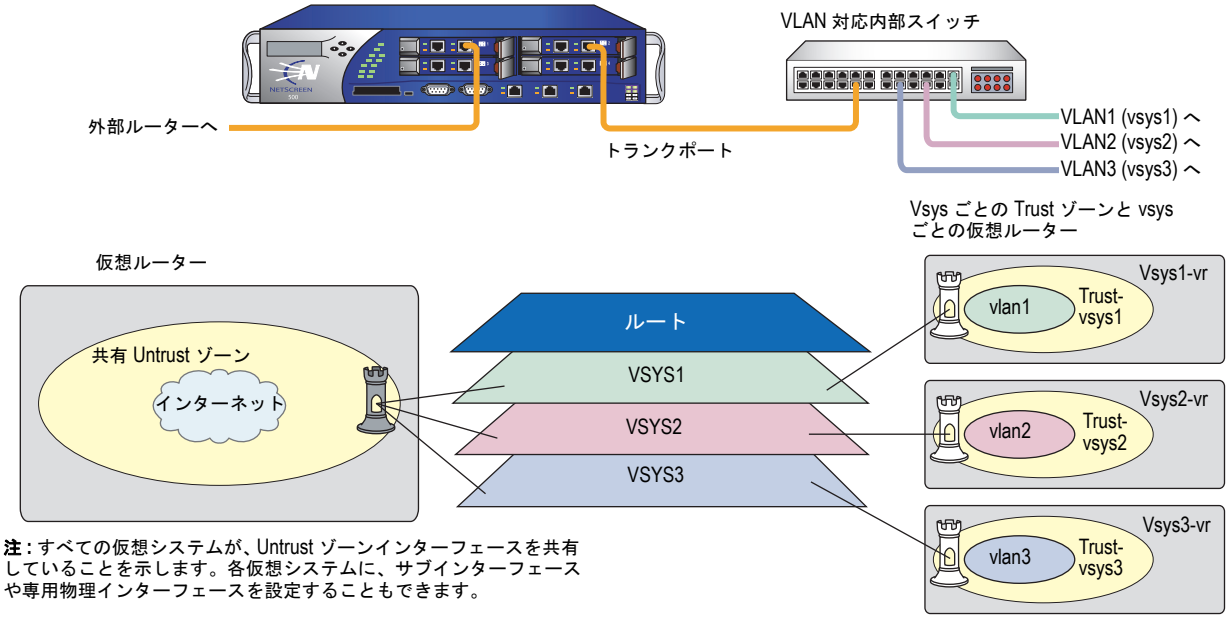
ルートシステムから仮想システムにインポートすることにより、物理インターフェースを仮想システムに専用化することができます (69 ページの「物理インターフェースのインポートとエクスポート」を参照。) 物理インターフェースを使用する場合、これを通過するトラフィックに VLAN タグは不要です。

VLAN

図 3 は VLAN のトラフィック分類を示します。各 VLAN はサブインターフェース経由でシステムにバインドされます。VLAN タグをサブインターフェースに割り当てるには、**set interface** *interface.subid* **tag** *vlanid* **zone** *zone_name* CLI コマンドを使用します。

Vsys がルートシステムと Untrust ゾーンインターフェースを共有し、そのサブインターフェースが Trust-*vsys_name* ゾーンにバインドされている場合、vsys は Trust-*vsys_name* ゾーンの VLAN と関連付けなければなりません。Vsys に Untrust ゾーンにバインドされた固有のサブインターフェースもあるならば、Untrust ゾーンにある他の VLAN とも関連付けなければなりません。

図 3: VLAN トラフィック分類



物理インターフェースから生じるサブインターフェースは、トランクポートとして動作します。トランクポートは、レイヤー 2 ネットワークデバイスが、1 つの物理ポートを経由する、複数の VLAN からのトラフィックをバンドルできます。各パケットは、フレームヘッダー中の VLAN 識別子 (VID) を手掛かりに振り分けます。VLAN トランク処理により、1 つの物理インターフェースで、複数の論理サブインターフェースをサポートできるようになります。各々のサブインターフェースは 固有の VLAN タグによって識別されなければなりません。受信 ethernet フレーム上の VLAN 識別子 (タグ) により、使用するサブインターフェース (および結果的使用するシステム) を判別します。VLAN をインターフェースまたはサブインターフェースと関連付けると、セキュリティデバイスは自動的に、物理ポートをトランクポートとして定義します。VLAN を透過モードのルートレベルで使用する場合は、CLI コマンド **set interface vlan1 vlan trunk** により、物理ポートをすべて、トランクポートとして明示的に定義しなければなりません。

VLANs with Vsys

Vsys が Trust-*vsys_name* ゾーンに関連付けられる (専用物理インターフェースではない) サブインターフェースを使用する場合、Trust-*vsys_name* ゾーンの内部スイッチや内部ルーターは、VLAN に対応したものでなければなりません。物理インターフェース上に複数のサブインターフェースを設定する場合、接続スイッチポートをトランクポートとして定義し、使用するすべての VLAN のメンバーにする必要があります。

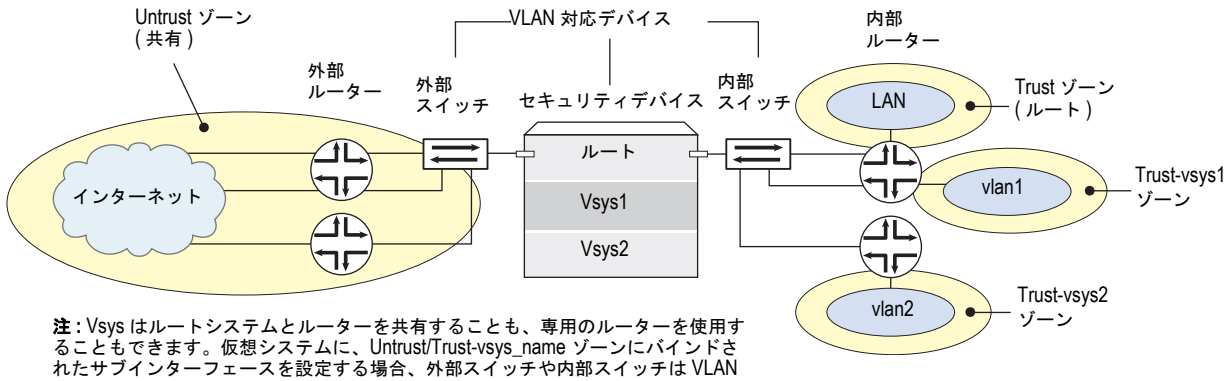
Vsys が、共有 Untrust ゾーンに関連付けられるサブインターフェース (共有インターフェースでも専用物理インターフェースでもない) を使用する場合、インバウンド / アウトバウンドトラフィックを受け取る外部スイッチや外部ルーターは、VLAN 機能を有しなければなりません。ルーターはセキュリティデバイスに到達する時、受信されたフレームが正しいサブインターフェースに転送されるためにそのフレームをタグ付けします。

Vsys は透過モードではそんざいすることができません。これは、特有のインターフェースあるいはサブインターフェース IP アドレスを求めるので、ルートシステムは透過モードとなります。透過モードのルートシステムが VLAN に対応するためには、**set interface vlan1 vlan trunk** という CLI コマンドを実行して、Layer 2 セキュリティゾーンにバインドされた物理インターフェースが、トランクポートとして動作するよう設定する必要があります。図 4 は VLAN が vsys を使用している例です。

Vsys のために VLAN を作成するために、ルートレベル管理者が行う必要のあるタスクには 3 段階あります。

1. Vsys を入力する。
2. サブインターフェースを定義する。
3. Vsys を VLAN と関連付けする。

図 4: Vsys の VLAN の例



注 : Vsys はルートシステムとルーターを共有することも、専用のルーターを使用することもできます。仮想システムに、Untrust/Trust-vsys_name ゾーンにバインドされたサブインターフェースを設定する場合、外部スイッチや内部スイッチは VLAN に対応したものを使用する必要があります。

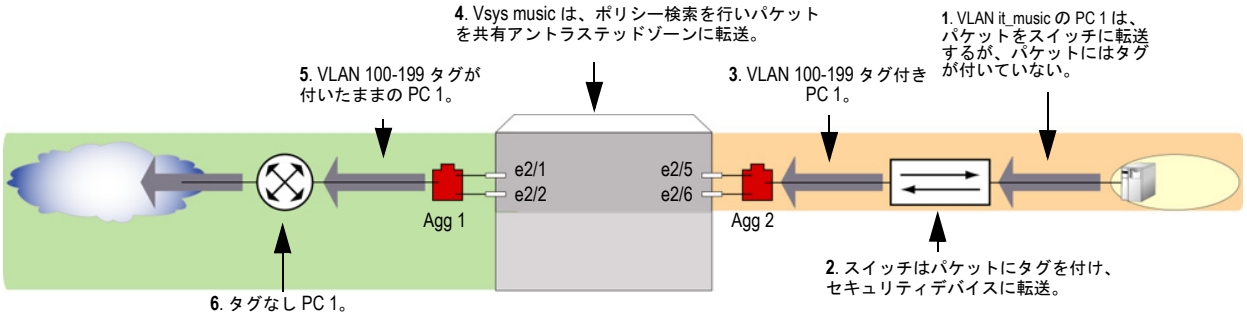
注 : ルートシステムが透過モードの場合、仮想システムには対応できません。しかし透過モードにしている間、ルートレベル VLAN には対応できます。

レイヤー 2 仮想システムの構成

透過モードの仮想システムを構成すると、セキュリティデバイスはレイヤー 2 スイッチまたはブリッジのように機能します。セキュリティデバイスを通過するパケットは、パケットヘッダーの仮想ローカルエリアネットワーク（VLAN）タグによって識別され、固有の仮想システム（vsys）に収束されます。収束されたパケットをポリシー検索し、変更を加えることなくセキュリティデバイスを経由して転送します。

セキュリティデバイス上で、セキュリティシステムを論理的に複数の仮想システムに分割して、マルチテナントサービスを提供することができます。各 vsys は、デバイス内の固有なセキュリティドメインです。各 vsys は、「仮想システム管理者」または略して「vsys 管理者」と呼ばれる専用の管理者を立てることができます。管理者は、アドレス帳、ユーザーリスト、カスタムサービス、ポリシーなどの独自のオブジェクトを設定することによりセキュリティドメインを個別化することができます。管理者はこれらのオブジェクトを使って、vsys 内のトラフィックや vsys と他のセキュリティドメインの間のトラフィックについてポリシーを定義します。

次の図に、セキュリティデバイスが vsys が設定したポリシーを使い、trusted VLAN にデータを転送する方法を示します。この図で、番号はデータ転送順序を表します。



透過モードの仮想システムは、VLAN タグによって分類されます。システム上で、ある範囲内の VLAN タグが VLAN グループオブジェクトに割り当てられ、次に VLAN グループオブジェクトは vsys に割り当てられているポートに適用されるセキュリティゾーンに割り当てられます。セキュリティシステムに入ったトラフィックは、VLAN タグによって該当 vsys に分類されます。Vsys に入ったトラフィックは、構成済みのセキュリティゾーンとポリシーを使って実施されます。セキュリティデバイスは、透過モードで仮想システムを最大 500 個までサポートできます。VLAN および vsys についての詳細については、1 ページの「仮想システム」を参照してください。

ScreenOS は、ゾーン vlan に管理インターフェースがバインドされる場合の vsys を管理する管理インターフェースも提供します。Vsys の作成時、セキュリティデバイスは自動的に管理ゾーン vlan を作成します。Vsys ごとに、管理ゾーンに複数のインターフェースをバインドすることができます。VLAN 管理インターフェースは vsys 内で作成されるため、vsys 管理者は固有の IP アドレスと VLAN ID で仮想システムを管理できます。この管理インターフェースによって、仮想システムのリモートおよびローカル管理が可能になります。

Vsys を作成しそれにリソースを割り当てることができるのは、ルート管理者だけです。CLI または WebUI で vsys 構成を作成および維持できるのは、ルート管理者と vsys 管理者です。

セキュリティデバイスは、vsys 内で VLAN タグ機能により分類される VLAN を最大 4,094 個までサポートします。Vsys ごとに 2 ～ 4,094 の範囲の VLAN を割り当てることができますが、割り当てられた VLAN を他の vsys で使用することはできません。ルートシステムは vlan1 とて識別されます。単一の 8G2 セキュアポートモジュール（SPM）の場合、最大 2 つの 4 ポート統合インターフェース（4 つの trusted と 4 つの untrusted）を構成できます。VLAN を統合インテーフェースに割り当てることによって、ASIC（Application-Specific Integrated Circuit）ごとに片方向 2Gps、双方向で 最大 4Gps のトラフィック帯域幅が提供されます。

8G SPM は 2 つの ASIC で構成されます。1 つの ASIC を ethernet2/1 ～ ethernet2/4 の範囲のポートが使用し、もう 1 つの ASIC を ethernet2/5 ～ ethernet2/8 のポートが使用します。統合インターフェースは、ethernet2/1 ポートから始まるペアで構成する必要があります。次の表に統合ポートの割り当てを示します。

表 4: 8G SPM

aggregate 1	ethernet2/1 と ethernet2/2
aggregate 2	ethernet2/3 と ethernet2/4
aggregate 3	ethernet2/5 と ethernet2/6
aggregate 4	ethernet2/7 と ethernet2/8

8G2 SPM と 5000M2 管理モジュールを使用している場合、次の表に示す構成を使用する必要があります。

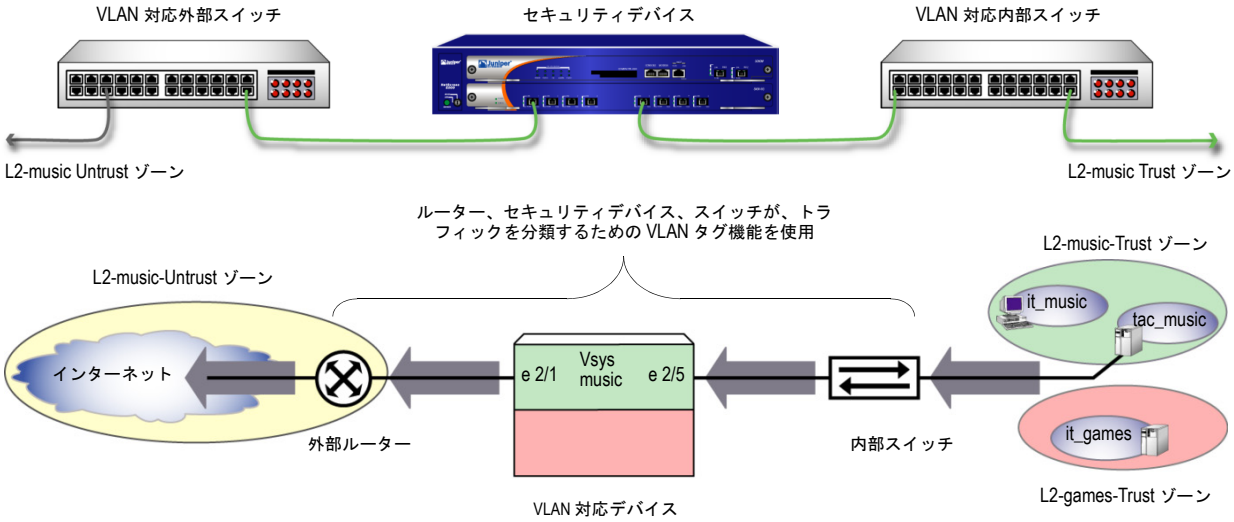
表 5: 8G2 SPM

aggregate1	ethernet2/1 と ethernet2/2 ethernet2/3 と ethernet2/4
aggregate 2	ethernet2/3 と ethernet2/4 ethernet2/7 と ethernet2/8

例 1: 1 ポートを構成

この例では、透過モードの vsys music をサポートするセキュリティデバイスを構成します。この vsys は、ルートシステムと L2-music-Untrust ゾーンを共有します。次の図に、セキュリティデバイスが Trust ゾーンと Untrust ゾーンを保護する構成を示します。VLAN にタグを付ける前に、vsys に VLAN をインポートする必要があります。

図 5: 単一ポート



1 つの透過モード仮想システム（vsys）を構成するには、次の手順に従います。

1. Vsys 名 music で vsys を作成し、vsys 管理者名とパスワードを設定します。
2. トラフィックを分類するために必要な VLAN タグをルートシステムからインポート（割り当て）します。
3. 各ポートでサポートされるために必要な VLAN タグを持つ VLAN グループを作成します。
4. Trust ポート用と Untrust ポート用に 2 つのレイヤー 2 ゾーンを作成します。
5. VLAN グループをポートにバインドします。

注： 仮想システム、VLAN タグ、レイヤー 2 ゾーンを作成できるのはルート管理者だけですが、管理インターフェースとポリシーの設定はルート管理者でも vsys 管理者でもできます。ルート管理者は、セキュリティデバイスの任意の vsys にアクセスできます。Vsys 管理者は、管理者が vsys に割り当てられている、ポリシーが作成された vsys にだけアクセスできます。

---

6. Vsys music のポリシーの構成この例で構成するポリシーは次のように機能します。
   a. L2-music-Untrust ゾーン から L2-music-Trust ゾーンの HTTP トラフィックを許可
   b. L2-music-Untrust ゾーン から L2-music-Trust ゾーンのその他すべてのトラフィックを拒否
   c. L2-music-Trust ゾーン から L2-music-Untrust ゾーンの すべてのトラフィックを許可

7. 管理インターフェースを作成します。VLAN 管理インターフェースは vsys 内で作成されるため、vsys 管理者は固有の IP アドレスと VLAND ID を使って vsys を管理することができます。

注 : セキュリティデバイス付き ScreenOS 5.0-L2 V は、最大 500 個の仮想システムをサポートすることができます。

WebUI

1. Vsys music を作成

Vsys > Configure > New: 次のように入力してから **OK** をクリックします。

Vsys Name: music
Vsys Admin Name: vsys_music
Vsys Admin New Password: xyz
Confirm New Password: xyz

2. VLAN をインポート

Vsys > Configure > **Enter** をクリックします (vsys_music)

Network > Vlan > Import: 次のように入力してから **Assign** をクリックします。

Import Vlan ID:
Start: 100
End: 199

3. ポートをバインド

Network > Vlan > Group > Edit (it_music) > Port: 次のように入力してから **Add** をクリックします。

port: (選択) ethernet2/5
zone: (選択) L2-music-Trust
port: (選択) ethernet2/1
zone: (選択) L2-music-Untrust

4. ポリシー

Policies (From: L2-music-Untrust, To: L2-music-Trust）> New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択) Any
Destination Address:
Address Book Entry: (選択) Any
Service: (選択) HTTP
Action: (選択）Permit

Policies (From: L2-music-Untrust, To: L2-music-Trust）> New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択) Any
Destination Address:
Address Book Entry: (選択) Any
Service: (選択) ANY
Action: (選択) Deny

Policies (From:L2-music-Trust, To:L2-music-Untrust）> New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択) Any
Destination Address:
Address Book Entry: (選択) Any
Service: (選択) ANY
Action: (選択) Permit

5. 管理インターフェースを作成

Network > Interfaces > （ドロップダウンリストで **VLAN** を選択） > New: 次のように入力してから **OK** をクリックします。

Interface Name Vlan: 199
IP Address/Netmask: 1.0.1.199/24
Management: (選択解除)
WebUI: (選択)
Telnet: (選択)
Ping: (選択)

CLI

1. Vsys music を作成

```
device-> set vsys music
device(music)-> set admin name vsys_music
device(music)-> set admin password xyz
device(music)-> save
```

2. VLAN タグをインポート

```
device(music)-> set vlan import 100 199
```

3. VLAN グループを作成

```
device(music)-> set vlan group name it_music
device(music)-> set vlan group it_music 100 199
```

4. レイヤー 2 ゾーンを作成

```
device(music)-> set zone name L2-music-Trust L2
device(music)-> set zone name L2-music-Untrust L2
```

5. ポートをバインド

```
device(music)-> set vlan port ethernet2/5 group it_music zone L2-music-Trust
device(music)-> set vlan port ethernet2/1 group it_music zone L2-music-Untrust
```

6. ポリシーを構成

```
device(music)-> set policy from L2-music-Untrust to L2-music-Trust any any http
permit
device(music)-> set policy from L2-music-Untrust to L2-music-Trust any any any
deny
device(music)-> set policy from L2-music-Trust to L2-music-Untrust any any any
permit
```

7. 管理インターフェースを作成

```
device(music)-> set interface vlan199 zone vlan
device(music)-> set interface vlan199 ip 1.0.1.199/24
device(music)-> unset interface vlan199 manage
device(music)-> set interface vlan199 manage web
device(music)-> set interface vlan199 manage telnet
```

```
device(music)-> set interface vlan199 manage ping
device(music)-> save
device(music)-> exit
```

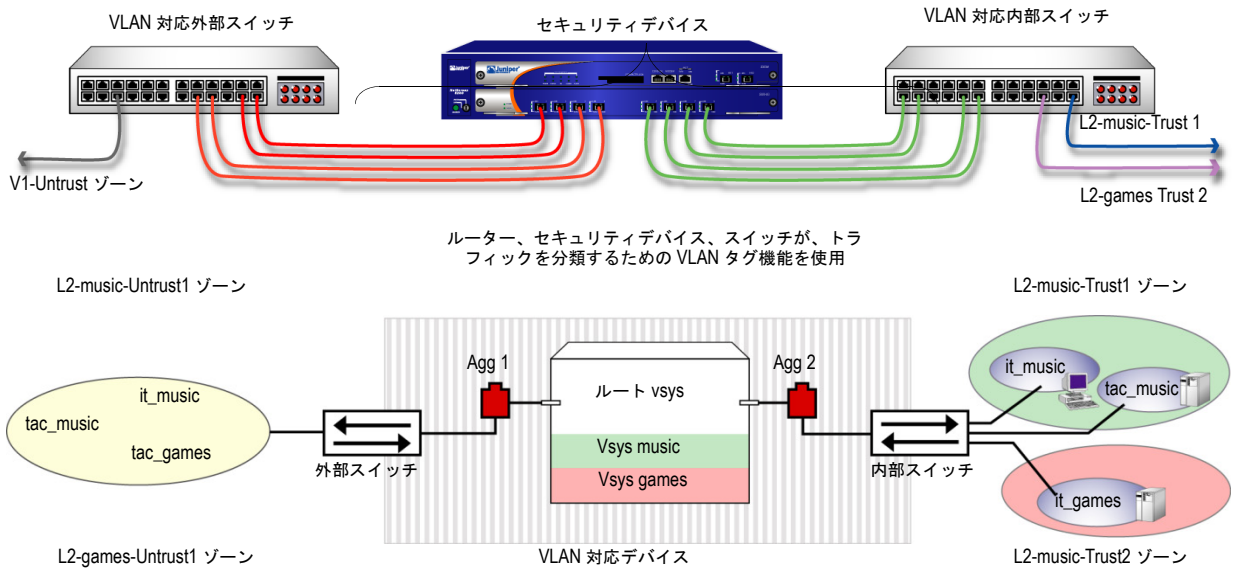
（オプション）VLAN グループを取得

```
device-> get vlan group it_music
```

例 2: それぞれが個別の Untrust ゾーンを持つ 2 つの 4 ポート統合の構成

この例では、2 つの透過モード仮想システム（vsys music と vsys games）をサポートするセキュリティデバイスを構成します。2 つの仮想システムはそれぞれ個別のセキュリティゾーンを持ちます。Vsys music は、it_music と tac_music の VLAN から成ります。Vsys games には、it_games VLAN だけがあります。図 6 に、セキュリティデバイスが Trust ゾーンと Untrust ゾーンを保護する構成を示します。VLAN にタグを付ける前に、vsys に VLAN をインポートする必要があります。

図 6: それぞれが個別の Untrust ゾーンを持つ 2 つの 4 ポート統合の構成



2 つの 4 ポート統合で 2 つの透過モード仮想システムを構成するには、次の手順に従います。

1. ルート管理レベルで統合ポートを設定します。
2. 統合ポートにインターフェースをバインドします。
3. *music* という vsys 名の vsys を作成し、vsys 管理者名とパスワードを設定します。
4. Vsys music トラフィックを分類するために必要な VLAN タグをルートシステムからインポート（割り当て）します。
5. VLAN グループを作成し、vsys music でサポートされる各ポート用の vsys タグを設定します。

6. Vsys music の Trust インターフェース、Untrust インターフェースのレイヤー 2 ゾーンを 1 つ作成します。

7. Vsys music の VLAN グループに統合ポートをバインドします。

注： 仮想システム、VLAN タグ、およびレイヤー 2 ゾーンを作成、または統合ポートをバインドできるのはルート管理者だけですが、ポリシーと管理モジュールの設定はルート管理者でも vsys 管理者でもできます。ルート管理者は、セキュリティデバイスの任意の vsys にアクセスできます。Vsys 管理者は、管理者が vsys に割り当てられている、ポリシーが作成された vsys にだけアクセスできます。

---

8. Vsys music の L2-music-Trust ゾーンの IP アドレスを設定します。
9. Vsys music のポリシーを構成します。この例で構成するポリシーは次のように機能します。
   a. L2-music-Untrust ゾーンから 10.0.1.200 の HTTP トラフィックを許可
   b. L2-music-Untrust ゾーン から L2-music-Trust ゾーンのその他すべてのトラフィックを拒否
   c. L2-music-Trust ゾーン から L2-music-Untrust ゾーンのすべてのトラフィックを許可
10. 管理インターフェースを作成します。VLAN 管理インターフェースは vsys 内で作成されるため、vsys 管理者は固有の IP アドレスと VLAND ID を使って vsys を管理することができます。
11. games という vsys 名の vsys を作成し、vsys 管理者名とパスワードを設定します。
12. Vsys games のトラフィックを分類するために必要な VLAN タグをルートシステムからインポート（割り当て）します。
13. に VLAN グループを作成し、vsys games でサポートされる各ポート用の vsys タグを設定します。
14. Vsys games の Trust インターフェースと Untrust インターフェースのレイヤー 2 ゾーンを 1 つ作成します。
15. Vsys games の VLAN グループに統合ポートをバインドします。
16. Vsys games のポリシーを構成します。この例で構成するポリシーは次のように機能します。
   a. L2-games-Untrust ゾーン から L2-games-Trust ゾーンの ftp トラフィックを許可
   b. L2-games-Untrust ゾーン から L2-games-Trust ゾーンのその他すべてのトラフィックを拒否
   c. L2-games-Trust ゾーン から L2-games-Untrust ゾーンのすべてのトラフィックを許可
17. 管理インターフェースを作成します。

注 : ScreenOS は、最大 500 個の仮想システムをサポートします。

注 : この例では、WebUI の各セクションは、デバイスの設定に必要なページに到るナビゲーションパスのみを一覧表示します。特定のパラメータや値を表示するには、WebUI のいずれかのセクションを設定し、その後の CLI セクションを参照してください。

WebUI

1. **ルートに統合ポートを設定**
   Network > Interfaces > （右側のドロップダウンリストで **Aggregate IF** を選択） > New
2. **統合ポートにインターフェースをバインド**
   Network > Interfaces > Edit (ethernet2/1)

   Network > Interfaces > Edit (ethernet2/2)

   Network > Interfaces > Edit (ethernet2/3)

   Network > Interfaces > Edit (ethernet2/4)

   Network > Interfaces > Edit (ethernet2/5)

   Network > Interfaces > Edit (ethernet2/6)

   Network > Interfaces > Edit (ethernet2/7)

   Network > Interfaces > Edit (ethernet2/8)
3. **Vsys music を作成**
   Vsys > Configure > New
4. **VLAN をインポート**
   Vsys > Configure > **Enter** をクリックします（vsys_music）

   Network > Vlan > Import
5. **グループを作成**
   Network > Vlan > Group > New
6. **レイヤー 2 ゾーンの作成**
   Network > Zones > New
7. **統合ポートをバインド**
   Network > Vlan > Group > Edit （it_music） > Port

   Network > Vlan > Group > Edit （tac_music） > Port

8. **IP アドレスを設定**
   Policy > Policy Elements > Addresses > List > V1-Untrust（ドロップダウンメニューで選択） > New

   Policy > Policy Elements > Addresses > List > From: L2-music-Untrust To: L2-music-Trust > New

   Policy > Policy Elements > Addresses > List > From: L2-music-Untrust To: L2-music-Trust > New

   Policy > Policy Elements > Addresses > List > From: L2-music-Untrust To: L2-music-Trust > New

   Policy > Policy Elements > Addresses > List > From: L2-music-Trust To: L2-music-Untrust > New

9. **ポリシー**
   Policies (From: L2-music-Untrust, To: L2-music-Trust） > New

   Policies (From: L2-music-Untrust, To: L2-music-Trust） > New

   Policies (From: L2-music-Untrust, To: L2-music-Trust） > New

   Policies (From: L2-music-Trust, To: L2-music-Untrust） > New

10. **管理インターフェースを作成**
    Network > Interfaces >（右側のドロップダウンメニューで **VLAN** を選択） > New

11. **Vsys games を作成**
    Vsys > Configure > New

12. **VLAN をインポート**
    Vsys > Configure > **Enter** をクリックします（vsys_games）

    Network > Vlan > Import

13. **グループを作成**
    Network > Vlan > Group > New

14. **レイヤー 2 ゾーンの作成**
    Network > Zones > New

15. **統合ポートをバインド**
    Network > Vlan > Group > Edit（games） > Port

16. **ポリシー**
    Policies (From: L2-games-Untrust, To: L2-games-Trust） > New

    Policies (From: L2-games-Untrust, To: L2-games-Trust） > New

    Policies (From: L2-games-Trust, To: L2-games-Untrust） > New

17. **管理インターフェースを作成**
    Network > Interfaces >（右側のドロップダウンメニューで **VLAN** を選択） > New

CLI

1. **ルートに統合ポートを設定**
   device-> set interface aggregate1 zone null
   device-> set interface aggregate2 zone null

2. **統合ポートにインターフェースをバインド**
   device-> set interface ethernet2/1 aggregate aggregate1
   device-> set interface ethernet2/2 aggregate aggregate1
   device-> set interface ethernet2/3 aggregate aggregate1
   device-> set interface ethernet2/4 aggregate aggregate1
   device-> set interface ethernet2/5 aggregate aggregate2
   device-> set interface ethernet2/6 aggregate aggregate2
   device-> set interface ethernet2/7 aggregate aggregate2
   device-> set interface ethernet2/8 aggregate aggregate2

3. **Vsys music を作成**
   device-> set vsys music
   device(music)-> set admin name vsys_music
   device(music)-> set admin password xyz
   device(music)-> save

4. **VLAN タグをインポート**
   device(music)-> set vlan import 100 199
   device(music)-> set vlan import 1033
   device(music)-> set vlan import 1133

5. **VLAN グループを作成**
   device(music)-> set vlan group name it_music
   device(music)-> set vlan group it_music 100 199
   device(music)-> set vlan group name tac_music
   device(music)-> set vlan group tac_music 1033
   device(music)-> set vlan group tac_music 1133

6. **レイヤー 2 ゾーンを作成**
   device(music)-> set zone name L2-music-Trust L2
   device(music)-> set zone name L2-music-Untrust L2

7. **統合ポートをバインド**
   device(music)-> set vlan port aggregate2 group it_music zone L2-music-Trust
   device(music)-> set vlan port aggregate1 group it_music zone L2-music-Untrust
   device(music)-> set vlan port aggregate2 group tac_music zone L2-music-Trust
   device(music)-> set vlan port aggregate1 group tac_music zone L2-music-Untrust

8. **IP アドレスを設定**
   device(music)-> set address L2-music-Trust 10.0.1.200 10.0.1.200 255.255.255.0

9. **ポリシーを構成**
   device(music)-> set policy from L2-music-Untrust to L2-music-Trust any 10.0.1.200 http permit
   device(music)-> set policy from L2-music-Untrust to L2-music-Trust any any http permit
   device(music)-> set policy from L2-music-Untrust to L2-music-Trust any any any deny
   device(music)-> set policy from L2-music-Trust to L2-music-Untrust any any any permit

10. 管理インターフェースを作成

```
device(music)-> set interface vlan1033 zone vlan
device(music)-> set interface vlan1033 ip 1.0.0.33/24
device(music)-> set interface vlan199 zone vlan
device(music)-> set interface vlan199 ip 1.0.1.199/24
device(music)-> unset interface vlan199 manage
device(music)-> set interface vlan199 manage ping
device(music)-> set interface vlan199 manage https
device(music)-> set interface vlan199 manage telnet
device(music)-> save
device(music)-> exit
```

（オプション）VLAN グループを取得

```
device-> get vlan group it_music
device-> get vlan group tac_music
```

11. Vsys games を作成

```
device-> set vsys games
device(games)-> set admin name vsys_games
device(games)-> set admin password abc
device(games)-> save
```

12. VLAN タグをインポート

```
device(games)-> set vlan import 200 250
```

13. VLAN グループを作成

```
device(games)-> set vlan group name games
device(games)-> set vlan group games 200 250
```

14. レイヤー 2 ゾーンを作成

```
device(games)-> set zone name L2-games-Trust L2
device(games)-> set zone name L2-games-Untrust L2
```

15. 統合ポートをバインド

```
device(games)-> set vlan port aggregate2 group games zone L2-games-trust
device(games)-> set vlan port aggregate1 group games zone L2-games-Untrust
```

16. ポリシーを構成

```
device(games)-> set policy from L2-games-Untrust to L2-games-Trust any any ftp
permit
device(games)-> set policy from L2-games-Untrust to L2-games-Trust any any any
deny
device(games)-> set policy from L2-games-Trust to L2-games-Untrust any any any
permit
```

17. 管理インターフェースを作成

```
device(games)-> set interface vlan300 zone vlan
device(games)-> set interface vlan300 ip 1.0.0.20/24
device(games)-> unset interface vlan300 manage
device(games)-> set interface vlan300 manage web
device(games)-> set interface vlan300 manage telnet
device(games)-> set interface vlan300 manage ping
device(games)-> save
device(games)-> exit
```

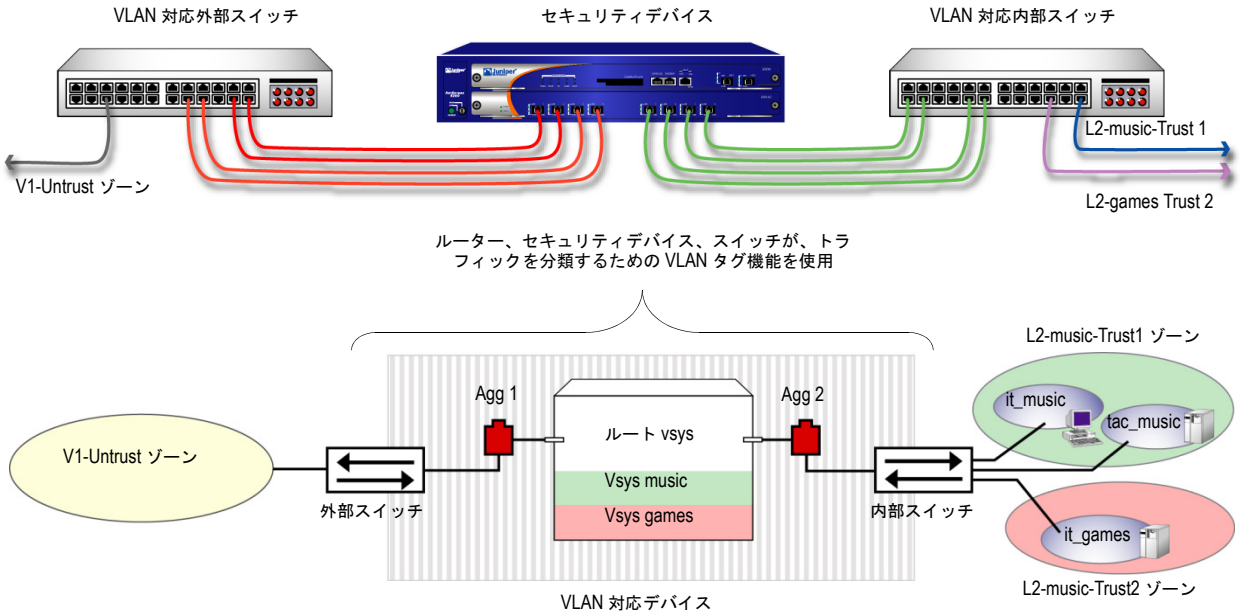
（オプション）VLAN グループを取得

```
device-> get vlan group games
```

例 3: 1 つの Untrusted ゾーンを共有する 2 つの 4 ポート統合の構成

この例では、2 つの透過モード仮想システム（vsys music と vsys games）をサポートするセキュリティデバイスを構成します。 2 つの仮想システムは、ルートシステムと Untrust ゾーンを共有します。Vsys music は、it_music と tac_music の VLAN から成ります。Vsys games には、it_games VLAN だけがあります。図 7 に、セキュリティデバイスが Trust ゾーンと Untrust ゾーンを保護する構成を示します。VLAN にタグを付ける前に、vsys に VLAN をインポートする必要があります。

図 7: 1 つの Untrusted ゾーンを共有する 2 つの 4 ポート統合



2 つの透過モード仮想システムを構成し、2 つの 統合ポートと共有 Untrust ゾーンを設定するには、次の手順に従います。

1. ルート管理レベルで統合ポートを設定します。
2. 統合ポートにインターフェースをバインドします。
3. Vsys 名 music で vsys を作成し、vsys 管理者名とパスワードを設定します。
4. Vsys music のトラフィックを分類するために必要な VLAN タグをルートシステムからインポート（割り当て）します。
5. VLAN グループを作成し、vsys music でサポートされる各ポート用の vsys タグを設定します。
6. Vsys music の Trust インターフェース用のレイヤー 2 ゾーンを作成します。
7. Vsys music の Trust ゾーンと Untrust ゾーンの VLAN グループに統合ポートをバインドします。

注： 仮想システム、VLAN タグ、およびレイヤー 2 ゾーンを作成、または統合ポートをバインドできるのはルート管理者だけですが、ポリシーと管理モジュールの設定はルート管理者でも vsys 管理者でもできます。ルート管理者は、セキュリティデバイスの任意の vsys にアクセスできます。Vsys 管理者は、管理者が vsys に割り当てられている、ポリシーが作成された vsys にだけアクセスできます。

8. Vsys music の各ゾーン用の IP アドレスを設定します。
9. Vsys music のポリシーの構成この例で構成するポリシーは次のように機能します。
   a. 10.0.1.200 から 10.0.1.100 のすべてのトラフィックを許可
   b. 10.0.1.201 から 10.0.1.101 のすべてのトラフィックを許可
   c. V1-Untrust ゾーンから L2-music-Trust ゾーンのすべてのトラフィックを拒否
10. 管理インターフェースを作成します。VLAN 管理インターフェースは vsys 内で作成されるため、vsys 管理者は固有の IP アドレスと VLAN ID を使って vsys を管理することができます。
11. Vsys 名 games で vsys を作成し、vsys 管理者名とパスワードを設定します。
12. Vsys games のトラフィックを分類するために必要な VLAN タグをルートシステムからインポートします。
13. に VLAN グループを作成し、vsys games でサポートされる各ポート用の vsys タグを設定します。
14. Vsys games の Trust インターフェース用のレイヤー 2 ゾーンを作成します。
15. Vsys games の VLAN グループに統合ポートをバインドします。
16. Vsys games の各ゾーン用の IP アドレスを設定します。
17. Vsys games のポリシーの構成この例で構成するポリシーは次のように機能します。
   a. 20.0.1.200 から 20.0.1.100 のすべてのトラフィックを許可
   b. 20.0.1.201 から 20.0.1.101 のすべてのトラフィックを許可
   c. V1-Untrust ゾーンから L2-games-Trust1 ゾーンのすべてのトラフィックを拒否
18. 管理インターフェースを作成します。

注： ScreenOS は、最大 500 個の仮想システムをサポートします。

注 : この例では、WebUI の各セクションは、デバイスの設定に必要なページに到るナビゲーションパスのみを一覧表示します。特定のパラメータや値を表示するには、WebUI のいずれかのセクションを設定し、その後の CLI セクションを参照してください。

WebUI

1. **ルートに統合ポートを設定**
   Network > Interfaces > （ドロップダウンメニューの **Aggregate IF** を 4 回選択）

2. **統合ポートにインターフェースをバインド**
   Network > Interfaces > Edit（ethernet2/1 から aggregate1）

   Network > Interfaces > Edit（ethernet2/2 から aggregate1）

   Network > Interfaces > Edit（ethernet2/3 から aggregate1）

   Network > Interfaces > Edit（ethernet2/4 から aggregate1）

   Network > Interfaces > Edit（ethernet2/5 から aggregate2）

   Network > Interfaces > Edit（ethernet2/6 から aggregate2）

   Network > Interfaces > Edit（ethernet2/7 から aggregate2）

   Network > Interfaces > Edit（ethernet2/8 から aggregate2）

3. **Vsys music を作成**
   Vsys > Configure > New

4. **VLAN をインポート**
   Vsys > Configure > **Enter** をクリックします（vsys_music）

   Network > Vlan > Import

5. **グループを作成**
   Network > Vlan > Group > New: 100-199

   Network > Vlan > Group > New: 1033-1033

   Network > Vlan > Group > New: 1133-1133

6. **レイヤー 2 ゾーンの作成**
   Network > Zones > New: L2-music-Trust1

   Network > Zones > New: L2-music-Trust2

7. **統合ポートをバインド**
   Network > Vlan > Group > Edit （music）> Port

8. IP アドレスを設定
Policy > Policy Elements > Addresses > List > **V1-Untrust**（ドロップダウンメニューで選択） > New

Policy > Policy Elements > Addresses > List > **L2-music-Trust1**（ドロップダウンメニューで選択）

Policy > Policy Elements > Addresses > List > **L2-music-Trust2**（ドロップダウンメニューで選択）

9. ポリシー
Policies (From: L2-music-Trust, To: V1-Untrust) > New

Policies (From: L2-music-Trust2, To: V1-Untrust) > New

Policies (From: V1-Untrust, To: L2-music-Trust2）> New

Policies (From: V1-Untrust, To: L2-music-Trust1）> New

10. 管理インターフェースを作成
Network > Interfaces >（右側のドロップダウンメニューで **VLAN** を選択） > New

Network > Interfaces >（右側のドロップダウンメニューで **VLAN** を選択） > New

11. Vsys games を作成
Vsys > Configure > New

12. VLAN をインポート
Vsys > Configure > **Enter** をクリックします（vsys_games）

Network > Vlan > Import

13. グループを作成
Network > Vlan > Group > New: 200-299

Network > Vlan > Group > New: 50-50

14. レイヤー 2 ゾーンの作成
Network > Zones > New: L2-games-Trust1

Network > Zones > New: L2-games-Trust2

15. 統合ポートをバインド
Network > Vlan > Group > Edit（games） > Port

16. IP アドレスを設定
Policy > Policy Elements > Addresses > List > **V1-Untrust**（右側のドロップダウンメニューで選択） > New

17. ポリシー
Policies (From: L2-games-Trust1、To: V1-Untrust) > New

18. 管理インターフェースを作成
Network > Interfaces >（ドロップダウンメニューで **VLAN** を選択） > New

CLI

1. **ルートに統合ポートを設定**
   device-> set interface aggregate1 zone null
   device-> set interface aggregate2 zone null

2. **統合ポートにインターフェースをバインド**
   device-> set interface ethernet2/1 aggregate aggregate1
   device-> set interface ethernet2/2 aggregate aggregate1
   device-> set interface ethernet2/3 aggregate aggregate1
   device-> set interface ethernet2/4 aggregate aggregate1
   device-> set interface ethernet2/5 aggregate aggregate2
   device-> set interface ethernet2/6 aggregate aggregate2
   device-> set interface ethernet2/7 aggregate aggregate2
   device-> set interface ethernet2/8 aggregate aggregate2

3. **Vsys music を作成**
   device-> set vsys music
   device(music)-> set admin name vsys_music
   device(music)-> set admin password xyz
   device(music)-> save

4. **VLAN タグをインポート**
   device(music)-> set vlan import 100 199
   device(music)-> set vlan import 1033

5. **VLAN グループを作成**
   device(music)-> set vlan group name music
   device(music)-> set vlan group music 100 199
   device(music)-> set vlan group music 1033

6. **レイヤー 2 ゾーンを作成**
   device(music)-> set zone name L2-music-Trust1 L2
   device(music)-> set zone name L2-music-Trust2 L2

7. **統合ポートをバインド**
   device(music)-> set vlan port aggregate2 group music zone L2-music-Trust1
   device(music)-> set vlan port aggregate2 group music zone L2-music-Trust2
   device(music)-> set vlan port aggregate1 group music zone V1-Untrust

8. **IP アドレスを設定**
   device(music)-> set address V1-Untrust 10.0.1.100 10.0.1.100 255.255.255.255
   device(music)-> set address V1-Untrust 10.0.1.101 10.0.1.101 255.255.255.255
   device(music)-> set address L2-music-Trust1 10.0.1.200 10.0.1.200 255.255.255.255
   device(music)-> set address L2-music-Trust2 10.0.1.201 10.0.1.201 255.255.255.255

9. **ポリシーを構成**
   device(music)-> set policy id 1 from L2-music-Trust1 to V1-Untrust 10.0.1.200 10.0.1.100 any permit
   device(music)-> set policy id 2 from L2-music-Trust2 to V1-Untrust 10.0.1.201 10.0.1.101 any permit
   device(music)-> set policy id 3 from V1-Untrust to L2-music-Trust2 any any any deny
   device(music)-> set policy id 4 from V1-Untrust to L2-music-Trust1 any any any deny

10. 管理インターフェースを作成

```
device(music)-> set interface vlan1033 zone vlan
device(music)-> set interface vlan1033 ip 1.0.0.33/24
device(music)-> set interface vlan199 zone vlan
device(music)-> set interface vlan199 ip 1.0.1.199/24
device(music)-> unset interface vlan199 manage
device(music)-> set interface vlan199 manage web
device(music)-> set interface vlan199 manage telnet
device(music)-> set interface vlan199 manage ping
device(music)-> save
device(music)-> exit
```

（オプション）VLAN グループを取得

```
device-> get vlan group music
```

11. Vsys games を作成

```
device-> set vsys games
device(games)-> set admin name vsys_games
device(games)-> set admin password abc
device(games)-> save
```

12. VLAN タグをインポート

```
device(games)-> set vlan import 200 299
device(games)-> set vlan import 50
```

13. VLAN グループを作成

```
device(games)-> set vlan group name games
device(games)-> set vlan group games 200 299
device(games)-> set vlan group games 50
```

14. レイヤー 2 ゾーンを作成

```
device(games)-> set zone name L2-games-Trust1 L2
device(games)-> set zone name L2-games-Trust2 L2
```

15. 統合ポートをバインド

```
device(games)-> set vlan port aggregate2 group games zone L2-games-Trust1
device(games)-> set vlan port aggregate2 group games zone L2-games-Trust2
device(games)-> set vlan port aggregate1 group games zone V1-Untrust
```

16. IP アドレスを設定

```
device(games)-> set address V1-Untrust 20.0.1.100 20.0.1.100
255.255.255.255
device(games)-> set address V1-Untrust 20.0.1.101 20.0.1.101
255.255.255.255
device(games)-> set address L2-games-Trust1 20.0.1.200 20.0.1.200
255.255.255.255
device(games)-> set address L2-games-Trust2 20.0.1.201 20.0.1.201
255.255.255.255
```

17. ポリシーを構成

```
device(games)-> set policy id 1 from L2-games-Trust1 to V1-Untrust 20.0.1.200
20.0.1.100 any permit
device(games)-> set policy id 2 from L2-games-Trust1 to V1-Untrust 20.0.1.201
20.0.1.101 any permit
device(games)-> set policy id 3 from V1-Untrust to L2-games-Trust1 any any any
deny
```

18. 管理インターフェースを作成

```
device(games)-> set interface vlan300 zone vlan
device(games)-> set interface vlan300 ip 1.0.0.20/24
device(games)-> unset interface vlan300 manage
device(games)-> set interface vlan300 manage web
device(games)-> set interface vlan300 manage telnet
device(games)-> set interface vlan300 manage ping
device(games)-> save
device(games)-> exit
```

（オプション）VLAN グループを取得

```
device-> get vlan group games
```

サブインターフェースと VLAN タグの定義

Trust-*vsys_name* ゾーンサブインターフェースには、vsys をその内部 VLAN にリンクする働きがあります。Untrust ゾーンサブインターフェースは、vsys をパブリック WAN (通常はインターネット) にリンクします。サブインターフェースには次のような属性があります。

- 固有の VLAN ID (1 ～ 4095)
- 公開 IP アドレスまたはプライベート IP アドレス (デフォルトによりプライベートです)
- サブネットクラス (A、B、C) に応じたネットマスク
- 関連付けられた VLAN

注 : 公開 IP アドレス、プライベート IP アドレスについて詳しくは、**2**-47 ページの「公開 IP アドレス」および **2**-48 ページの「非公開 IP アドレス」を参照してください。

Vsys には、1 つの Untrust ゾーンサブインターフェースのほか、複数の Trust-*vsys_name* ゾーンサブインターフェースを設定できます。仮想システムに独自の Untrust ゾーンサブインターフェースがない場合は、ルートレベル Untrust ゾーンインターフェースを共有します。セキュリティデバイスはサブインターフェース、ルートレベルの VLAN および IEEE 802.1Q 準拠の VLAN タグもサポートします。

図 8: VLAN サブインターフェース

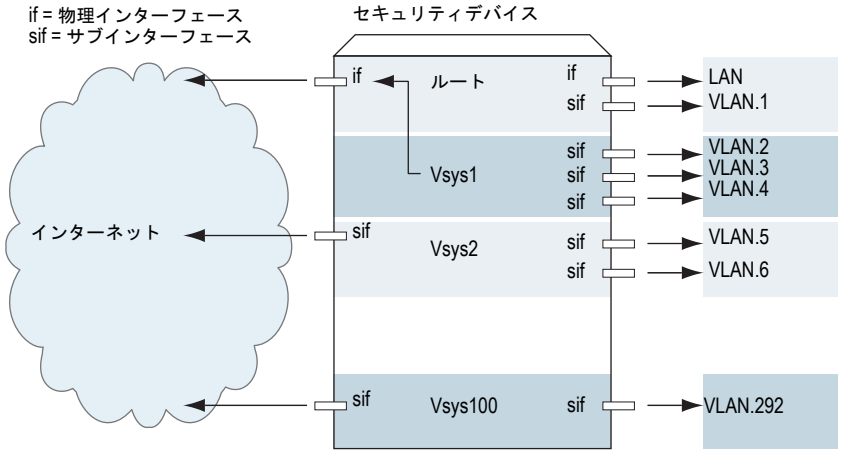
Vsys1 は Untrust ゾーン インターフェースをルートシステムと共有しています。Vsys2 と vsys100 には、自分自身の Untrust ゾーンにバインドされた、専用サブインターフェースがあります。

ルートシステムには、Trust ゾーンにバインドされた物理インターフェースとサブインターフェースがあります。

Vsys1 には、Trust-vsys1 ゾーンにバインドされた 3 つのサブインターフェースがあり、それぞれ異なる VLAN につながっています。

Vsys2 には、Trust-vsys2 ゾーンにバインドされた 2 つのサブインターフェースがあり、それぞれ異なる VLAN につながっています。

Vsys100 には、Trust-vsys100 ゾーンにバインドされた 1 つのサブインターフェースがあります。



注 : VLAN ID はすべて、物理インターフェースごとに固有でなければなりません。

VLAN タグとは、ethernet フレームヘッダーに追加されたビットで、どの VLAN に属しているか識別するためのものです。VLAN を vsys にバインドすることにより、フレームがどの vsys に属し、したがってどのポリシーが適用されるか、の判断にタグを使います。VLAN が vsys にバインドされていなければ、セキュリティデバイスのルートシステムで設定されたポリシーを適用することになります。

ルートレベル管理者には、VLAN の作成、メンバーを割り当てること、vsys にバインドすることが可能です (複数の方法 (プロトコルタイプ、MAC アドレス、ポート数) で VLAN にメンバーを割り当てることができますが、本書では扱っていません)。Vsys 管理者がいれば、アドレス、ユーザー、サービス、VPN、ポリシーを作成して、vsys を管理します。いない場合はルートレベル管理者がこのような作業を行います。

注 : ルートレベル管理者が VLAN を vsys と関連付けていない場合、VLAN はセキュリティデバイスのルートシステム内で動作します。

Vsys 以下のサブネットはすべて分離している必要があります。すなわち、同一 vsys のサブネット間で重複する IP アドレスが存在することは許可されません。例えば、次のように表示されます。Subinterface1 ー 10.2.2.1 255.255.255.0 と、Subinterface2 ー 10.2.3.1 255.255.255.0 は分離しており、適切なサブネットにリンクされています。

しかし、以下のサブインターフェース設定を持つサブネット間では、重複する IP アドレスが存在するため、同一 vsys 以下で設定が許可されません。subinterface1 ー 10.2.2.1 255.255.0.0、subinterface2 ー 10.2.3.1 255.255.0.0

異なる vsys 間では、サブネットのアドレス範囲を重複させることが可能です。

この例では、4 ページの「Vsys オブジェクトと管理者の作成」で作成した 3 つの仮想システム (vsys1、vsys2、vsys3) に、サブインターフェースと VLAN タグを定義します。1 番目と 2 番目のサブインターフェースは、NAT モードで動作するプライベート仮想システム用、3 番目のサブインターフェースは Route モードで動作するパブリック仮想システム用です。サブインターフェースはそれぞれ 10.1.1.1/24、10.2.2.1/24、1.3.3.1/24 です。どれも ethernet3/2 上に作成します。

どの仮想システムも、Untrust ゾーンおよびインターフェース (ethernet1/1; 1.1.1.1/24) をルートシステムと共有します。Untrust ゾーンは untrust-vr ルーティングドメインにあります。

WebUI

1. **Vsys1 のサブインターフェースと VLAN タグ**
   Vsys > Configure > (vsys1 の) **Enter** をクリックします。

   Network > Interfaces > New Sub-IF (ethernet3/2): 次のように入力してから **OK** をクリックします。

   Interface Name: ethernet3/2.1
   Zone Name: Trust-vsys1
   IP Address/Netmask: 10.1.1.1/24
   VLAN Tag: 1

注 : 仮想システムは、Route モードまたは NAT モードで動作するよう定義できます。デフォルトでは NAT モードになっているので、この例の場合、1 番目と 2 番目のサブインターフェースを作成する際に指定する必要はありません。

2. **Vsys2 のサブインターフェースと VLAN タグ**
   Vsys > Configure > (vsys2 の) **Enter** をクリックします。

   Network > Interfaces > New Sub-IF (ethernet3/2): 次のように入力してから **OK** をクリックします。

   Interface Name: ethernet3/2.2
   Zone Name: Trust-vsys2
   IP Address/Netmask: 10.2.2.1/24
   VLAN Tag: 2

3. **Vsys3 のサブインターフェースと VLAN タグ**
   Vsys > Configure > (vsys3 の) **Enter** をクリックします。

   Network > Interfaces > New Sub-IF (ethernet3/2): 以下を入力して **Apply** をクリックします。

   Interface Name: ethernet3/2.3
   Zone Name: Trust-vsys3
   IP Address/Netmask: 1.3.3.1/24
   VLAN Tag: 3

   Interface Mode: Route を選択し、**OK** をクリックします。

   Exit Vsys をクリックし、ルートレベルに戻ります。

CLI

1. **Vsys1 のサブインターフェースと VLAN タグ**
   device-> enter vsys vsys1
   device(vsys1)-> set interface ethernet3/2.1 zone trust-vsys1
   device(vsys1)-> set interface ethernet3/2.1 ip 10.1.1.1/24 tag 1
   device(vsys1)-> save
   device(vsys1)-> exit

注 : 仮想システムは、Route モードまたは NAT モードで動作するよう定義できます。デフォルトでは NAT モードになっているので、この例の場合、1 番目と 2 番目のサブインターフェースを作成する際に指定する必要はありません。

2. **Vsys2 のサブインターフェースと VLAN タグ**
   device-> enter vsys vsys2
   device(vsys2)-> set interface ethernet3/2.2 zone trust-vsys2
   device(vsys2)-> set interface ethernet3/2.2 ip 10.2.2.1/24 tag 2
   device(vsys2)-> save
   device(vsys2)-> exit

3. **Vsys3 のサブインターフェースと VLAN タグ**
   device-> enter vsys vsys3
   device(vsys3)-> set interface ethernet3/2.3 zone trust-vsys3
   device(vsys3)-> set interface ethernet3/2.3 ip 1.3.3.1/24 tag 3
   device(vsys3)-> set interface ethernet3/2.3 route
   device(vsys3)-> save
   device(vsys3)-> exit

仮想システム間の通信

Vsys の VLAN メンバーは、互いの通信アクセスには制限はありません。通常、異なる vsys に属する VLAN メンバーは互いに通信することはできませんが、2 つの vsys システムの管理者が互いに通信できるようポリシーを設定すれば、通信できるようになります。

ルートレベル VLAN 間のトラフィックは、ルートレベルのポリシーで設定されたパラメータが許す範囲で動作します。仮想システム VLAN 間のトラフィックは、参加している仮想システムのポリシーのパラメータ設定内で動作します。セキュリティデバイスは、送信側の仮想システムを通過することが可能で、さらに宛先側の仮想システムへ到達することが可能なトラフィックだけを通過します。換言すれば、両仮想システムの vsys 管理者は、トラフィックが入力と出力で適切な方向で通信可能なポリシーを設定しなければなりません。

注 : ルートシステムと仮想システムで設定したポリシーは、相互に影響を与えません。

図 9 で示したこの構成例では、vsys1 および vsys2 の管理者 (51 ページの「サブインターフェースと VLAN タグの定義」を参照) が、VLAN1 のワークステーション (work_js、IP アドレス 10.1.1.10/32) と、VLAN2 のサーバー (ftp_server、IP アドレス 10.2.2.20/32) との間でトラフィックが行き来できるよう、ポリシーを設定します。次の 2 つの作業を行えば、接続が可能になります。

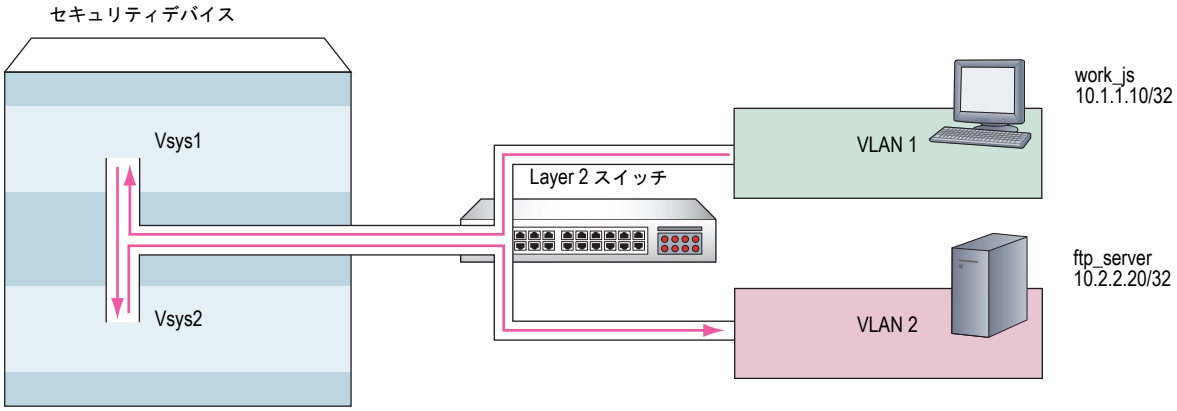
- Vsys1 の vsys 管理者が、Trust-vsys1 のワークステーションから Untrust ゾーン宛のトラフィックを許可するポリシーを設定。

- Vsys2 の vsys 管理者が、Untrust ゾーンにあるワークステーションから Trust-vsys2 のサーバー宛のトラフィックを許可するポリシーを設定。

セキュリティデバイスの内部インターフェースの前にあるネットワークデバイスは、レイヤー 2 スイッチです。これにより、VLAN1 から VLAN2 へスイッチを通過するトラフィックは、レイヤー 3 ルーティングのために強制的にスイッチからセキュリティデバイスへ転送されます。これに対しネットワークデバイスがレイヤー 3 ルーターの場合、VLAN1 と VLAN2 の間のトラフィックはルーター内部で通過可能なため、セキュリティデバイス上に設定されたすべてのポリシーがバイパスされてしまいます。

Vsys1 および vsys2 の管理者は、ルートも適切に設定しなければなりません。共有 Untrust ゾーンは untrust-vr にあり、Trust ゾーンは vsys1 と vsys2 にあります。

図 9: Vsys 間通信



WebUI

1. Vsys1

アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: work_js
IP Address/Domain Name:
IP/Netmask: (選択), 10.1.1.10/32
Zone: Trust-vsys1

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: ftp_server
IP Address/Domain Name:
IP/Netmask: (選択), 10.2.2.20/32
Zone: Untrust

ルート

Network > Routing > Routing Entries > untrust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.1.1.0/24
Next Hop Virtual Router Name: (選択); vsys1-vr

Network > Routing > Routing Entries > vsys1-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Next Hop Virtual Router Name: (選択); untrust-vr

ポリシー

Policies > (From: Trust-vsys1, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), work_js
Destination Address:
    Address Book Entry: (選択), ftp_server
Service: FTP-Get
Action: Permit

2. Vsys2

アドレス

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: ftp_server
IP Address/Domain Name:
    IP/Netmask: (選択), 10.2.2.2/32
Zone: Trust-vsys2

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: work_js
IP Address/Domain Name:
    IP/Netmask: (選択), 10.1.1.10/32
Zone: Untrust

ルート

Network > Routing > Routing Entries > untrust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.2.2.0/24
Next Hop Virtual Router Name: (選択); vsys2-vr

Network > Routing > Routing Entries > vsys2-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Next Hop Virtual Router Name: (選択); untrust-vr

ポリシー

Policies > (From: Untrust, To: Trust-vsys2) New: 次のように入力してから **OK** をクリックします。

Source Address:
    Address Book Entry: (選択), work_js
Destination Address:
    Address Book Entry: (選択), ftp_server
Service: FTP-Get
Action: Permit

CLI

1. Vsys1

アドレス

```
set address trust-vsys1 work_js 10.1.1.10/32
set address untrust ftp_server 10.2.2.20/32
```

ルート

```
set vrouter untrust-vr route 10.1.1.0/24 vrouter vsys1-vr
set vrouter vsys1-vr route 0.0.0.0/0 vrouter untrust-vr
```

ポリシー

```
set policy from trust-vsys1 to untrust work_js ftp_server ftp-get permit
保存
```

2. Vsys2

アドレス

```
set address trust-vsys2 ftp_server 10.2.2.20/32
set address untrust work_js 10.1.1.10/32
```

ルート

```
set vrouter untrust-vr route 10.2.2.0/24 vrouter vsys2-vr
set vrouter vsys2-vr route 0.0.0.0/0 vrouter untrust-vr
```

Vsys2 ポリシー

```
set policy from untrust to trust-vsys2 work_js ftp_server ftp-get permit
保存
```

Network > Zones > Edit (Internet): **IP Classification** チェックボックスを選択して **OK** をクリックします。

VLAN の再タグ付け

VLAN 再タグ付けでは、選択的に VLAN 間のトラフィックを遮蔽できます。これには、受信および出力トラフィックの直接のパスの外側にセキュリティデバイスを配置し（図 10 を参照）、遮蔽したい VLAN からのトラフィックだけをセキュリティデバイスに転送するようレイヤ 2 スイッチを構成します。一方、他の VLAN との間のトラフィックは直接スイッチを通過します。このように、VLAN トラフィックをすべてセキュリティデバイスを通すことにより発生する可能性があるスループットへの影響を回避しながら、ネットワークの脅威となる可能性があるトラフィックだけを遮蔽することができます。ただ 1 つ必要なのは、再タグ付けしたトラフィックが、異なる ID を持つ VLAN からでなければならないという点です。すなわち、VLAN 10 からの VLAN トラフィックを同じ ID を持つ別の VLAN に再タグ付けできません。

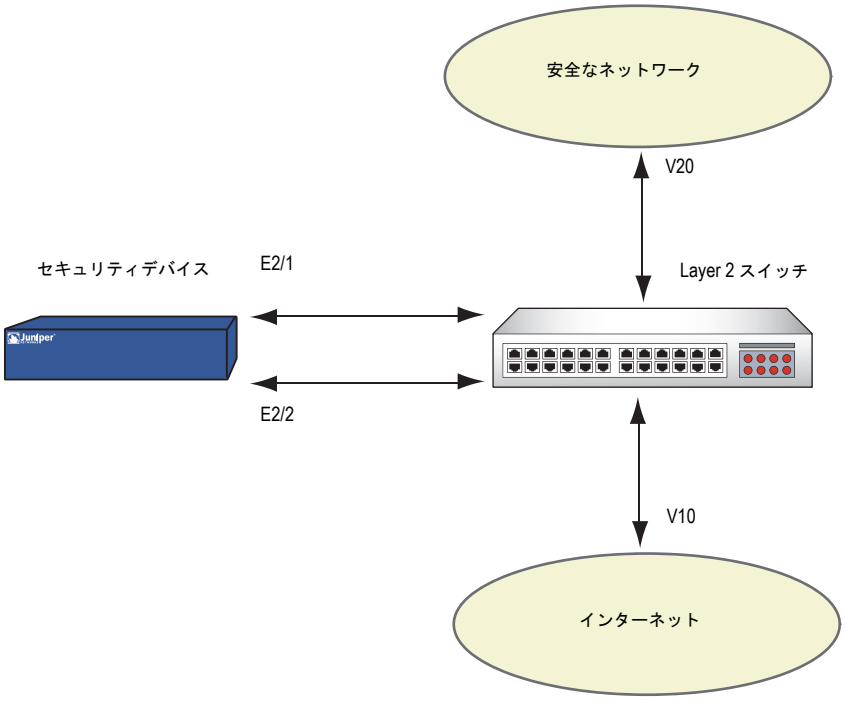
双方向の VLAN 再タグ付けオブジェクトの作成および、トラフィックを遮蔽したい 2 つの VLAN の指定により、セキュリティデバイスの VLAN 再タグ付けを構成します。（さらに、それをインターフェースにバインドし、ポリシーを作成しなければなりません。）たとえば、以下のコマンドは、VLAN 10 から VLAN 20、および VLAN 20 から 10 へのトラフィックに再タグ付けする secure_vlan と呼ばれる VLAN 再タグ付けオブジェクトを作成します。

```
set vlan retag name secure_vlan 10 20
```

セキュリティデバイスはハッシュテーブルにこの再タグ付けペアを格納し、これらの VLAN いずれかからのトラフィックを受信すると、それを参照します。さらに、セキュリティデバイスに接続するレイヤ 2 スイッチのポートに適切な VLAN タグを割り当てなければなりません。

図 10 は、このシナリオを示しています。

図 10: VLAN の再タグ付け操作



例：

この例では、v10 という名前の VLAN グループを作成し、受信インターフェースをゾーン V1-Untrust に割り当て、出力インターフェースをゾーン V1-Trust に割り当てます。次に、それらのゾーン間を往来するトラフィックをすべて許可するセキュリティポリシーを作成します。最後に、secure_vlan という名前の双方向 VLAN 再タグ付けオブジェクトを作成し、VLAN 10 と VLAN 20 との間のトラフィックを遮蔽し、かつそれを V1-Trust インターフェースにバインドします。

WebUI

この例は、ルートレベルでの VLAN 再タグ付け構成を示します。既存の vsys を構成するには、最初に vsys に入る必要があります。vsys に入るには、Vsys > Configure > Enter（vsys 名の）へ移動し、VLAN の再タグ付けを以下のように構成します。

Network > VLAN > Group > New: 次のように入力し **Add** をクリックします。

VLAN Group Name: v10
Start: 10
End: 10

Network > VLAN > Group > Edit (group v10) > Port: 以下を選択して、**Add** をクリックします。

Port: (ethernet2/1 を選択)
Zone: (V1-Trust を選択)

Network > VLAN > Group > Edit (group v10) > Port: 以下を選択して、**Add** をクリックします。

Port: (ethernet2/2 を選択)
Zone: (V1-Untrust を選択)

Network > VLAN > Retagging > New: 次のように入力してから **OK** をクリックします。

Name: secure_vlan
From Vlan: 10
To Vlan: 20

Network > VLAN > Retagging Bind > New: 次のように入力してから **OK** をクリックします。

Interface Name: (選択) ethernet2/1
Binding: (選択) secure_vlan

注 : WebUI は、**From Vlan** および **To Vlan** を示していますが、上の構成は、双方向の再タグ付けを行います。つまり、VLAN 10 からのトラフィックには ID 20 で再タグ付けされ、VLAN 20 からのトラフィックには ID 10 で再タグ付けされます。

CLI

この例は、ルートレベルからの VLAN 再タグ付け構成を示します。ルートレベルから既存の vsys に入るには、以下のコマンドを使用します。**enter vsys** *name_str*、次に VLAN 再タグ付けを以下のように構成します。

```
set vlan group name v10
set vlan group v10 10 10
set vlan port eth2/1 group v10 zone v1-trust
set vlan port eth2/2 group v10 zone v1-untrust

set policy from v1-trust to v1-untrust any any any permit
set vlan retag name secure_vlan 10 20
set vlan port eth2/1 retag secure_vlan
```

コマンドラインインターフェースで VLAN 再タグ付け情報を確認するには、**get vlan retag name [name | all]** コマンドを使用します。

注 : 既存の Vsys で VLAN を使用するには、VLAN グループを作成する前に、ルートの Vsys から VLAN ID をインポートしなければなりません。この例でこれを行うには、コマンド **set vlan import 10 10** を使用します。WebUI で vsys に入り、Network > Vlan > import に移動します。

第 3 章
トラフィックの振り分け

この章では ScreenOS がトラフィックを振り分ける方法を説明します。本章のセクションは、以下のようになります。

- 61 ページの「概要」
  - 61 ページの「トラフィックの振り分け」
  - 62 ページの「通過トラフィックの振り分け」
  - 67 ページの「専用および共有インターフェース」
- 69 ページの「物理インターフェースのインポートとエクスポート」
  - 69 ページの「物理インターフェースを仮想システムにインポートする」
  - 70 ページの「物理インターフェースを仮想システムからエクスポートする」

概要

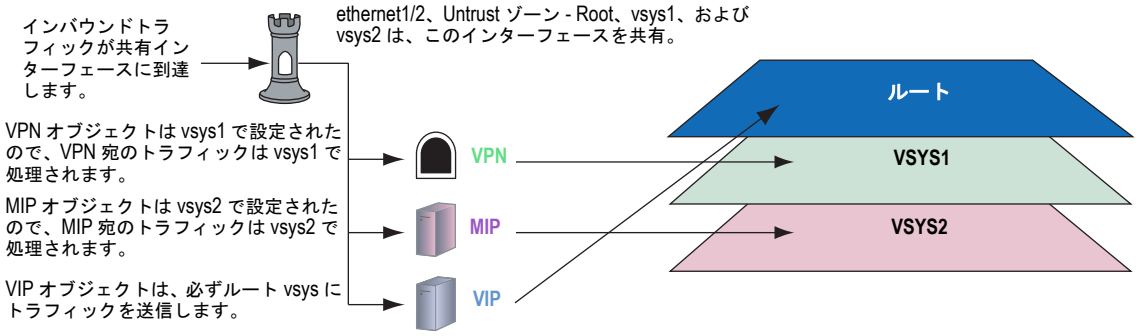
ScreenOS は適切な仮想システム (vsys) に送信するすべてのパケットを振り分けします。セキュリティデバイスが受け取るユーザートラフィックには以下の 2 種類があり、振り分け方法も 2 とおりあります。

- 当該システムに設定された IP アドレス宛のトラフィック。暗号化 VPN トラフィック、MIP や VIP を宛先とするトラフィックなど。
- 当該デバイス以外の IP アドレスに宛てたトラフィック。

トラフィックの振り分け

セキュリティデバイスに設定されたオブジェクト (VPN、MIP、VIP) 宛のトラフィックについては、各オブジェクトを設定した vsys とオブジェクトとの関連で、トラフィックが属している vsys を判断します。ただし、アントラステッドインターフェースで構成された VIP は、ルート vsys に常に割り当てられます。図 11 は、トラフィックの振り分け方を示しています。

図 11: VPN 、MIP および VIP 関連



インバウンドトラフィックは VPN トンネル経由で仮想システムに接続することが可能です。ただし、出力インターフェースが共有インターフェースの場合、同一のリモートサイトへの vsys とルートシステムに対して AutoKey IKE VPN トンネルを作成することはできません。

通過トラフィックの振り分け

トラフィックの宛先がセキュリティデバイス以外の IP アドレスである場合（通過トラフィック）の分類方法には、VLAN ベースと IP ベースの、2 つの方式があります。VLAN ベースのトラフィック分類とは、フレームヘッダー中の VLAN タグを使って、インバウンドトラフィックをどのシステムで処理するか判定する方式です。一方 IP ベースのトラフィック分類とは、IP パケットヘッダー中の宛先 IP アドレスによって分類する方式です。パケットが属するシステムを判断するためにセキュリティデバイスが使用する手順は、以下の 3 つのステップからなります。

注： VLAN タグの処理にはサブインターフェースが必要です。サブインターフェースは当該システム専用でなければなりません。すべてのシステムが共用する、共有インターフェースとは異なります。

---

1. **Ingress インターフェース / ソース IP トラフィック分類**
   セキュリティデバイスは、ingress が専用インターフェースか共有インターフェースかを確認します。

注： 共有インターフェース、専用インターフェースについては、67 ページの「専用および共有インターフェース」を参照してください。

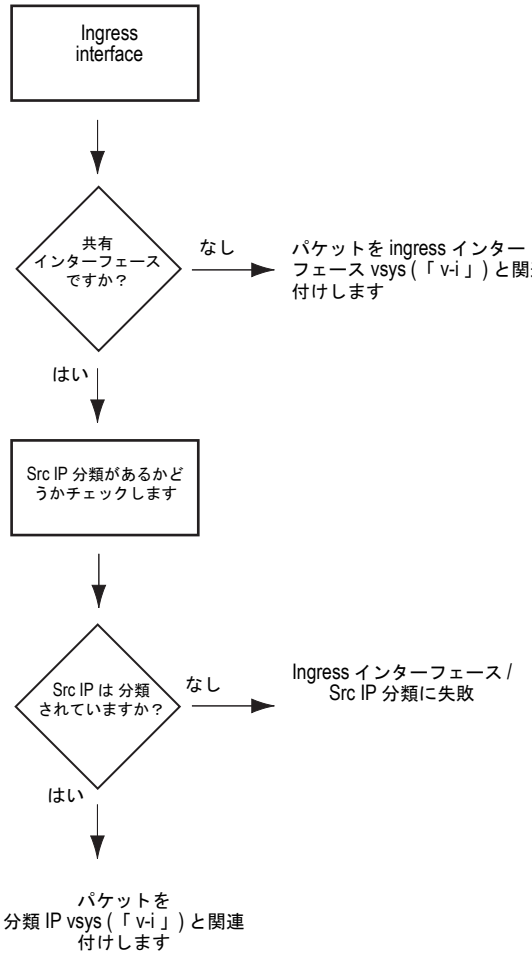
---

   a. Ingress インターフェースが vsys 専用であれば (例 :「 v-I 」)、このインターフェースを専有するシステムにトラフィックの処理を委ねます。

   b. 逆に共有インターフェースであれば、IP ベースの分類方式により、ソース IP アドレスが特定の vsys に関連付けられていないかどうか確認します。図 12 を参照。

      - どの vsys にも関連付けられていなければ、ingress IP 分類は失敗します。
      - 特定の vsys に関連付けられていれば、ingress IP 分類は成功です。

図 12: ステップ 1 - Ingress インターフェース、およびソース IP トラフィック分類



* LAN 上の拡張認証プロトコル (EAPOL) は、IEEE 802.1X に説明されているプロトコルです。ローカルエリアネットワークの中で送信するために、EAP メッセージをカプセル化することを意図に作られました。

2. Egress インターフェース / 宛先 IP トラフィック分類

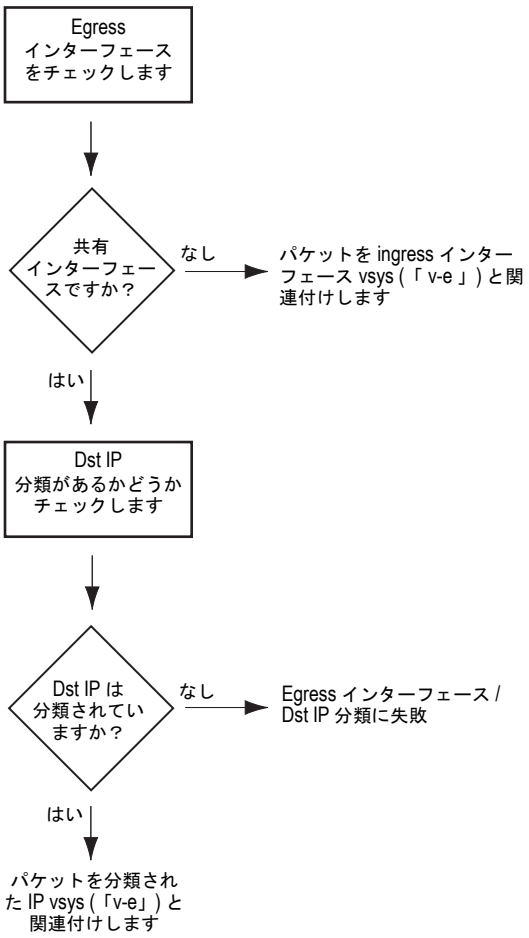
セキュリティデバイスは、egress が専用インターフェースか共有インターフェースかを確認します。

a. Egress インターフェースが vsys 専用であれば (例 :「 v-e 」)、このインターフェースを専有するシステムにトラフィックの処理を委ねます。アントラステッドインターフェース上の VIP トラフィックは、ルート vsys に必ずルーティングされることに注意してください。

b. 逆に共有インターフェースであれば、IP ベースの分類方式により、宛先 IP アドレスが特定の vsys に関連付けられていないかどうか確認します。図 13 を参照。

- どの vsys にも関連付けられていなければ、egress IP 分類は失敗します。
- 特定の vsys に関連付けられていれば、egress IP 分類は成功です。

図 13: ステップ 2 - Egress インターフェース / 宛先 IP トラフィック分類



* LAN 上の拡張認証プロトコル (EAPOL) は、IEEE 802.1X に説明されているプロトコルです。LAN 経由で転送される EAP メッセージを 暗号化する目的で作成されました。

3. Vsys トラフィックの割り当て

Ingress インターフェース / ソース IP (I/S) および egress インターフェース / 宛先 IP (E/D) のトラフィック分類結果にもとづき、セキュリティデバイスは、トラフィックがどの vsys に属するかを判断します。図 14 を参照。

a. I/S トラフィック分類に成功、しかし E/D トラフィック分類には失敗した場合、ingress インターフェースまたはソース IP アドレスに対応する vsys （たとえば「 v-i 」）のポリシー群やルートテーブルを使います。

I/S トラフィック分類が特に有用なのは、vsys から公開ネットワーク (インターネットなど) へのアウトバウンドトラフィックを許可する場合です。

b. E/D トラフィック分類に成功、しかし I/S トラフィック分類には失敗した場合、egress インターフェースまたは宛先 IP アドレスに対応する vsys （たとえば「 v-e 」) のポリシー群やルートテーブルを使います。アントラステッドインターフェース上の VIP トラフィックは、ルート vsys に必ずルーティングされることに注意してください。

E/D トラフィック分類が特に有用なのは、公開ネットワーク (インターネットなど) から vsys へのインバウンドトラフィックを許可する場合です。

c. どちらの分類にも成功し、対応する仮想システムが同じであれば、その vsys のポリシー群やルートテーブルを使います。

I/S および E/D の両方の IP トラフィック分類を使用すると、あるゾーンの特定のアドレスから、同じ vsys に属する別のゾーンの特定のアドレスに向かうトラフィックを許可することができます。

d. どちらの分類にも成功したけれども、対応する仮想システムが異なる場合、インターフェースの向かう先が同じ共有セキュリティゾーンであれば、まず I/S vsys、次に E/D vsys のポリシー群やルートテーブルを使います。

ScreenOS は、ゾーン内の vsys 間トラフィックも、同じ共有ゾーンに現れるものであれば処理できます。セキュリティデバイスはまず「 v-i 」のポリシー群やルートテーブルを使い、Untrust インターフェースにトラフィックをループバックした上で、「 v-e 」のポリシー群やルートテーブルを適用します。このようなゾーン内トラフィックは、門ごとに別々の仮想システムから成る共有内部ゾーンを運用している企業で、部門間のトラフィックを許可する場合には普通に現れます。

e. どちらの分類にも成功したけれども、対応する仮想システムが異なる場合、インターフェースの向かう先が別々の共有セキュリティゾーンであれば、パケットを破棄します。

注 : ScreenOS は、共有セキュリティゾーン間の vsys 間トラフィックには対応していません。Untrust ゾーンの代わりにカスタムゾーンを使用することはできません。

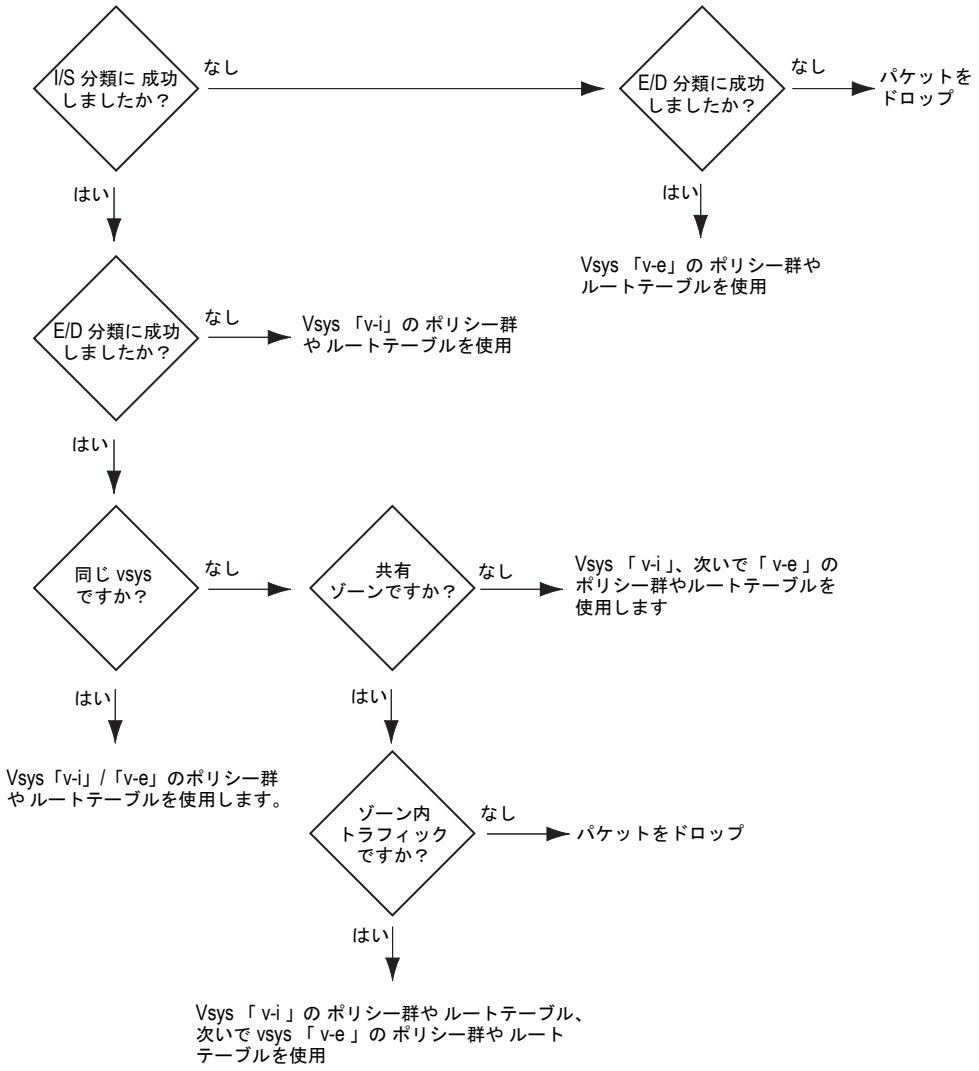
---

f. どちらの分類にも成功したけれども、対応する仮想システムが異なる場合、ingress および egress インターフェースの向かう先が異なる仮想システムのゾーンであれば、セキュリティデバイスはまず、「 v-i 」のポリシー群やルートテーブルを適用します。次に、Untrust インターフェースにトラフィックをループバックした上で、「v-e」のポリシー群やルートテーブルを適用します（54 ページの「仮想システム間の通信」を参照）。

ScreenOS は、専用セキュリティゾーン間の vsys 間トラフィックにも対応しています。

g. どちらの類にも失敗した場合はパケットを破棄します。

図 14: ステップ 3 - Vsys トラフィックの割り当て



* LAN 上の拡張認証プロトコル（EAPOL）は、IEEE 802.1X に記述されているプロトコルです。LAN の中で送信するために、EAP メッセージをカプセル化することを意図に作られました。

専用および共有インターフェース

専用および共有インターフェースへのインバウンドトラフィックは、異なる方法で振り分けされます。

専用インターフェース

仮想システム、ルートシステムとも、専有的に使用する複数のインターフェースあるいはサブインターフェースを有することができます。これらのインターフェースは、他のシステムによって共有可能ではありません。

インターフェースを以下のようにしてシステムに専用化することができます。

- ルートシステムに物理インターフェース、サブインターフェース、冗長インターフェース、または統合インターフェースを設定し、非共有ゾーンにバインドすれば、このインターフェースはルートシステム専用になります。
- 物理インターフェース、集約インターフェースを vsys にインポートし、共有 Untrust ゾーンまたは Trust-*vsys_name* ゾーンにバインドすれば、このインターフェースは vsys 専用になります。
- Vsys のサブインターフェースを設定すると、これは当該 vsys 専用になります。

注 : システムに専用サブインターフェースがあれば、セキュリティデバイスは VLAN ベースのトラフィック分類により、インバウンドトラフィックを適切に振り分けます。

共有インターフェース

仮想システム、およびルートシステムは、他のシステムとインターフェースを共有することができます。インターフェースが共用可能となるためには、インターフェースをルートレベルで構成し、共有仮想ルーターの共有ゾーンにバインドしなければなりません。デフォルトでは、untrust-vr が共有仮想ルーター、Untrust が共有ゾーンとして定義済みです。したがって、ルートレベルの物理インターフェース、サブインターフェース、冗長インターフェース、集約インターフェースを Untrust ゾーンにバインドすれば、vsys 間で共有が可能になります。

Untrust ゾーン以外のゾーンで共有インターフェースを作成するために、ルートレベルでゾーンを共有ゾーンとして定義しなければなりません。そのためには、ゾーンが共有仮想ルーター (untrust-vr、共有可能と定義したルートレベルの仮想ルーターなど) に属している必要があります。この場合、ルートレベルインターフェースを共有ゾーンにバインドすれば、自動的に共有インターフェースになります。

注 : 共有ゾーン機能を使用するためには、セキュリティデバイスがレイヤー 3 で動作していなければなりません（ルートモード)。すなわち、少なくとも 1 つのルートレベルインターフェースに、IP アドレスを割り当てている必要があります。

仮想ルーターを作成するためには vsys ライセンスキーを入手する必要があります。これは、仮想システム、仮想ルーター、セキュリティゾーンを、vsys やルートシステムに定義するために必要です。

共有仮想ルーターは、共有、非共有の、どちらのルートレベルセキュリティゾーンにも対応しています。共有仮想ルーターは、共有、非共有の、どちらのルートレベルセキュリティゾーンにも対応しています。共有仮想ルーターにバインドされるルートレベルゾーンは、共有可能または共有不可のどちらとしても定義できます。

共有仮想ルーターにバインドし、共有不可と定義したルートレベルゾーンは、専用ゾーンにとどまり、ルートシステムだけが使できます。共有仮想ルーターにバインドし、共有不可と定義したルートレベルゾーンは、ルートシステムの専用ゾーンになります。vsys 専用の仮想ルーターまたはルートシステムで作成した共有仮想ルーターにバインドした vsys レベルゾーンは、当該 vsys の専用ゾーンになります。

共有ゾーンには、共有インターフェース、専用インターフェースのどちらも設定できます。共有ゾーンにバインドしたルートレベルインターフェースは、共有インターフェースとなり、仮想システムでも使えます。共有ゾーンにバインドした vsys レベルインターフェースは、当該 vsys の専用インターフェースになります。

共有不可ゾーンは、それを作成したシステムのみが使え、当該システム用の専用インターフェースしか設定できません。Vsys レベルゾーンはすべて共有不可です。

共有インターフェースを作成するためには、共有仮想ルーターを作成 (または定義済みの untrust-vr を使用) し、共有セキュリティゾーンを作成 (または定義済みの Untrust ゾーンを使用) した上で、この共有ゾーンにインターフェースをバインドします。以上の操作はすべてルートシステム上で実行しなければなりません。

WebUI および CLI それぞれの操作手順を以下に示します。

1. 共有仮想ルーターの作成 :

WebUI

Network > Routing > Virtual Routers > New: **Shared and accessible by other vsys** を選択し、**Apply** をクリックします。

CLI

set vrouter name *name_str*
set vrouter *name_str* shared

(既存の共有仮想ルーターを非共有に変更するためには、仮想システムをすべて削除しておく必要があります。逆に非共有から共有への変更はいつでも可能です)

2. 共有ゾーンの作成 (ルートレベルで実行):

WebUI

注 : 現行バージョンでは、共有ゾーンは CLI でしか定義できません。

CLI

set zone name *name_str*
set zone *zone* vrouter *sharable_vr_name_str*
set zone *zone* shared

3. 共有インターフェースの作成 (ルートレベルで実行):

WebUI

Network > Interfaces > New (既存のインターフェースを開く場合は Edit: インターフェースを設定し、共有ゾーンにバインドして **OK** をクリックします。

CLI

set interface *interface* zone *shared_zone_name_str*

2 つ以上の仮想システムがインターフェースを共有する時、インバインドトラフィックを適切にソートするためセキュリティデバイスは IP ベーストラフィック分類を使用しなければなりません (それぞれの vsys で IP ベース トラフィック分類を構成する方法を示す例を含む詳細については、71 ページの「IP ベースのトラフィック分類」を参照してください)。

物理インターフェースのインポートとエクスポート

物理インターフェースをある vsys の専用にすることができます。これは、ルートシステムから仮想システムに、物理インターフェースをインポートする形で行います。インポートされた物理インターフェースは、当該 vsys が専有できます。

注 : 仮想システムにインポートするインターフェースは、ルートレベルの Null ゾーンに属するものでなければりません。

物理インターフェースを仮想システムにインポートする

この例では、ルート管理者となって、物理インターフェース ethernet4/1 を vsys1 にインポートします。次に、これを Untrust ゾーンにバインドし、IP アドレス 1.1.1.1/24 を割り当てます。

WebUI

1. Vsys1 にログイン
Vsys > Configure > **Enter** をクリックします (vsys1)。

2. インターフェースのインポートと定義
Network > Interfaces: **Import** をクリックします (ethernet4/1)。

Network > Interfaces > Edit (ethernet4/1): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
IP Address/Netmask: 1.1.1.1/24

3. Vsys1 からのログアウト
(メニューの一番下にある) **Exit Vsys** ボタンをクリックします。ルートレベルに戻ります。

CLI

1. **Vsys1 にログイン**
   device-> enter vsys vsys1

2. **インターフェースのインポートと定義**
   device(vsys1)-> set interface ethernet4/1 import
   device(vsys1)-> set interface ethernet4/1 zone untrust
   device(vsys1)-> set interface ethernet4/1 ip 1.1.1.1/24
   device(vsys1)-> save

3. **Vsys1 からのログアウト**
   device(vsys1)-> exit

物理インターフェースを仮想システムからエクスポートする

この例では、物理インターフェース ethernet4/1 を vsys1 の Null ゾーンにバインドし、IP アドレス 0.0.0.0/0 を割り当てて、ethernet4/1 をルートシステムにエクスポートします。

WebUI

1. **Vsys1 にログイン**
   Vsys > Configure > Click **Enter** (for vsys1).

2. **インターフェースのエクスポート**
   Network > Interfaces > Edit (ethernet4/1): 次のように入力してから **OK** をクリックします。

   Zone Name: Null
   IP Address/Netmask: 0.0.0.0/0

   Network > Interfaces: **Export** をクリック (ethernet4/1 を選択)。

   (これで ethernet4/1 はルートシステムや他の vsys で使える状態になりました)

3. **Vsys1 からのログアウト**
   (メニューの一番下にある) **Exit Vsys** ボタンをクリックします。ルートレベルに戻ります。

CLI

1. **Vsys1 にログイン**
   device-> enter vsys vsys1

2. **インターフェースのエクスポート**
   device(vsys1)-> unset interface ethernet4/1 ip
   device(vsys1)-> unset interface ethernet4/1 zone
   device(vsys1)-> unset interface ethernet4/1 import
   This command will remove all objects associated with interface, continue? y/[n]
   device(vsys1)-> save

   (これで ethernet4/1 はルートシステムや他の vsys で使える状態になりました)

3. **Vsys1 からのログアウト**
   device(vsys1)-> exit

第 4 章

IP ベースのトラフィック分類

この章は仮想システムの IP ベーストラフィック分類を説明します。本章のセクションは、以下のようになります。

- 71 ページの「概要」
- 72 ページの「ルートシステムに IP 範囲を指定する」
- 73 ページの「IP ベースのトラフィック分類を設定する」

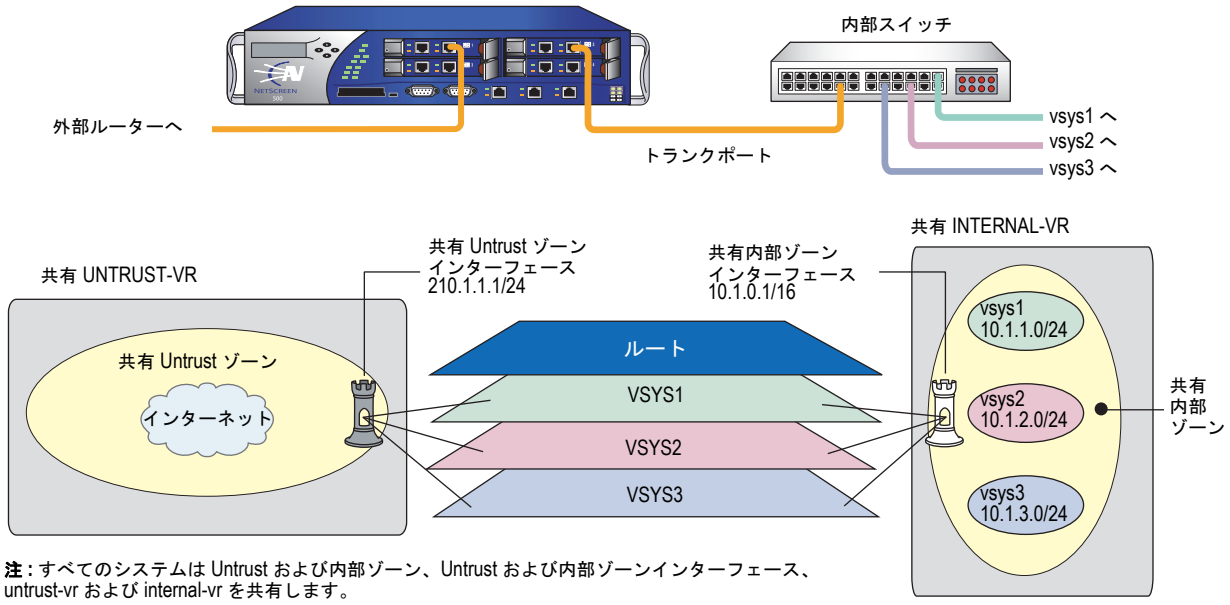
概要

図 15 は、IP ベースのトラフィック分類により、VLAN なしで仮想システムを使用できることを示しています。セキュリティデバイスは、トラフィックをソートするために VLAN タグの代わりに IP アドレスを使用し、IP アドレスのサブネットあるいは範囲を特定のシステム（ルートシステムまたは vsys ）に関連付けます。IP ベースのトラフィック分類は排他的にトラフィックをソートするために使用するため、すべてのシステムはで以下を共有します。

- untrust-vr およびユーザー定義の internal-vr
- Untrust ゾーンおよびユーザー定義の内部ゾーン
- Untrust ゾーンインターフェースおよびユーザー定義の内部ゾーンインターフェース

注： 内部トラフィックのために VLAN ベーストラフィック分類を使用するときでも、外部トラフィックのための共有 Untrust ゾーンを使用し、さらに専用インターフェースを持たない場合には、共有 Untrust ゾーンインターフェースも使用します。一方で共有インターフェースを使用し、他方で専用インターフェース (VLAN タギング) を使用することは、混合アプローチを構成します。VLAN ベースおよび IP ベースのトラフィック分類は、同時に同じシステムあるいは異なるシステム内で存在することができます。

図 15: IP ベースのトラフィック分類



注 : すべてのシステムは Untrust および内部ゾーン、Untrust および内部ゾーンインターフェース、untrust-vr および internal-vr を共有します。

ルートシステムに IP 範囲を指定する

サブネットあるいは IP アドレスの範囲を、ルートシステムあるいは既存の仮想システムに指定するには、次の CLI コマンドうちいずれかを、ルートレベルで実行しなければなりません。

WebUI

Network > Zones > Edit (*zone*) > IP Classification: 次のように入力してから **OK** をクリックします。

System: (**root** または ***vsys_name_str*** を選択)
Address Type: (**Subnet** を選択して ***ip_addr/mask*** を入力、または **Range** を選択して ***ip_addr1*** – ***ip_addr2*** を入力)

CLI

set zone *zone* ip-classification net *ip_addr/mask* { root | vsys *name_str* }
set zone *zone* ip-classification range *ip_addr1-ip_addr2* { root | vsys *name_str* }

IP ベースのトラフィック分類は共有セキュリティゾーンを使用する必要があるので、仮想システム間で重複する内部アドレスを使用することはできません。(VLAN ベーストラフィック分類では可能)。さらにすべてのシステムは同じ内部インターフェースを共有するので、そのインターフェースの動作モードは NAT または Route のいずれかでなければなりません。システムによって NAT と Route が混在させることも不可能です。IP ベースのアドレス指定方式はこの点で、より一般的に使用される VLAN ベースの方式ほど柔軟ではないといえるでしょう。

仮想ルーター、セキュリティゾーン、インターフェースの共有は、安全性の面でも、vsys ごとに専用の内部仮想ルーター、内部セキュリティゾーン、内部 / 外部インターフェースを用意する方式に比べて劣ります。仮想システムがすべて同じインターフェースを共有するならば、ある vsys の管理者が **snoop** コマンドを使って、別の vsys のトラフィック状況を収集することもできてしまいます。ま

た、内部的には IP スプーフィング（なりすまし）も可能なので、共有内部インターフェースでは IP spoofing SCREEN オプションをオフにするようお勧めします。いずれのトラフィック分類方法を使用するかを決める時、VLAN ベースアプローチにより提供されるセキュリティの向上とアドレス指定の柔軟性と、IP ベースアプローチにより提供される管理の容易さを比較して考慮してください。

IP ベースのトラフィック分類を設定する

この例では、4 ページの「Vsys オブジェクトと管理者の作成」で作成した 3 つの仮想システムを対象に、IP ベースのトラフィック分類を設定します。trust-vr は共有可能と定義します。新しいゾーンを作成して *内部* と名付け、trust-vr にバインドします。次に、この内部ゾーンを共有可能にします。ethernet3/2 を共有内部ゾーンにバインドし、IP アドレス 10.1.0.1/16 を割り当て、NAT モードを選択します。

ethernet1/2 を共有 Untrust ゾーンにバインドし、IP アドレス 210.1.1.1/24 を割り当てます。Untrust ゾーンのデフォルトゲートウェイの IP アドレスは、210.1.1.250 です。内部ゾーン、Untrust ゾーンとも、共有 trust-vr ルーティングドメインに属します。

サブネットと各 vsys を次のように対応付けます。

- 10.1.1.0/24 - vsys1
- 10.1.2.0/24 - vsys2
- 10.1.3.0/24 - vsys3

WebUI

1. **仮想ルーター、セキュリティゾーン、インターフェース**
   Network > Routing > Virtual Routers > Edit (trust-vr): **Shared and accessible by other vsys** チェックボックスを選択し、**OK** をクリックします。

   Network > Zones > New: 次のように入力してから **OK** をクリックします。

   Zone Name: Internal
   Virtual Router Name: trust-vr
   Zone Type: Layer 3

   Network > Zones > Edit (Internet): **Share Zone** チェックボックスを選択して **OK** をクリックします。

   Network > Interfaces > Edit (ethernet3/2): 次のように入力してから **OK** をクリックします。

   Zone Name: Internal
   IP Address/Netmask: 10.1.0.1/16

   Network > Interfaces > Edit (ethernet1/2): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   IP Address/Netmask: 210.1.1.1/24

2. ルート

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (選択)
Interface: ethernet1/2
Gateway IP Address: 210.1.1.250

3. Trust ゾーンの IP 分類

Network > Zones > Edit (Internet) > IP Classification: 次のように入力してから **OK** をクリックします。

System: vsys1
Address Type:
Subnet: (選択); 10.1.1.0/24

Network > Zones > Edit (Internet) > IP Classification: 次のように入力してから **OK** をクリックします。

System: vsys2
Address Type:
Subnet: (選択); 10.1.2.0/24

Network > Zones > Edit (Internet) > IP Classification: 次のように入力してから **OK** をクリックします。

System: vsys3
Address Type:
Subnet: (選択); 10.1.3.0/24

Network > Zones > Edit (Internet): **IP Classification** チェックボックスを選択して **OK** をクリックします。

CLI

1. 仮想ルーター、セキュリティゾーン、インターフェース

```
set vrouter trust-vr shared
set zone name Internal
set zone Internal shared
set interface ethernet3/2 zone Internal
set interface ethernet3/2 ip 10.1.0.1/16
set interface ethernet3/2 nat
set interface ethernet1/2 zone untrust
set interface ethernet1/2 ip 210.1.1.1/24
```

2. ルート

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet1/2 gateway 210.1.1.250
```

3. Trust ゾーンの IP 分類

```
set zone Internal ip-classification net 10.1.1.0/24 vsys1
set zone Internal ip-classification net 10.1.2.0/24 vsys2
set zone Internal ip-classification net 10.1.3.0/24 vsys3
set zone Internal ip-classification
save
```

索引

A

admins 2
　種類 4
　パスワードの変更 4, 7

I

IEEE 802.1Q VLAN 規格 31
IP ベースのトラフィック分類 71

S

ScreenOS
　VR 6
　ゾーン 6

V

VLAN
　VLAN ベースのトラフィック分類 31–57, 70
　作成 33–54
　サブインターフェース 51
　タグ 33, 51
　透過モード 32, 33
　トランク処理 32
　別の VLAN との通信 54–57, 69
VLAN ベースのトラフィック分類 31–57, 70
VR 6
　共有 67
　共有、作成 68
vsys
　admin 7
　オブジェクト、作成 4

あ

アドレス、重複範囲 52, 72

い

インターフェース
　物理、vsys からのエクスポート 70
　物理、vsys へのインポート 69
　共有 67, 71
　専用 67, 71

か

MIP、仮想システム MIP 61
仮想システム
　VIP 61
　管理性とセキュリティ 73
管理、vsys 7

き

共有ゾーン 67

さ

サブインターフェース 51
　vsys ごとに複数 51
　作成 (vsys) 51
　設定 (vsys) 51
サブネット、重複 52

せ

セキュリティゾーン
　ゾーンを参照

そ

ゾーン 6
　Vsys 6
　共有 67
ソフトウェアキー 67

と

透過モード 32, 33
トラフィック
　VLAN ベース 31–57, 70
　通過トラフィック、vsys への振り分け 62–65
トランクポート 33
トランクポート、透過モード 32

は

パスワード、管理者の変更 4, 7

ふ

物理インターフェース
　vsys からのエクスポート 70
　vsys へのインポート 69

ほ

ポート、トランク 32, 33

も

モード、透過 32

よ

要件、基本機能 4

概念と用例
ScreenOS リファレンス ガイド

第 11 部 :
高可用性

リリース 6.0.0、改訂 02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

品番 : 530-017777-01-JP, 改訂 02

Copyright Notice

Copyright © 2007 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

目次

本編について v

ドキュメントの規則 v
Web ユーザーインターフェースの規則 vi
コマンドラインインターフェースの規則 vi
ネーミング規則および文字タイプ vii
説明図の規則 viii
技術ドキュメンおよびテクニカルサポート ix

第 1 章 NetScreen 冗長プロトコル 1

高可用性の概要 1
NSRP の概要 2
NSRP デフォルト設定 4
NSRP-Lite 4
NSRP-Lite の デフォルト設定 6
NSRP の基本設定 6
コントロールリンクメッセージ 6
データリンクメッセージ 7
動的ルーティング勧告 8
2 重リンク精査 9
NSRP クラスタ 10
クラスタ名 11
アクティブ / パッシブ構成 11
アクティブ / アクティブ構成 12
アクティブ / アクティブ ー フルメッシュ構成 14
NSRP クラスタの認証および暗号化 15
ランタイムオブジェクト 15
RTO ミラー動作状態 16
NSRP クラスタの同期 18
ファイルの同期 18
構成同期化 18
ルートの同期化 19
ランタイムオブジェクトの同期化 19
システムクロックの同期化 20
VSD グループ 20
プリエンプトオプション 21
メンバー状態 22
ハートビートメッセージ 23
VSI と静的ルート 24
設定例 25
アクティブ / アクティブ、フルメッシュ NSRP のためのデバイスの配線 25
NSRP クラスタの作成 28
アクティブ / パッシブ NSRP クラスタの構成 30
アクティブ / アクティブ NSRP クラスタの構成 34

設定例（続き）
手作業での RTO の同期化 40
手動リンク精査の設定 40
自動リンク精査の設定 41

第 2 章 インターフェースの冗長性およびフェールオーバー 43

冗長インターフェースとゾーン 43
ホールドダウンタイム設定 44
統合インターフェース 45
インターフェースフェールオーバー 46
バックアップインターフェーストラフィック 46
1 次インターフェース トラフィック 47
トラフィックの自動フェールオーバー 47
シリアルインターフェース 48
デフォルトルートの削除 48
デフォルトルートの追加 49
ポリシーの無効化 49
フェールオーバーの監視 49
IP トラッキングによるインターフェースフォールオーバー 50
アクティブトンネルからバックアップトンネルへのフェールオーバー 51
VPN トンネル監視を使用したインターフェースフェールオーバー 51
フェールオーバーのトリガーを監視する NSRP オブジェクト 52
セキュリティモジュール 53
物理インターフェース 54
ゾーンオブジェクト 54
トラック IP オブジェクト 55
デバイスフェールオーバー用のトラック IP 57
仮想セキュリティデバイスグループのフェールオーバー 57
仮想システムのフェールオーバー 58
デバイスフェールオーバー 59
構成例 60
デバイスフェールオーバー用のトラック IP の構成 60
冗長 VPN トンネルの構成 63
仮想セキュリティインターフェースの構成 67
2 系統のアクティブなトンネルの構成 70
トラック IP を使用したインターフェースフォールオーバーの構成 74
トンネルのフェールオーバーウェイトの構成 77
仮想システムのフェールオーバーの構成 83

索引 ..... IX-I

本編について

*第 11 部 : 高可用性*では、NetScreen Redundancy Protocol (NSRP) 操作の概要を説明し、NSRP を使用して高可用性 (HA) サービスを提供する冗長グループにおける Juniper Networks セキュリティデバイスの配線、構成、管理の方法が記述されています。また、NSRP の軽量化バージョンである NSRP-Lite についても解説します。これは Run-Time Objects (RTO) の動機機能を外したものです。

本編の章は、以下のようになります。

- 第 1 章「NetScreen 冗長プロトコル」、は、NetScreen 冗長性プロトコル (NSRP) を使用した高い可用性 (HA) を提供するために冗長グループで Juniper Networks セキュリティデバイスを配線、構成、および管理する方法を説明します。
- 第 2 章「インターフェースの冗長性およびフェールオーバー」、は、Juniper Networks セキュリティデバイスがインターフェースの冗長性を提供する種々の方法を説明します。

ドキュメントの規則

このドキュメントは、次のセクションで説明されている規則を使用しています。

- vi ページの「Web ユーザーインターフェースの規則」
- vi ページの「コマンドラインインターフェースの規則」
- vii ページの「ネーミング規則および文字タイプ」
- viii ページの「説明図の規則」

Web ユーザーインターフェースの規則

WebUI（Web ユーザーインターフェース）では、各作業の操作指示は、操作手順と構成設定値に分かれています。構成設定を入力できる WebUI ページを開くには、画面の左側にあるナビゲーション ツリーのメニュー項目をクリックして、そのページに移動します。先へ進むと、ナビゲーション パスが画面の上部に表示されます。各ページは角括弧で分離されています。

WebUI のパスおよびアドレスを定義するためのパラメータは、以下のとおりです。

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.2.2.5/32
Zone: Untrust

構成設定のオンライン ヘルプを開くには、画面の左上にある疑問符（?）をクリックします。

ナビゲーションツリーにも、Help > Config Guide 構成ページがあり、セキュリティポリシーおよび IPSec （インターネットプロトコルセキュリティ）の構成に役立ちます。ドロップダウンメニューからオプションを選択して、そのページの指示に従います。構成設定のオンラインヘルプを開くには、左上にある **?** 文字をクリックします。

コマンドラインインターフェースの規則

次の規則は、例とテキストにおいて、コマンドラインインターフェース（CLI）コマンドの構文を示すために使用されます。

例においては、次のように使用されます。

- 角括弧 [ ] 内にあるものはすべてオプションです。
- 中括弧 { } 内にあるものはすべて必須です。
- 選択肢が複数ある場合、各選択肢はパイプ (|) で区切られています。例えば、次のように表示されます。

  set interface { ethernet1 | ethernet2 | ethernet3 } manage

- 変数は*斜体*で表示されます。

  set admin user *name1* password *xyz*

テキストにおいては、コマンドは**太字**で、変数は*斜体*で表示されます。

注： キーワード入力時には、単語を間違いなく識別できる数の文字を入力すれば十分です。**set admin user wheezer j12fmt54** というコマンドを入力する際には、**set adm u whee j12fmt54** と入力するだけで十分です。ただし、本編に記載されたコマンドはすべて本来の形式で記載されています。

ネーミング規則および文字タイプ

ScreenOS はオブジェクトの名前 (アドレス、管理ユーザー、認証サーバー、IKE ゲートウェイ、仮想システム、VPN トンネルおよびゾーンなど、ScreenOS 構成に定義されているもの) に関して、次の規則に従います。

- 名前文字列に 1 つまたは複数のスペースが含まれる場合、文字列全体を二重引用符で囲む必要があります。例 :

  set address trust “local LAN” 10.1.1.0/24

- 二重引用符で囲まれた文字列の先頭または末尾のスペースを取り除きます。たとえば、**「 local LAN 」**は**「local LAN」**となります。

- 連続した複数のスペースは、一つのスペースとして扱われます。

- CLI キーワードの多くはケースセンシティブではありませんが、名前文字列はケースセンシティブです。たとえば、**「local LAN」**は**「local lan」**とは異なります。

ScreenOS は、次の文字タイプをサポートします。

- 1 バイト文字セット (SBCS) およびマルチバイト文字セット (MBCS)。SBCS の例に、ASCII、欧州言語、およびヘブライ語があります。2 バイト文字セット (DBCS) とも呼ばれる MBCS の例に、中国語、韓国語、および日本語があります。

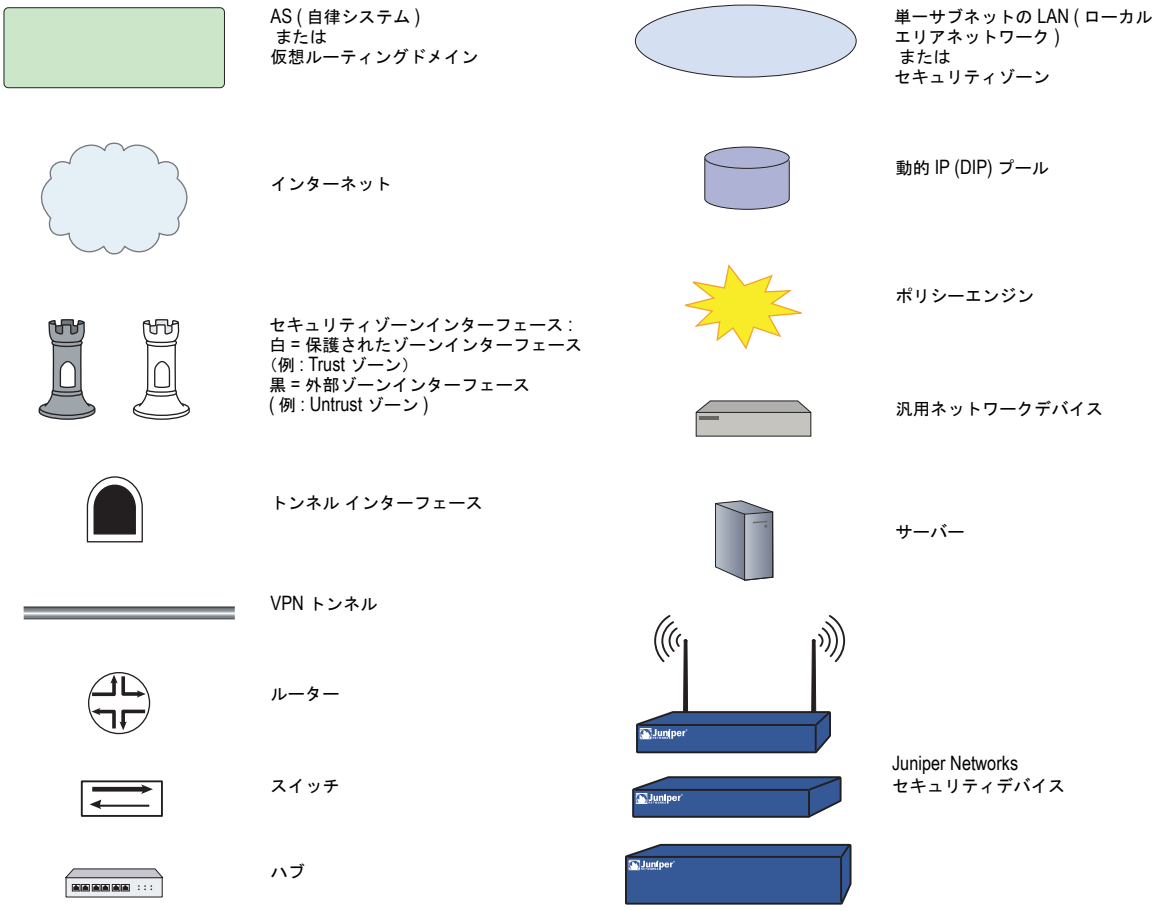
- ASCII 文字の 32（16 進数の 0x20）から 255（0xff)。ただし二重引用符 (“) は、スペースを含む名前文字列の先頭と末尾を示す特殊な意味をもつため、例外とします。

注 : コンソール接続では、SBCS のみがサポートされます。ご利用のブラウザがサポートする文字セットに応じて、WebUI は SBCS および MBCS の両方をサポートします。

説明図の規則

次の図は、本編を通して説明図に使用されている画像の基本的なものです。

図 1: 説明図の画像



技術ドキュメンおよびテクニカルサポート

Juniper Networks 製品のいずれかの技術ドキュメントを入手するには、www.juniper.net/techpubs/ をご覧になってください。

テクニカルサポートについては、http://www.juniper.net/customers/support/ にある Case Manager を使って事例サポートを開くか、1-888-314-JTAC (米国内) か 1-408-745-9500 (その他の国) までお問い合わせください。

本書に間違いや欠落があった場合は、techpubs-comments@juniper.net までお知らせください。

第 1 章

NetScreen 冗長プロトコル

この章は NetScreen 冗長プロトコル (NSRP) のコンポーネントおよび NSRP を使用して高可用性 (HA) をサポートする方法について説明します。本章のセクションは、以下のようになります。

- 1 ページの「高可用性の概要」
- 2 ページの「NSRP の概要」
- 10 ページの「NSRP クラスタ」
- 20 ページの「VSD グループ」
- 25 ページの「設定例」

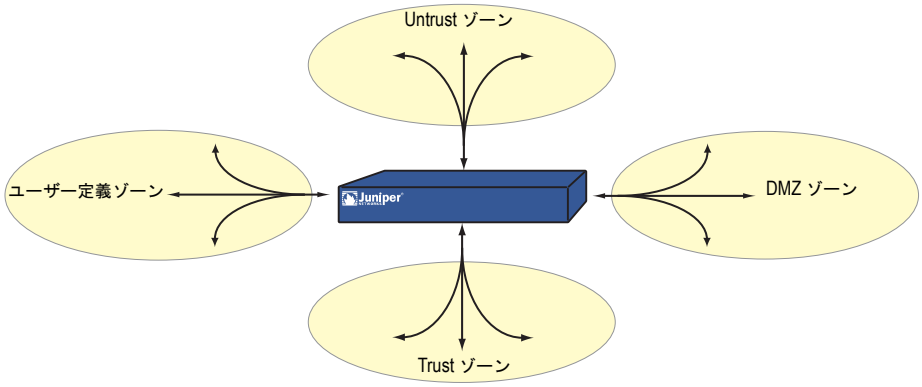
高可用性の概要

高可用性（HA）はネットワーク内のデバイスが障害を生じる可能性を最小限にする方法です。ネットワークトラフィックはすべて、Juniper Networks セキュリティデバイスを通るので、障害が起きた場合にデバイスのバックアップを用意することにより、ネットワークから障害が生じる可能性のあるポイントをできるだけ多く排除する必要があります。

セキュリティデバイスを HA ペアでセットアップすると、ネットワーク設計から障害が生じる可能性を 1 つ排除することになります。セキュリティデバイスの HA ペアの両側に冗長スイッチをセットアップし、さらに障害が生じる可能性を減らすことができます。

HA がネットワークファイアウォールとして正しく機能するためには、図 2 に示すように、セキュリティデバイスはすべてのゾーン間トラフィックが通過するシングルポイントに設置されている必要があります。

図 2: すべてのゾーン間トラフィックがファイアウォールを流れる様子



ルートモードまたは NAT モードのセキュリティデバイスでは、冗長クラスタの両方のデバイスがアクティブになるように構成し、仮想ルーター冗長プロトコル (VRRP) などのプロトコルを実行しているような、ロードバランス機能を備えたルーターによってデバイス間に分散されたトラフィックを共有させる事ができます。これを実行するには、NetScreen 冗長プロトコル (NSRP) を使用して、独自の 仮想セキュリティインターフェース (VSI) をもつ仮想セキュリティデバイス (VSD) グループを 2 つ作成します。

表 1 は、2 台のセキュリティデバイス上で NSRP が有効な場合利用可能な HA 機能を示します。

表 1: HA 機能

HA 機能	NSRP-Lite	NSRP
ダイヤルアップへのフォールバック		
アクティブ / パッシブ	はい	はい
アクティブ / アクティブ	なし	はい
アクティブ / アクティブ ー フルメッシュ	なし	はい

NSRP の概要

セキュリティデバイスがレイヤー 3 (NAT モードまたはルートモード) またはレイヤー 2 で動作している場合は（透過モード)、アクティブ / アクティブまたはアクティブ / パッシブ NetScreen 冗長プロトコル (NSRP) 構成で動作が可能です。いずれのモードのバックアップデバイスを管理するには、セキュリティゾーンインターフェースごとに設定した管理 IP アドレスを使用する必要があります。NSRP クラスタ内のセキュリティデバイスを設定すると、セキュリティデバイスは自動的に VSD グループ 0 を作成し、物理インターフェースを VSD グループ 0 の仮想セキュリティインターフェース (VSI) に変換します。NSRP の基本原則はシングルポイント障害がないということです。すべての NSRP 情報は 2 つの HA インターフェースを介して、クラスタメンバー間で転送されます。

注： VSD グループ 0 以外 VSD グループの VSI では、管理 IP アドレスを設定することはできません。

注 : NSRP 機能を有効にする前に、お使いのデバイスのハードウェア設置および構成ガイドで説明されているように、事前に 2 台のセキュリティデバイス同士を配線する必要があります。また、NSRP クラスタのセキュリティデバイス上の 1 つまたは複数の物理インターフェースへの管理トラフィックに対するネットワーク接続を維持する場合は、3-31 ページの「複数のインターフェースに対して管理 IP を設定する」で説明されているように、最初にこれらのインターフェースの管理 IP アドレスを設定してから、NSRP を使用可能にします。

WebUI

Network > NSRP > Synchronization: **NSRP RTO Synchronization** を選択してから **Apply** をクリックします。

CLI

1. **NSRP クラスタおよび VSD グループのバインド**
   set nsrp cluster id *number*
2. **自動 RTO 同期の有効化**
   set nsrp rto sync all
3. **ポートの構成**
   set interface *interface* zone ha
   set interface *interface* zone ha

NSRP デフォルト設定

NSRP デフォルト設定	値
VSD グループ情報	■ VSD group ID: 0 ■ Device priority in the VSD group: 100 ■ Preempt option: 無効 ■ Preempt hold-down time: 0 秒 ■ Initial state hold-down time: 5 秒 ■ Heartbeat interval:1000 ミリ秒 ■ Lost heartbeat threshold: 3 ■ Master (Primary) always exist: いいえ
RTO ミラー情報	■ RTO synchronization: 無効 ■ Heartbeat interval: 4 秒 ■ Lost heartbeat threshold: 16
NSRP リンク情報	■ Number of gratuitous ARPs: 4 ■ NSRP encryption: 無効 ■ NSRP authentication: 無効 ■ Track IP: なし ■ Interfaces monitored: なし ■ Secondary path: なし ■ HA link probe: なし ■ 間隔 : 15 ■ しきい値 : 5

注 : VSI を示すための規則は、*interface_name*:*VSD_group_ID* です。次の例は、冗長インターフェース **red1** が VSD グループ 1 の VSI であることを示しています。**red1:1**. ただし、VSD グループ ID が 0 の場合は、VSD グループ ID は明示されません。たとえば、冗長インターフェース **red2** が VSD グループ 0 の VSI である場合は、**red2** とだけ表示されます。

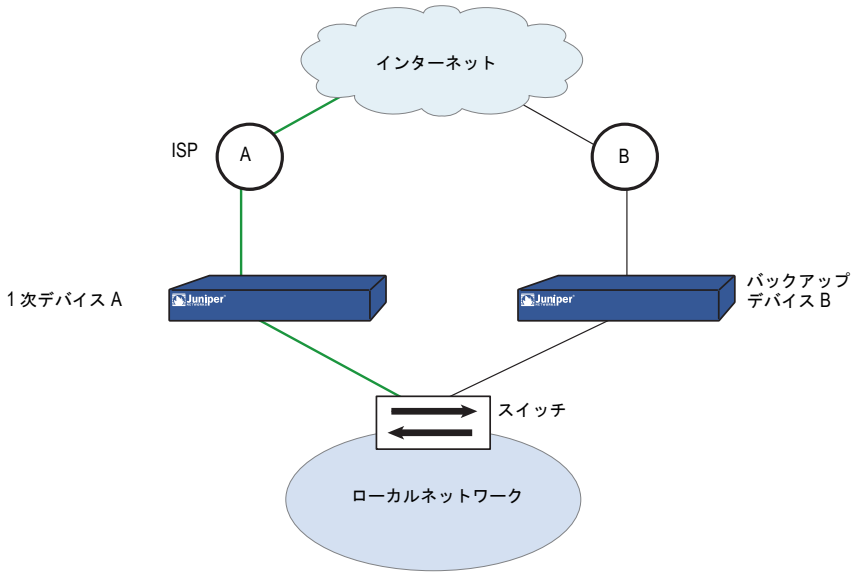
NSRP-Lite

NSRP-Lite は特定の NSRP 機能をサポートし、ルートまたは NAT モードで ScreenOS を実行しているいくつかの Juniper Networks セキュリティプラットフォームにのみサポートされています。NSRP-Lite では以下のことができます。

- アクティブ / パッシブ構成のみ
- 構成同期化 同期、ただしデフォルト設定ではない
- RTO 同期が起きないためにフェールオーバーが生じた際、ユーザーセッションおよび VPN 接続が中断する。

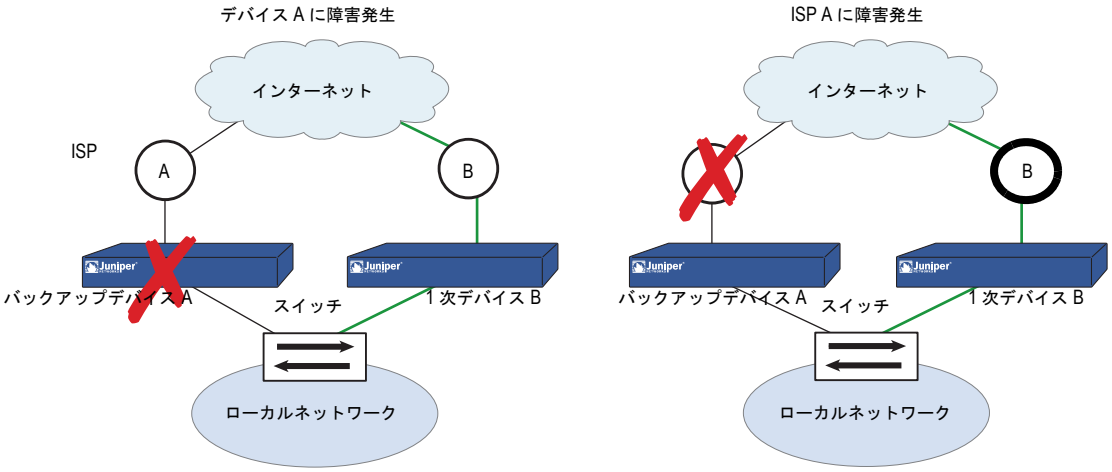
注 : VPN トンネルは再確立しなければなりません。このため VPN トンネルで VPN 監視を再入力オプションで有効にして、これらが自動的に再確立されるようにすることを推奨します。

図 3: NSRP-Lite の設定



デバイス A または ISP A のいずれかが失敗した場合、デバイス B は 1 次デバイスとなり、デバイス A はバックアップになります (または、内部システム問題が発生している場合、デバイス A は動作不能になります)。図 4 を参照してください。

図 4: NSRP-Lite のフェールオーバー



NSRP-Lite の デフォルト設定

基本的な NSRP-lite 設定では、次のデフォルトの設定が使用されます。

表 2: NSRP-Lite の デフォルト設定

設定	デフォルト
Configure sync	無効
RTO sync	なし
VSD グループ情報	■ VSD group ID: 0 ■ Device priority in the VSD group: 100 ■ Preempt option: 無効 ■ Preempt hold-down time: 0 秒 ■ Initial state hold-down time: 5 秒 ■ Heartbeat interval: 1000 ミリ秒 ■ Lost heartbeat threshold: 3
NSRP リンク情報	■ Number of gratuitous ARPs: 4 ■ NSRP encryption: 無効 ■ NSRP authentication: 無効 ■ Interfaces monitored: なし ■ Secondary path: なし

NSRP の基本設定

2 つのインターフェース (ギガビットまたは 100 メガビット) を HA ゾーンにバインドすると、小さい番号を持つインターフェースがコントロールリンクとなり、大きい番号を持つインターフェースがデータリンクとなります。たとえば、ethernet8 のみを HA ゾーンにバインドすると、これはコントロールリンクになります。次に ethernet7 を HA ゾーンにバインドすると、これはコントロールになり (ethernet8 より番号が小さいため)、ethernet8 の方がデータリンクになります。

専用の HA インターフェースを持たないセキュリティデバイスでは、1 つまたは 2 つの物理イーサネットインターフェースを HA ゾーンにバインドする必要があります。単一のギガビットインターフェースを HA インターフェースにバインドすると、HA リンクはコントロールメッセージとデータメッセージの両方をサポートします。単一の 100 メガビットのインターフェースを HA ゾーンにバインドすると、HA リンクはコントロールメッセージのみをサポートします。

注 : HA ゾーンには 4 つ以上のインターフェースをバインドすることができますが、最初の 3 つのエントリーだけが HA リンクとして設定できます。

コントロールリンクメッセージ

コントロールメッセージには 2 種類あります。ハートビートと HA メッセージです。

ハートビート : ハートビートは、NSRP クラスタメンバー、VSD グループメンバー、RTO ミラーの間での通信を確立し、維持するために定期的に送信されます。ハートビートは送信側のメンバー状態、システムのヘルスチェック状態、ネットワークの接続性を頻繁に通知します。表 3 は、3 種類のハートビートメッセージを説明しています。

表 3: ハートビートメッセージの説明

ハートビート メッセージ	説明
HA 物理リンク	NSRP クラスタの各メンバーの HA1 と HA2 インターフェースからもう一方のメンバーへのブロードキャストメッセージ。これらのメッセージの目的は、HA インターフェースのヘルスチェック状態を監視することです。たとえば、あるメンバーが HA1 から 3 回連続したハートビートを受信しなかった場合、両方のデバイスはコントロールメッセージを HA2 に転送します。すべての NSRP 構成で利用可能。
VSD	VSD グループの各メンバーの HA1 インターフェースからのブロードキャストメッセージ。VSD グループはこれらのメッセージを使用して、すべてのメンバーのメンバーシップ状態を監視します。たとえば、1 次デバイスが自身が動作不能になったことを通知すると、1 次バックアップがただちに VSD グループの 1 次デバイスになります。すべての NSRP 構成で利用可能。
RTORTO	各 HA1 から送信されるブロードキャストメッセージ。これらのメッセージの目的は、アクティブなピアを探し出し、グループアクティブメッセージを送信することでミラー関係を維持することです。たとえば、あるデバイスがピアからの 16 回連続した RTO ハートビートを受信しなかった場合は、そのデバイスはアクティブ状態からセット状態に変化します。アクティブ / パッシブおよびアクティブ / パッシブ、フルメッシュ NSRP 構成のみ。

注 : ミラーグループからデバイスを削除すると、そのデバイスは不確定状態に変わり、「グループ切り離し」メッセージをピアに送信します。ピアは、消失したのハートビートがしきい値を超えるのを待たずに、ただちにアクティブからセット状態に変化します。

HA メッセージ : HA メッセージには、次の 2 種類があります。

- 設定メッセージ - 1 次デバイスが他の VSD グループのメンバーに送信するネットワークと設定内容
- RTO メッセージ - 1 次デバイスが他の RTO ミラーに送信する RTO

HA メッセージには、サービスを中断せずにバックアップを 1 次デバイスにすることを可能にする情報が含まれています。

データリンクメッセージ

データメッセージとは、ファイアウォールを通過する IP パケットであり、VSD グループのバックアップは、1 次デバイスとして機能しているデバイスにこの IP パケットを転送する必要があります。アクティブ / アクティブ構成のセキュリティデバイスのインターフェースにパケットが到達すると、デバイスは、最初にどちらの VSD グループがパケットを処理するべきかを識別します。パケットを受信するデバイスが、識別された VSD グループの 1 次デバイスであれば、そのデバイスがパケットを処理します。そのデバイスが 1 次デバイスでない場合は、HA データリンクを介して 1 次デバイスにパケットを転送します。

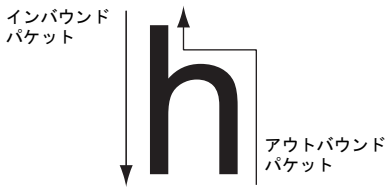
たとえば、ロードバランスを行なうルーターはセッションの最初のパケットをデバイス A (VSD グループ 1 の 1 次デバイス) に送信することがあります。このデバイス A では、セッションテーブルにエントリが作成されます。ルーターがラウンドロビンでパケットを送信することによって、ロードバランスを行う場合は (すなわち、ルーターがセキュリティデバイスにそれぞれのパケットを順に送信

する場合)、ルーターは次のパケットをデバイス B (VSD グループ 1 のバックアップ) に送信することもあります。この場合、セッションエントリはデバイス A にあるので、デバイス B はデータリンクを介してデバイス A にパケットを転送し、デバイス A がパケットを処理します。

注 : データリンクが存在しない場合、パケットを受信したセキュリティデバイスは、ただちにそのパケットを破棄します。

データリンクを介して転送されるインバウンドパケットは、セキュリティデバイスがルートモードでアクティブ / アクティブ構成になっている場合にのみ発生します。NAT モードの場合、ルーターは常に MIP、VIP または VPN トンネルゲートウェイにインバウンドパケットを送信します。ただし、返信されたアウトバウンドパケットを受け取ったセキュリティデバイスは、データリンクを経由してパケットが所属するセッションエントリを持つもう一方のデバイスへと転送する場合もあります。この形式のパケット転送では、h 形状パスが形成されます。文字 *h* を綴る際の動作のように、インバウンドパケットは 1 つのデバイスを直進しますが、アウトバウンドパケットはもう一方のデバイスを通って途中まで送信されてから、データリンクを介して最初のデバイスに転送されます。図 5 を参照してください。

図 5: データリンクを通してのパケット転送



動的ルーティング勧告

NSRP クラスタが動的ルーティング環境にあり、パケット転送を使用不可にしている場合、非アクティブなインターフェースに到達したトラフィックが失われることがあります。セキュリティデバイスは、データリンクを介して、インターフェースがアクティブなセキュリティデバイスにトラフィックを転送できないため、そのトラフィックをドロップします。これを回避するためにパケット転送を使用不可にした場合は、セキュリティデバイスはデバイス上の 1 次デバイスでない VSD に属するインターフェースの状態を、単に「 inactive 」としてではなく「 down 」として示します。この状態は、これらのインターフェースにトラフィックを送信しないようにルーターに知らせます。

NSRP クラスタでパケット転送を使用不可にするには、**unset nsrp data-forwarding** CLI コマンドを使用します。

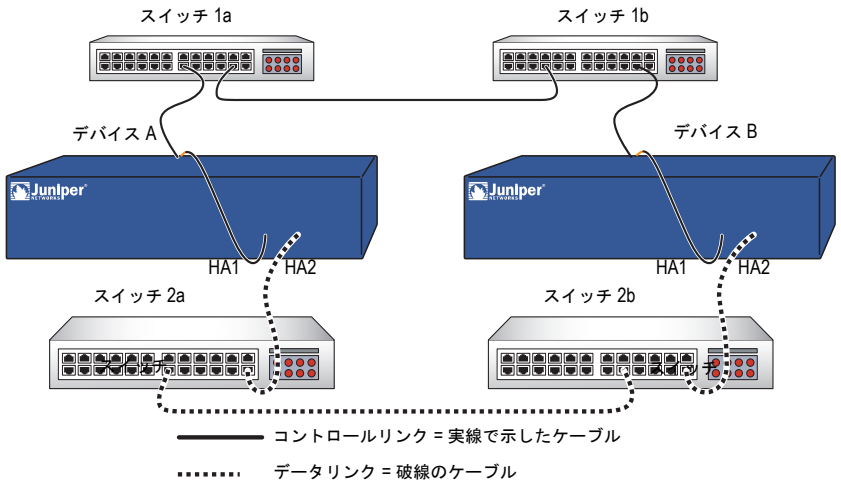
WebUI

注 : パケット転送を使用不可にするには CLI を使用する必要があります。

2 重リンク精査

冗長 HA インターフェースの接続は、1 台のデバイスの HA ポートを別のデバイスの HA ポートに直接配線することによって可能になります。あるいは、1 台または複数台のスイッチを持つネットワークを介して、2 台のデバイス上の HA ポートを接続することもできます。図 6 の構成では、デバイス デバイス A の HA1 ポートは、2 台のスイッチ、スイッチ 1a と 1b を介して、デバイス B の HA1 ポートに接続されています。冗長 HA インターフェースを実現するために、デバイス A の HA2 ポートは、Switch-2a と Switch-2b を介して、デバイス B の HA2 ポートに接続されています。この構成では、デバイス A およびデバイス B の HA1 ポートの間のリンクで NSRP コントロールメッセージを処理し、HA2 リンクでネットワークデータメッセージを処理します。デバイス A の HA1 ポートと Switch-1a 間のリンクがダウンすると、デバイス A はコントロールメッセージの伝送を HA2 ポートに変更します。しかしながら、HA1 ポートはまだアクティブであるためデバイス B は HA1 リンクに障害が発生したことを認識せず、HA2 リンク上のデバイス A が送信した NSRP コントロールメッセージを拒否します。

図 6: スイッチを接続する HA リンク



このような状況を防止するために、HA リンク上の NSRP 精査要求をピアに送信することによって HA リンクの状態を監視するように、セキュリティデバイスを構成することができます。HA リンク上のピアから応答を受信すると、要求は正常に処理されたと解釈され、HA リンクは動作中であると推測されます。指定された制約のもとでピアから応答が受信できなければ、HA リンクは動作していないと解釈されます。仮にいずれのデバイスの HA ポート上にも物理的な障害がない場合でも、この方法によってセキュリティデバイスは、必要な時にコントロールメッセージの伝送を利用可能な HA リンクに切り換えることができます。

HA リンク上に精査要求を送信するには、次の 2 つの方法があります。

- **管理者による手動精査** - 指定された回数、1 秒毎に 1 回、精査が特定の HA リンク上で送信されます。精査を指定された回数送信視しても応答が受信できなければ、HA リンクは動作していないと解釈されます。精査は、コマンドを実行した直後に送信されます。

- **ScreenOS により自動的に** - 精査要求は毎秒すべての HA リンクに送信されます。（オプションとして HA ゾーンインターフェースを指定して、精査要求

を送信する間隔を設定することができます。）デフォルトでは、5 回連続して精査を送信してもピアから応答が受信できなければ、リンクが動作していないと解釈されます。リンクが動作していないと判断するしきい値に異なる値を指定することもできます。1 次 HA リンクが動作していなくても、セキュリティデバイスはそのリンク上で精査を送信し続けることに注意が必要です。1 次 HA リンクが復旧し、ピアの応答が再度そのリンク上で受信されれば、セキュリティデバイスはコントロールメッセージの伝送を 1 次 HA リンクに戻すことができます。

NSRP クラスタ

NSRP クラスタは、同一のセキュリティポリシーを全体にわたって実行し、同一の構成設定を共有するセキュリティデバイスのグループから構成されています。デバイスを NSRP クラスタに割り当てている場合は、そのクラスタの 1 メンバーの構成に加えた変更は、他のメンバーにも設定同期します。

同一の NSRP クラスタのメンバーは、以下について同一の設定を維持しています。

- ポリシーとポリシーオブジェクト (アドレス、サービス、VPN、ユーザー、スケジュールなど)
- システムパラメータ (認証サーバー、DNS、SNMP、syslog、URL 遮断、ファイアウォール検出オプションなど)

クラスタのメンバーは、表 4 の構成は設定同期しません。

表 4: 設定同期されないコマンド

NSRP	■ set/unset nsrp cluster id *number* ■ set/unset nsrp auth password *pswd_str* ■ set/unset nsrp encrypt password *pswd_str* ■ set/unset nsrp monitor interface *interface* ■ set/unset nsrp vsd-group id *id_num* { mode *string* | preempt | priority *number* }
インターフェース	■ set/unset interface *interface* manage-ip *ip_addr* ■ set/unset interface *interface* phy… ■ set/unset interface *interface* bandwidth *number* ■ set/unset interface redundant *number* phy primary *interface* ■ ローカルインターフェースに属するすべてのコマンド
Monitored Objects	すべての IP トラッキングコマンド、ゾーンモニタリング、およびインターフェースモニタリングコマンド
Console Settings	すべてのコンソールコマンド (set/unset console …)
Hostname	set/unset hostname *name_str*
SNMP	set/unset snmp name *name_str*
Virtual Router	set/unset vrouter *name_str* router-id *ip_addr*
Clear	すべてのクリアコマンド (clear admin, clear dhcp, …)
Debug	すべてのデバッグコマンド (debug alarm, debug arp, …)

クラスタ名

NSRP クラスタはメンバーごとに異なるホスト名を持つことができるので、フェールオーバーによって SNMP 通信とデジタル証明書の有効性が阻害されることがあります。というのは、SNMP 通信と証明書はデバイスのホスト名によって、正しく機能するからです。

全クラスタメンバーについて 1 つの名前を定義するには、**set nsrp cluster name** *name_str* CLI コマンドを使用します。

注 : NSRP クラスタ名の設定には CLI を使う必要があります。

注 : 専用の HA ポートを持たないデバイスでは、NSRP クラスタを構成する前に、インターフェースを HA ゾーンにバインドする必要があります。

セキュリティデバイスの SNMP ホスト名を構成する場合 (**set snmp name** *name_str*)、および PKCS10 証明書要求ファイルで共通名を定義する場合は、クラスタ名を使用します。

クラスタメンバーすべてに単一の名前を使用すると、SNMP 通信およびデジタル証明書利用はデバイスのフェールオーバー後も中断せずに実行されます。

ScreenOS では、以下の HA クラスタ構成が可能です。

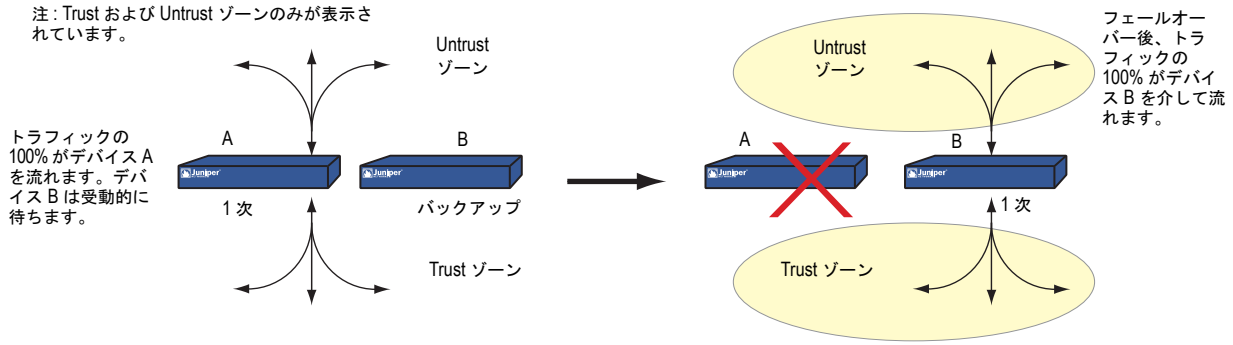
- アクティブ / パッシブ構成
- アクティブ / アクティブ構成
- アクティブ / アクティブ ー フルメッシュ構成

アクティブ / パッシブ構成

連続したトラフィックフローを確実に通過させるために、2 台のセキュリティデバイスを配線、設定し、2 台のうち 1 台を 1 次デバイス、もう 1 台をバックアップとして冗長クラスタを構成することが可能です。1 次デバイスは、そのすべてのネットワークおよび構成の設定と現在のセッションの情報をバックアップに設定同期します。1 次デバイスに障害が発生した場合は、バックアップが 1 次デバイスに昇格し、トラフィックの処理を引き継ぎます。

図 7 では、2 台のデバイスはアクティブ / パッシブ構成になります。すなわち、1 次デバイスはアクティブで、ファイアウォールおよび VPN のすべての活動を処理し、バックアップはパッシブで、1 次デバイスがダウンした時に処理を引き継ぐために待機します。

図 7: アクティブ / パッシブ

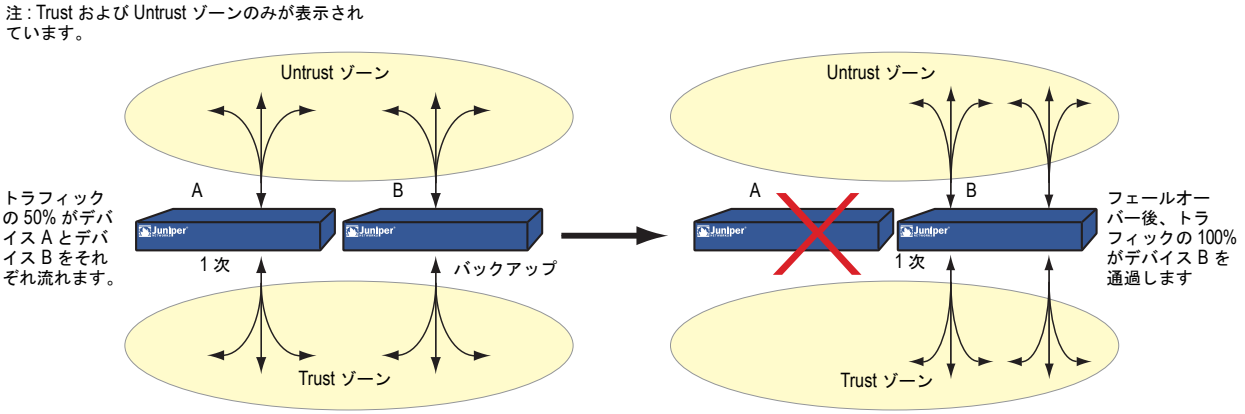


注 : バックアップデバイスは、トラフィックを処理しないという意味ではパッシブですが、1 次デバイスから構成の設定とセッション情報を継続的に同期して受信を行っています。

アクティブ / アクティブ構成

デバイス A およびデバイス B は、それぞれネットワークと VPN のトラフィックの 50% を受信します。デバイス A に障害が発生した場合は、デバイス B が VSD グループ 1 の 1 次デバイスになりますが、依然として VSD グループ 2 の 1 次デバイスでもあるため、トラフィックの 100% を処理します。アクティブ / アクティブ構成のフェールオーバーによって生じるトラフィック転送が 図 8 に示されています。

図 8: アクティブ / アクティブ

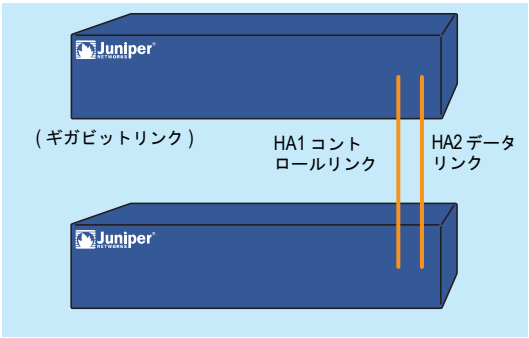


アクティブ / アクティブ構成で 2 つのデバイスの間で分割されたセッションの合計数は、単一のセキュリティデバイスの容量を超えることはできませんが (そうでなければ、フェールオーバー時に超過セッションが消失することがあります)、2 台目のデバイスを追加することによって、利用できる帯域幅は 2 倍になります。また 2 台目 Ã アクティブデバイスは、両方のデバイスのネットワーク接続が正常に機能することを保証します。

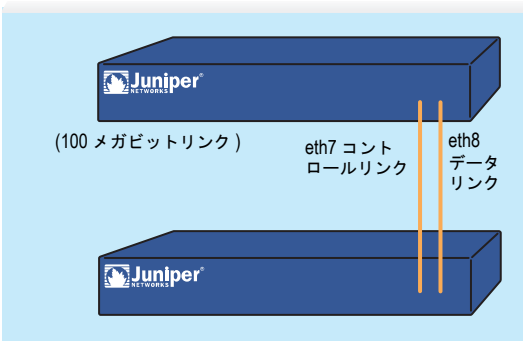
注 : アクティブ / アクティブ構成におけるそれぞれのデバイスは、短時間ならば単一デバイスの容量の 50% を超えるトラフィックバーストに耐えることができまが、その間にフェールオーバーが起こった場合は、超過トラフィックが消失することもあります。

帯域外の帯域幅をより適切に分散するために、HA1 が NSRP コントロールメッセージを処理する一方で、HA2 がネットワークデータメッセージを処理します。ギガビット HA1 および HA2 インターフェースを備えるセキュリティデバイス上でいずれかのポートに障害が発生した場合、残りのアクティブなポートは両方の種類のトラフィックを引き受けます。データリンク用に 100 メガビットのインターフェースを使用する必要のあるセキュリティデバイスの場合、データリンクに障害が発生すると、アクティブな HA リンクはコントロールメッセージ用の 1 つのみとなります。そのようなデバイス上でコントロールリンクに障害が発生すると、データリンクがコントロールリンクとなり、コントロールメッセージのみを送受信します。図 9 を参照してください。

図 9: 専用高可用性リンクおよびユーザー割り当て高可用性リンク



HA1 または HA2 のいずれかに障害が発生すると、コントロールメッセージとデータメッセージの両方が残りの HA リンクを介して送信されます。

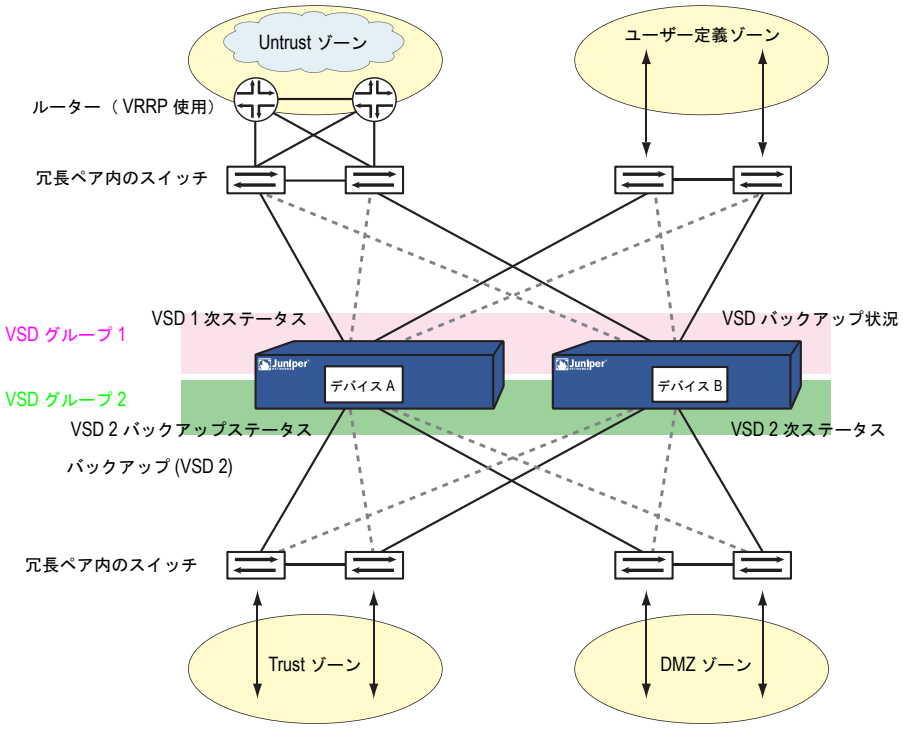


ethernet7 または ethernet8 のいずれかに障害が発生すると、コントロールメッセージのみが残りの HA リンクを介して送信されます。

注 : HA ポート間でスイッチを使用する場合は、転送されるパケットの VLAN タグと競合しないポートベースの VLAN を使用してください。

アクティブ / アクティブ ー フルメッシュ構成

図 10: フォールトトレランスをネットワークに導入



グループメンバー間での設定の同期および各メンバーの現在の VSD グループ状態の通知を実行する NSRP クラスタに加えて、1 組のデバイスの間のランタイムオブジェクト (RTO) の同期の維持を実行する RTO のミラーグループのメンバーとして、デバイス A とデバイス B を構成するこができます。1 次デバイスがダウンした場合、バックアップは、現在のすべてのセッションを維持することによって、最小限のサービスダウンタイムでただちに 1 次デバイスの役割を引き継ぎます。

注： RTO とは、デバイスの通常動作中にセキュリティデバイスメモリー内に動的に作成されたオブジェクトのことです。RTO によって、デバイスはデバイスの周囲のネットワークを把握し、デバイスのポリシーを実施します。RTO の例としては、TCP/UDP セッション、IPSec フェーズ 2 セキュリティアソシエーション (SA), 、DHCP 割り当て、RSA および DSS 鍵のペア、ARP テーブル、DNS キャッシュがあります。

暗号化および認証ですべての NSRP トラフィックを確保できます。NSRP は DES および MD5 アルゴリズムをサポートします。(これらのアルゴリズムの詳細については、5-6 ページの「プロトコル」を参照してください。)

注： HA ケーブルが、あるセキュリティデバイスから他のセキュリティデバイスまでを直接 (その他の種類のネットワークトラフィックを転送するスイッチを介してではなく) 接続している場合は、暗号化や認証を利用する必要はありません。

簡易ネットワーク管理プロトコル (SNMP) を使用してセキュリティデバイスを監視しようとする場合は、NSRP プライベート MIB を http://www.juniper.net/support からダウンロードして、使用することができます。（SNMP の詳細については、3-74 ページの「簡易ネットワーク管理プロトコル」を参照してください。）

NSRP クラスタの認証および暗号化

NSRP は、重要なデータをやり取りする通信のため、暗号化や認証によってすべての NSRP トラフィックのセキュリティを保証することができます。暗号化と認証については、NSRP では DES と MD5 のアルゴリズムがサポートされています。

注 : デバイスが、別のデバイスに直接配線されている場合、認証や暗号化の必要はありません。ただし、デバイスが、他のデバイスが接続されているスイッチを介して配線されている場合、これらの追加セキュリティ実装の考慮が必要な場合があります。

認証や暗号化を使用可能にするには、クラスタの各デバイスにパスワードを提供する必要があります。

WebUI

Network > NSRP > Cluster: 以下を入力して **Apply** をクリックします。

NSRP Authentication Password: (**選択**), *pswd_str*
NSRP Encryption Password: (**選択**), *pswd_str*

CLI

set nsrp auth password *pswd_str*
set nsrp encrypt password *pswd_str*

ランタイムオブジェクト

ランタイムオブジェクト (RTO) とは、通常の動作中にメモリー内に動的に作成されたコードオブジェクトです。RTO の例としては、セッションテーブルエントリ、ARP キャッシュエントリ、DHCP リース、IPSec SA (セキュリティアソシエーション) などがあります。フェールオーバーが起こった際は、サービスが中断されないよう、現在の RTO を新しい 1 次デバイスによって維持することが重要です。

注 : ポリシーを使用して、バックアップするセッションとバックアップしないセッションを指定できます。バックアップしたくないセッションのトラフィックについては、HA セッションのバックアップオプションを使用不可にしてあるポリシーを適用します。WebUI で **HA Session Backup** チェックボックスをクリアにします。CLI では、**set policy** コマンドで、**no-session-backup** 引数を使用します。デフォルトでは、セッションのバックアップは使用可能になっています。

これを可能にするために、RTO は NSRP クラスタのメンバーによってバックアップされています。

それぞれのメンバーは他のメンバーの RTO をバックアップするため、アクティブ / アクティブ HA スキームのいずれかの VSD グループの 1 次デバイスがダウンした場合でも RTO は維持されます。

現在の ScreenOS のリリースでは、NSRP クラスタのメンバー間で RTO の同期を行うために 1 つまたは複数の RTO ミラーグループを構成する必要はありません。セキュリティデバイスをクラスタのメンバーとして定義して RTO 同期を指定すると、ローカルデバイスは RTO の送信および受信ができるようになります。

デフォルトでは、NSRP クラスタメンバーは RTO を同期しません。RTO の同期を使用可能にする前に、最初にクラスタメンバー間で構成を同期する必要があります。クラスタ内の両方のメンバーの構成が同一でない場合は、RTO の同期に失敗することがあります。

RTO 同期を使用可にするには、以下を行います。

WebUI

Network > NSRP > Synchronization: NSRP **RTO Synchronization** を選択してから **Apply** をクリックします。

CLI

```
set nsrp rto-mirror sync
save
```

注： フェールオーバーが起きた場合、たとえその他の VSD グループメンバーの優先順位の方が高くても、1 次デバイスをミラーしているデバイスと交代するのが最も望ましい方法です。ScreenOS の現行リリースでは、1 つの NSRP クラスタで 2 つのデバイスしか存在できないので、この手順は該当しません。

NSRP クラスタで送信側となっているデバイスでの RTO セッション同期を使用不可にするには、以下を行います。

WebUI

Network > NSRP > Synchronization: **NSRP Session Synchronization** を選択解除してから **Apply** をクリックします。

CLI

```
set nsrp rto-mirror session off
save
```

デバイス上でこのコマンドを発行すると、クラスタ内のそのデバイスから他のデバイスへのセッション同期がのみが使用不可になります。

RTO ミラー動作状態

2 台の NSRP クラスタメンバーが RTO のミラー関係を起動する手順は、セット（Set）とアクティブ（Active）という 2 つの動作状態から構成されています。デバイスはこれらの状態を経て、次のように移行します。

1. 最初のデバイスをグループに追加した後、デバイスの状態はセット (*set*) になります。set 状態では、デバイスはピアがグループに参加するのを待ちます。RTO の受信側としては、周期的にレシーバレディメッセージを送信し、自身が利用可能であることを通知します。RTO の送信側としては、同一のクラスタ ID を持つデバイスからレシーバレディメッセージを受け取るまで待機します。

2. ピアを追加し、2 台のデバイスが HA のために正しく配線された後、以下のことが実行されます。

a. 受信者がレシーバレディメッセージを送信しています。

b. 送信側はレシーバレディメッセージを受け取るとただちにグループアクティブメッセージを送信し、状態が *アクティブ*になったことをピアに通知します。

c. 受信側も同様に状態をアクティブに変更します。

送信側から受信側に RTO を転送することに加えて、両方のアクティブミラーはユーザー定義間隔で RTO ハートビートを送信し、動作状態を通知します。

ハートビート間隔を定義するには、以下を行います。

WebUI

Network > NSRP > Link: **Interval** フィールドに値を入力して、**Apply** をクリックします。

CLI

set nsrp rto-mirror hb-interval *number*
save

デバイスが、ピアからの指定された回数の連続したハートビートを受信しなかった場合、デバイスはアクティブ (active) からセット (set) へ状態を変更します。

状態を切り替えるのに必要な消失ハートビートしきい値を定義するには、以下を行います。

WebUI

Network > NSRP > Link: **Threshold** フィールドに値を入力して、**Apply** をクリックします。

CLI

set nsrp rto-mirror hb-threshold *number*
save

注 : 同一の RTO ハートビート設定を維持するために、**set nsrp rto-mirror hb-interval** *番号* および **set nsrp rto-mirror hb-threshold** *番号* CLI コマンドが設定同期されます。

非アクティブな VSI のセッションをクリアしたい場合は、以下を行います。

WebUI

注 : CLI を使用して rto-mirror セッションをクリアする必要があります。

CLI

set nsrp rto-mirror session clear-on-inactive
save

NSRP クラスタの同期

アクティブな NSRP クラスタに新しいデバイスを追加する場合は、1 つ以上の VSD グループの 1 次デバイスから新しいデバイスに設定とファイル (PKI 公開 / 秘密鍵ファイルなど) を同期化する必要があります。設定とファイルが同期化された後、ランタイムオブジェクト (RTO) を同期化する必要があります。クラスタのメンバーが何かの理由で非同期化された場合は、設定、ファイル、RTO を同期化する必要があります。

NSRP では、以下の情報を同期化できます。

- ファイル
- 構成
- ルート
- ランタイムオブジェクト
- システムクロック

ファイルの同期

すべてのファイルを同期化するには

WebUI

注 : ファイルを同期化するには、CLI を使用してください。

CLI

1. **ファイルを同期化します。**
   exec nsrp sync file from peer

   または、1 つのファイルを同期化します。

   exec nsrp sync file name *name_str* from peer

2. **全ライセンスを再適用します。**
   exec license-key update

注 : license-key update は、全ファイルを同期化する場合のみ適用されます。

ローカルおよび CA 認証、鍵ペア、CRL などの PKI オブジェクトを同期化するには、**exec nsrp sync global-config save** CLI コマンドを使用します。

構成同期化

クラスタ内の別のデバイスが再起動している間に、あるデバイスの設定に何らかの変更を加えた場合 (または、すべての HA リンクに障害が発生した場合) は、設定内容が非同期になる可能性があります。

デフォルト設定では、NSRP クラスタ内のデバイスは構成とファイルを同期化しません。この設定は、たとえばすべての設定変更を NetScreen-Security Manager から送り出したい場合に便利です。

設定の自動同期を有効にするには、クラスタ内の全メンバーに **set nsrp config sync** CLI コマンドを使用します（WebUI はこのオプションをサポートしていません）。

自動設定同期化を有効にする前に、たとえば PKI オブジェクトなどのファイルを最初にクラスタメンバー間で手動により同期化されることを推奨します。設定を同期化してもあるクラスタメンバーにその設定内で参照されるファイルが欠落していると、設定はそのメンバーにとって無効になります。そうならないようにするため、最初にファイルを同期化し、それから設定を同期化します。

あるデバイスの設定が別のデバイスの設定と同期していないことを発見するには、**exec nsrp sync global-config check-sum** CLI コマンドを使用します。この出力は、2 台のデバイスの設定が同期しているかどうかを示し、ローカルデバイスとリモートデバイスのチェックムを提供します。

設定が同期していない場合は、**exec nsrp sync global-config save** CLI コマンドを使用して、設定の再同期を行います。設定の同期化の後で、デバイスを再起動する必要があります。

注 : クラスタのアクティブデバイスの設定は、めったに非同期になることはありません。というのは、NetScreen Reliable Transport Protocol (NRTP) は TCP プロトコルに似た、オーバーヘッドが低いものだからです。

ルートの同期化

フェールオーバーが、DRP（動的ルーティングプロトコル）のルートで構成された NSRP アクティブ / パッシブクラスタのデバイスで発生すると、トラフィックは中断され、バックアップデバイスが 1 次になり、そのピアとそのルートテーブルを集約します。ただし、1 次デバイスがルートを同期化するように構成されている場合、バックアップデバイスが 1 次となり、そのピアと集約する時でも、バックアップデバイスはトラフィックを送り続けることができます。

1 次 NSRP デバイス上でルートの同期化を構成すると、ローカルの仮想ルートを持たない VSD インターフェースでルートを設定する必要があります。同期要求がルートにだけ適用されることを除いて、DRP ルートは RTO ミラー同期と同様に同期化されます。

NSRP アクティブ / パッシブクラスタでルート同期化を構成するには、以下を行います。

WebUI

Network > NSRP > Synchronization: **Route Synchronization** を選択し、**Threshold** 値を入力して、**Apply** をクリックします。

CLI

```
set nsrp rto-mirror route number
save
exec nsrp sync rto route from peer
```

ランタイムオブジェクトの同期化

クラスタ内のデバイスの RTO ミラー同期を使用可能にした場合は (40 ページの「手作業での RTO の同期化」を参照)、デバイスの再起動時に RTO は自動的に再同期化します。ただし、(例えば、デバイス上でデバッグや保守を行うために) RTO ミラー同期を使用不可にし、再び RTO 同期を使用可能にする場合は、すべての RTO の再同期を手作業で行う必要があります。

表 5 は、RTO を同期化するのに必要な CLI コマンドを示しています。

WebUI

注： RTO を同期化するには、CLI を使用してください。

表 5: RTO 同期化用 CLI コマンド

同期化方法	CLI コマンド
手動	exec nsrp sync rto all
ARP、DNS、セッションまたは VPN のような選択された RTO	exec nsrp sync rto {...}
自動	set nsrp rto-mirror sync

システムクロックの同期化

NSRP には、NSRP クラスタメンバーのシステムクロックを同期化するための機構が組み込まれています。システムクロックを手作業で設定すると、NSRP 時間同期化機構はメンバーのクロックを適切に同期化した状態に維持します。ただし、ネットワークタイムプロトコル (NTP) を使用してすべてのクラスタメンバーのシステムクロックを設定し、さらに時刻を同期化するために NSRP を使用した場合、時刻は非同期化することがあります。NSRP 同期化の分解能は秒単位ですが、NTP には別の秒単位の分解能があります。各クラスタメンバーの時刻は、処理の遅延により数秒異なることがあるので、NTP がすべてのクラスタメンバーで使用可能になっていて、各メンバーがそれぞれのシステムクロックを NTP サーバーから更新できる場合、NSRP 時間同期化を使用不可にしておくことをお勧めします。NSRP 時間同期化機能を使用不可にするには、**set ntp no-ha-sync** CLI コマンドを使用します。

WebUI

注： システムクロックを同期化するには、CLI を使用してください。

VSD グループ

仮想セキュリティデバイス (VSD) グループとは、2 台で単一の VSD を構成する 1 組の物理セキュリティデバイスです。1 台の物理デバイスが VSD グループの 1 次デバイスとして機能します。VSD の 仮想セキュリティインターフェース (VSI) は、1 次デバイスの物理インターフェースにバインドされています。もう一方の物理デバイスはバックアップとして機能します。1 次デバイスに障害が発生すると、VSD はバックアップにフェールオーバーし、また VSI バインディングはバックアップの物理インターフェースに移動し、ただちに 1 次デバイスに昇格します。

注： 現在のリリースでは、VSD グループには 2 つのメンバーが存在します。今後のリリースでは、3 つの以上のメンバーが存在する可能性があります。このケースでは、1 台のデバイスが 1 次デバイス、もう 1 台のデバイスが 1 次バックアップ、残りの VSD グループメンバーがバックアップとして機能します。

2 台のセキュリティデバイスを 2 つの VSD グループにグループ化し、それぞれの物理デバイスが 1 つのグループの 1 次デバイス、およびもう 1 つのグループのバックアップになることによって、フェールオーバー時に両方のデバイスは互いにバックアップしながらトラフィックをアクティブに処理します。

初期の NSRP 構成では、0 に最も近い優先順位番号を持つ VSD グループメンバーが 1 次デバイスになります。(デフォルトは 100 です。)2 台のデバイスの優先順位値が同じ場合は、MAC アドレスの大きい方のデバイスが 1 次デバイスになります。

プリエンプトオプション

プリエンプトオプションで 1 次デバイスにするデバイスを設定して、高い (ゼロに近い) 優先順位がフェールオーバーを起動できるか決定します。そのデバイスのプリエンプトオプションを使用可能にすると、現在の 1 次デバイスの優先順位の方が低い (ゼロからさらに遠い番号) 場合は、このデバイスが VSD グループの 1 次デバイスになります。このオプションを使用不可にすると、バックアップよりも優先順位の低い 1 次デバイスでも、1 次デバイスのポジションに留まることができます (ただし、内部に問題があったりネットワーク接続に欠陥があるなど、その他の要因によってフェールオーバーが起こる場合は除きます)。

Hold-down 時間を利用してフォールオーバーを遅らせることによって、隣接接続スイッチでポートフリッカが起こった場合の急激なフェールオーバーによる混乱を防ぐことができ、新しい 1 次デバイスが利用できるようになる前に、周囲のネットワークデバイスが新しいリンクをネゴシエートするための十分な時間が確保されます。

VSD グループを設定するには、以下を行います。

WebUI

Network > NSRP > VSD Group > Configuration:

Group ID: **2**
Priority: **1**
Enable Preempt: (**選択**)
Preempt Hold-down Time: **0**
Status: (Read Only)

CLI

set nsrp vsd-group id 2 preempt hold-down 0

メンバー状態

表 6 は、VSD グループのメンバーの状態を説明しています。

WebUI

注： VSD グループメンバーを設定するには、CLI を使用する必要があります。

表 6: VSD グループ状態

状況	説明
Master（マスタ）	VSI に送信されたトラフィックを処理する VSD グループメンバーの状態。1 次デバイスです。
Primary Backup（1 次バックアップ）	1 次デバイスに障害が起きた場合、1 次デバイスになる VSD グループメンバーの状態。選定プロセスでは、デバイスの優先順位を使用しどのメンバーが昇格するかを決定します。新しい 1 次デバイスを選定する場合は、他の VSD グループメンバーの優先度の方が高くても、RTO ピアの方が優先されることに注意が必要です。
Backup（バックアップ）	1 次バックアップの状態を監視し、現在の 1 次バックアップがダウンした場合にバックアップデバイスの 1 つを 1 次バックアップに選定する VSD グループメンバーの状態。
Initial（初期状態）	デバイスの起動時、または **set nsrp vsd-group id** *id_num* コマンドによってデバイスが追加された場合に、VSD グループに参加しようとしている VSD グループメンバーの過渡状態。VSD グループメンバーが初期状態に留まる時間を指定するには、**set nsrp vsd-group init-hold** *number* CLI コマンドを使用します。
Ineligible（不適格状態）	デバイスが選定プロセスに参加できないよう管理者が意図的に VSD グループメンバーに割り当てた状態。VSD グループメンバーを不適格状態に設定するには、**set nsrp vsd-group id id_num mode ineligible** CLI コマンドを使用します。
Inoperable（動作不能状態）	システムチェックによりデバイスの内部問題 (処理ボードがないなど) やネットワーク接続問題 (インターフェースリンクに障害がある場合など) のあることが判明した後の VSD グループメンバーの状態。

初期状態の hold-down 時間を決定するには、初期ホールド値と VSD のハートビート間隔を掛け算します (初期ホールド x ハートビート間隔 = 初期状態の hold-down 時間)。たとえば、初期ホールドが 5 ミリ秒でハートビート間隔が 1000 ミリ秒の場合は、初期状態の hold-down 時間は 5,000 ミリ秒、すなわち 5 秒になります (5 x 1000 = 5000)。

注： VSD ハートビート間隔を小さくする場合は、初期ホールド値を大きくする必要があります。ハートビート間隔の構成については、23 ページの「ハートビートメッセージ」を参照してください。

注： デバイスが、不適格状態 (**exec nsrp vsd-group id** *id_num* **mode backup** コマンドを発行する場合) または動作不能状態 (システムやネットワークの問題が修正された場合) から復帰した場合は、デバイスは、まず初期状態を経過する必要があります。

ハートビートメッセージ

すべての VSD グループメンバーは、たとえ初期、不適格、使用不能の状態になっていたとしても、ハートビートメッセージを間隔ごとに送信することによって、グループメンバーと通信します。これらのメッセージによって、すべてのメンバーは、他のメンバーすべての現在の状態を知ることができます。ハートビートメッセージには、以下の内容が含まれています。

- デバイスのユニット ID
- VSD グループ ID
- VSD グループメンバーステータス (マスタ、1 次バックアップまたはバックアップ)
- デバイス優先順位
- RTO ピア情報

注 : デバイスが動作不能な状態にあり、すべての HA リンクがダウンしている場合は、VSD ハートビートメッセージの 2 次パスを構成しない限り、これらのメッセージは送受信できません。

VSD ハートビートの送信間隔は構成可能です (200、600、800、または 1,000 ミリ秒。デフォルトは 1,000 ミリ秒)。ScreenOS では、VSD グループメンバーが欠けていると見なされる場合を決定するために使用される、ハートビート消失しきい値を構成することもできます。

VSD グループのハートビート値を構成するには、以下を行います。

WebUI

注 : VSD グループのハートビート値を設定するには、CLI を使用する必要があります。

CLI

```
set nsrp vsd-group hb-interval number
set nsrp vsd-group hb-threshold number
```

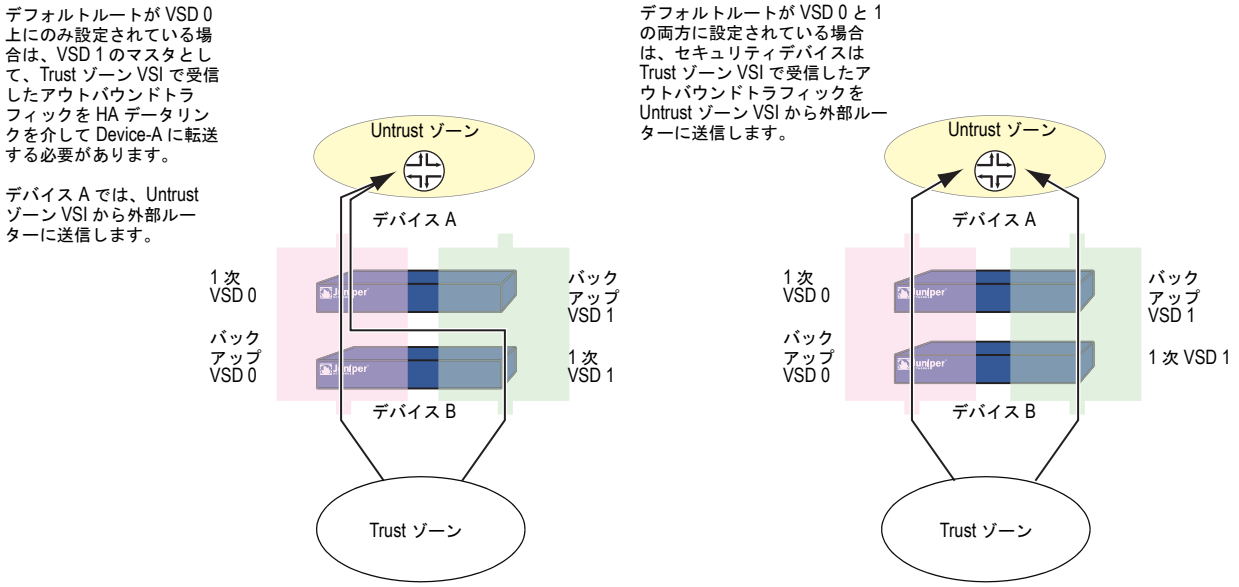
ハートビートメッセージは、HA1 リンクを介して送信されます。HA1 および HA2 インターフェース、相互にやり取りするメッセージの種類に関する詳細については、9 ページの「2 重リンク精査」を参照してください。

VSI と静的ルート

VSD グループの作成後に、仮想セキュリティインターフェース (VSI) を VSD にバインドする必要があります。NSRP クラスタにセキュリティデバイスを組み込む場合は、すべてのセキュリティゾーンインターフェースは自動的に VSD グループ 0 の VSI になります。VSI は、セキュリティデバイス上に設定されたセキュリティゾーンごとに他の ID を持つ VSD に割り当てる必要があります。

デフォルトでは、セキュリティデバイスは VSI の接続サブネットのエントリをルーティングテーブルに追加します。リモートサブネットへの静的ルートを設定する場合、トラフィックを転送したい各 VSI ごとに、ルーティングのエントリをルーティングテーブル内に手動で設定する必要があります。たとえば、2 つの VSD があり、Untrust ゾーン内のルーターへのデフォルトルートを構成しようとする場合は、両方の VSD の Untrust ゾーン VSI 用 のルーティングテーブルエントリを作成する必要があります。単一の VSD (たとえば VSD 0) 上にのみデフォルトルートを設定する場合は、もう一方の VSD (たとえば VSD 1) の 1 次デバイスとして機能するセキュリティデバイスは、そこに送信されたすべてのアウトバウンドトラフィックを HA データリンクを介して VSD 0 の 1 次デバイスとして機能しているデバイスに転送する必要があります。図 11 を参照してください。

図 11: 静的ルートを使用して、VSI を介してトラフィックを転送する



設定例

高可用性を実現するために 2 台のセキュリティデバイスを構成するには、それぞれのデバイスをネットワークに接続し、また両デバイス間で配線し、そして NSRP を使用する HA 用にこれらを構成する必要があります。

このセクションには、以下の NSRP 設定例があります。

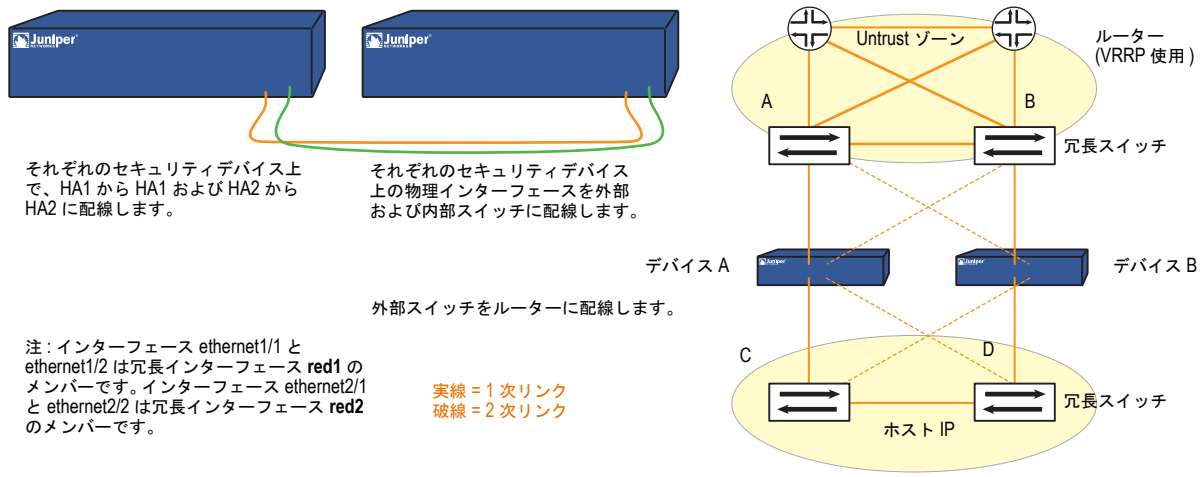
- 25 ページの「アクティブ / アクティブ、フルメッシュ NSRP のためのデバイスの配線」
- 28 ページの「NSRP クラスタの作成」
- 30 ページの「アクティブ / パッシブ NSRP クラスタの構成」
- 34 ページの「アクティブ / アクティブ NSRP クラスタの構成」
- 40 ページの「手作業での RTO の同期化」
- 40 ページの「手動リンク精査の設定」
- 41 ページの「自動リンク精査の設定」

アクティブ / アクティブ、フルメッシュ NSRP のためのデバイスの配線

スイッチ、ルーターまたは Juniper Networks デバイスのいずれの場合でも、シングルポイント障害がないことを保証するので、アクティブ / アクティブ、フルメッシュは、最高水準の可用性を提供します。各デバイスは、接続するスイッチまたはルーターに 2 度配線されます。必要ではありませんが、2 重 HA リンクも各セキュリティデバイス間で接続されます。これにより、各デバイスは、HA リンクの 1 つが切断された場合にも通信を続けることができます。図 12 および図 13 は、2 台のセキュリティバイスをお互いに配線し、内部スイッチと外部スイッチの冗長ペアに配線する様子を示しています。外部スイッチを VRRP を実行している冗長ルーターペアに配線し、これによりフルメッシュ構成が完成します。図 12 は専用インターフェースがある 2 つのセキュリティデバイスを示します。図 13 はネットワークインターフェースを HA トラフィックに使用している 2 つのセキュリティデバイスを示します。

注 : セキュリティデバイスを配備するトポロジ、および使用するスイッチやルーターの種類によっては、図 12 に示す配線は、ユーザーのネットワーク環境で必要となるものとは異なることがあります。

図 12: 専用 HA インターフェースを備えたセキュリティデバイスの配線



フルメッシュ構成での NSRP 用に、次のように 2 台のセキュリティデバイス (デバイス A とデバイス B) を配線します。

デバイス A およびデバイス B: HA リンク

1. それぞれのセキュリティデバイスの HA1 インターフェース同士を配線します。
2. それぞれのセキュリティデバイスの HA2 インターフェース同士を配線します。

デバイス A: Redundant1 (eth1/1 と eth1/2)、Untrust ゾーン

3. ethernet1/1 を外部スイッチ A に配線します (ethernet1/1 は、Untrust ゾーン内の冗長インターフェース red1 にバインドされている 2 つの物理インターフェースの 1 つです)。
4. ethernet1/2 を外部スイッチ B に配線します (ethernet1/2 は Untrust ゾーン内の red1 にバインドされているもう一方の物理インターフェースです)。

デバイス A: Redundant2 (eth2/1 と eth2/2)、Trust ゾーン

5. ethernet2/1 を内部スイッチ C に配線します (ethernet2/1 は Trust ゾーン内の冗長インターフェース red2 にバインドされている 2 つの物理インターフェースの 1 つです)。
6. ethernet2/2 を内部スイッチ D に配線します (ethernet2/2 は Trust ゾーン内の red2 にバインドされているもう一方の物理インターフェースです)。

デバイス B: Redundant1 (eth1/1 と eth1/2)、Untrust ゾーン

7. ethernet1/1 を外部スイッチ B に配線します (ethernet1/1 は Untrust ゾーン内の冗長インターフェース red1 にバインドされている 2 つの物理インターフェースの 1 つです)。
8. ethernet1/2 を外部スイッチ A に配線します (ethernet1/2 は Untrust ゾーン内の red1 にバインドされているもう一方の物理インターフェースです)。

デバイス B: Redundant2 (eth2/1 と eth2/2)、Trust ゾーン

9. ethernet2/1 を内部スイッチ D に配線します (ethernet2/1 は Trust ゾーン内の冗長インターフェース red2 にバインドされている 2 つの物理インターフェースの 1 つです)。
10. ethernet2/2 を内部スイッチ C に配線します (ethernet2/2 は Trust ゾーン内の red2 にバインドされているもう一方の物理インターフェースです)。

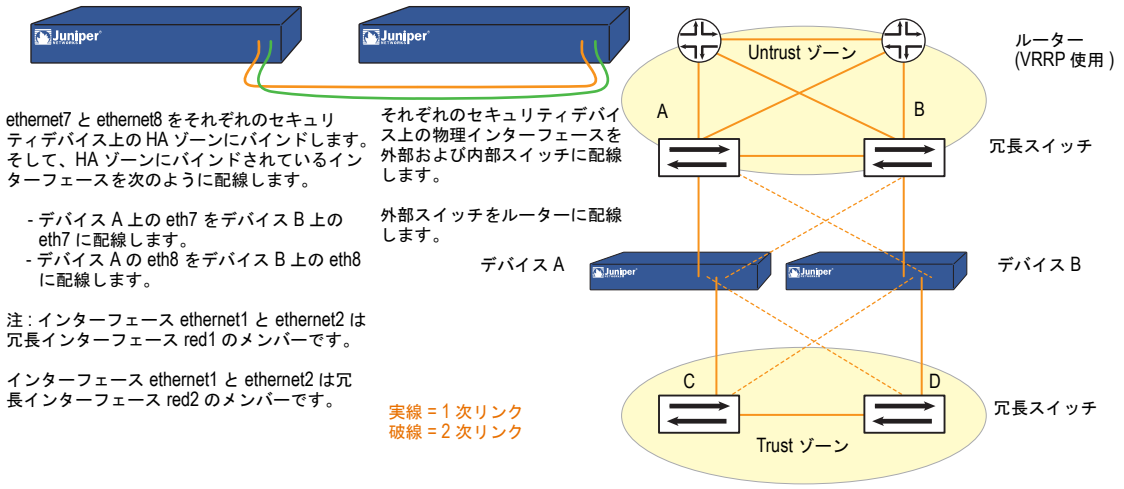
スイッチとルーター

11. 冗長外部スイッチ同士を配線します。

12. セキュリティデバイをスイッチに配線するのに使用した構成と同一の構成で、外部スイッチを冗長ルーターに配線します。

13. 冗長内部スイッチ同士を配線します。

図 13: ネットワークインターフェースを HA リンクに使用するセキュリティデバイスの場合



ethernet7 と ethernet8 を両方のセキュリティデバイス (デバイス A とデバイス B) の HA ゾーンにバインドした後、次のようにフルメッシュ構成で NSRP 用にセキュリティデバイスを配線します。

デバイス A およびデバイス B: HA リンク

1. それぞれのセキュリティデバイスの ethernet7 インターフェース同士を配線します。

2. それぞれのセキュリティデバイスの ethernet8 インターフェース同士を配線します。

デバイス A: Redundant1 (ethernet1 と ethernet2)、Untrust ゾーン

3. ethernet1 を外部スイッチ A に配線します (ethernet1 は Untrust ゾーン内の冗長インターフェース red1 にバインドされている 2 つの物理インターフェースの 1 つです)。

4. ethernet2 を外部スイッチ B に配線します (ethernet2 は Untrust ゾーン内の red1 にバインドされているもう一方の物理インターフェースです)。

デバイス A: Redundant2 (ethernet3 と ethernet4)、Trust ゾーン

5. ethernet3 を内部スイッチ C に配線します (ethernet3 は Trust ゾーン内の冗長インターフェース red2 にバインドされている 2 つの物理インターフェースの 1 つです)。

6. ethernet4 を内部スイッチ D に配線します (ethernet4 は Trust ゾーン内の red2 にバインドされているもう一方の物理インターフェースです)。

デバイス B: Redundant1 (ethernet1 と ethernet2)、Untrust ゾーン

7. ethernet1 を外部スイッチ B に配線します (ethernet1 は Untrust ゾーン内の冗長インターフェース red1 にバインドされている 2 つの物理インターフェースの 1 つです)。

8. ethernet2 を外部スイッチ A に配線します (ethernet2 は Untrust ゾーン内の red1 にバインドされているもう一方の物理インターフェースです)。

デバイス B: Redundant2 (ethernet3 と ethernet4)、Trust ゾーン

9. ethernet3 を内部スイッチ D に配線します (ethernet3 は Trust ゾーン内の冗長インターフェース red2 にバインドされている 2 つの物理インターフェースの 1 つです)。

10. ethernet4 を内部スイッチ C に配線します (ethernet4 は Trust ゾーン内の red2 にバインドされているもう一方の物理インターフェースです)。

スイッチとルーター

11. 冗長外部スイッチ同士を配線します。

12. セキュリティデバイをスイッチに配線するのに使用した構成と同一の構成で、外部スイッチを冗長ルーターに配線します。

13. 冗長内部スイッチ同士を配線します。

NSRP クラスタの作成

ネットワークの信頼性は、組織にとって最重要項目の 1 つです。ネットワークが常に利用可能であることを保証するため、ネットワークデバイスは、冗長なデバイスへフェールオーバーできなければなりません。これに対する最も基礎的な設定は、最初のデバイスが故障した場合に、冗長デバイスが引き継ぎできるよう準備しておくことです（アクティブ / パッシブ）。ScreenOS では、この冗長性は、NSRP クラスタによって保証されます。NSRP クラスタはメンバーごとに異なるホスト名を持つことができるので、フェールオーバーによって SNMP 通信とデジタル証明書の有効性が阻害されることがあります。というのは、SNMP 通信と証明書はデバイスのホスト名によって、正しく機能するからです。

すべてのクラスタメンバーに単一の名前を定義するには、以下の CLI コマンドを入力します。

```
set nsrp cluster name name_str
```

注 : 専用の HA ポートを持たないデバイスでは、NSRP クラスタを構成する前に、インターフェースを HA ゾーンにバインドする必要があります。

セキュリティデバイスの SNMP ホスト名を構成する場合 (**set snmp name** *name_str*)、および PKCS10 証明書要求ファイルで共通名を定義する場合は、クラスタ名を使用します。

クラスタメンバーすべてに単一の名前を使用すると、SNMP 通信およびデジタル証明書利用はデバイスのフェールオーバー後も中断せずに実行されます。

図 14 の例では、NSRP クラスタ ID 1 の NSRP クラスタ内にデバイス A と デバイス B をクラスタ名 “cluster1” でグループ化します。また、それぞれのデバイスで次の設定を指定します。

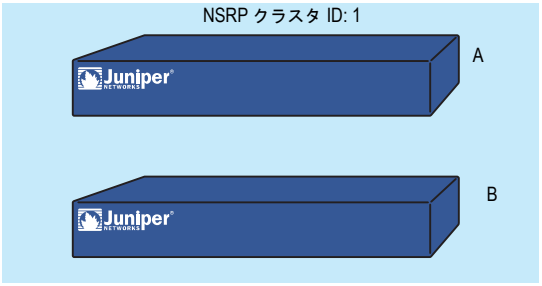
NSRP 通信のセキュリティ設定 : 認証および暗号鍵を作成するためのパスワード (725dCaIgDL と WiJoaw4177) を割り当て、セキュアな NSRP 通信を確保します。

両方のデバイスを同一のクラスタにグループ化し、それらに同一の認証と暗号化パスワードを付与すると、デバイス A またはデバイス B のいずれかに次の設定を入力できます (クラスタ内のデバイスに入力された設定のほとんどは、他のデバイスに同期します。設定同期されないコマンドのリストは、10 ページの表 4 を参照してください)。

- **Interface monitoring:** レイヤー 2 のネットワーク接続のモニターのために、ethernet1 (Untrust ゾーンにバインドされている) および ethernet2 (Trust ゾーンにバインドされている) を選択します。
- **Secondary link:** HA1 と HA2 のリンクの両方がダウンした場合に、ethernet2 インターフェースが VSD ハートビートを伝搬するように指定します。この機能の目的は、両方の HA リンクに障害が発生した場合に VSD グループの 1 次デバイスが複数現れることを防ぐことです。
- **無償 ARP ブロードキャスティング :** ARP ブロードキャストを行う回数を 5 (デフォルトでは 4) に指定します。ARP ブロードキャストにより、フェールオーバーの起動後に、周囲のネットワークデバイスに新しい 1 次デバイスの MAC アドレスを通知します。

(これらのデバイスのすべてのインターフェースは、VSD グループ 0 の VSI になります。20 ページの「VSD グループ」では、これらのデバイスの 2 番目の VSD グループを作成します。)

図 14: NSRP クラスタ



WebUI (デバイス A)

1. **NSRP クラスタおよび通信セキュリティ**
   Network > NSRP > Cluster: 以下を入力して **Apply** をクリックします。

   Cluster ID: 1
   NSRP Authentication Password: (選択) 725dCaIgDL
   NSRP Encryption Password: (選択) WiJoaw4177

注 : クラスタ名は、CLI によってのみ設定できます。

WebUI (デバイス B)

2. **NSRP クラスタおよび通信セキュリティ**
   Network > NSRP > Cluster: 以下を入力して **Apply** をクリックします。

   Cluster ID: 1
   Number of Gratuitous ARPs to Resend: 5
   NSRP Authentication Password: (選択) 725dCaIgDL
   NSRP Encryption Password: (選択) WiJoaw4177

3. **NSRP 設定**
   Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: **ethernet1** と **ethernet2** を選択してから **Apply** をクリックします。

   Network > NSRP > Link: Secondary Link ドロップダウンリストから **ethernet2** を選択してから **Apply** をクリックします。

CLI (デバイス A)

1. **NSRP クラスタおよび通信セキュリティ**
   set nsrp cluster id 1
   set nsrp auth password 725dCaIgDL
   set nsrp encrypt password WiJoaw4177
   save

CLI (デバイス B)

2. **NSRP クラスタおよび通信セキュリティ**
   set nsrp cluster id 1
   set nsrp auth password 725dCaIgDL
   set nsrp encrypt password WiJoaw4177
   save

3. **NSRP 設定**
   set nsrp cluster name cluster1
   set nsrp monitor interface ethernet1
   set nsrp monitor interface ethernet2
   set nsrp secondary-path ethernet2
   set nsrp arp 5
   save

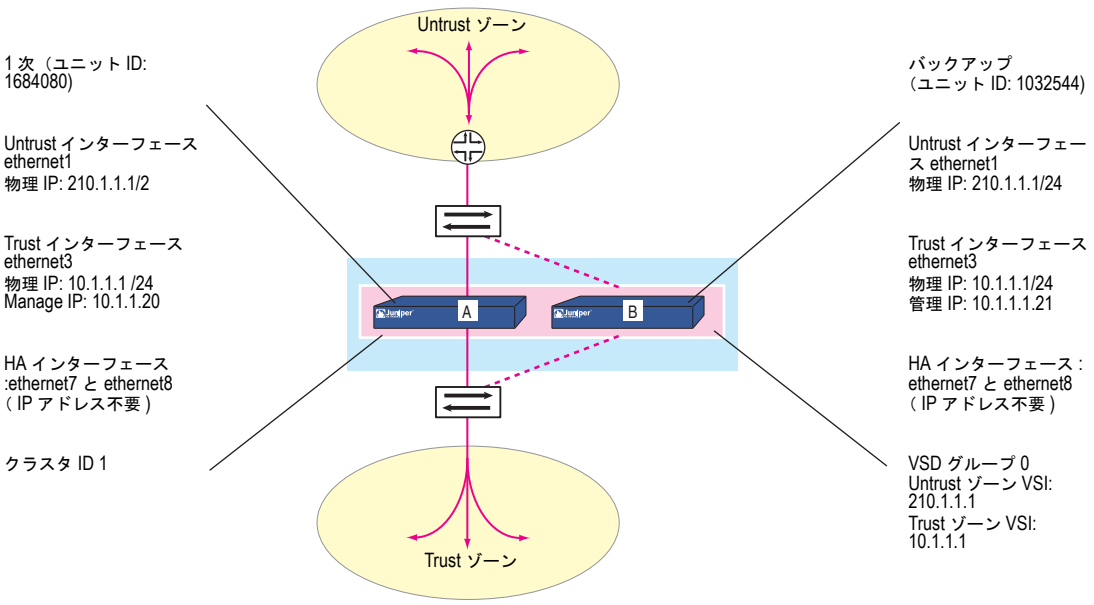
アクティブ/ パッシブNSRP クラスタの構成

図 15 の例では、デバイス A 上の ethernet7 を デバイス B 上の ethernet7 に配線します。同様に、ethernet8 インターフェースを配線します。そして、ethernet7 および ethernet8 を HA ゾーンにバインドします。Trust ゾーンインターフェースの管理 IP アドレスを両方のデバイス上で、すなわちデバイス A 用の 10.1.1.20 およびデバイス B 用の 10.1.1.21 上で設定します。次に、それぞれのデバイスを NSRP クラスタ ID 1 に割り当てます。デバイスが NSRP クラスタのメンバーになると、それらの物理インターフェースの IP アドレスは自動的に VSD グループ ID 0 の仮想セキュリティインターフェース (VSI) の IP アドレスになります。それぞれの VSD メンバーのデフォルト優先順位は 100 で、高いユニット ID を持つデバイスが VSD グループの 1 次デバイスになります

注 : デフォルトでは、ethernet8 は HA ゾーンにバインドされています。HA ゾーンへのバインドは、異なるゾーンにバインド済みでなければ不要です。また、専用の HA ポートを持たないデバイスでは、NSRP クラスタを構成する前に、インターフェースを HA ゾーンにバインドする必要があります。

ethernet1 または ethernet3 のどちらかのポート上でネットワークの接続性が消失すると、デバイスフェールオーバーが起動するように、これらのポートをモニターするデバイスを構成します。さらに、RTO の自動同期を使用可能にします。

図 15: 基本的なアクティブ / パッシブ構成



WebUI (デバイス A)

1. インターフェース

Network > Interfaces > Edit (ethernet7): 次のように入力してから **OK** をクリックします。

Zone Name: HA

Network > Interfaces > Edit (ethernet8): 次のように入力してから **OK** をクリックします。

Zone Name: HA

Network > Interfaces > Edit (ethernet1): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 210.1.1.1/24

Network > Interfaces > Edit (ethernet3): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24
Manage IP: 10.1.1.20

次のように入力してから **OK** をクリックします。

Interface Mode: NAT

2. **NSRP**

Network > NSRP > Monitor > Interface > VSD ID:Device Edit Interface: 以下を入力して **Apply** をクリックします。

ethernet1: (選択); Weight: 255
ethernet3: (選択); Weight: 255

注 : NSRP フェールオーバーしきい値のデフォルト設定は 255 です。そのため、ウェイトが 255 の ethernet1 または ethernet3 が障害を起こすと、デバイスフェールオーバーになります。

Network > NSRP > Synchronization: NSRP **RTO Synchronization** を選択してから **Apply** をクリックします。

注 : 自動 RTO 同期オプションを使用可能にしない場合、CLI コマンド **exec nsrp sync rto all** によって手作業で RTO を同期化することができません。同期化を使用可能にしないと、RTO はドロップされます。

Network > NSRP > Cluster:Cluster ID フィールドに **1** を入力してから **Apply** をクリックします。

WebUI (デバイス B)

3. **インターフェース**

Network > Interfaces > Edit (ethernet7): 次のように入力してから **OK** をクリックします。

Zone Name: HA

Network > Interfaces > Edit (ethernet8): 次のように入力してから **OK** をクリックします。

Zone Name: HA

Network > Interfaces > Edit (ethernet1): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust
Static IP: (ある場合は選択する)
IP Address/Netmask: 210.1.1.1/24

Network > Interfaces > Edit (ethernet3): 以下を入力して **Apply** をクリックします。

Zone Name: Trust
Static IP: (ある場合は選択する)
IP Address/Netmask: 10.1.1.1/24
管理 IP: 10.1.1.21

次のように入力してから **OK** をクリックします。

Interface Mode: NAT

4. **NSRP**

Network > NSRP > Monitor > Interface > VSD ID:Device Edit Interface: 以下を入力して **Apply** をクリックします。

ethernet1: (選択); Weight: 255
ethernet3: (選択); Weight: 255

Network > NSRP > Synchronization: NSRP **RTO Synchronization** を選択してから **Apply** をクリックします。

Network > NSRP > Cluster: Cluster ID フィールドに **1** を入力してから **Apply** をクリックします。

CLI (デバイス A)

1. **インターフェース**

```
set interface ethernet7 zone ha
set interface ethernet8 zone ha
set interface ethernet1 zone untrust
set interface ethernet1 ip 210.1.1.1/24
set interface ethernet3 zone trust
set interface ethernet3 ip 10.1.1.1/24
set interface ethernet3 manage-ip 10.1.1.20
set interface ethernet3 nat
```

2. **NSRP**

```
set nsrp rto-mirror sync
set nsrp monitor interface ethernet1
set nsrp monitor interface ethernet3
set nsrp cluster id 1
save
```

注 : 自動 RTO 同期オプションを使用可能にしない場合、CLI コマンド **exec nsrp sync rto all** によって手作業で RTO を同期化することができません。

監視しているインターフェースのデフォルトウェイトは 255 で、NSRP フェールオーバーしきい値のデフォルト設定は 255 です。そのため、ウェイトが 255 の ethernet1 または ethernet3 が障害を起こすと、デバイスフェールオーバーになります。CLI では、監視しているインターフェースのウェイトを指定しなければ、デフォルト値 (255) がそのまま設定されます。

CLI (デバイス B)

3. インターフェース

```
set interface ethernet7 zone ha
set interface ethernet8 zone ha
set interface ethernet1 zone untrust
set interface ethernet1 ip 210.1.1.1/24
set interface ethernet3 zone trust
set interface ethernet3 ip 10.1.1.1/24
set interface ethernet3 manage-ip 10.1.1.21
set interface ethernet3 nat
```

4. NSRP

```
set nsrp rto-mirror sync
set nsrp monitor interface ethernet1
set nsrp monitor interface ethernet3
set nsrp cluster id 1
save
```

注 : この構成を実行した後、**get nsrp** コマンドを入力し、デバイスが自動的に作成するデフォルト NSRP 設定をチェックします (この設定については、6 ページを参照してください)。

アクティブ/ アクティブNSRP クラスタの構成

セキュリティデバイス同士を配線し、周囲のネットワークデバイスに配線した後、HA のためにこれらのデバイスを設定する必要があります。以下のステップに従い、完全なアクティブ / アクティブ設定を実効します。

1. NSRP クラスタを作成します。この NSRP クラスタでは、VSD グループ 0 の作成が自動的に行われます。
2. クラスタ内に 2 つ目の VSD グループ を作成します。
3. インターフェースモニターおよびパスモニターなどのデバイス障害トラッキング方法を使用可能にします。

図 16 の例では、62 ページの「save」で構成したインターフェースを基にして、ユーザー定義の設定が構成されていない 2 台のセキュリティデバイス（デバイス A とデバイス B）用に、クラスタ ID を 1、クラスタ名を “cluster1” という NSRP クラスタを作成します。

注 : コマンド設定同期を使用可能にするには、最初に各デバイス上でクラスタ ID 番号を定義する必要があります。次に挙げる設定は設定同期されないので、最初にクラスタのそれぞれのデバイスで設定する必要があります。VSD グループ、VSD 優先順位、認証と暗号化パスワード、管理 IP アドレス、トラック IP を設定します。その他のすべてのコマンドは、クラスタ内のデバイス間で設定同期します。

NSRP クラスタを作成すると、セキュリティデバイスは自動的に VSD グループ 0 を作成します。VSD グループ 1 を定義します。VSD グループ 0 にはデバイス A 優先順位 1 を割り当て、VSD グループ 1 には優先順位 100 （デフォルト）を割り当てます。VSD グループ 1 にはデバイス B 優先順位 1 を割り当て、VSD グループ 0 には優先順位はデフォルト (100) のままにしておきます。

注 : VSD グループ ID 「0」は VSD 0 の VSI の名前には表示されません。*redundant1:0* の代わりに、VSI は単純に *redundant1* として識別されます。

レイヤー 2 ネットワーク接続用に 2 つの冗長インターフェース redundant1 および redundant2 をモニターするように、インターフェースモニターオプションを設定します。モニターされているインターフェースのいずれかの 1 次インターフェースに障害が発生すると、そのデバイスはただちに 2 次インターフェースにフェールオーバーします。モニターされている冗長インターフェースのメンバーを含む物理インターフェースの両方に障害が発生すると、そのデバイスは他のデバイスにフェールオーバーします。

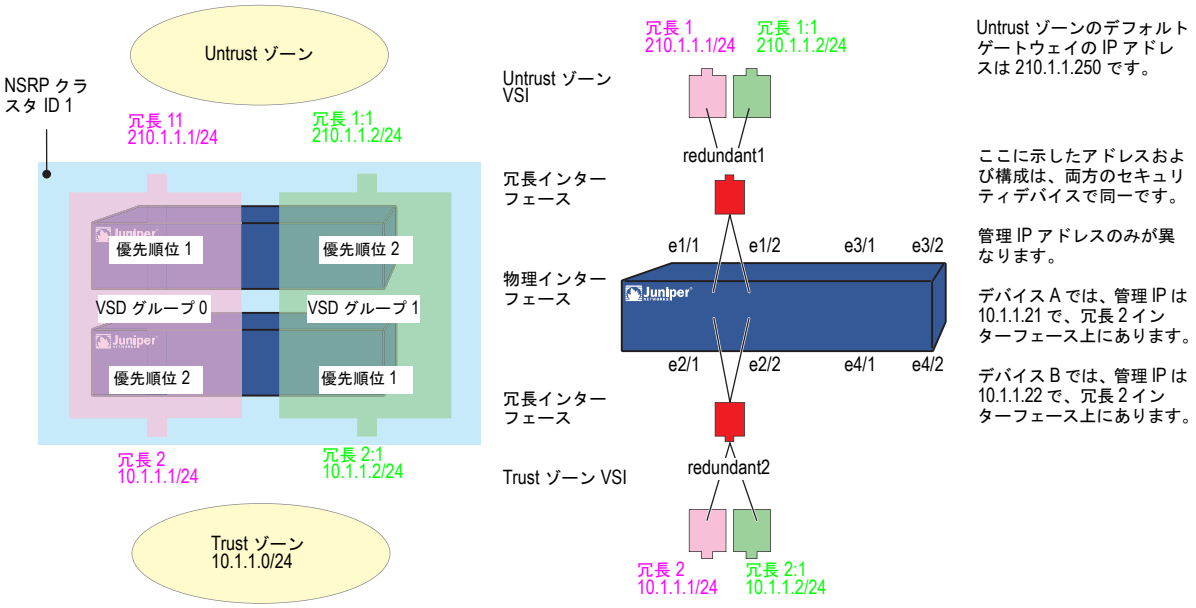
注 : 冗長インターフェースはオプションで、アクティブ / アクティブ構成に必要ではありません。

また、VSD ハートビートメッセージのための 2 次リンクとして ethernet2/1 を定義し、デバイスフェールオーバーが起こった後の Gratuitous ARP の回数を 5 回に定義します。HA ケーブルは 2 台のセキュリティデバイスを直接接続するため、NSRP クラスタのメンバー間の通信は、認証や暗号化は行いません。

また、Untrust ゾーン VSI ごとにデフォルトゲートウェイ (210.1.1.250) へのルート、および Trust ゾーン VSI ごとに内部ネットワークへのルートを設定します。セキュリティゾーンはすべて trust-vr ルーティングドメインにあります。

最後に、両方のデバイスの構成が同期化された後に、RTO 同期化を使用可能にします。

図 16: アクティブ / パッシブ NSRP 構成



WebUI (デバイス A)

1. **クラスタと VSD グループ**
   Network > NSRP > Cluster: Cluster ID フィールド内に **1** を入力してから **Apply** をクリックします。

   Network > NSRP > VSD Group > Edit (Group ID 0): 次のように入力してから **OK** をクリックします。

   Priority: 1
   Enable Preempt: (**選択**)
   Preempt Hold-Down Time (sec): 10

注 : hold-down 時間は、0 から 255 までの任意の長さが可能で、フォールオーバーを遅延させ、急激なフェールオーバーの繰り返しによる混乱を防ぐために効果的です。

Network > NSRP > VSD Group > New: 次のように入力してから **OK** をクリックします。

Group ID: 1
Priority: 100
Enable Preempt: (**オフ**)
Preempt Hold-Down Time (sec): 0

WebUI (デバイス B)

2. **クラスタと VSD グループ**
   Network > NSRP > Cluster: 以下を入力して **Apply** をクリックします。

   Cluster ID: 1
   Number of Gratuitous ARPs to Resend: 5

注 : クラスタ名は、CLI によってのみ設定できます。

この設定では、デバイスのフェールオーバー後、新しい VSD グループ 1 次デバイスは 5 つの Gratuitous ARP パケットを送信し、VSI の関連付けと新しい 1 次デバイスへの仮想 MAC アドレスを通知します。

Network > NSRP > Link: Secondary Link ドロップダウンリストから **ethernet2/1** を選択し、**Apply** をクリックします。

注 : HA1 と HA2 のリンクが両方とも消失した場合は、VSD ハートビートメッセージは Trust ゾーン内の ethernet2/1 を通過します。

Network > NSRP > Synchronization: NSRP **RTO Synchronization** を選択してから **Apply** をクリックします。

Network > NSRP > VSD Group > New: 次のように入力してから **OK** をクリックします。

Group ID: 1
Priority: 1
Enable Preempt: (**選択**)
Preempt Hold-Down Time (sec): 10

3. **冗長インターフェースおよび管理 IP**
   Network > Interfaces > New Redundant IF: 次のように入力してから **OK** をクリックします。

   Interface Name: redundant1
   Zone Name: Untrust
   IP Address/Netmask: 210.1.1.1/24

   Network > Interfaces > Edit (ethernet1/1): "As member of" ドロップダウンリストから **redundant1** を選択して **OK** をクリックします。

   Network > Interfaces > Edit (ethernet1/2): "As member of" ドロップダウンリストから **redundant1** を選択して **OK** をクリックします。

   Network > Interfaces > New Redundant IF: 以下を入力して **Apply** をクリックします。

   インターフェース名 : redundant2
   Zone Name: Trust
   IP Address/Netmask: 10.1.1.1/24
   > 管理 IP フィールドに **10.1.1.22** と入力してから **OK** をクリックします。

   Network > Interfaces > Edit (ethernet2/1): "As member of" ドロップダウンリストから **redundant2** を選択して **OK** をクリックします。

   Network > Interfaces > Edit (ethernet2/2): "As member of" ドロップダウンリストから **redundant2** を選択して **OK** をクリックします。

   Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: **redundant1** および **redundant2** を選択してから **Apply** をクリックします。

4. **仮想セキュリティインターフェース**
   Network > Interfaces > New VSI IF: 次のように入力してから **OK** をクリックします。

   Interface Name: VSI Base: Redundant1
   VSD Group: 1
   IP Address/Netmask: 210.1.1.2/24

   Network > Interfaces > New VSI IF: 次のように入力してから **OK** をクリックします。

   Interface Name: VSI Base: Redundant2
   VSD Group: 1
   IP Address/Netmask: 10.1.1.2/24

5. **ルート**
   Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (選択)
   Interface: redundant1
   Gateway IP Address: 210.1.1.250

Network > Routing > Routing Entries > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address: 0.0.0.0/0
Gateway: (選択)
Interface: redundant1:1
Gateway IP Address: 210.1.1.250

WebUI (デバイス A)

6. 管理 IP アドレス

Network > Interfaces > Edit (redundant2): 管理 IP フィールドに **10.1.1.21** と入力してから **OK** をクリックします。

7. RTO 同期化

Network > NSRP > Synchronization: NSRP **RTO Mirror Synchronization** を選択してから **Apply** をクリックします。

CLI (デバイス A)

1. クラスタと VSD グループ

```
set nsrp cluster id 1
set nsrp vsd-group id 0 preempt hold-down 10
set nsrp vsd-group id 0 preempt
set nsrp vsd-group id 0 priority 1
set nsrp vsd-group id 1
set nsrp rto-mirror sync
save
```

注 : hold-down 時間は、0 から 255 までの任意の長さが可能で、フォールオーバーを遅延させ、急激なフェールオーバーの繰り返しによる混乱を防ぐために効果的です。

CLI (デバイス B)

2. クラスタと VSD グループ

```
set nsrp cluster id 1
set nsrp cluster name cluster1
set nsrp rto-mirror sync
set nsrp vsd-group id 1 priority 1
set nsrp vsd-group id 1 preempt hold-down 10
set nsrp vsd-group id 1 preempt
set nsrp secondary-path ethernet2/1
set nsrp arp 5
set arp always-on-dest
```

注 : デバイス A とデバイス B はともに同じ NSRP クラスタのメンバーであるため、以降、デバイス B に入力するコマンド (注に示したものを除く) はすべてデバイス A に設定同期します。

例では **set nsrp vsd-group id 1 priority 1** および **set nsrp vsd-group id 1 preempt hold-down 10** コマンドは設定同期されません。

HA1 と HA2 のリンクが両方とも消失した場合は、VSD ハートビートメッセージは Trust ゾーン内の ethernet2/1 を通過します。

set nsrp arp 5 設定では、デバイスのフェールオーバー後、新しい VSD グループ 1 次デバイスは 5 つの Gratuitous ARP パケットを送信し、VSI の関連付けと新しい 1 次デバイスへの仮想 MAC アドレスを通知します。

set arp always-on-dest コマンドを入力した後、セキュリティデバイスは、生成元のイーサネットフレームのソース MAC から学習するかわりに、常に ARP ルックアップを実行して宛先 MAC アドレスを学習します。この例における外部ルーターは VRRP を実行している仮想ルーターとしてグループ化されます。このルーターから送信されるフレームは、ソース IP に仮想 IP アドレスを使用しますが、ソース MAC には物理 MAC アドレスを使用します。ルーターがフェールオーバーし、セキュリティデバイスが受信フレーム内のソース MAC から MAC を学習した場合は、返信トラフィックが誤った場所に転送されてしまう場合があります。宛先 MAC のために ARP ルックアップを実行することによって、セキュリティデバイスは新しい物理 MAC アドレスに正しくトラフィックを送信できます。

3. **冗長インターフェースおよび管理 IP**
```
set interface redundant1 zone untrust
set interface redundant1 ip 210.1.1.1/24
set interface ethernet1/1 group redundant1
set interface ethernet1/2 group redundant1
set interface redundant2 zone trust
set interface redundant2 ip 10.1.1.1/24
set interface redundant2 manage-ip 10.1.1.22
set interface ethernet2/1 group redundant2
set interface ethernet2/2 group redundant2
set nsrp monitor interface redundant1
set nsrp monitor interface redundant2
```

4. **仮想セキュリティインターフェース**
```
set interface redundant1:1 ip 210.1.1.2/24
set interface redundant2:1 ip 10.1.1.2/24
```

5. **ルート**
```
set vrouter trust-vr route 0.0.0.0/0 interface redundant1 gateway 210.1.1.250
set vrouter trust-vr route 0.0.0.0/0 interface redundant1:1 gateway 210.1.1.250
save
```

CLI (デバイス A)

6. **管理 IP アドレス**
```
set interface redundant2 manage-ip 10.1.1.21
```

7. **RTO 同期化**
```
set nsrp rto-mirror sync
save
```

手作業での RTO の同期化

デバイス上の RTO が非同期になり、RTO 同期を使用可能にしていない状況があります。このような場合では、動的な情報がすべて全デバイスに渡ってミラーリングされるように、RTO を手動で同期化しなければなりません。

この例では、デバイス A と デバイス B が NSRP クラスタ 1 および VSD グループ 1 と VSD グループ 2 内にあります。デバイス A は VSD グループ 1 の 1 次デバイスで、VSD グループ 2 のバックアップです。デバイス は VSD グループ 2 の 1 次デバイスで、VSD group 1 のバックアップです。

デバイス B 上で何らかのトラブルシュートを行う予定であり、ネットワークからこのデバイスを切断するのを避けます。デバイス B を VSD グループ 2 のバックアップにしてから、RTO 同期化を使用不可にします。デバイス A が両方の VSD グループの 1 次デバイスになります。デバイス B のトラブルシュートを終えた後、再び RTO ミラー同期を使用可能にした後、デバイス A からデバイス B への RTO の再同期を手作業で行います。最後に、デバイス B を VSD グループ 2 の 1 次デバイスに再割り当てします。

WebUI

注 : 手作業での RTO の同期化は、CLI によってのみ可能です。

CLI

デバイス B

```
exec nsrp vsd-group id 2 mode backup
unset nsrp rto-mirror sync
```

デバイス B では、トラフィックの処理およびデバイス A との RTO の同期が停止されました。この時点で、デバイス A のトラフィック処理性能に影響を及ぼさずにデバイス B のトラブルシュートを行うことができます。

```
set nsrp rto-mirror sync
exec nsrp sync rto all from peer
exec nsrp vsd-group id 2 mode master
```

手動リンク精査の設定

この例では、セキュリティデバイスの ethernet7 および ethernet8 インターフェースが HA ゾーンにバインドされています。5 つのリンク精査を ethernet8 インターフェースからピアの MAC 00e02000080 アドレスに送信するように設定します。(MAC アドレスを指定しない場合、デフォルトの NSRP MAC アドレスが使用されます。)

WebUI

注 : HA リンク上で手動で精査を送信するには、CLI を使用する必要があります。

CLI

```
exec nsrp probe ethernet8 00e02000080 count 5
```

自動リンク精査の設定

HA リンクが実際には NSRP 構成で最も弱いリンクである可能性がある場合があります。これは、Juniper デバイスにはリンクがアクティブであるように見えても、そのリンクがダウンしているからです。このような場合、各デバイスだけでなくそれらを接続する HA リンクの状態も、一貫してチェックすることが重要です。この例では、セキュリティデバイスの ethernet7 および ethernet8 インターフェースが HA ゾーンにバインドされています。リンク精査が両方のインターフェースに 3 秒間隔で自動的に送信されるように構成します。さらに、4 回連続して要求を送信してもピアから応答がなければ、HA リンクが動作していないと解釈されるようにしきい値を設定します。

WebUI

Network > NSRP > Link: 以下を入力して **Apply** をクリックします。

Enable HA Link Probe: (選択)
Interval: 3
Threshold: 5

CLI

```
set nsrp ha-link probe interval 3 threshold 5
```

第 2 章

インターフェースの冗長性およびフェールオーバー

本章では、セキュリティデバイスがインターフェースの冗長性およびフェールオーバーを提供するさまざまな方法について説明します。本章のセクションは、以下のようになります。

- 43 ページの「冗長インターフェースとゾーン」
- 46 ページの「インターフェースフェールオーバー」
- 52 ページの「フェールオーバーのトリガーを監視する NSRP オブジェクト」
- 57 ページの「仮想セキュリティデバイスグループのフェールオーバー」
- 58 ページの「仮想システムのフェールオーバー」
- 59 ページの「デバイスフェールオーバー」
- 60 ページの「構成例」

冗長インターフェースとゾーン

HA インターフェースの冗長性を確保するため、Juniper Networks セキュリティデバイスでは専用の物理冗長 HA インターフェースを提供したり、ユーザーが 2 つの汎用インターフェースを HA ゾーンにバインドしたりできるようになっています。また、このセクションで説明されているように、冗長セキュリティゾーンインターフェースを作成することもできます。

VSI に対して、1 台のデバイスの物理インターフェースから別のデバイスの物理インターフェースにバインドをシフトできるように仮想化を適用すると、冗長インターフェースでは同一デバイス上の一方の物理インターフェースから他方の物理インターフェースへとバインドを変更できます。たとえば、1 次インターフェースからスイッチへのリンクが切断されると、リンクは 2 次インターフェースにフェールオーバーし、VSD 1 次デバイスから VSD バックアップへのデバイスのフェールオーバーを防ぎます。

WebUI または CLI で冗長インターフェースを作成することができます。

WebUI

Network > Interfaces > New Redundant IF: 次のように入力してから **OK** をクリックします。

Interface Name: redundant1
Zone Name: Untrust
IP Address/Netmask: 210.1.1.1/24

CLI

set interface redundant1 zone untrust

ホールドダウンタイム設定

インターフェースフェールオーバーが発生した後に、物理インターフェースが 1 次インターフェースになるまで待機するホールドダウンタイムも設定することができます。冗長インターフェースのメンバーにホールドダウンタイムを設定するには、インターフェース名が物理インターフェース名となっている次のコマンドを使用します。**set interface** *interface* **phy holddown** *number*。図 17 を参照してください。

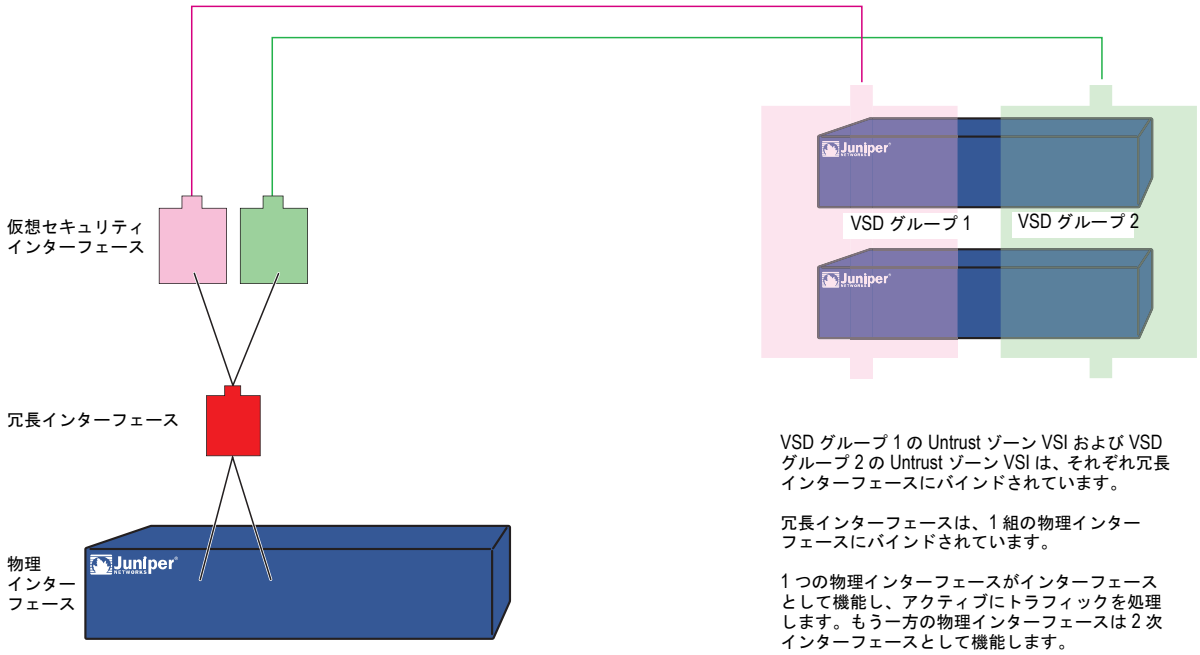
注： インターフェースを冗長グループのメンバーにする前にこのコマンドを入力する必要があります。

次のいずれかのタイプのインターフェースに VSI をバインドすることができます。

- サブインターフェース
- 物理インターフェース
- 2 つの物理インターフェースに順にバインドされる冗長インターフェース
- ループバックインターフェース

注： 冗長インターフェースにサブインターフェースまたはループバックインターフェースをグループ化することはできません。しかし、サブインターフェース上に VLAN を定義するのと同じ方法で、冗長インターフェース上に VLAN を定義することができます。

図 17: 物理、冗長および仮想セキュリティインターフェースの関係



統合インターフェース

統合セキュリティゲートウェイ (ISG) システムなどのいくつかのシステムプラットフォームおよび NetScreen-5000 システムでは、1 つまたは 1 つ以上の物理ポートペアのスループットを組み合わせて、単一の仮想ポートに送ることができます。この仮想ポートは*統合インターフェース*と呼ばれます。セキュアポートモジュール (SPM) のみがこの機能をサポートし、同じモジュール内に存在する、隣接するポートだけを統合できます。

注 : I/O にわたり統合することはできません。

---

2 つの 2 ギガビットポートを統合して、1 つの全二重 4 ギガビットパイプを作成することができます。また、8 つの高速イーサネットポートを 1 つの全二重 1.6 ギガビットパイプ統合することもできます。

統合インターフェースには、次の名前の 1 つを割り当てます。**aggregate1**、**aggregate2**、**aggregate3**、あるいは **aggregate4**。

注 : 他のほとんどのポートやインターフェースと同じように統合インターフェースにも IP アドレス を割り当てて、ネットワーク上の他のホストが接続できるようにする必要があります。

以下の例では、それぞれが 1 Gbps で動作している 2 つの Gigabit Ethernet mini-GBIC ポートを組み合わせ、2-Gbps で動作する統合インターフェース aggregate1 を作成します。この統合インターフェースは 5000-8G SPM (Slot 2 に存在) 上の Ethernet ポート 1 とポート 2 から成っており、Trust ゾーンにバインドされています。

注： システムで使用できる物理ポートを確認するには、WebUI で Network > Interfaces 画面を表示するか、CLI コマンド **get interface** を入力します。

WebUI

Network > Interfaces > Aggregate IF > New: 以下を入力して **Apply** をクリックします。

Interface Name: aggregate1
Zone Name: Trust (**選択**)
IP Address/Netmask: 10.1.1.0/24

次のように入力してから **OK** をクリックします。

Interface Mode: NAT

Network > Interfaces > Edit (ethernet2/1): 次のように入力してから **OK** をクリックします。

As member of: aggregate1 (**選択**)

Network > Interfaces > Edit (ethernet2/2): 次のように入力してから **OK** をクリックします。

As member of: aggregate1 (**選択**)

CLI

```
set interface aggregate1 zone trust
set interface aggregate1 ip 10.1.1.0/24
set interface aggregate1 nat
set interface ethernet2/1 aggregate aggregate1
set interface ethernet2/2 aggregate aggregate1
save
```

インターフェースフェールオーバー

Untrust ゾーンにバインドされた 1 次インターフェースと Untrust ゾーンにバインドされたバックアップ インターフェースの両方が存在する場合、WebUI または CLI から手動で 1 次インターフェースからのトラフィックを強制的にバックアップ インターフェースに送ることができます。1 次インターフェースの接続が機能していないのを ScreenOS が 検知した場合に、自動的にバックアップインターフェースにトラフィックを転送するようセキュリティデバイスを構成することも可能です。

バックアップインターフェーストラフィック

この例では、1 次インターフェースのトラフィックを、強制的にバックアップインターフェースで転送するようにします。

WebUI

Network > Untrust Failover: **Failover** を選択して **Apply** をクリックします。次いで **Force to Failover** をクリックします。

CLI

```
set failover enable
save
exec failover force
```

1 次インターフェースが再び使用可能になったとき、WebUI または CLI を使用して、トラフィックをバックアップインターフェースから 1 次インターフェースに切り替える必要があります。

1 次インターフェース トラフィック

先の例では、強制的にフェールオーバーを起こし、1 次インターフェースのトラフィックをバックアップインターフェースで転送するようにしました。この例では、このトラフィックを、元どおり 1 次インターフェースで転送するようにします。

WebUI

Network > Untrust Failover: **Force to Revert** をクリックします。

CLI

```
exec failover revert
```

トラフィックの自動フェールオーバー

この例では、セキュリティが 1 次インターフェースで IP トラッキングに失敗したとき、自動的にフェールオーバーを引き起こし、バックアップインターフェースに切り替えるよう設定します。1 次インターフェースの IP トラッキングが復旧すれば、再び自動的に、1 次インターフェースに切り替えます。

注 : IP トラッキングに失敗したときフェールオーバーを引き起こすよう設定する手順については、50 ページの「IP トラッキングによるインターフェースフォールオーバー」を参照してください。

デフォルトでは、IP トラッキングに失敗してから実際にフェールオーバーを引き起こすまでに、30 秒の猶予時間（ホールドダウンタイム）があります。これは、間欠的な遅延やネットワークの障害により、実際には必要ないのにフェールオーバーが起こってしまうことを防ぐのが目的です。この例では、ホールドダウンタイムを短縮して 20 秒にします。

WebUI

Network > Untrust Failover: 以下を選択して **Apply** をクリックします。

Track IP: (**選択**)
Automatic Failover: (**選択**)
Failover: (**選択**)
Failover Holddown Time: 20

CLI

```
set failover type track-ip
set failover auto
set failover enable
set failover holddown 20
save
```

シリアルインターフェース

デフォルトでは、1 次インターフェース (Untrust または ethernet3 インターフェース) 接続が失敗したとき、WebUI または CLI を使用して強制的に ScreenOS でシリアルインターフェースに切り替え、さらに、1 次インターフェースが再び使用可能になったときに、切り替えて 1 次インターフェースに戻さなければなりません。このインターフェースフェールオーバーが自動的に行われるように構成することができます。さらに、Untrust または ethernet3 インターフェース上の失敗を監視するため IP トラッキングを構成することも可能です。

デフォルトでは、Trust ゾーンから Untrust ゾーンへのトラフィックまたは Untrust ゾーンから Trust ゾーンへのトラフィック用に使用可能にされたポリシーは、シリアルインターフェースへのフェールオーバーの後もまだアクティブな状態です。ただし、一次インターフェースを介したトラフィックが多すぎてダイヤルアップリンクで扱うことができない場合があります。ポリシーを定義するときに、ScreenOS がシリアルインターフェースに切り替えてもポリシーをアクティブにするかどうかを指定することができます。これを WebUI と CLI で構成する方法については 49 ページの「ポリシーの無効化」を参照してください。

デフォルトでは、シリアルインターフェースは Null ゾーンにバインドされているため、バックアップインターフェースとして使用するには明確に Untrust ゾーンにバインドしなければなりません。WebUI を使用してシリアルインターフェースを Untrust ゾーンにバインドすると、ScreenOS は自動的にシリアルインターフェース用のデフォルトルートを追加します。CLI を使用してシリアルインターフェースを Untrust ゾーンにバインドした場合、ScreenOS はシリアルインターフェースにデフォルトルートを*追加しません*。このため、トラフィックがシリアルインターフェースを介す必要がある場合は、明確にシリアルインターフェース用にデフォルトルートを追加しなければなりません。これを WebUI と CLI で構成する方法については 48 ページの「デフォルトルートの削除」を参照してください。

デフォルトルートの削除

WebUI を使用してシリアルインターフェースを Untrust ゾーンにバインドすると、ScreenOS は自動的にシリアルインターフェース用のデフォルトルートを追加します。この例では、WebUI を使用してシリアルインターフェースを Untrust ゾーンにバインドします。次に、シリアルインターフェース用に自動的に作成されたデフォルトルートを削除します。

WebUI

Network > Interfaces > Edit (シリアル): 次のように入力してから **OK** をクリックします。

Zone Name: (選択) Untrust

Network > Routing > Routing Entries: Configure 列で、シリアルインターフェースから 0.0.0.0/0 へのデフォルトルートで **Remove** をクリックします。

デフォルトルートの追加

CLI を使用してシリアルインターフェースを Untrust ゾーンにバインドした場合、ScreenOS はシリアルインターフェースにデフォルトルートを*追加しません*。このため、セキュリティデバイスにシリアルインターフェースを介してトラフィックをルーティングさせる場合は、明確にシリアルインターフェース用にデフォルトルートを追加しなければなりません。この例では、CLI を使用してシリアルインターフェースを Untrust ゾーンにバインドします。次にシリアルインターフェース用に Untrust ゾーンにバインドするデフォルトルートを追加します。

CLI

```
set interface serial zone untrust
set vrouter trust-vr route 0.0.0.0/0 interface serial
save
```

ポリシーの無効化

この例では、1 次インターフェース (ethernet3) を介した Untrust ゾーン への正常なトラフィックに、Trust ゾーン の host22 から FTP を介して Untrust ゾーンの ftp_srv へ転送される大容量のファイルが含まれています。シリアルインターフェースへのフェールオーバーが起きた場合、ダイヤルアップリンクはこのような大容量の FTP トラフィックをドロップする可能性があります。シリアルインターフェースのフェールオーバーが発生し場合は、シリアルインターフェースでは非アクティブになるように構成されたポリシーはいずれも無効になり、ポリシールックアップ手順はその次のポリシーに続きます。

WebUI

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

```
Source Address:
    Address Book Entry: ( 選択 ), host22
Destination Address:
    Address Book Entry: ( 選択 ), ftp_srv
Service: FTP
Action: Permit
```

> Advanced: **Valid for Serial** をクリアして、**Return** をクリックし、拡張オプションを設定して基本構成ページに戻ります。

CLI

```
set policy from trust to untrust host22 ftp_srv ftp permit no-session-backup
save
```

フェールオーバーの監視

1 次インターフェース接続でケーブルが接続されていないなど、物理リンクの問題を ScreenOS が検知した場合、インターフェースフェールオーバーが起きることがあります。次のタイプのインターフェースフェールオーバーも定義できます。

- IP トラッキングを使用して、指定したインターフェース経由で特定の IP アドレスが宛先不明となる場合
- VPN トンネル監視を使用して、1 次 Untrust インターフェースの特定の VPN トンネルが宛先不明となる場合

インターフェースフェールオーバーは次の流れに沿って引き起こされます。

1. セキュリティデバイスは、1 次インターフェースを監視しているインターフェースの障害を検出します。物理的に切断されたか、あるいは IP トラッキングや VPN 監視処理により障害が検出されたと考えられます。
2. セキュリティデバイスは所定の猶予時間だけ待機します。
3. 猶予時間が経過すると、1 次インターフェースをオフ、バックアップインターフェースをオンに切り替え、1 次インターフェースに送り出していたトラフィックもバックアップインターフェースに切り替えます。
4. セキュリティデバイスは DHCP や PPPoE を使って、バックアップインターフェース経由で ISP に接続し直します。

注： セキュリティデバイスが新たに PPPoE 接続を確立するのは、新しい外向きトラフィックを受け取ってからでも、フェールオーバー直後であっても構いません (***set pppoe name*** *name* ***auto-connect***)。

---

1 次インターフェースに復旧する手順は、これとちょうど反対の流れになります。

1. セキュリティデバイスは、1 次インターフェースを監視しているインターフェースが成功したことを確認します。物理的に接続し直されたか、あるいは IP トラッキングや VPN 監視処理により復旧を確認したことになります。
2. セキュリティデバイスは所定の猶予時間だけ待機します。
3. 猶予時間が経過すると、バックアップインターフェースをオフ、1 次インターフェースをオンに切り替え、バックアップインターフェースに送り出していたトラフィックも 1 次インターフェースに切り替えます。
4. セキュリティデバイスは DHCP や PPPoE を使って、1 次インターフェース経由で ISP に接続し直します。

注： 接続し直す ISP は、それまでバックアップインターフェース経由でつながっていた ISP と同じでも、別であっても構いません。

IP トラッキングによるインターフェースフォールオーバー

ある IP アドレスが 1 次 Untrust ゾーンインターフェースから到達不能になったとき、物理リンクがアクティブな場合でもセキュリティデバイスがバックアップ Untrust ゾーンインターフェースにフェールオーバーにするように指定できます。ScreenOS は、レイヤー 3 パスモニタリング、つまり *IP トラッキング* (NSRP で使用するものと同じ) を使用して 1 次インターフェースを通る IP アドレスを監視します。IP アドレスが 1 次 Untrust ゾーンインターフェースを経て到達不能になった場合、セキュリティデバイスはそのインターフェースが停止したものと見なし、そのインターフェースに関連したすべてのルートが非アクティブとなります。1 次 Untrust ゾーンインターフェースが停止状態に変わると、バックアップ Untrust ゾーンインターフェースへのフォールオーバーが生じます。IP トラッキングの構成は、自動インターフェースフェールオーバーを構成せずに行うことが可能です。

アクティブトンネルからバックアップトンネルへのフェールオーバー

リモートの IKE ピアへのセキュリティデバイス上に冗長な双方向 VPN トンネルを構成できます。ある時点を取れば、いずれか一方のトンネルのみが稼動しています。当初は 1 次インターフェースの VPN トンネル (この例では vpn1) が稼動します。1 次トンネルに障害が起こると、フェールオーバー処理により、リモートピアへの VPN トラフィックは、バックアップトンネル (この例では vpn2) に切り替わります。

VPN トンネル監視を使用したインターフェースフェールオーバー

1 次インターフェースにある特定の VPN トンネルが「 down 」状態と判断される場合にインターフェースフェールオーバーが起きるように設定できます。各 VPN トンネルにパーセント単位でフェールオーバーウェイトを指定します。割り当てられたウェイトは、監視している 1 つまたは複数のトンネルの状態が「 down 」になったときのみ作用を開始します。ダウンした VPN トンネルの累計ウェイトが 100 % 以上になると、ScreenOS はバックアップインターフェースにフェールオーバーします。

*ウェイト*または値を VPN トンネルに適用することによって、他のトンネルと比較したそのトンネルの状態の重要度を調整することができます。相対的に重要度の高いトンネルには比較的大きなウェイトを割り当て、相対的に重要度の低いトンネルには比較的小さなウェイトを割り当てることができます。監視している VPN トンネルすべての累計ウェイトが、インターフェースフェールオーバーの起きる時期を左右します。たとえば、ウェイトが 50 の VPN トンネルの障害は、ウェイトが 10 の VPN トンネルの障害よりも 1 次インターフェースのフェールオーバーが起こりやすいといえます。また、「 inactive 」、「 ready 」、または判断不可能な状態のトンネルは割り当てられたウェイトの 50 % がカウントされます。つまり、ウェイト 50 を割り当てたトンネルが非アクティブ状態の場合、インターフェースフェールオーバーに対してカウントされるこのトンネルのウェイトは 25 になります。

バックアップインターフェースへのフェールオーバーが起きたとしても、VPN 監視再入力機能が使用可能な場合、ScreenOS は 1 次インターフェースに新しい VPN トンネルの確立を試みることができます。1 次インターフェースの 1 つまたは複数の VPN トンネルが「 up 」状態に戻り、フェールオーバーウェイトの累計が 100 % 未満になった場合、ScreenOS はトラフィックを 1 次インターフェースに戻すことができます。ScreenOS がバックアップインターフェースから 1 次インターフェースにトラフィックを切り替えることができるように、VPN 監視再入力機能を使用可能にしてください。

フェールオーバーのトリガーを監視する NSRP オブジェクト

NSRP では、特定のオブジェクトを監視してセキュリティデバイスや VSD グループのフェールオーバーを判断することができます。NSRP の監視には次のオブジェクトを含めることができます。

表 7: NSRP 監視オブジェクト

オブジェクトのタイプ	説明
物理インターフェース	物理ポートがアクティブであり、他のデバイスに接続されていることを確認します。
セキュリティモジュール	ご使用のデバイスのセキュリティモジュールがアクティブであることを確認します。
ゾーン	ゾーンの全物理ポートがアクティブであることを確認します。
特定のターゲット IP アドレス	デバイスは、1 オブジェクトにつき最高 16 個の指定 IP アドレスに指定した間隔で ping または ARP 要求を送信し、ターゲットからの応答を監視します。デバイスや指定した VSD グループ用に構成した IP アドレスはすべて単一の監視オブジェクトを形成します。デバイスごとに 1 つの監視オブジェクト、VSD グループもそれぞれ監視オブジェクトを持つことができます。

注 : セキュリティデバイスは、NSRP およびインターフェースベースの監視用に最大 32 の監視オブジェクトを持ち、最大 64 の IP アドレスを追跡することができます。

監視オブジェクトを使用してデバイスや VSD グループのフェールオーバーを構成する場合、次の内容を設定します。

- **デバイスまたは VSD フェールオーバーしきい値** - デバイスまたは VSD グループのフェールオーバーしきい値とは、デバイスの VSD グループや NSRP クラスタのデバイスがバックアップデバイスにフェールオーバーするのに必要とされる、障害が発生した監視オブジェクトの合計ウェイトです。監視オブジェクトすべての障害の累計ウェイトがしきい値を超えると、VSD グループやデバイスはバックアップ VSD グループやバックアップデバイスにフェールオーバーします。デバイスまたは VSD のフェールオーバーしきい値は 1 から 255 までの任意の値を設定することができます。デフォルトのしきい値は 255 です。

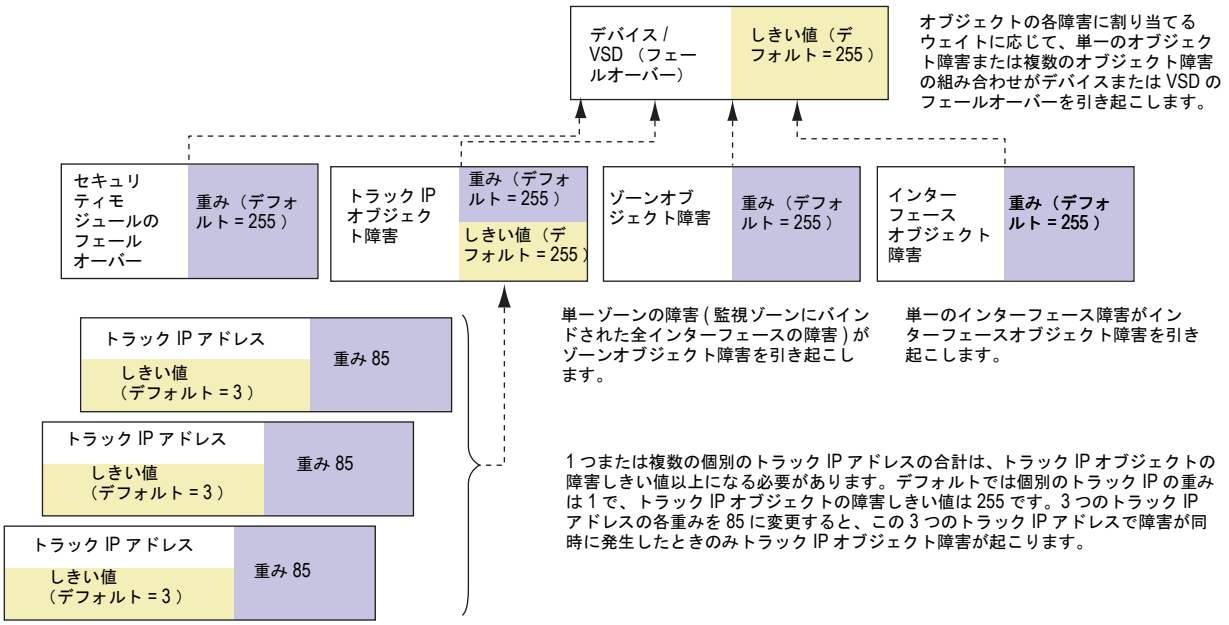
- **各監視オブジェクトの障害ウェイト** - 各監視オブジェクトには構成可能な障害ウェイトがあります。このウェイトは、監視オブジェクトの障害によりデバイスまたは VSD のフェールオーバーしきい値に対して加算されます。このしきい値には、1 から 255 までの任意の値を設定することができます。

トラック IP アドレスでは、個々の IP アドレスとその監視方法を指定する必要があります。また、各トラック IP アドレスの障害とみなされる事柄 (しきい値) と、障害が発生した IP アドレスによって加算されるウェイトも定義する必要があります。トラック IP オブジェクトには、障害しきい値も指定します。このしきい値は、障害が発生したトラック IP アドレスの合計ウェイトで、トラック IP オブジェクトで障害が発生したとみなされるのに必要な値です。

VSD グループ用に監視されているオブジェクトは、デバイス用に監視されているオブジェクトとは無関係です。このため、VSD グループ用とデバイス用に異なるセットのオブジェクト、ウェイト、しきい値を構成できます。また、異なる VSD グループに別個の監視オブジェクトのセットを構成することもできます。たとえば、2 つの VSD グループに同じ監視オブジェクトを構成し、各 VSD グループでオブジェクトに対して異なるウェイトやしきい値を指定することができます。

図 18 は、さまざまな監視オブジェクトの、デバイスや VSD グループのフェールオーバーに対する関係を示しています。障害が発生した監視オブジェクトすべてのウェイトが、デバイスまたは VSD フェールオーバーのしきい値に対して加算されます。監視オブジェクトのデフォルトウェイトや、デバイスまたは VSD フェールオーバーのしきい値を変更しない場合、どの監視オブジェクトの障害によってもデバイスまたは VSD のフェールオーバーが起きる可能性があります。トラック IP アドレスでは、障害が発生したすべてのトラック IP アドレスのウェイトが、トラック IP オブジェクトの障害しきい値に対して加算されます。トラック IP オブジェクトの障害しきい値に達した場合、トラック IP オブジェクトの障害ウェイトがデバイスまたは VSD フェールオーバーのしきい値と比較されます。

図 18: オブジェクト監視ウェイトおよびフェールオーバーしきい値



セキュリティモジュール

ご使用のデバイスがセキュリティモジュールを含んでおり、そこで障害が発生した場合、各障害のウェイトを設定できます。これにより、そのデバイス上のセキュリティモジュールに障害が発生した場合に、デバイス全体に障害が発生したとするかどうかを決定する柔軟性が与えられます。この例では、セキュリティモジュール 2 の障害ウェイトを 100 に設定します。

CLI

```
set nsrp monitor sm 2 100
save
```

物理インターフェース

レイヤー 2 パスモニタリングは、物理ポートがアクティブで他のネットワークデバイスに接続しているか確認することによって機能します。ポートがアクティブでなくなると、物理インターフェースオブジェクトの障害が起こります。

この例では、ethernet2/1 でデバイスフェールオーバーの監視を使用可能にします。このインターフェースに対して障害ウェイト 100 を設定します。

WebUI

Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: 以下を入力して **Apply** をクリックします。

Interface Name: ethernet2/1 (**選択**)
Weight: 100

CLI

```
set nsrp monitor interface ethernet2/1 weight 100
save
```

ゾーンオブジェクト

ゾーンオブジェクト障害は、監視ゾーンのインターフェースが *すべて*ダウンした場合にのみ発生します。ゾーン内にアクティブなポートが 1 つでもある限りゾーン障害は起きません。監視ゾーンにインターフェースがバインドされていない場合、ゾーンオブジェクトに障害は発生しません。セキュリティデバイスは常に障害が起こっていないと認識します。ダウンしたインターフェースが監視ゾーンにバインドされている唯一のゾーンの場合、ゾーンオブジェクトに障害が発生します。ゾーンからそのインターフェースをアンバインドすると、ゾーンオブジェクトの障害はなくなります。監視ゾーンからアクティブなインターフェースをアンバインドしたときに、ダウンしたインターフェースが残る場合、そのゾーンオブジェクトは障害が発生しているとみなされます。

この例では、Trust ゾーンでデバイスフェールオーバーの監視を使用可能にします。このゾーンに対して障害ウェイト 100 を設定します。

WebUI

Network > NSRP > Monitor > Zone > VSD ID: Device Edit Zone: 以下を入力して **Apply** をクリックします。

Zone Name: Trust (**選択**)
Weight: 100

CLI

```
set nsrp monitor zone trust weight 100
save
```

トラック IP オブジェクト

IP トラッキングは、ユーザーが定義した間隔で最高 16 個の指定 IP アドレスに ping または ARP 要求を送信し、ターゲットが応答するかどうかを監視することで機能します。IP トラッキングを構成する場合、デバイスは物理インターフェース、冗長インターフェース、またはサブインターフェースにバインドされた管理 IP アドレスから ping または ARP 要求を送信します。(管理 IP アドレスはインターフェースの IP アドレスとは異なる IP アドレスでなければなりません。)IP アドレスのバインディングは複数のデバイスの間を移動できるので、IP トラッキングのためには VSI を使用できないことに注意してください。

注 : ルーターが 仮想ルーター冗長プロトコル (VRRP) を使用する冗長クラスタにグループ化されている場合、1 次デバイスとして機能しているルーターは、(フェールオーバー後の場合など) IP アドレスの所有者でないかぎり仮想 IP アドレスへの ping 要求に応答することはできません。ただし、1 次デバイス仮想ルーターは IP アドレスの所有権にかかわらず、仮想 MAC アドレスをともなった ARP 要求には応答する必要があります (詳細については、RFC 2338 を参照してください)。IP トラッキング時に ARP を使用するには、ポーリングデバイスは管理 IP アドレスと同じ物理サブネット上にある必要があります。

各トラック IP アドレスには以下を指定します。

- **トラック IP 障害しきい値** - 試行失敗と見なされる、特定の IP アドレスからの ping や ARP 応答の引き出しに連続して障害が発生した回数。しきい値を超えないことは、そのアドレスとの接続性が受け入れ可能なレベルであることを示し、しきい値を超えることは受け入れ不可能なレベルであることを示します。しきい値には 1 から 200 までの任意の値を設定することができます。デフォルト値は 3 です。
- **トラック IP 障害ウェイト** - トラック IP アドレスからの応答を引き出すのに障害が発生した場合にトラック IP オブジェクトの障害ウェイトに加算されるウェイト。トラック IP アドレスにウェイトを適用することによって、他のトラック IP アドレスへの到達に対するそのアドレスへの接続性の重要度を調整することができます。相対的に重要度の高いアドレスには大きなウェイトを割り当て、相対的に重要度の低いアドレスには小さなウェイトを割り当てることができます。割り当てられたウェイトは、トラック IP の障害しきい値に達すると、作用し始めます。たとえば、ウェイトが 10 に設定されているアドレスのトラック IP の障害しきい値を超えた場合の方が、ウェイトが 1 に設定されているアドレスのトラック IP 障害に比べて、トラック IP オブジェクト障害ウェイトに加算されるウェイトが多くなります。ウェイトには、1 から 255 までの値を割り当てることができます。デフォルトは 1 です。

また、デバイスまたは VSD のフェールオーバーしきい値に加算されるトラック IP オブジェクトの障害しきい値も構成します。1 つまたは複数のトラック IP アドレスが障害しきい値を超えると、障害が発生した個々のアドレスのウェイトが合計されます。合計数がトラック IP オブジェクトの障害しきい値以上になった場合、トラック IP オブジェクトの障害ウェイトがデバイスまたは VSD フェールオーバーのしきい値に適用されます。トラック IP オブジェクトの障害ウェイトだけがデバイスまたは VSD フェールオーバーしきい値に適用されます。個々のトラック IP アドレスの障害ウェイトがデバイスまたは VSD フェールオーバーしきい値に適用されることはありません。以下の例を考察してみてください。

トラック IP アドレス	障害ウェイト			
10.10.10.250	100	トラック IP オブジェクト障害 しきい値	トラック IP オブジェクト障害 ウェイト	デバイスフェールオーバーしきい値
1.1.1.30	75	125	255	255
2.2.2.40	75			

トラック IP アドレス 10.10.10.250 に障害が発生した場合、トラック IP の障害ウェイト (100) がトラック IP オブジェクトの障害しきい値 (125) と比較されます。トラック IP の障害ウェイトはトラック IP オブジェクトの障害しきい値よりも低いため、トラック IP オブジェクトに障害が発生しているとはみなされません。トラック IP アドレス 1.1.1.30 と 2.2.2.40 の両方に障害が発生した場合、障害ウェイトの合計 (150) がトラック IP オブジェクトの障害しきい値 (125) と比較されます。障害ウェイトの合計がトラック IP オブジェクトの障害ウェイトを超えているため、トラック IP オブジェクトに障害が発生しているとみなされます。トラック IP オブジェクトの障害ウェイト (255) はデバイスフェールオーバーしきい値 (255) と比較されます。トラック IP オブジェクトの障害ウェイトがデバイスフェールオーバーしきい値と等しいため、デバイスはフェールオーバーします。

トラック IP アドレス 10.10.10.250 に障害ウェイト 100 を設定するには、以下を入力します。

WebUI

Network > NSRP > Track IP > New: 次のように入力してから **OK** をクリックします。

Track IP: 10.10.10.250
Weight: 100

CLI

```
set nsrp track-ip ip 10.10.10.250 weight 100
save
```

デバイスフェールオーバー用にトラック IP オブジェクトの障害しきい値を 125 に設定するには、以下のように入力します。

WebUI

Network > NSRP > Monitor > Track IP > VSD ID: Device Edit: 以下を入力して **Apply** をクリックします。

Enable Track IP: (選択)
Failover Threshold: 125

CLI

```
set nsrp monitor track-ip threshold 125
save
```

デバイスフェールオーバー用のトラック IP

2 台のセキュリティデバイスは、アクティブ / アクティブ構成になっています。10 秒ごとに、両方のデバイスは Untrust ゾーンの冗長クラスタ内で VRRP を実行している 2 台の外部ルーターの物理 IP アドレス（ VRRP クラスタを構成する物理ルーター専用のアドレス）に ARP 要求を送信し、また Trust ゾーン内の 2 つの Web サーバーに ping 要求を送信します。トラック IP オブジェクトの障害しきい値は 51 です。トラック IP オブジェクトのウェイトとデバイスフェールオーバーしきい値はデフォルト値 (255) です。トラック IP アドレスのウェイトと障害しきい値は以下のとおりです。

- Untrust ゾーン内の冗長ルーター
  - 210.1.1.250 - Weight: 16, threshold 5
  - 210.1.1.251 - Weight: 16, threshold 5
- Trust ゾーンの Web サーバー
  - 10.1.1.30 - Weight: 10, threshold 3
  - 10.1.1.40 - Weight: 10, threshold 3

あるルーターへ 5 回連続試行した後に ARP 応答を受信しない場合、試行失敗とみなされ、フェールオーバーしきい値の合計にウェイト値 16 が加算されます。あるサーバーへの 3 回連続の試みの後に ping 反応がないことは、試行失敗とみなされ、フェールオーバーのしきい値合計に対して 10 の重みが加算されます。

デバイスフェールオーバーのしきい値は 51 なので、デバイスフェールオーバーが起こるには、4 つのトラック IP アドレスすべてに障害が発生する必要があります。その障害量に耐えるつもりがない場合は、さらに受け入れ可能なレベルまでしきい値を下げることができます。

仮想セキュリティデバイスグループのフェールオーバー

NSRP では、デバイスフェールオーバーに加えて VSD グループフェールオーバーを構成することができます。デバイスフェールオーバーと同じように、監視オブジェクトの 1 つまたは複数に障害が発生した場合、VSD グループのマスタ 次デバイスがそのグループのバックアップデバイスにフェールオーバーします。オブジェクトに関する詳細、およびこれらのオブジェクトを構成する方法については、52 ページの「フェールオーバーのトリガーを監視する NSRP オブジェクト」を参照してください。 VSD フェールオーバーでは、デバイスフェールオーバーと同じオブジェクトを監視するように構成できます。

図 19 の例では、VSD グループの 1 次デバイスにあるポートに障害が発生した場合、必ずしもデバイス全体がバックアップデバイスにフェールオーバーする必要はありません。次の構成では、ethernet 2/1 に障害が発生した場合、VSD 1 はデバイス A の 1 次 VSD グループからデバイス B のバックアップ VSD グループにフェールオーバーします。VSD 2 はアクティブな状態を保ち、デバイス A のセッションをバックアップします。

図 19: VSD グループ 1 フェールオーバー



仮想システムのフェールオーバー

仮想システムがフェールオーバーするためには、仮想システムは VSD グループ内にある必要があります。VSD グループが仮想システムをサポートするためには、仮想システムごとに VSI を作成する必要があります。仮想システムには、独自の Trust ゾーン VSI を持ち、また独自の Untrust ゾーン VSI を持つ場合があります。仮想システムは、Untrust ゾーン VSI をルートレベルと共有することもできます。仮想システムに独自の Untrust ゾーン VSI がある場合は、これらはお互いに異なるサブネット、およびルートレベルの Untrust ゾーン VSI とは異なるサブネット内になければなりません。また、Trust ゾーンの仮想システム VSI は、すべてお互いに異なるサブネット内になければなりません。

表 8 は、アクティブ / アクティブフルメッシュ構成になっている、2 台の セキュリティデバイス（デバイス A とデバイス B）を示しています。デバイス A のルートシステムを VSD 0 の 1 次デバイスとして、デバイス B のルートシステムを VSD グループ 1 の 1 次デバイスとして構成しています。ルートシステム内の VSD 0 および VSD 1 の Trust ゾーン VSI および Untrust ゾーン VSI は以下のとおりです。

表 8: VSD の IP アドレス

VSD グループ 0 の VSI		VSD グループ 1 の VSI	
redundant1	210.1.1.1/24	redundant1:1	210.1.1.2/24
redundant2	10.1.1.1/24	redundant2:1	10.1.1.2/24

デバイスフェールオーバー

1 つの NSRP クラスタに 2 つのセキュリティデバイスを構成すると、1 次デバイスはすべての構成情報と状態情報をバックアップデバイスと同期し、必要な場合にバックアップデバイスが 1 次デバイスの役割を果たせるようにします。たとえば、クラスタ内の 1 次デバイスに障害が発生した場合は、バックアップデバイスが 1 次デバイスに昇格し、トラフィックの処理を引き継ぎます。元の 1 次デバイスが障害発生前の状態に戻った場合は、元の 1 次デバイスが再びトラフィック処理を行います。

NSRP クラスタの 1 次デバイスがバックアップにフェールオーバーする条件は数多くあります。例えば次の物理的問題や、管理者がしきい値やウェイトを導入した場合があります。

- **物理的問題** : システムクラッシュ、停電、ダウンリンク、デバイスの CPU やメモリーボードの取り外し
- **管理者がもたらしたフェールオーバー** : 特定のゲートウェイやサーバーへの接続が失われた場合に、1 次デバイスがバックアップにフェールオーバーすることがあります

NSRP が異なるオブジェクトを監視し、監視オブジェクトの 1 つまたは複数で障害が発生した場合、1 次デバイスのフェールオーバーが起きるように構成できます。これらのオブジェクトに関する詳細、およびこれらのオブジェクトを構成する方法については、51 ページの「VPN トンネル監視を使用したインターフェースフェールオーバー」を参照してください。

クラスタ内でフェールオーバーが重複して発生した場合でも、少なくとも 1 デバイスは 1 次デバイスのままである必要があります。あるデバイスが障害が発生していない、または 1 次デバイスとして不適格になっていないクラスタ内最後のデバイスとして残った場合、そのデバイスは 1 次デバイスとして動作し続けます。特定の条件下では、監視オブジェクトの障害によってクラスタ内の両方のデバイスが不適格状態になり、トラフィックの「ブラックホール」が発生することがあります。少なくとも 1 つのデバイスが 1 次デバイスとして選定されトラフィックを転送できるように、CLI コマンド **set nsrp vsd-group master-always-exist** を発行します。これによって、NSRP オブジェクトの監視のためクラスタ内の全ユニットに障害が発生したと思われる場合でも、NSRP クラスタのデバイスがトラフィックを転送し続けることができます。クラスタ内の全デバイスが同時に障害状態になったと思われる場合は、デバイスに対して構成された優先使用および優先順位の値に基づいて新しい 1 次デバイスが選定されます。

構成例

このセクションには、以下の構成例の手順を示します。

- 60 ページの「デバイスフェールオーバー用のトラック IP の構成」
- 63 ページの「冗長 VPN トンネルの構成」
- 67 ページの「仮想セキュリティインターフェースの構成」
- 70 ページの「2 系統のアクティブなトンネルの構成」
- 74 ページの「トラック IP を使用したインターフェースフォールオーバーの構成」
- 77 ページの「トンネルのフェールオーバーウェイトの構成」
- 83 ページの「仮想システムのフェールオーバーの構成」

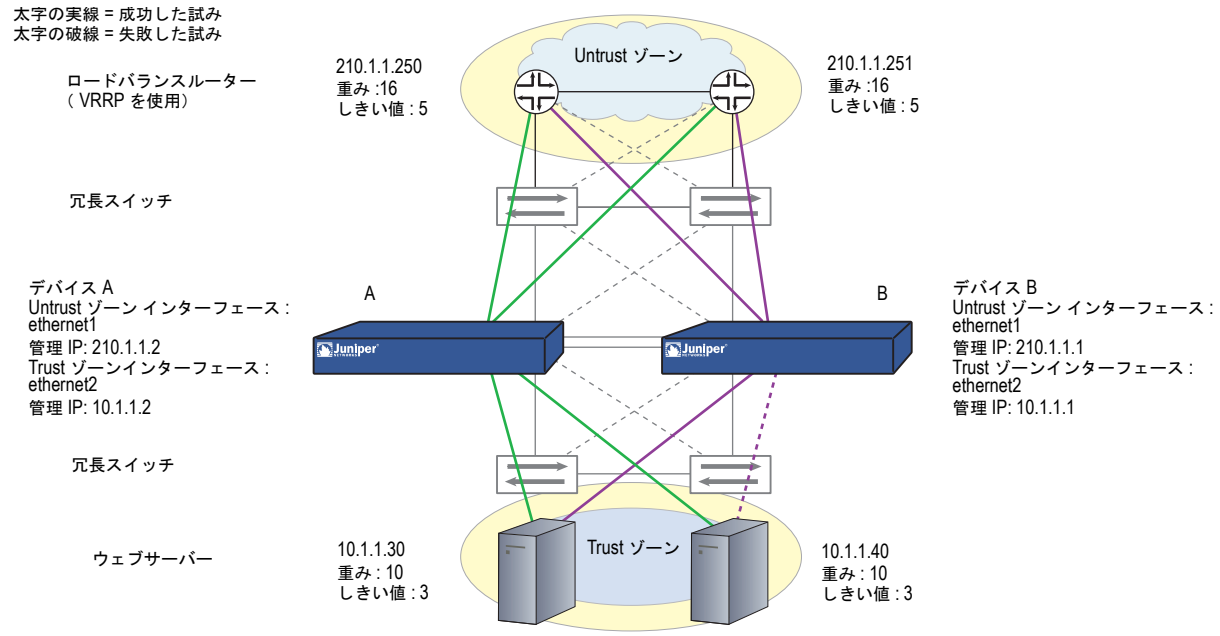
デバイスフェールオーバー用のトラック IP の構成

IP トラッキングの使用は、インターフェース監視およびゾーン監視に加えて、デバイスの障害を追跡するためのオプションです。図 20 の例では、デバイス A の成功率は 100% ですが、デバイス B は 3 回連続で 10.1.1.40 からの応答の受信に失敗し、51 というフェールオーバーのしきい値合計に対して 10 の値が加算されます。

注： NSRP 監視設定はすべて、ローカルユニットにのみ適用されます。トラック IP の設定は、VSD グループ内の他のデバイスには伝播しません。必要な場合はグループ内のすべてのデバイスに同一の設定を入力する必要があります。

両方のデバイス上で、Untrust ゾーンインターフェースは ethernet1、Trust ゾーンインターフェースは ethernet2 です。ethernet1 の管理 IP アドレスは、デバイス A では 210.1.1.1、デバイス B では 210.1.1.2 です。ethernet2 の管理 IP アドレスは、デバイス A では 10.1.1.1、デバイス B では 10.1.1.2 です。セキュリティゾーンはすべて trust-vr ルーティングドメイン内にあります。

図 20: デバイスフェールオーバー用のトラック IP



WebUI

1. **トラック IP アドレス**

   Network > NSRP > Monitor > Track IP > New: 次のように入力してから **OK** をクリックします。

   Track IP: 210.1.1.250
   Method: ARP
   Weight: 16
   Interval (sec): 10
   Threshold: 5
   Interface: ethernet1
   VSD Group ID: Device

   Network > NSRP > Monitor > Track IP > New: 次のように入力してから **OK** をクリックします。

   Track IP: 210.1.1.251
   Method: ARP
   Weight: 16
   Interval (sec): 10
   Threshold: 5
   Interface: ethernet1
   VSD Group ID: Device

   Network > NSRP > Monitor > Track IP > New: 次のように入力してから **OK** をクリックします。

   Track IP: 10.1.1.30
   Method: Ping
   Weight: 10
   Interval (sec): 10
   Threshold: 3
   Interface: ethernet2
   VSD Group ID: Device

Network > NSRP > Monitor > Track IP > New: 次のように入力してから **OK** をクリックします。

Track IP: 10.1.1.40
Method: Ping
Weight: 10
Interval (sec): 10
Threshold: 3
Interface: ethernet2
VSD Group ID: Device

2. **トラック IP オブジェクト障害しきい値**
Network > NSRP > Monitor > Track IP > Edit (VSD: デバイス）: 以下を入力して **Apply** をクリックします。

Enable Track IP: (選択)
Failover Threshold: 51

CLI

1. **トラック IP アドレス**

```
set nsrp track-ip ip 210.1.1.250 interface ethernet1
set nsrp track-ip ip 210.1.1.250 interval 10
set nsrp track-ip ip 210.1.1.250 method arp
set nsrp track-ip ip 210.1.1.250 threshold 5
set nsrp track-ip ip 210.1.1.250 weight 16

set nsrp track-ip ip 210.1.1.251 interface ethernet1
set nsrp track-ip ip 210.1.1.251 interval 10
set nsrp track-ip ip 210.1.1.251 method arp
set nsrp track-ip ip 210.1.1.251 threshold 5
set nsrp track-ip ip 210.1.1.251 weight 16

set nsrp track-ip ip 10.1.1.30 interface ethernet2
set nsrp track-ip ip 10.1.1.30 interval 10
set nsrp track-ip ip 10.1.1.30 method ping
set nsrp track-ip ip 10.1.1.30 threshold 3
set nsrp track-ip ip 10.1.1.30 weight 10

set nsrp track-ip ip 10.1.1.40 interface ethernet2
set nsrp track-ip ip 10.1.1.40 interval 10
set nsrp track-ip ip 10.1.1.40 method ping
set nsrp track-ip ip 10.1.1.40 threshold 3
set nsrp track-ip ip 10.1.1.40 weight 10
set nsrp track-ip
```

注 : デフォルトでは、ping を行うことは IP トラッキングの方法で、トラック IP の障害しきい値は 3 です。そのため、これらのしきい値を指定する必要はありません。コマンド **set nsrp track-ip ip 10.1.1.30** と **set nsrp track-ip ip 10.1.1.40** で十分です。

---

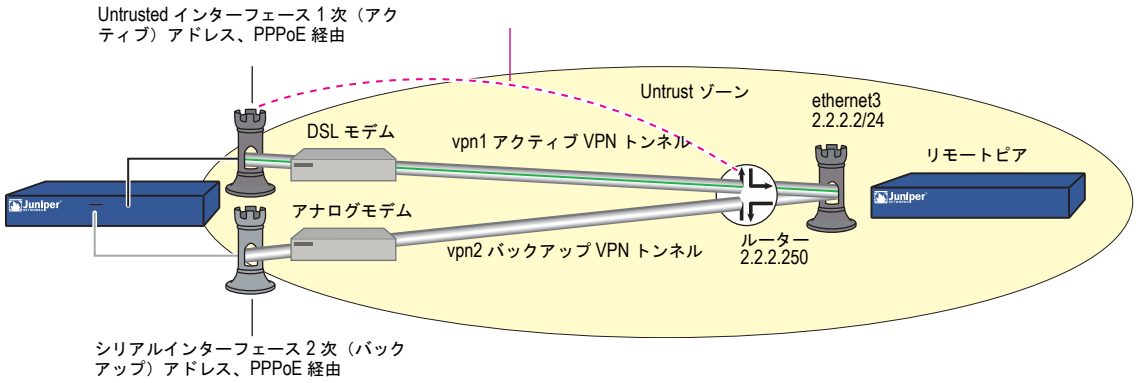
2. **トラック IP オブジェクト障害しきい値**

```
set nsrp track-ip threshold 51
save
```

冗長 VPN トンネルの構成

図 21 は、リモートの IKE ピアへのセキュリティデバイス上に冗長な双方向 VPN トンネルを構成する方法を示します。ある時点を取れば、いずれか一方のトンネルのみが稼動しています。当初は 1 次インターフェースの VPN トンネル (この例では vpn1) が稼動します。1 次トンネルに障害が起こると、フェールオーバー処理により、リモートピアへの VPN トラフィックは、バックアップトンネル (この例では vpn2) に切り替わります。

図 21: Untrusted インターフェースからシリアルインターフェースへのトンネルフェールオーバー



リモートピア側では VPN トンネルを 1 つだけ設定します。リモートピア側からは、デバイスからの VPN トンネルが 1 つだけあるように見えるからです。その結果、VPN のルートは Y 字型になります。

注 : Y 字型の VPN を設定する場合、バックアップインターフェースが ethernet (この例では Dual-Untrust モード) であれば、このインターフェースを使う VPN トンネルの VPN 監視設定において、rekey オプションを有効にしないでください。有効にすると、セキュリティデバイスを停止しようとしても、トンネルを立ち上げようと繰り返し試みるようになってしまいます。バックアップインターフェースが (この例のように) シリアルインターフェースであれば、このインターフェース上の VPN トンネルに対しては、rekey オプションが有効であっても無効であっても構いません。

IP トラッキング機能により、Untrusted インターフェースからシリアルインターフェースへのフェールオーバーが必要でないかどうか監視します。そのため、リモートピア側の外部ルーターである 2.2.2.250 に ping します。そのアドレスをトラッキングし、リモートピアの Untrust ゾーンインターフェースである 2.2.2.2 に ping するわけではありません。このインターフェースに ICMP エコー要求が届いても、リモート再とのセキュリティデバイスが応答するようには設定されていないからです。次のように IP トラッキングの設定をします。

- Track IP: 2.2.2.250
  - Weight: 255
  - Interval: 4
  - Threshold: 3

- Track IP failure threshold: 255
- Monitor failure threshold: 255
- Failover holddown: 16

上記の設定で、vpn1 から vpn2 へのフェールオーバーは、IP トラッキングがトラッキングしているアドレス (2.2.2.250) との接続を失ってから 30 秒後に起きます。4 秒間隔で 3 回エコー要求が失敗 = 12 秒 + 16 秒のホールドダウンタイム。猶予時間中も、NetScreen-5GT は 4 秒間隔で ICMP エコー要求を送り続けています。したがって、合計すると 7 回の ICMP エコー要求に応答がなかった場合 (最初の 3 回と猶予時間中の 4 回を加算) に、フェールオーバーが起こることになります。

注 : この例は長いので、CLI による設定例のみ完全に示します。WebUI セクションでは、さまざまな設定要素が示されているページを開く手順のみを示します。各パラメータの設定値については、CLI コマンドを参照してください。

WebUI

1. **ログインおよびインターフェース**
   セキュリティデバイスに再びログインします。それから次の構成を行います。

   Network > Interfaces > Edit (trust):

   Network > Interfaces > Edit (シリアル)

   Network > Interfaces > New Tunnel IF

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New

3. **PPPoE**
   Network > PPPoE > New

4. **VPN トンネル**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > AutoKey IKE > New

5. **非対称 VPN**
   Network > Zones > Edit (Trust)

6. **IP トラッキング**
   Network > Interfaces > Edit (untrust) > Monitor

   Network > Interfaces > Edit (untrust) > Monitor > Monitor Track IP ADD

7. **トンネルフェールオーバー**
   Network > Untrust Failover

   Network > Untrust Failover > Edit Weight

8. **ルート**
   Network > Routing > Routing Entries > trust-vr New

9. **ポリシー**
   Policies > (From: Trust, To: Untrust) New

   Policies > (From: Untrust, To: Trust) New

WebUI （リモートピア）

1. **インターフェース**
   Network > Interfaces > Edit (ethernet3)

   Network > Interfaces > Edit (ethernet1)

   Network > Interfaces > New Tunnel IF

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New

3. **VPN トンネル**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > AutoKey IKE > New

4. **ルート**
   Network > Routing > Routing Entries > trust-vr New

5. **ポリシー**
   Policies > (From: Trust, To: Untrust) New

   Policies > (From: Untrust, To: Trust) New

CLI

1. **ログインおよびインターフェース**
   セキュリティデバイスに再びログインします。それから次の構成を行います。

```
set interface trust ip 10.1.1.1/24
set interface trust nat
set interface serial zone untrust
set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface trust
set interface tunnel.2 zone trust
set interface tunnel.2 ip unnumbered interface trust
```

2. **アドレス**

```
set address untrust peer1 10.2.2.0/24
```

3. **PPPoE**

```
set pppoe name isp1a
set pppoe name isp1a username ns5gt password juniper
set pppoe name isp1a idle 0
set pppoe name isp1a interface untrust
exec pppoe name isp1a connect
```

4. **VPN トンネル**

```
set ike gateway gw1 address 2.2.2.2 aggressive local-id ns5gt outgoing-interface
    untrust preshare netscreen1 sec-level compatible
```

```
set ike gateway gw2 address 2.2.2.2 aggressive local-id ns5gt outgoing-interface
    serial preshare netscreen1 sec-level compatible
set vpn vpn1 gateway gw1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set vpn vpn2 gateway gw2 sec-level compatible
set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

5. **非対称 VPN**

```
set zone trust asymmetric-vpn
```

6. **IP トラッキング**

```
set interface untrust monitor track-ip ip
set interface untrust monitor track-ip ip 2.2.2.250 interval 4
set interface untrust monitor track-ip ip 2.2.2.250 threshold 3
set interface untrust monitor track-ip ip 2.2.2.250 weight 255
```

7. **トンネルフェールオーバー**

```
set failover enable
set failover auto
set failover holddown 16
set failover type track-ip
set interface untrust track-ip threshold 255
```

8. **ルート**

```
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.2
set vrouter trust-vr route 10.2.2.0/24 interface null metric 100
```

9. **ポリシー**

```
set policy from trust to untrust any any any permit
set policy from untrust to trust peer1 any any permit
save
```

CLI （リモートピア）

1. **インターフェース**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface ethernet1
```

2. **アドレス**

```
set address untrust ns5gt 10.1.1.0/24
```

3. **VPN トンネル**

```
set ike gateway ns5gt dynamic ns5gt aggressive outgoing-interface ethernet3
    preshare netscreen1 sec-level compatible
set vpn vpn1 gateway ns5gt sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. **ルート**

```
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
set vrouter trust-vr route 10.1.1.0/24 interface null metric 100
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
```

5. ポリシー

```
set policy from untrust to trust ns5gt any any permit
set policy from trust to untrust any ns5gt any permit
save
```

仮想セキュリティインターフェースの構成

図 22 の例では、デバイス A とデバイス B はアクティブ / アクティブ構成の 2 つの VSD グループ（VSD グループ 0 と VSD グループ 1）のメンバーです。デバイス A は VSD グループ 0 の 1 次デバイスで、VSD グループ 1 のバックアップです。デバイス B は VSD グループ 1 の 1 次デバイスで、VSD グループ 0 のバックアップです。セキュリティデバイスは Untrust ゾーンのスイッチ A とスイッチ B、および Trust ゾーンのスイッチ C とスイッチ D という 2 組の冗長スイッチに接続されています。

注 : この例では、デバイス A での冗長インターフェースの作成のみを示しています。デバイス A とデバイス B は同一の NSRP クラスタのメンバーなので、デバイス A は、両方のデバイスの redundant2 インターフェースに入力する管理 IP アドレスを除いたすべてのインターフェース構成をデバイス B に設定同期します。デバイス A 10.1.1.21 、デバイス B 10.1.1.22 。

---

ethernet1/1 と ethernet1/2 を redundant1 に、ethernet2/1 と ethernet2/2 を redundant2 に組み入れます。redundant2 インターフェース上で、デバイス A に対して管理 IP 10.1.1.21、デバイス B に対して管理 IP 10.1.1.22 を定義します。

同一の冗長インターフェースにバインドされている物理インターフェースは、以下のように異なるスイッチに接続します。

- Untrust ゾーン内の冗長インターフェースにバインドされている物理インターフェース : ethernet1/1 はスイッチ A に、ethernet1/2 はスイッチ B に接続
- Trust ゾーン内の冗長インターェースにバインドされている物理インターフェース : ethernet2/1 はスイッチ C に、ethernet2/2 はスイッチ D に接続

注 : 物理インターフェースは、バインド先の冗長インターフェースのように同一のセキュリティゾーン内に存在する必要はありません。

最初に ethernet1/1 と ethernet2/1 をそれぞれの冗長インターフェースに組み入れることによって、これらを 1 次インターフェースに指定します。(CLI コマンド **set interface** *redundant1* **primary** *interface1/1* によって、1 次状態の割り当てを変更することができます。)1 次インターフェースへのリンクが切断されると、セキュリティデバイスは、VSD 1 次デバイスのフェールオーバーを要求せずに、2 次インターフェースを介してもう一方のスイッチにトラフィックを再ルーティングします。

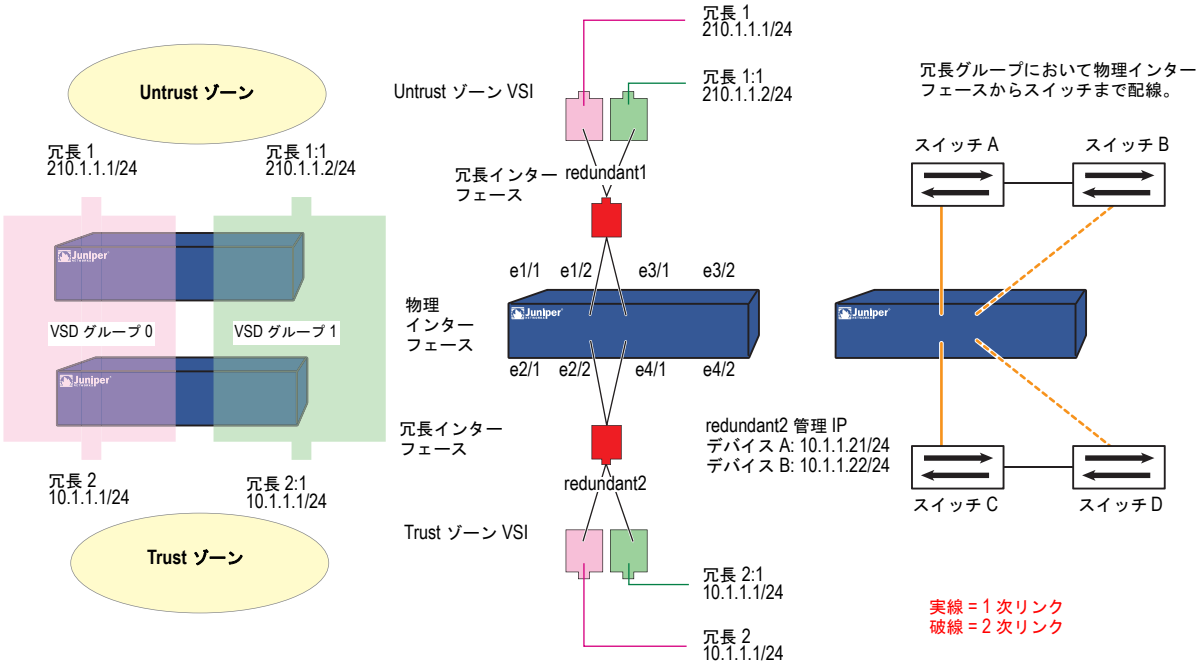
この例では、ethernet1/1 からの配線が切断されることによって、ethernet1/2 へのポートフェールオーバーが起こります。その結果、デバイス A とデバイス B を行き来するトラフィックはすべてスイッチ B を通過します。デバイス A の ethernet1/1 からスイッチ A への配線を再接続することで、そのインターフェースは以前の優先順位を取り戻します。

VSI の IP アドレス :

VSD グループ 0 の VSI		VSD グループ 1 の VSI	
redundant	210.1.1.1/24	redundant1:1	210.1.1.2/24
redundant2	10.1.1.1/24	redundant2:1	10.1.1.2/24

注 : VSI が同一の冗長インターフェース、物理インターフェース、またはサブインターフェース上にある場合は、複数の VSI の IP アドレスが同一のサブネット内にあることも、また異なるサブネット内にあることも可能です。VSI が異なるインターフェース上にある場合は、これらは異なるサブネット内にある必要があります。

図 22: VSI の冗長インターフェース



WebUI (デバイス A)

1. **冗長インターフェース**

   Network > Interfaces > New Redundant IF: 次のように入力してから **OK** をクリックします。

   Interface Name: redundant1
   Zone Name: Untrust
   IP Address/Netmask: 210.1.1.1/24

   Network > Interfaces > Edit (ethernet1/1):「 As member of 」ドロップダウンリストから **redundant1** を選択してから **OK** をクリックします。

   Network > Interfaces > Edit (ethernet1/2):「 As member of 」ドロップダウンリストから **redundant1** を選択してから **OK** をクリックします。

Network > Interfaces > New Redundant IF: 以下を入力して **Apply** をクリックします。

Interface Name: redundant2
Zone Name: Trust
IP Address/Netmask: 10.1.1.1/24

Manage IP フィールドに **10.1.1.21** と入力してから **OK** をクリックします。

Network > Interfaces > Edit (ethernet2/1):「 As member of 」ドロップダウンリストから **redundant2** を選択してから **OK** をクリックします。

Network > Interfaces > Edit (ethernet2/2):「 As member of 」ドロップダウンリストから **redundant2** を選択してから **OK** をクリックします。

2. 仮想セキュリティインターフェース

Network > Interfaces > New VSI IF: 次のように入力してから **OK** をクリックします。

Interface Name: VSI Base: Redundant1
VSD Group: 1
IP Address/Netmask: 210.1.1.2/24

Network > Interfaces > New VSI IF: 次のように入力してから **OK** をクリックします。

Interface Name: VSI Base: Redundant2
VSD Group: 1
IP Address/Netmask: 10.1.1.2/24

WebUI (デバイス B)

Network > Interfaces > Edit (redundant2): 管理 IP フィールドで **10.1.1.22** と入力し、**OK** をクリックします。

注 : それぞれの VSD の VSI ごとに、VSI の接続サブネットからリモートサブネットアドレスへの静的ルートを入力する必要があります。

CLI (デバイス A)

1. 冗長インターフェース

```
set interface redundant1 zone untrust
set interface redundant1 ip 210.1.1.1/24
set interface ethernet1/1 group redundant1
set interface ethernet1/2 group redundant1
set interface redundant2 zone trust
set interface redundant2 ip 10.1.1.1/24
set interface redundant2 manage-ip 10.1.1.21
set interface redundant2 nat
set interface ethernet2/1 group redundant2
set interface ethernet2/2 group redundant2
set interface redundant1 primary ethernet1/1
set interface redundant2 primary ethernet2/1
```

2. 仮想セキュリティインターフェース

```
set interface redundant1:1 ip 210.1.1.2/24
set interface redundant2:1 ip 10.1.1.2/24
save
```

CLI (デバイス B)

```
set interface redundant2 manage-ip 10.1.1.22
save
```

注 : それぞれの VSD の VSI ごとに、VSI の接続サブネットからリモートサブネットアドレスへの静的ルートを入力する必要があります。

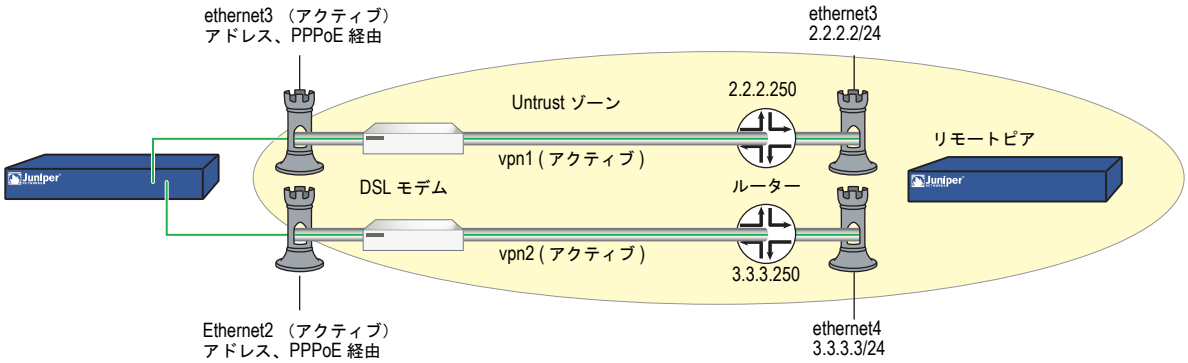
2 系統のアクティブなトンネルの構成

この構成の目的は、2 系統の VPN トンネルをアクティブにしておいて、必要なときにフェールオーバーできるようにすることです。

ここでは、NetScreen-5GT からリモート IKE ピアへの、双方向 VPN トンネルを 2 系統 (vpn1 および vpn2) 用意して、冗長構成します。平常時でも両方をアクティブにしておいて NetScreen-5GT が負荷分散を図り、セッションごとに 2 つのトンネルを切り替えながら動作するようにします。(これは本当の意味での負荷分散ではありません。セッションによってトラフィック量は大きく異なるので、均等に分散されるとは限らないからです。) いずれかのトンネルに障害が発生すると、NetScreen-5GT は VPN トラフィックをすべてもう一方のトンネルに振り分けます。

NetScreen-5GT は Dual-Untrust モードです。ethernet3、ethernet2 とも、DSL モデムにつながっています。フェールオーバーオプションを無効にすると、両方がアクティブになります。図 23 を参照してください。

図 23: 2 系統のアクティブなトンネルでのフェールオーバー



両サイトの Trust ゾーンに非対称 VPN オプションを設定して、一方の VPN トンネルで確立されたセッションをもう一方に切り替えても、トンネルの先にあるセキュリティデバイスがこれを拒否しないようにします。

注 : この例は長いので、CLI による設定例のみ完全に示します。WebUI セクションでは、さまざまな設定要素が示されているページを開く手順のみを示します。各パラメータの設定値については、CLI コマンドを参照してください。

WebUI

1. **ログインおよびインターフェース**
   セキュリティデバイスに再びログインします。それから次の構成を行います。

   Network > Interfaces > Edit (ethernet1)

   Network > Interfaces > New Tunnel IF

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New

3. **PPPoE**
   Network > PPPoE > New

4. **VPN トンネル**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > AutoKey IKE > New

5. **2 重トンネル**
   Network > Untrust Failover

6. **非対称 VPN**
   Network > Zones > Edit (Trust)

7. **ルート**
   Network > Routing > Routing Entries > trust-vr New

8. **ポリシー**
   Policies > (From: Trust, To: Untrust) New

   Policies > (From: Untrust, To: Trust) New

WebUI （リモートピア）

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1)

   Network > Interfaces > Edit (ethernet3)

   Network > Interfaces > Edit (ethernet4)

   Network > Interfaces > New Tunnel IF

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New

3. **VPN トンネル**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > AutoKey IKE > New

4. **非対称 VPN**
   Network > Zones > Edit (Trust)

5. **ルート**
   Network > Routing > Routing Entries > trust-vr New
6. **ポリシー**
   Policies > (From: Trust, To: Untrust) New

   Policies > (From: Untrust, To: Trust) New

CLI

1. **ログインおよびインターフェース**
   セキュリティデバイスに再びログインします。それから次の構成を行います。

```
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface ethernet1
set interface tunnel.2 zone trust
set interface tunnel.2 ip unnumbered interface ethernet1
```

2. **アドレス**

```
set address untrust peer1 10.2.2.0/24
```

3. **PPPoE**

```
set pppoe name isp1a
set pppoe name isp1a username ns5gt1a password juniper1a
set pppoe name isp1a idle 0
set pppoe name isp1a interface ethernet3
exec pppoe name isp1a connect
set pppoe name isp1b
set pppoe name isp1b username ns5gt1b password juniper1b
set pppoe name isp1b idle 0
set pppoe name isp1b interface ethernet2
exec pppoe name isp1b connect
```

4. **VPN トンネル**

```
set ike gateway gw1 address 2.2.2.2 aggressive local-id 5gt-e3 outgoing-interface
    ethernet3 preshare netscreen1 sec-level compatible
set ike gateway gw2 address 3.3.3.3 aggressive local-id 5gt-e2 outgoing-interface
    ethernet2 preshare netscreen2 sec-level compatible
set vpn vpn1 gateway gw1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set vpn vpn1 monitor source-interface ethernet1 destination-ip 2.2.2.2 rekey
set vpn vpn2 gateway gw2 sec-level compatible
set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set vpn vpn2 monitor source-interface ethernet1 destination-ip 3.3.3.3 rekey
```

5. **2 重トンネル**

```
unset failover enable
```

6. **非対称 VPN**

```
set zone trust asymmetric-vpn
```

7. **ルート**

```
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.2
set vrouter trust-vr route 10.2.2.0/24 interface null metric 100
```

8. ポリシー

```
set policy from trust to untrust any any any permit
set policy from untrust to trust peer1 any any permit
save
```

CLI （リモートピア）

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface ethernet4 zone untrust
set interface ethernet4 ip 3.3.3.3/24
set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface ethernet1
set interface tunnel.2 zone trust
set interface tunnel.2 ip unnumbered interface ethernet1
```

2. アドレス

```
set address untrust ns5gt 10.1.1.0/24
```

3. VPN トンネル

```
set ike gateway gw1 dynamic ns5gt-e3 aggressive outgoing-interface ethernet3
    preshare netscreen1 sec-level compatible
set ike gateway branch2 dynamic ns5gt-e2 aggressive outgoing-interface ethernet4
    preshare netscreen2 sec-level compatible
set vpn vpn1 gateway gw1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set vpn vpn2 gateway gw2 sec-level compatible
set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. 非対称 VPN

```
set zone trust asymmetric-vpn
```

5. ルート

```
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.2
set vrouter trust-vr route 10.1.1.0/24 interface null metric 100
```

6. ポリシー

```
set policy from trust to untrust any any any permit
set policy from untrust to trust ns5gt any any permit
save
```

トラック IP を使用したインターフェースフォールオーバーの構成

この例では、まず NetScreen-5GT を Dual Untrust モードに構成します。続いて、デバイスに自動フェールオーバーを構成します。1 次インターフェースからバックアップインターフェースへの自動フェールオーバーが起きた場合、1 次インターフェースが回復するまでの間、Untrust ゾーンを行き来するすべてのトラフィックを、バックアップインターフェースが運びます。

1 次インターフェースでは、セキュリティデバイスが 3 つの IP アドレスを監視してフェールオーバーが起きる時期を判断します。追跡する各 IP アドレスには、次のようにウェイトを設定します。

- 2.2.2.2 - Weight = 6
- 3.3.3.3 - Weight = 6
- 4.4.4.4 - Weight = 6

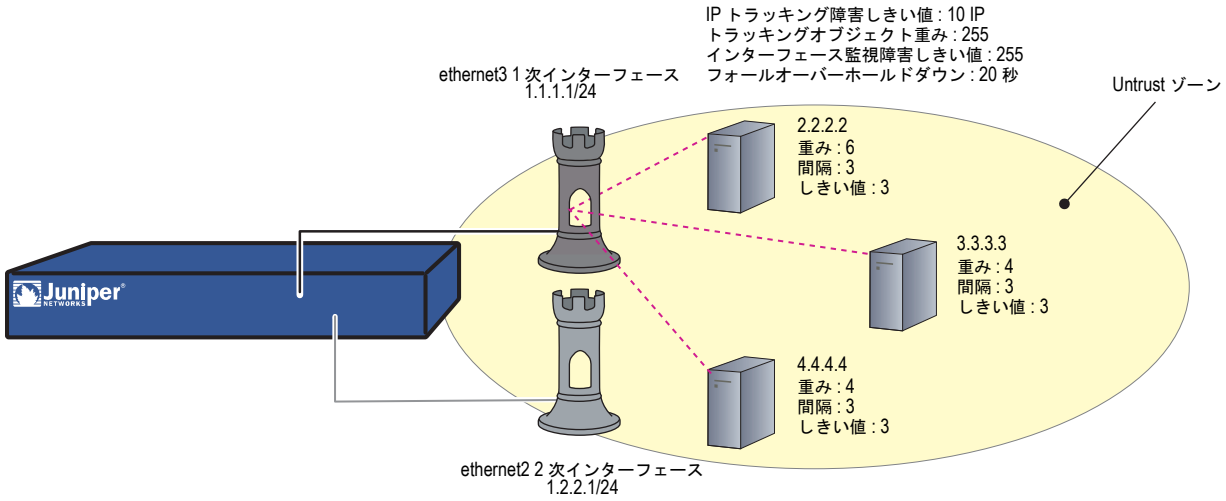
上記の各 IP アドレスについて、障害と看做すしきい値はデフォルトである 3 のままとし、ICMP エコー要求の間隔は 3 秒と設定します。上記 IP アドレスに対する ICMP 要求 (3 秒間隔) の応答が 3 回続けて得られなければ、1 次インターフェース経由で到達できなくなったと看做します。

IP トラッキングにより障害と判断する都度、セキュリティデバイスはそのアドレスの重み値を累積していきます。その結果、所定のしきい値 (この例では 10) 以上になった場合、IP トラッキングオブジェクトの重み値を、インターフェース監視オブジェクトの重み値に加算します。この例では、IP トラッキングオブジェクトの重み値、インターフェース監視オブジェクトが障害と判断するしきい値とも、デフォルト値である 255 を採用します。

そのため、IP トラッキングオブジェクトの重み値の合計が 10 になると、インターフェースフェールオーバーが起きます。このとき、両 IP アドレス 2.2.2.2 および 3.3.3.3 （または 2.2.2.2 および 4.4.4.4 ）が同時に 1 次インターフェースから到達できない状態でなければなりません。一方、3.3.3.3 と 4.4.4.4 が 1 次インターフェースを通して不達になっても、重み値の累計が 7 の場合は、フェールオーバーは起こりません。

図 24 の例では、障害が起こってから、9 秒（3 秒間隔の ICMP 要求が 3 回連続で失敗）で不達とみなすことになります。しかし猶予時間を 20 秒と設定すれば、不達と看做してから (IP トラッキングオブジェクトの重み値である 255 を積算した結果が、インターフェース監視オブジェクトが障害と判断するしきい値である 255 に達してから)、実際にバックアップインターフェースに切り替えるまでに、20 秒間待機するようになります。

図 24: インターフェースフェールオーバー



WebUI

1. **ログインおよびインターフェース**
   再びログインして、インターフェース IP アドレスを設定します。それから次の構成を行います。

2. **自動フェールオーバーと IP トラッキング**
   Network > Untrust Failover: 以下を選択して **Apply** をクリックします。

   Track IP: (選択)
   Automatic Failover: (選択)
   Failover: (選択)
   Failover Holddown Time: 20

   Network > Interfaces > Edit (ethernet3) > Monitor > Monitor Track IP ADD: 次のように入力してから **Add** をクリックします。

   Static: (選択)
   Track IP: 2.2.2.2
   Weight: 6
   Interval: 3
   Threshold: 3

   Monitor Track IP ADD: 次のように入力してから **Add** をクリックします。

   Static: (選択)
   Track IP: 3.3.3.3
   Weight: 4
   Interval: 3
   Threshold: 3

Monitor Track IP ADD: 次のように入力してから **Add** をクリックします。

Static: (選択)
Track IP: 4.4.4.4
Weight: 4
Interval: 3
Threshold: 3

Network > Interfaces > Edit (ethernet3) > Track IP Options: 以下を入力して **Apply** をクリックします。

Monitor Option:
Enable Track IP: (選択)
Monitor Threshold: 255
Track IP Option:
Threshold: 10
Weight: 255

CLI

1. **ログインおよびインターフェース**
   再びログインして、インターフェース IP アドレスを設定します。それから次の構成を行います。

2. **自動フェールオーバーと IP トラッキング**

```
set failover enable
set failover auto
set failover holddown 12
set failover type track-ip
set interface ethernet3 track-ip threshold 10
set interface ethernet3 track-ip ip 2.2.2.2 weight 6
set interface ethernet3 track-ip ip 2.2.2.2 interval 3
set interface ethernet3 track-ip ip 2.2.2.2 threshold 3
set interface ethernet3 track-ip ip 3.3.3.3 weight 4
set interface ethernet3 track-ip ip 3.3.3.3 interval 3
set interface ethernet3 track-ip ip 3.3.3.3 threshold 3
set interface ethernet3 track-ip ip 4.4.4.4 weight 4
set interface ethernet3 track-ip ip 4.4.4.4 interval 3
set interface ethernet3 track-ip ip 4.4.4.4 threshold 3
set interface ethernet3 track-ip
save
```

トンネルのフェールオーバーウェイトの構成

図 25 の例では、一方向の VPN トンネルのペアを 3 組作ります。各ペアは 1 次トンネルとバックアップトンネルから成ります。トンネルは、支社サイトの Trust ゾーンにあるホストと、企業サイトの Trust ゾーンにある DNS、SMTP、HTTP サーバーを結びます。各サイトのすべてのゾーンは、trust-vr ルーティングドメインに存在します。

まず、支社サイトの NetScreen-5XT （支社サイトを保護しているセキュリティデバイス）を Dual-Untrust モードにします。次に 3 系統の VPN トンネルを設定します。1 次 Untrust ゾーンインターフェース (ethernet3) を外向きインターフェース、さらに、バックアップ Untrust ゾーンインターフェース (ethernet2) も外向きインターフェースとします。セキュリティデバイスは 1 次 VPN トンネルを監視し、必要な場合にはフェールオーバー処理を起動します。各 VPN トンネルには、次のフェールオーバーウェイトがあります :

- vpn1 - Weight = 60
- vpn2 - Weight = 40
- vpn3 - Weight = 40

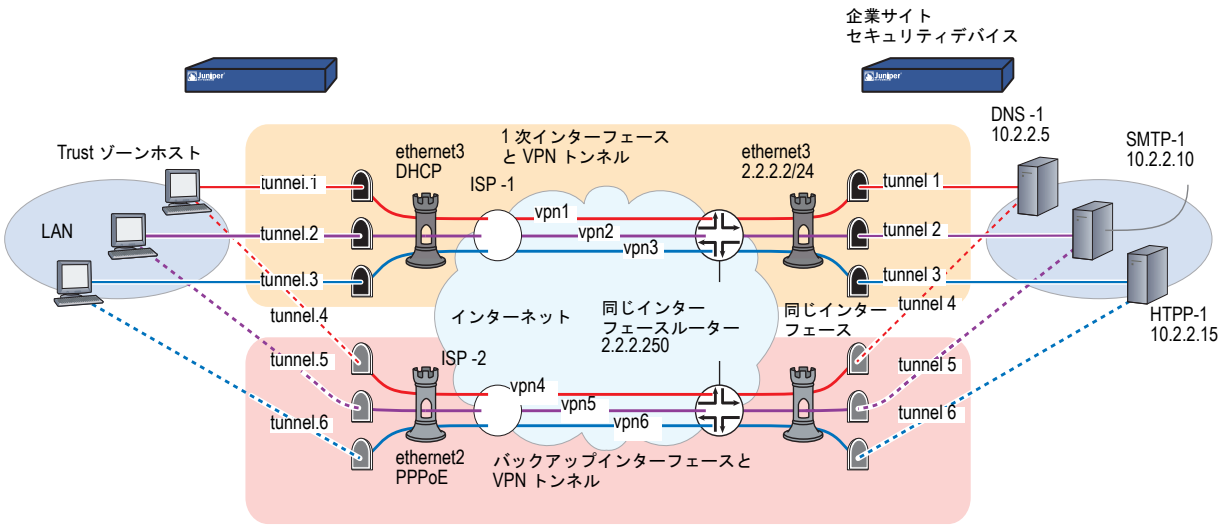
セキュリティデバイスに自動フェールオーバーを構成します。1 次インターフェースからバックアップインターフェースへの自動フェールオーバーが起きた場合、1 次インターフェースが回復するまでの間、Untrust ゾーンを行き来するすべてのトラフィックを、バックアップインターフェースが運びます。1 次インターフェースのフェールオーバーは、フェールオーバーウェイトの累計が 100% 以上になったときに起きます。このため、vpn1 と vpn2 の両方がダウンした場合、失敗の累計ウェイトが 100% になるため、バックアップインターフェースへの自動フェールオーバーが起きます。vpn2 と vpn3 だけがダウンした場合、失敗の累計ウェイトは 80% となり、フェールオーバーは起こりません。

VPN 監視の rekey 機能も有効にします。この機能では、フェールオーバーが発生したときでも 1 次インターフェースにある VPN トンネルの累計ウェイトが 100% 未満になった場合は、セキュリティデバイスがバックアップインターフェースから 1 次インターフェースにトラフィックを戻します。

最後に、両サイトの Trust ゾーンに非対称 VPN オプションを設定して、一方の VPN トンネルで確立されたセッションをもう一方に切り替えても、トンネルの先にあるセキュリティデバイスがこれを拒否しないようにします。

デバイスは Untrust ゾーンインターフェースのアドレス、デフォルトゲートウェイ、DNS サーバーのアドレスを、2 つの異なる ISP から動的に取得します。ISP はそれぞれ別のプロトコルを使います。ISP-1 は DHCP を使って ethernet3 にアドレスを割り当て、ISP-2 は PPPoE で ethernet2 にアドレスを割り当てます。企業サイトのセキュリティデバイスには、静的 IP アドレス (2.2.2.2) が割り当てられています。デフォルトゲートウェイの IP アドレスは 2.2.2.250 です。

図 25: 1 次およびバックアップインターフェースと VPN トンネル



VPN 監視の対象である宛先アドレスは、デフォルトであるリモートゲートウェイの IP アドレス (2.2.2.2) ではなく、3 台のサーバーのアドレス (10.2.2.5、10.2.2.10、10.2.2.15) です。仮に、(デフォルトのまま) リモートゲートウェイの IP アドレスを監視対象にしたとすると、フェールオーバーが起こった場合、3 系統の 1 次トンネルが一斉にバックアップトンネルに切り替わります。これは、2 系統のトンネル (vpn1 + vpn2、または vpn1 + vpn3) に障害が生じればフェールオーバーを引き起こす、という重み設定と矛盾する動作です。一方、各トンネルの先にあるサーバーのアドレスをそれぞれ VPN 監視の対象にした場合、vpn1 経由で DNS-1 に ping できなくなっても、それだけではフェールオーバーとなりません。この状態でさらに vpn2 経由の SMTP-1 も不達になれば、重みの和は 100% (60 + 40) となるので、フェールオーバーが発生して vpn1 は vpn4 に、vpn2 は vpn5 に切り替わります。vpn3 は元のままです。

注 : この例は長いので、CLI による設定例のみ完全に示します。WebUI セクションでは、さまざまな設定要素が示されているページを開く手順のみを示します。各パラメータの設定値については、CLI コマンドを参照してください。

WebUI (支社)

1. **ログインおよびインターフェース**
   セキュリティデバイスに再びログインします。それから次の構成を行います。

   Network > Interfaces > Edit (ethernet1)

   Network > Interfaces > Edit (ethernet3)

   Network > Interfaces > Edit (ethernet2)

   Network > Interfaces > New Tunnel IF

2. **VPN トンネル**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > AutoKey IKE > New

3. **トンネルフェールオーバー**
   Network > Untrust Failover

   Network > Untrust Failover > Edit Weight

4. **非対称 VPN**
   Network > Zones > Edit (Trust)

5. **ルート**
   Network > Routing > Routing Entries > trust-vr New

6. **ポリシー**
   Policies > (From: Trust, To: Untrust) New

WebUI (本社)

1. **インターフェース**
   Network > Interfaces > Edit (ethernet1)

   Network > Interfaces > Edit (ethernet3)

   Network > Interfaces > New Tunnel IF

2. **アドレス**
   Policy > Policy Elements > Addresses > List > New

3. **サービスグループ**
   Policy > Policy Elements > Services > Groups > New

4. **VPN トンネル**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > AutoKey IKE > New

5. **非対称 VPN**
   Network > Zones > Edit (Trust)

6. **ルート**
   Network > Routing > Routing Entries > trust-vr New

7. **ポリシー**
   Policies > (From: Trust, To: Untrust) New

CLI (支社)

1. **ログインおよびインターフェース**
   セキュリティデバイスに再びログインします。それから次の構成を行います。

```
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
```

```
set interface ethernet3 dhcp client
exec dhcp client ethernet3 renew
set pppoe interface ethernet2
set pppoe username ns5gt password juniper
set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface ethernet1
set interface tunnel.2 zone trust
set interface tunnel.2 ip unnumbered interface ethernet1
set interface tunnel.3 zone trust
set interface tunnel.3 ip unnumbered interface ethernet1
set interface tunnel.4 zone trust
set interface tunnel.4 ip unnumbered interface ethernet1
set interface tunnel.5 zone trust
set interface tunnel.5 ip unnumbered interface ethernet1
set interface tunnel.6 zone trust
set interface tunnel.6 ip unnumbered interface ethernet1
```

2. VPN トンネル

```
set ike gateway corp1 address 2.2.2.2 aggressive local-id 5gt-e3
    outgoing-interface ethernet3 preshare netscreen1 sec-level basic
set ike gateway corp2 address 2.2.2.2 aggressive local-id 5gt-e2
    outgoing-interface ethernet2 preshare netscreen2 sec-level basic

set vpn vpn1 gateway corp1 sec-level basic
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 DNS
set vpn vpn1 monitor source-interface ethernet1 destination-ip 10.2.2.5 rekey
set vpn vpn2 gateway corp1 sec-level basic

set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 SMTP
set vpn vpn2 monitor source-interface ethernet1 destination-ip 10.2.2.10 rekey
set vpn vpn3 gateway corp1 sec-level basic
set vpn vpn3 bind interface tunnel.3

set vpn vpn3 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 HTTP
set vpn vpn3 monitor source-interface ethernet1 destination-ip 10.2.2.15 rekey
set vpn vpn4 gateway corp2 sec-level basic
set vpn vpn4 bind interface tunnel.4
set vpn vpn4 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 DNS
set vpn vpn4 monitor source-interface ethernet1 destination-ip 10.2.2.5 rekey
set vpn vpn5 gateway corp2 sec-level basic
set vpn vpn5 bind interface tunnel.5
set vpn vpn5 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 SMTP

set vpn vpn5 monitor source-interface ethernet1 destination-ip 10.2.2.10 rekey
set vpn vpn6 gateway corp2 sec-level basic
set vpn vpn6 bind interface tunnel.6
set vpn vpn6 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 HTTP
set vpn vpn6 monitor source-interface ethernet1 destination-ip 10.2.2.15 rekey
```

注： 通常は、プロキシ ID を「 local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any 」としても構いません。上記の例にある **set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 SMTP** では、それぞれのトンネルのプロキシ ID は、トンネル同士を識別するために、異なるものでなければなりません。各プロキシ ID でサービスが同じであれば、設定に矛盾が生じるため、セキュリティデバイスは vpn2 と vpn3 (したがって vpn5 と vpn6) のプロキシ ID を拒否します。

3. **トンネルフェールオーバー**
   set failover type tunnel-if
   set failover auto
   set vpn vpn1 failover-weight 60
   set vpn vpn2 failover-weight 40
   set vpn vpn3 failover-weight 40

4. **非対称 VPN**
   set zone trust asymmetric-vpn

5. **ルート**
   set vrouter trust-vr route 10.2.2.5/32 interface tunnel.1
   set vrouter trust-vr route 10.2.2.10/32 interface tunnel.2
   set vrouter trust-vr route 10.2.2.15/32 interface tunnel.3
   set vrouter trust-vr route 10.2.2.5/32 interface tunnel.4
   set vrouter trust-vr route 10.2.2.10/32 interface tunnel.5
   set vrouter trust-vr route 10.2.2.15/32 interface tunnel.6
   set vrouter trust-vr route 10.2.2.0/24 interface null metric 100

6. **ポリシー**
   set policy from trust to untrust any any any permit
   save

CLI (本社)

1. **インターフェース**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.2.2.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 2.2.2.2/24
   set interface tunnel.1 zone trust

   set interface tunnel.1 ip unnumbered interface ethernet1
   set interface tunnel.2 zone trust
   set interface tunnel.2 ip unnumbered interface ethernet1
   set interface tunnel.3 zone trust
   set interface tunnel.3 ip unnumbered interface ethernet1
   set interface tunnel.4 zone trust
   set interface tunnel.4 ip unnumbered interface ethernet1
   set interface tunnel.5 zone trust
   set interface tunnel.5 ip unnumbered interface ethernet1
   set interface tunnel.6 zone trust
   set interface tunnel.6 ip unnumbered interface ethernet1

注 : トンネルインターフェースを VPN トンネルごとに合計 6 つ作成する代わりに、1 つだけ作成して、VPN トンネルを多重にバインドする方法もあります。セキュリティデバイスは各トンネルを区別するために、Next Hop Tunnel Binding (NHTB) テーブルを使います。NHTB の詳細については、**5**-256 ページの「1 つのトンネルインターフェースに対する複数のトンネル」を参照してください。

---

2. **アドレス**
   set address untrust branch 10.1.1.0/24
   set address trust DNS-1 10.2.2.5/32
   set address trust SMTP-1 10.2.2.10/32
   set address trust HTTP-1 10.2.2.15/32
   set group address trust servers add DNS-1

```
set group address trust servers add SMTP-1
set group address trust servers add HTTP-1
```

3. **サービスグループ**

```
set group service vpn-srv add DNS
set group service vpn-srv add SMTP
set group service vpn-srv add HTTP
set group service vpn-srv add ICMP
```

4. **VPN トンネル**

```
set ike gateway branch1 dynamic ns5gt-e3 aggressive outgoing-interface ethernet3
    preshare netscreen1 sec-level basic
set ike gateway branch2 dynamic ns5gt-e2 aggressive outgoing-interface ethernet3
    preshare netscreen2 sec-level basic

set vpn vpn1 gateway branch1 sec-level basic
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 DNS

set vpn vpn2 gateway branch1 sec-level basic
set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 SMTP

set vpn vpn3 gateway branch1 sec-level basic
set vpn vpn3 bind interface tunnel.3
set vpn vpn3 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 HTTP

set vpn vpn4 gateway branch2 sec-level basic
set vpn vpn4 bind interface tunnel.4
set vpn vpn4 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 DNS

set vpn vpn5 gateway branch2 sec-level basic
set vpn vpn5 bind interface tunnel.5
set vpn vpn5 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 SMTP

set vpn vpn6 gateway branch2 sec-level basic
set vpn vpn6 bind interface tunnel.6
set vpn vpn6 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 HTTP
```

5. **非対称 VPN**

```
set zone trust asymmetric-vpn
```

6. **ルート**

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
```

7. **ポリシー**

```
set policy from untrust to trust branch servers vpn-srv permit
save
```

仮想システムのフェールオーバーの構成

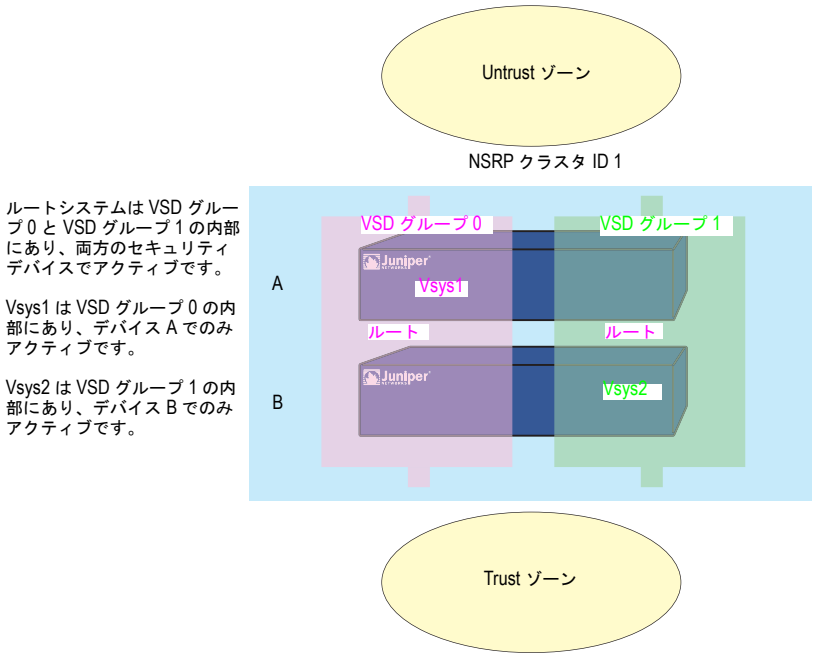
図 26 の例では、NSRP のための仮想システムを 2 つ（vsys1 と vsys2）構成します。仮想システムへの受信トラフィックにロードシェアリングを提供するには、VSD メンバーシップを以下のように割り当てます。

- Vsys1 を VSD グループ 0 のメンバー
- Vsys2 を VSD グループ 1 のメンバー

注 : 図 26 では、負荷は均等に配分されてなく、ロードバランスも行われていません。2 台のセキュリティデバイスに負荷を分散します。ここでは、デバイス A と デバイス B が動的に変化する割合 (60/40％、70/30％ など) でトラフィックを受信します。

セキュリティデバイスは、仮想システムの VSD グループ化をすることによって、受信トラフィックの負荷を分散します。デバイス A 上に vsys1 を、デバイス B 上 に vsys2 を構成するという初期設計によって、これらの仮想システムへの受信トラフィックはその設定で規定された仮想システムに転送されます。

図 26: NSRP 構成の仮想システム

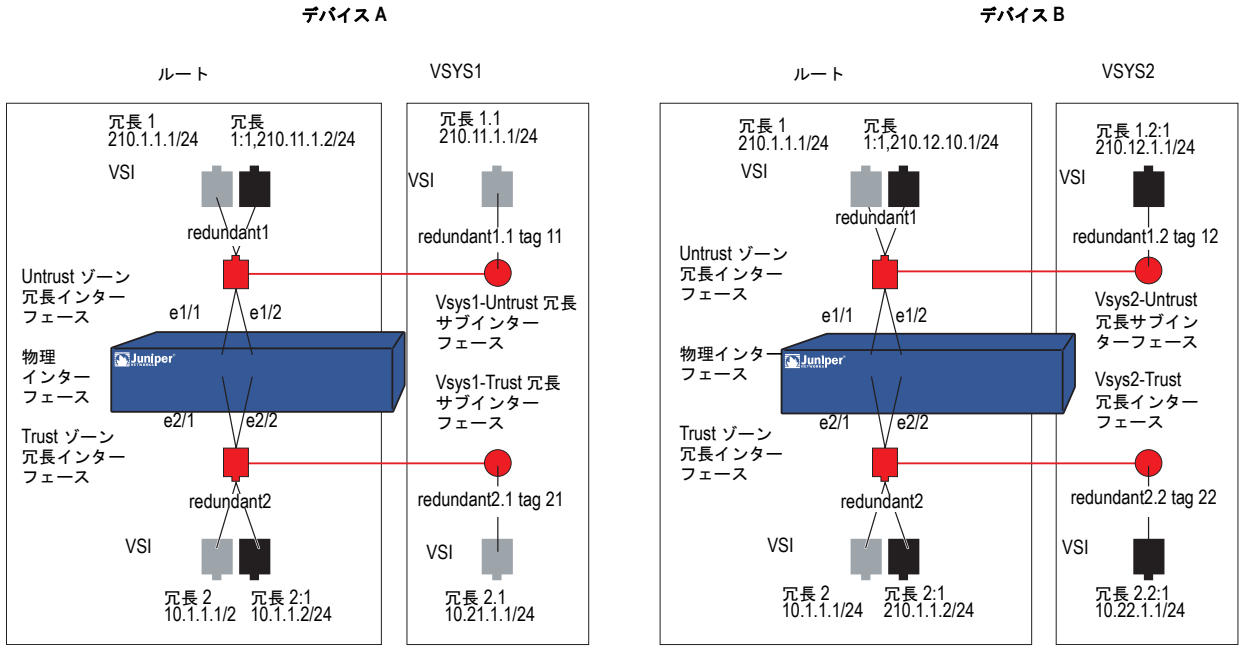


アウトバウンドトラフィックのデフォルトゲートウェイは、ルートシステムごと、および仮想システムごとに異なっています。

- Root: 210.1.1.250
- Vsys1: 210.11.1.250
- Vsys2: 210.12.1.250

図 27 の例は 12 ページの「アクティブ / アクティブ構成」をもとにして作成されており、ここでは VSD グループ 0 と VSD グループ 1 をセットアップし、NSRP クラスタ ID 1 内のデバイスを設定しているので、NSRP は使用可能になっています。そのため、デバイス A で構成した設定は、自動的にデバイス B に設定同期します。

図 27: 物理インターフェース、冗長インターフェース、サブインターフェースおよび VSI の関係



WebUI

1. **デバイス A: ルート**

注： ルートシステムのための NSRP 構成は、12 ページの「アクティブ / アクティブ構成」と同一です。

2. **デバイス A: Vsys1**
   Vsys > New: 次のように入力してから **OK** をクリックします。

   VSYS Name: vsys1

注 : 仮想システム管理を定義していない場合は、セキュリティデバイスは、「vsys_」を仮想システム名に付加することで、自動的に仮想システム名を作成します。この例では、vsys1 の仮想システム管理は vsys_vsys1 です。

Vsys > Enter (vsys1) > Network > Interface > New Sub-IF: 次のように入力してから **OK** をクリックします。

Interface Name: redundant1.1
Zone Name: Untrust
VLAN Tag: 11

Network > Interfaces > New VSI IF: 次のように入力してから **OK** をクリックします。

VSI Base: Redundant1.1
VSD Group: 0
IP Address/Netmask: 210.11.1.1/24

Network > Interfaces > New Sub-IF: 次のように入力してから **OK** をクリックします。

Interface Name: redundant2.1
Zone Name: Trust-vsys-vsys1
VLAN Tag: 21

Network > Interfaces > New VSI IF: 次のように入力してから **OK** をクリックします。

VSD Group ID: 0
IP Address/Netmask: 10.21.1.1/24
Interface Mode: Route

注 : 仮想システムは、ルートレベルで設定したモードとは無関係に、ルートモードまたは NAT モードのいずれかになることができます。

Network > Routing > Routing Entries > untrust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: Redundant1
Gateway IP Address: 210.11.1.250

Exit Vsys をクリックし、ルートレベルに戻ります。

3. デバイス A: Vsys2

Vsys > New: 次のように入力してから **OK** をクリックします。

VSYS Name: vsys2

Vsys > Enter (vsys2) > Network > Interface > New Sub-IF: 次のように入力してから **OK** をクリックします。

Interface Name: redundant1.2

Zone Name: Untrust
VLAN Tag: 12

Network > Interfaces > New VSI IF: 次のように入力してから **OK** をクリックします。

VSI Base: Redundant1.2
VSD Group: 1
IP Address/Netmask: 210.12.1.1

Network > Interfaces > New Sub-IF: 次のように入力してから **OK** をクリックします。

Interface Name: redundant2.2
Zone Name: Trust-vsys-vsys2
VLAN Tag: 22

Network > Interfaces > New VSI IF: 次のように入力してから **OK** をクリックします。

VSD Group ID: 1
IP Address/Netmask: 10.22.1.1/24
Interface Mode: Route

Network > Routing > Routing Entries > untrust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: Redundant1
Gateway IP Address: 210.12.1.250

Exit Vsys をクリックし、ルートレベルに戻ります。

4. デバイス B

注 : デバイス A はこれらの設定内容をデバイス B に同期設定するので、デバイス B でこの設定をもう一度入力する必要はありません。

CLI

1. デバイス A: ルート

注 : ルートシステムのための NSRP 構成は、12 ページの「アクティブ / アクティブ構成」と同一です。

2. デバイス A: VSYS 1

```
set vsys vsys1
ns(vsys1)-> set interface redundant1.1 tag 11 zone untrust
ns(vsys1)-> set interface redundant1.1 ip 210.11.1.1/24
ns(vsys1)-> set interface redundant2.1 tag 21 zone trust-vsys1
ns(vsys1)-> set interface redundant2.1 ip 10.21.1.1/24
ns(vsys1)-> set interface redundant2.1 route
ns(vsys1)-> set vrouter untrust-vr route 0.0.0.0/0 interface redundant1 gateway
    210.11.1.250
ns(vsys1)-> save
ns(vsys1)-> exit
```

注 : 仮想システムは、ルートレベルで設定したモードとは無関係に、ルートモードまたは NAT モードのいずれかになることができます。

3. デバイス A: VSYS 2

```
set vsys vsys2
ns(vsys2)-> set interface redundant1.2 tag 12 zone untrust
ns(vsys2)-> set interface redundant1.2:1 ip 210.12.1.1/24
ns(vsys2)-> set interface redundant2.2 tag 22 zone trust-vsys2
ns(vsys2)-> set interface redundant2.2:1 ip 10.22.1.1/24
ns(vsys2)-> set interface redundant2.2:1 route
ns(vsys2)-> set vrouter untrust-vr route 0.0.0.0/0 interface redundant1 gateway
    210.12.1.250
ns(vsys2)-> save
ns(vsys2)-> exit
```

4. デバイス B

注 : デバイス A はこれらの設定内容をデバイス B に同期設定するので、デバイス B でこの設定をもう一度入力する必要はありません。

索引

A

ARP....55
　ブロードキャスト....29
　ルックアップ....39

H

HA
　高可用性を参照

I

IP トラッキング....55
　ping と ARP....55

N

NAT モード....2
NetScreen Reliable Transport Protocol
　NSTP を参照
NetScreen 冗長プロトコル
　NSRP を参照
NRTP....19
NSRP....1
　ARP ブロードキャスト....29
　ARP ルックアップ....39
　clear cluster コマンド....10
　debug cluster コマンド....10
　hold-down 時間....36, 38
　NAT モードとルートモード....2
　NTP 同期化....20
　RTO....34
　VSD グループ....20, 34
　VSI....2
　VSI、静的ルート....24, 69, 70
　インターフェース監視....29
　仮想システム....58–87
　管理 IP....55
　冗長ポート....2
　制御メッセージ....7, 13
　セカンダリパス....29
　セキュア通信....29
　デフォルトの設定....6
　同期設定....19
　配線....25–28
　パケット転送と動的ルーティング....8
　バックアップ....11
　負荷分散....83
　プリエンプトモード....21
　フルメッシュ構成....25, 58
　マスタ....11
　優先順位番号....21
NSRP HA
　インターフェース....6
　セッションバックアップ....15
　配線、ネットワークインターフェース....27
　ポート、冗長インターフェース....43
NSRP-Lite....19
　クラスタ....11
　セキュア通信....15
NSRP-Lite 同期化
　使用不可....18
NSRP RTO....15–16
　状態....16
　同期....19
NSRP クラスタ....30, 34
　名前....11, 28

NSRP データ 8
メッセージ 7
NSRP 同期化
NTP, NSRPNTP, NSRP 20
RTO 19
NSRP ポート
フェールオーバー 43
NTP 、NSRP 同期化 NTP 、NSRP 同期化 20

R

RTO 15–16
同期 19
動作状態 16
ピア 22

V

VRRP 55
VSD グループ 20
hold-down 時間 36, 38
ハートビート 23, 29
フェールオーバー 57
メンバー状態 22
優先順位番号 21
VSI 2, 20
VSD ごとの複数の VSI 58
静的ルーティング 24

あ

暗号化
NSRP 29
NSRP-Lite 15

い

インターフェース
HA、二重 8
VSI 24
仮想 HA 27
監視 29
冗長 43
統合 45

お

オブジェクト、監視 52

か

仮想 HA インターフェース 27
仮想システム
NSRP 58
フェールオーバー 58
負荷分散 83
仮想セキュリティインターフェース
VSI を参照
仮想セキュリティデバイスグループ
VSD グループを参照
管理 IP, VSD グループ 0 2

く

クラスタ 11, 34
クラスタ名、NSRP 11, 28

こ

高可用性
IP トラッキング 55
仮想インターフェース 27
データリンク 8
配線 25–28
メッセージ 7
リンク精査 9
高可用性インターフェース
HA リンクとしてネットワークを配線 27
冗長 43
統合 45
高可用性フェールオーバー
アクティブ / パッシブ 11
アクティブ / アクティブ 12
構成
フルメッシュ 58

せ

制御メッセージ 13
HA 7
HA 物理リンクハートビート 7
RTO ハートビート 7
セカンダリパス 29

て

データメッセージ 7
デバイスフェールオーバー 59

と

同期
RTO 19
構成 19
統合インターフェース 45

に

認証
NSRP 29
NSRP-Lite 15

は

ハートビート
HA 物理リンク 7
RTO 7

ふ

フェールオーバー
Dual Untrust インターフェース....46, 49
VSD グループ....57
オブジェクト監視....52
仮想システム....58
デバイス....59
負荷分散....83
プリエンプトモード....21
フルメッシュ構成....58
プロトコル
NRTP....19
NSRP....1
VRRP....55

ほ

ポート
1 次トラステッドとアントラステッド....43
2 次トラステッドとアントラステッド....43
冗長....2
フェールオーバー....43

め

メッセージ
HA....7
制御....13

も

モード
NAT とルート....2
優先使用....21

ら

ランタイムオブジェクト
RTO を参照

る

ルートモード....2

概念と用例
ScreenOS リファレンス ガイド

第 12 部 :
WAN、DSL、ダイアル、およびワイヤレス

リリース 6.0.0、改訂 02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

品番 : 530-017778-01-JP, 改訂 02

Copyright Notice

Copyright © 2007 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

目次

本編について ix

ドキュメントの規則 ix
Web ユーザーインターフェースの規則 x
コマンドラインインターフェースの規則 x
ネーミング規則および文字タイプ xi
説明図の規則 xii
技術ドキュメンおよびテクニカルサポート xiii

第 1 章 ワイドエリアネットワーク 1

WAN の概要 1
シリアル 2
T1 3
E1 3
T3 4
E3 4
ISDN 5
WAN インターフェースのオプション 7
Hold Time (保持時間) 8
フレームチェックサム 9
アイドルサイクルフラグ 9
開始 / 終了フラグ 10
ラインエンコーディング 10
Alternate Mark Inversion エンコーディング 10
B8ZS および HDB3 ラインエンコーディング 11
バイトエンコーディング 11
ラインビルドアウト 12
フレーミングモード 12
T1 用のスーパーフレーム 13
T1 用の拡張スーパーフレーム 13
T3 用の C ビットパリティフレーミング 13
クロッキング 13
クロッキングモード 14
クロッキングソース 15
内部クロック速度 15
送信クロックの反転 16
信号処理 17
ループバック信号 18
リモートループバックとローカルループバック 18
ループバックモード 18
CSU 互換モード 20
リモートループバック応答 21
FEAC 応答 22

WAN インターフェースのオプション（続き）
タイムスロット 22
フラクショナル T1 22
フラクショナル E1 23
ビット誤り率テスト 23
ISDN オプション 25
スイッチタイプ 25
SPID 25
TEI ネゴシエーション 26
発呼者番号 26
T310 値 26
送信完了 27
BRI モード 27
専用回線モード 27
Dialer Enable 27
ダイヤラーオプション 28
WAN インターフェースの使用不可 29
WAN インターフェースのカプセル化 29
ポイントツーポイントプロトコル 30
フレームリレー 30
Cisco ハイレベルデータリンク伝送制御手順（Cisco-HDLC） 31
基本的なカプセル化オプション 32
番号なしインターフェース 32
プロトコル最大送信単位の構成 32
静的 IP アドレスの構成 33
キープアライブ 33
PPP カプセル化オプション 34
PPP アクセスプロファイル 34
PPP 認証方法 35
パスワード 36
PPP 認証プロトコル 36
チャレンジハンドシェイク認証プロトコル（CHAP） 36
パスワード認証プロトコル 37
ローカルデータベースユーザー 37
フレームリレーカプセル化オプション 38
キープアライブメッセージ 38
フレームリレー LMI タイプ 38
PVC の作成と構成 39
逆アドレス解決プロトコル 40
マルチリンクカプセル化 41
概要 41
基本的なマルチリンクバンドルの設定 42
バンドル識別子 42
ドロップタイムアウト 43
フラグメントしきい値 43
最小リンク 44
基本的な設定手順 45
最大受信再構築単位 45
シーケンスヘッダーの形式 46
マルチリンクフレームリレー構成オプション 46
基本的な設定手順 46
MLFR のリンク割り当て 47
確認リトライ 47
肯定応答タイマー 48

ハロータイマー 48
WAN インターフェース構成例 48
シリアルインターフェースの構成 49
T1 インターフェースの構成 49
E1 インターフェースの構成 50
T3 インターフェースの構成 51
E3 インターフェースの構成 51
ISDN 接続用のデバイスの構成 52
手順 1: ISDN スイッチタイプの選択 52
手順 2: PPP プロファイルの構成 52
手順 3: ISDN BRI インターフェースのセットアップ 53
1 つの宛先のみのダイヤルアウト 53
ダイヤラーインターフェースを使用したダイヤルアウト 54
専用回線モードの使用 57
手順 4: 宛先へのトラフィックのルーティング 58
カプセル化設定例 59
PPP カプセル化の構成 59
MLPPP カプセル化の構成 60
フレームリレーカプセル化の構成 62
MLFR カプセル化の構成 62
Cisco HDLC カプセル化の構成 64

第 2 章 デジタル加入者線 65

デジタル加入者線の概要 65
非同期転送モード 66
ATM 通信品質 67
Point-to-Point Protocol over ATM 68
マルチリンクポイントツーポイントプロトコル 69
DSL インターフェースの Discrete Multitone 69
アネックスモード 70
仮想回路 71
VPI/VCI および複合方式 71
PPPoE または PPPoA 72
静的 IP アドレスおよびネットマスク 73
ADSL インターフェース 74
G.SHDSL インターフェース 75
ループバックモード 75
操作、管理、および保守 76
信号対雑音比 77
ADSL 設定例 77
例 1:（小規模なビジネス / 自宅）ADSL インターフェース上の PPPoA .. 78
例 2:（小規模なビジネス / 自宅）ADSL インターフェース上の 1483 ブリッジング 81
例 3:（小規模なビジネス）ADSL インターフェース上の 1483 ブリッジング 83
例 4:（小規模なビジネス / 自宅）ダイヤルアップバックアップ 85
例 5:（小規模なビジネス / 自宅）Ethernet バックアップ 88
例 6:（小規模なビジネス / 自宅）ADSL バックアップ 91
例 7:（小規模なビジネス）MLPPP ADSL 94
例 8:（小規模なビジネス）ローカルサーバーへのアクセスを許可 96
例 9:（支店）ADSL を通した VPN トンネル 99
例 10:（支社）2 次 VPN トンネル 103

第 3 章 ISP フェールオーバーとダイヤル回復 109

フェールオーバーの ISP 優先順位の設定 109
ISP フェールオーバーの条件の定義 110
ダイヤルアップ回復ソリューションの構成 111

第 4 章 ワイヤレス ローカル エリア ネットワーク 115

概要 116
ワイヤレス製品によるインターフェース名指定の違い 117
基本的なワイヤレスネットワーク機能の構成 118
サービスセット識別子の作成 118
SSID ブロードキャストの抑制 118
クライアントの分離 119
2.4 GHz トランシーバへの操作モードの設定 119
5GHz トランシーバへの操作モードの設定 120
データ送信最低速度の構成 120
送信パワーの設定 121
WLAN 構成の再起動 122
SSID への認証と暗号化の設定 122
WEP（有線と同等のプライバシー）の構成 123
複数の WEP 鍵 123
オープン認証の設定 125
WEP 共有鍵認証の設定 127
Wi-Fi 保護アクセスの構成 128
WPA と WPA2 の 802.1X 認証の構成 129
WPA と WPA2 のため事前共有鍵認証の構成 130
アンテナ使用の指定 131
国コード、チャネルおよび周波数の設定 131
拡張チャネルの使用 132
サイト調査の実行 132
利用可能なチャネルの発見 133
アクセス制御リストエントリの設定 133
Super G の構成 134
Atheros XR（拡張範囲）の構成 135
Wi-Fi マルチメディアサービス品質の構成 136
WMM を有効にする 136
WMM サービス品質の構成 136
アクセスのカテゴリ 136
デフォルトの WMM 設定 137
例 139
詳細なワイヤレスパラメーターの設定 140
エージング間隔の構成 140
ビーコン間隔の設定 141
DTIM（Delivery Traffic Indication Message）期間の構成 142
バーストしきい値の構成 142
フラグメントしきい値の構成 143
送信要求しきい値の構成 143
送信可モードの構成 144
送信可速度の構成 144
送信可タイプの構成 144
スロット時間の設定 145
プリアンブル長の構成 145

ワイヤレスインターフェースでの作業 146
SSID のワイヤレスインターフェースへのバインド 146
ワイヤレスインターフェースのトランシーバへのバインド 146
ワイヤレスブリッジグループの作成 147
ワイヤレスインターフェースの使用不可 148
ワイヤレス構成情報の表示 148
設定例 149
例 1: オープン認証および WEP 暗号化 149
例 2: パスフレーズおよび自動暗号化を持っている WPA-PSK 認証 150
例 3: 透過モードの WLAN 150
例 4: 複数および差別化されたプロファイル 154

索引 ..... IX-I

本編について

第 12 部 : WAN、DSL、ダイアル、およびワイヤレス、ワイドエリアネットワーク（WAN）、非対称デジタル加入者線（ADSL）およびワイヤレスローカルエリアネットワーク（WLAN）インターフェースを説明します。本編の章は、以下のようになります。

- 第 1 章「ワイドエリアネットワーク」では、ワイドエリアネットワーク（WAN）を構成する方法を説明します。
- 第 2 章「デジタル加入者線」、は asymmetric digital subscriber line (ADSL) および G. 対称デジタル加入者線 (G.SHDSL) を説明します。
- 第 3 章「ISP フェールオーバーとダイヤル回復」では、ISP フォールオーバーの際の優先順位の設定方法および条件の定義方法、そしてダイヤルアップリカバリソリューションの設定方法について説明します。
- 第 4 章「ワイヤレス ローカル エリア ネットワーク」では、Juniper Networks ワイヤレスデバイス上のワイヤレスインターフェースについて説明し、その構成例を示します。

ドキュメントの規則

このドキュメントは、次のセクションで説明されている規則を使用しています。

- x ページの「Web ユーザーインターフェースの規則」
- x ページの「コマンドラインインターフェースの規則」
- xi ページの「ネーミング規則および文字タイプ」
- xii ページの「説明図の規則」

Web ユーザーインターフェースの規則

WebUI（Web ユーザーインターフェース）では、各作業の操作指示は、操作手順と構成設定値に分かれています。構成設定を入力できる WebUI ページを開くには、画面の左側にあるナビゲーション ツリーのメニュー項目をクリックして、そのページに移動します。先へ進むと、ナビゲーション パスが画面の上部に表示されます。各ページは角括弧で分離されています。

WebUI のパスおよびアドレスを定義するためのパラメータは、以下のとおりです。

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.2.2.5/32
Zone: Untrust

構成設定のオンラインヘルプを開くには、画面の左上にある疑問符（?）をクリックします。

ナビゲーションツリーにも、Help > Config Guide 構成ページがあり、セキュリティポリシーおよび IPSec （インターネットプロトコルセキュリティ）の構成に役立ちます。ドロップダウンメニューからオプションを選択して、そのページの指示に従います。構成設定のオンラインヘルプを開くには、左上にある **?** 文字をクリックします。

コマンドラインインターフェースの規則

次の規則は、例とテキストにおいて、コマンドラインインターフェース（CLI）コマンドの構文を示すために使用されます。

例においては、次のように使用されます。

- 角括弧 [ ] 内にあるものはすべてオプションです。
- 中括弧 { } 内にあるものはすべて必須です。
- 選択肢が複数ある場合、各選択肢はパイプ (|) で区切られています。例えば、次のように表示されます。

  set interface { ethernet1 | ethernet2 | ethernet3 } manage

- 変数は*斜体*で表示されます。

  set admin user *name1* password *xyz*

テキストにおいては、コマンドは**太字**で、変数は*斜体*で表示されます。

注： キーワード入力時には、単語を間違いなく識別できる数の文字を入力すれば十分です。**set admin user wheezer j12fmt54** というコマンドを入力する際には、**set adm u whee j12fmt54** と入力するだけで十分です。ただし、本編に記載されたコマンドはすべて本来の形式で記載されています。

ネーミング規則および文字タイプ

ScreenOS はオブジェクトの名前 (アドレス、管理ユーザー、認証サーバー、IKE ゲートウェイ、仮想システム、VPN トンネルおよびゾーンなど、ScreenOS 構成に定義されているもの) に関して、次の規則に従います。

- 名前文字列に 1 つまたは複数のスペースが含まれる場合、文字列全体を二重引用符で囲む必要があります。例 :

  set address trust “local LAN” 10.1.1.0/24

- 二重引用符で囲まれた文字列の先頭または末尾のスペースを取り除きます。たとえば、**「 local LAN 」**は**「local LAN」**となります。

- 連続した複数のスペースは、一つのスペースとして扱われます。

- CLI キーワードの多くはケースセンシティブではありませんが、名前文字列はケースセンシティブです。たとえば、**「local LAN」**は**「local lan」**とは異なります。

ScreenOS は、次の文字タイプをサポートします。

- 1 バイト文字セット (SBCS) およびマルチバイト文字セット (MBCS)。SBCS の例に、ASCII、欧州言語、およびヘブライ語があります。2 バイト文字セット (DBCS) とも呼ばれる MBCS の例に、中国語、韓国語、および日本語があります。

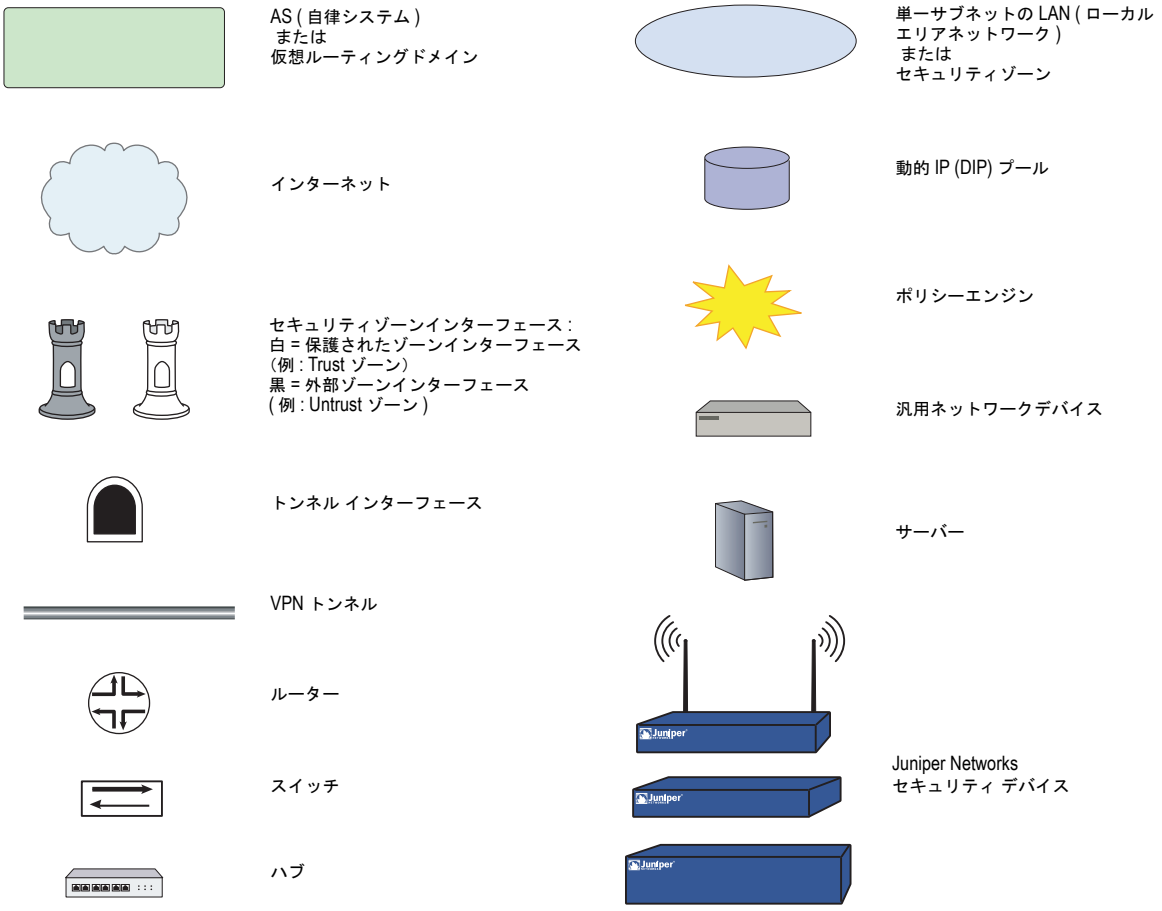
- ASCII 文字の 32（16 進数の 0x20）から 255（0xff)。ただし二重引用符 (“) は、スペースを含む名前文字列の先頭と末尾を示す特殊な意味をもつため、例外とします。

注 : コンソール接続では、SBCS のみがサポートされます。ご利用のブラウザがサポートする文字セットに応じて、WebUI は SBCS および MBCS の両方をサポートします。

説明図の規則

次の図は、本編を通して説明図に使用されている画像の基本的なものです。

図 1: 説明図の画像



技術ドキュメンおよびテクニカルサポート

Juniper Networks 製品のいずれかの技術ドキュメントを入手するには、www.juniper.net/techpubs/ をご覧になってください。

テクニカルサポートについては、http://www.juniper.net/customers/support/ にある Case Manager を使って事例サポートを開くか、1-888-314-JTAC (米国内) か 1-408-745-9500 (その他の国) までお問い合わせください。

本書に間違いや欠落があった場合は、techpubs-comments@juniper.net までお知らせください。

第 1 章

ワイドエリアネットワーク

セキュリティデバイスには、地理的に分散したネットワークを介してトラフィックを送受信するため、ワイドエリアネットワーク（WAN）データリンクを使用できるものがあります。これらのネットワークは、私有できますが、通常は公開または共用のネットワークを含んでいます。WAN リンクが正しく動作するには、（物理ラインでは）クロッキングおよび信号処理のオプションおよび（WAN を横断してデータを転送するための）カプセル化の方法など、プロパティを構成する必要があります。

本章のセクションは、以下のようになります。

- 1 ページの「WAN の概要」
- 7 ページの「WAN インターフェースのオプション」
- 29 ページの「WAN インターフェースのカプセル化」
- 41 ページの「マルチリンクカプセル化」
- 48 ページの「WAN インターフェース構成例」
- 59 ページの「カプセル化設定例」

WAN の概要

このセクションでは次の WAN インターフェースを定義します。

- 2 ページの「シリアル」
- 3 ページの「T1」
- 3 ページの「E1」
- 4 ページの「T3」
- 4 ページの「E3」
- 5 ページの「ISDN」

シリアル

シリアルリンクは、制御信号をほとんど必要としない双方向リンクを提供します。基本的なシリアルのセットアップでは、データ回線終端装置（DCE）は接続の確立、維持、および終了を担当します。モデムは典型的な DCE デバイスです。最終的にリンクがデータ端末装置（DTE）で確立されるテレフォニーネットワークに、シリアルケーブルは DCE を接続します。DTE は通常、リンクが終端する場所です。

セキュリティデバイスには、次のタイプのシリアルインターフェースをサポートするものがあります。

- TIA/EIA 530 — The Telecommunications Industry Association/Electronics Industries Alliance (TIA/EIA) Standard 530, *High-Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment* では、個別の制御回路上で交換された制御情報を持つシリアルの 2 進データ交換を使用する、DTE と DCE の相互接続について説明しています。

- V.35 — The Telecommunication Standardization Sector of the International Telecommunications Union (ITU-T) Recommendation V.35, *Data Transmission at 48 kbit/s Using 60-108 kHz Group Band Circuits* では、ネットワークアクセスデバイスとパケットネットワークの間の通信に使用される、同期物理層プロトコルについて説明しています。V.35 は、米国とヨーロッパで最も一般に使用されています。

- X.21 — The ITU-T Recommendation X.21, *Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment for Synchronous Operation on Public Data Networks* は、同期デジタル回線上でのシリアル通信を説明しています。X.21 プロトコルは、主としてヨーロッパと日本で使用されています。

- RS-232 — TIA/EIA-232-F（the current revision）、*Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange* は、モデムや他のシリアルデバイスとの通信用の物理インターフェースおよびプロトコルを説明しています。

- RS-449 — The EIA standard *EIA-449 General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange* では、DTE と DCE との間のインターフェースを指定しています。

シリアル接続が行われる場合、EIA-530、X.21、RS-422/449、RS-232、V.35 などのシリアルラインプロトコルは、以下のようにラインを横断して信号の送信を制御し始めます。

1. DCE が、DTE に DSR 信号を送信し、DTE は DTR 信号で応答します。この送信の後、リンクが確立され、トラフィックが通過できるようになります。

2. DTE デバイスがデータ受信の準備ができている場合、データを送信できることを DCE に示すため、その RTS 信号をマークされた状態（すべて 1）に設定します。

3. DCE デバイスがデータ受信の準備ができている場合、データを送信できることを DTE に示すため、その CTS（clear-to-send）信号をマークされた状態に設定します。

4. 情報を送信するためのネゴシエーションが行われると、データは、送信データ（TD）ラインと受信データ（RD）ラインを横断して送信されます。

   - TD ライン ー DTE デバイスからのデータが DCE デバイスに送信されるライン。
   - RD ライン ー DCE デバイスからのデータが DTE デバイスに送信されるライン。

T1

データ信号 1（DS1）とも呼ばれる T1 は、合計して 1.544 Mbps で動作している 24 本の同時接続（時間スロットまたはチャンネルとも呼ばれる）を処理できるデジタルデータ伝送メディアです。T1 は、これらの 24 本の別々の接続を 1 つのリンクに統合します。

T1 データストリームはフレームに分解されます。各フレームは、1 つのフレーミングビットと 24 の 8 ビットチャネルから構成され、T1 フレーム 1 つ当たり合計 193 ビットになります。フレームは、1 秒間に 8,000 回送信され、データ転送速度は 544 Mbps になります（8,000 x 193 = 1.544 Mbps）。各フレームが受信、処理されるので、各 8 ビットチャネルのデータは、前のフレームからのチャネルデータとともに維持され、T1 トラフィックは、単一媒体を横断して 24 の個別のフローへ分離できます。

サポートされている T1 標準は次の通りです。

- American National Standards Institute (ANSI) T1.107、*Digital Hierarchy - Formats Specifications,* は、デジタル階層形式を説明し、T1.102, *Digital Hierarchy - Electrical Interfaces* と使用されます。
- Telcordia GR 499-CORE, *Transport Systems Generic Requirements（TSGR）: Common Requirements* は、トランスポートシステムに共通の基本的な一般要件を説明しています。Telcordia GR 253-CORE, *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria* は、一般的な SONET 基準を説明しています。
- AT&T Technical Reference 54014, *ACCUNET T45 and T45R Service Description and Interface Specification* は、AT&T ACCUNET T45 および T45R サービスのサービス内容とインターフェースの仕様を説明しています。
- 国際電気通信連合（ITU-T）勧告 G.751 および G.703 は、階層構造デジタルインタフェースの物理的、電気的特性を説明しています。

E1

E1 は DS1 デジタル伝送用のヨーロッパの形式です。E1 リンクは、信号の転送速度が 2.048 Mbps である点を除いて、T1 リンクに似ています。各信号には 32 チャネルあり、各チャネルが 64 Kbps で送信します。すべてが 8 ビットチャネルを使用するので、E1 リンクは T1 リンクより帯域幅が高くなっています。

次の標準が E1 インターフェースに適用されます。

- ITU-T 勧告 G.703, *Physical/Electrical Characteristics of Hierarchical Digital Interfaces* は、データ転送速度と多重スキームを説明しています。

- ITU-T 勧告 G.751, *General Aspects of Digital Transmission Systems: Terminal Equipment* は、フレーミングの方法を説明しています。
- ITU-T 勧告 G.775, *Loss of Signal（LOS）and Alarm Indication Signal（AIS）Defect Detection and Clearance Criteria* は、アラームをレポートする方法を説明しています。

T3

データ信号 3（DS3）とも呼ばれる T3 は、7 つの別個の DS2 信号へ 28 個の DS1 信号を多重化し、単一の DS3 信号へ DS2 信号を統合することにより構成された、高速データ通信媒体です。T3 リンクは 43.736 Mbps で動作します。

サポートされている T3 標準は次の通りです。

- American National Standards Institute (ANSI) T1.107、*Digital Hierarchy - Formats Specifications,* は、デジタル階層形式を説明し、T1.102, *Digital Hierarchy - Electrical Interfaces* と使用されます。
- Telcordia GR 499-CORE, *Transport Systems Generic Requirements (TSGR): Common Requirements* は、トランスポートシステムに共通の基本的な一般要件を説明しています。Telcordia GR 253-CORE, *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria* は、一般的な SONET 基準を説明しています。
- Telcordia TR-TSY-000009, A*synchronous Digital Multiplexes, Requirements and Objectives* は、DS1C（3.152 Mbps）、DS2（6.312 Mbps）や DS3（44.736 Mbps）デジタル速度で動作する、非同期多重化の一般的な技術的要件と目標を説明しています。
- AT&T Technical Reference 54014, *ACCUNET T45 and T45R Service Description and Interface Specification* は、AT&T ACCUNET T45 および T45R サービスのサービスの内容とインターフェースの仕様を説明しています。
- ITU G.751, *Digital multiplex equipment operating at the third order bit rate of 34 368 kbit/s and the fourth order bit rate of 139 264 kbit/s and using positive justification*、G.703, *Physical/electrical characteristics of hierarchical digital interfaces*、および G.823, *The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy* は、送信システムと媒体、デジタルシステムおよびネットワークを説明しています。

E3

E3 は、ヨーロッパで使用される T3 と類似の標準です。16 の個別の E1 信号をいっしょに多重化することにより形成されます。34.368 Mbps で動作します。

サポートされている E3 標準は次の通りです。

- ITU G.751, *Digital multiplex equipment operating at the third order bit rate of 34 368 kbit/s and the fourth order bit rate of 139 264 kbit/s and using positive justification*、G.703, *Physical/electrical characteristics of hierarchical digital interfaces*、および G.823, *The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy* は、送信システムと媒体、デジタルシステムおよびネットワークを説明しています。

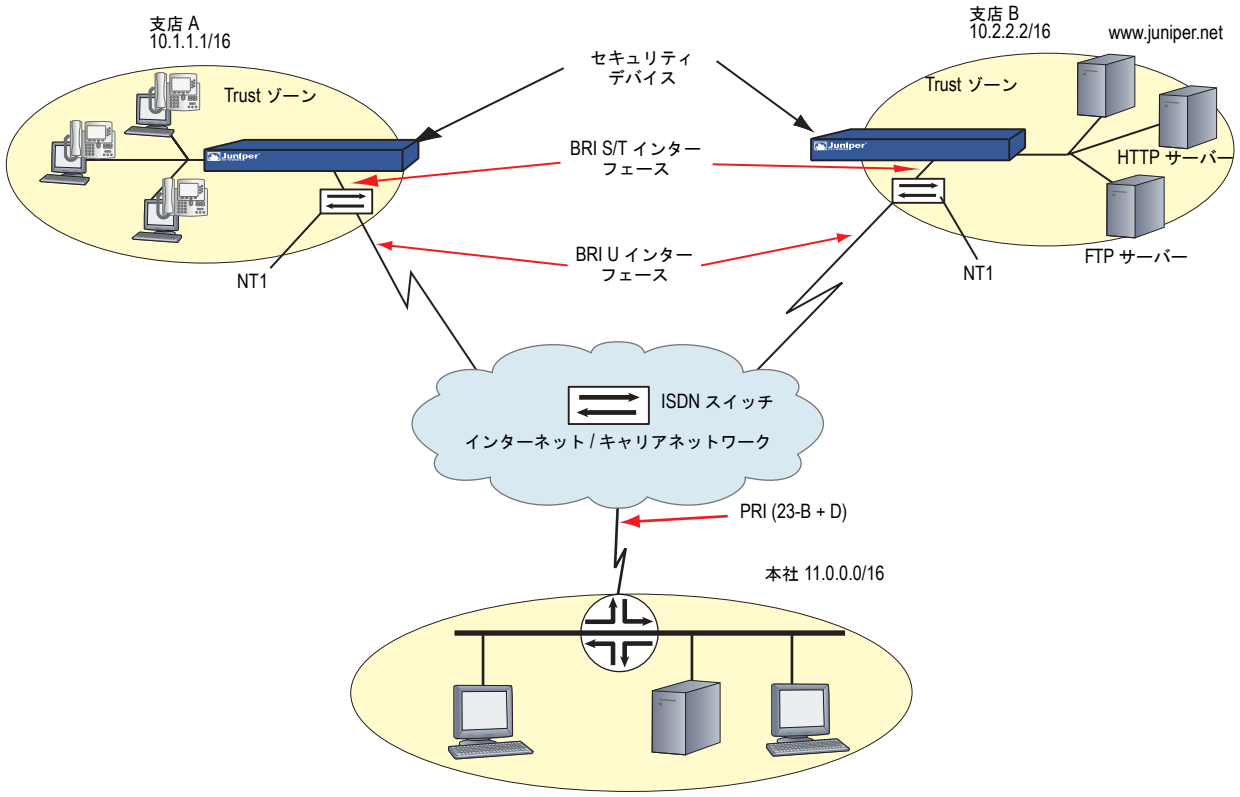
- Telcordia GR 499-CORE, *Transport Systems Generic Requirements (TSGR): Common Requirements* は、トランスポートシステムに共通の基本的な一般要件を説明しています。Telcordia GR 253-CORE, *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria* は、一般的な SONET 基準を説明しています。

ISDN

統合サービスデジタル網（ISDN）は、デジタル電話ラインに関する、音声、ビデオおよびデータの送信のための国際通信標準です。ダイヤルオンデマンドサービスとして、ISDN は、高品質の音声、データ、ビデオ送信を行う機能を持ち、呼設定が高速でレイテンシーも低くなっています。ISDN はまた、マルチポイント接続とポイントツーポイント接続の両方で利用できる、回線交換サービスです。

図 2 は、ISDN 接続の基本セットアップを示します。支店は ISDN を使用して、本社に接続されています。この接続は、インターネットにパケットを送信する要求に対して、自動的に確立されます。また、設定した秒数がトラフィックなしで経過した後、接続が切られます。ISDN 接続は通常、数ミリ秒（ほとんど一瞬）で確立できるので、要求に応じて、接続は簡単に確立および切断できます。

図 2: 基本的な ISDN トポロジ



北米では、ほとんどのキャリアは ISDN 接続に U インターフェースを提供します。ご使用のセキュリティデバイスと通信するには、U インターフェースを S/T インターフェースに変換するため、追加装置のネットワーク終端装置（NT1）を使用しなければなりません。Juniper Networks のセキュリティデバイスには、S/T インターフェースのみが提供されています。NT1 は顧客サイトに配置します（図 2 の支店を参照）が、キャリアが提供する場合もあります。

ScreenOS の ISDN は、セキュリティデバイスの次の機能をサポートします。

- ダイヤルオンデマンドルーティング（DDR）

  DDR により、セキュリティデバイスは、送信ステーションの要求に応じて、自動的にセッションを開始、終了できます。そのセッションをアクティブであると終端ステーションが処理するように、デバイスはキープアライブをスプーフィングできます。DDR は、必要な場合だけ、ユーザーに WAN リンクを呼び出し、したがって、リモートサイトアクセスコストを削減します。

- 基本レートインタフェース（BRI）

  2 つの 64 Kbps B チャネルと 1 つの 16 Kbps D チャネルから構成されるので、BRI は 2B + D とも呼ばれます。B チャネルは、ユーザーデータに使用されます。また、D チャネルは、サイト間の接続を確立、終了するための信号トラフィックの転送を担当します。

  各 ISDN BRI では bri*x*/0 といった命名規則を使用します。ここでは *x* はスロット ID、*x*/0 は **slot-id/port-id** を表します。たとえば、Bri0/0 の 2 つの B チャネルは、*bri0/0.1* および *bri0/0.2* となります。

- オンデマンド帯域幅

  2 つの 64Kbps B チャネルは、必要に応じて、1 つの 128Kbps 接続を構成するよう組み合わせることができます。デバイスは、ISDN インターフェースのオンデマンド帯域幅を以下のようにサポートします。

  - トラフィックが設定されたしきい値を越えると、より多くのチャネルを呼び出します。
  - トラフィックが設定されたしきい値未満でる場合、チャネルを切断します。

  オンデマンド帯域幅は、マルチリンク PPP（MLPPP）カプセル化を使用して、ご使用のセキュリティデバイスで実装されます。

- ダイヤラーインターフェースとダイヤラープール

  ダイヤラーインターフェースとダイヤラープールにより、宛先の数が利用可能な物理ラインの数を超過すると、ISDN インターフェースは、複数の宛先へダイヤルアウトできます。ISDN インターフェースは、複数のプールに所属することができ、1 本のラインを複数の宛先へダイヤルアウトするのに使用できます。

  この機能の詳細については、54 ページの「ダイヤラーインターフェースを使用したダイヤルアウト」を参照してください。

- ダイヤルバックアップ

  一次同期ラインが失敗した場合に、二次 WAN リンクを有効にするため、ISDN インターフェースをダイヤルバックアップに使用できます。

- リース回線

  ISDN 専用回線は 128 Kbps でサポートされています。専用回線モードにおいて、ISDN インターフェースは、データだけを運ぶことができるレイヤ 3 インターフェースとして動作します。したがって、D チャネルは必要ありません。

- ISDN インターフェースとダイヤラーインターフェースの監視

WAN インターフェースのオプション

このセクションでは、セキュリティデバイスのいくつかで利用可能な WAN インターフェースのオプションを説明します。表 1 は、どの物理的な属性が WAN インターフェースで利用可能かを示します。

表 1: WAN インターフェースの物理属性

物理属性	シリアル	T1	E1	T3	E3	ISDN（BRI）
Hold time	X	X	X	X	X	X
DTE オプション	X					
フレームチェックサム		X	X	X	X	
アイドルサイクルフラグ		X	X	X	X	X
開始 / 終了フラグ		X	X	X	X	
信号処理	X					
クロッキング						
クロッキングモード	X					
クロッキングソース		X	X	X	X	
内部クロック速度	X					
送信クロックの反転	X					
タイムスロット						
フラクショナル T1 タイムスロット		X				
フラクショナル E1 タイムスロット			X			
ラインエンコーディング						
AMI		X				
B8ZS		X				
HDB3			X			
バイトエンコーディング		X				
データ反転		X	X			

物理属性	シリアル	T1	E1	T3	E3	ISDN（BRI）
フレーミング						
スーパーフレーム		X				
拡張フレーム		X				
G.704 フレーム			X			
G0.751 フレーム					X	
C ビットパリティフレーム				X		
ループバック信号						
ループバックモード		X			X	X
ビット誤り率テスト（BERT）		X	X	X	X	
CSU 互換モード				X		
リモートループバック応答		X		X	X	
FEAC 応答				X		
ISDN オプション						
スイッチタイプ						X
SPID1						
SPID2						X
TEI ネゴシエーション						X
発呼者番号						X
T310 値						X
送信完了						X
BRI モード （専用回線 / ダイヤラー）						X
ダイヤラーオプション						
主要 / 代替番号						X
ロードしきい値						X
アイドル時間						X
リトライ回数						X
間隔						X
ダイヤラープール						X

Hold Time (保持時間)

保持時間は、インターフェース接続が有効か無効かをデバイスが判断する前に、どれだけの時間が経過してもよいかを指定します。インターフェースが追加ドロップマルチプレクサ（ADM）または波長分割マルチプレクサ（WDM）に接続されているといった状況や、インターフェースがその接続が有効または無効であるか通知したくないので、SONET/SDH（Synchronous Optical Network/Synchronous Digital Hierarchy）フレーマーホールを防ぐために、保持時間が役立ちます。

たとえば、インターフェースが有効から無効になる場合、指定された保持時間の間、無効であってから、システムの他の部分に通知されます。同様に、インターフェースは、指定された保持時間、有効であるまで、有効であるとシステムの他の部分に通知されません。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: 以下を入力して **Apply** をクリックします。

Hold Time (**保持時間**)
Down: 500
Up: 500

CLI

```
set interface interface hold-time { down 500 | up 500 }
save
```

注 : 保持時間が 0 の場合、デバイスはインターフェースが無効であるというメッセージを受信すると、インターフェースはトラフィックをドロップします。

フレームチェックサム

フレームチェックサムは、ビットエンコードスキームを使用して、デバイスを通過するフレームが有効であることを確認します。WAN インターフェースには 16 ビットのフレームチェックサムを使用するものがありますが、もっと信頼できるパケット確認を行うため 32 ビットのチェックサムを設定できます。

32 ビットのチェックサムを使用するよう WAN インターフェースを構成するには、次を行います（x は t1、e1、または t3）。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: **Frame Checksum** オプションで、**32-bits** を選択し、**Apply** をクリックします。

CLI

```
set interface interface x-options fcs 32
save
```

アイドルサイクルフラグ

アイドルサイクルとは、デバイスに送信するべきデータがない期間のことです。アイドルサイクルフラグでは、WAN インターフェースはアイドルサイクルの間に、値 0x7E を送信できます。WAN インターフェースが値 0xFF（すべて 1）を送信するよう構成するには、以下を行います（x は t1、e1、または bri）。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: **Idle-cycle Flags** オプションで、**0xFF (All ones)** を選択し、**Apply** をクリックします。

CLI

```
set interface interface x-options idle-cycle-flag ones
save
```

開始 / 終了フラグ

T1 または E1 インターフェースの開始 / 終了フラグは、開始フラグと終了フラグとを送信する間に、2 アイドルサイクル分待ちます。インターフェースが、開始フラグと終了フラグの送信を共有するよう構成するには、以下を行います（x は t1 または e1）。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: **Start/End Flags on Transmission** オプションで、**Shared** を選択し、**Apply** をクリックします。

CLI

set interface *interface* x-options start-end-flag shared

T3 インターフェースで開始フラグと終了フラグの送信を共有するには、以下を行います。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: ラインエンコーディングタイプを選択して **Apply** をクリックします。

CLI

set interface *interface* t3-options start-end-flag
save

ラインエンコーディング

次に一般的な T1 および E1 エンコーディング技術を示します。

- AMI（Alternate mark inversion）— T1 および E1
- B8ZS（Bipolar with 8-zero substitution）— T1 のみ
- HDB3（High-density bipolar 3 code）— E1 のみ

エンコーディングタイプを変更するには、以下を行います（x は t1 または e1）。

WebUI

Network > Interfaces > List > Edit (*X Interface*) > WAN: ラインエンコーディングタイプを選択して **Apply** をクリックします。

CLI

set interface *interface* x-options line-encoding *option*
save

Alternate Mark Inversion エンコーディング

AMI エンコーディングは、T1 または E1 ライン上の 1 信号について、連続するそれぞれ送信について、電圧の正負を交互に変更します。AMI（Alternate Mark Inversion）エンコーディングが使用される場合、長い 0 の連続を持つデータ送信では、ライン上の電圧変化がありません。この状況では、送信するクロックと絶えず同期するのに電圧の変化に依存しているので、デバイスは、クロック同期を維持するのに苦労します。この影響を防ぐため、データストリーム中の連続す

る 0 の数を 15 に制限します。送信される 15 個の 0 ごとに、ある数の 1 が必要となるので、この制限は、1 の密度要件と呼ばれます。AMI でエンコードされたラインでは、同じ極性の 2 つの連続パルスは、正か負かに関係なく、バイポーラ違反（BPV）と呼ばれ、一般にエラーのフラグが立てられます。

データ反転

データ反転を有効にすると、データストリーム中のデータビットはすべて逆に送信されます。すなわち、0 は 1 として、1 は 0 として送信されます。データ反転は通常、送信したストリームに密度を提供するため、AMI モードのみで使用されます。データ反転を有効にするには、以下を行います。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: Invert Data チェックボックスをオンにして、**Apply** をクリックします。

CLI

set interface *interface* t1-options invert-data
save

B8ZS および HDB3 ラインエンコーディング

B8ZS（both bipolar with 8-zero substitution）および HDB3（high-density bipolar 3 code）エンコーディングは両方とも、ライン上で送信できる 0 の数を制限しません。代わりに、これらのエンコーディング方法は、リンク上でタイミングを維持するのに必要な信号の発振を提供するため、0 の連続を検出して、その場所のビットパターンを置換します。T1 ラインの B8ZS エンコーディング方法では、8 つの連続する 0 の送信を検知し、2 つの連続する BPV（11110000）のパターンと置換します。受信側は同じエンコーディングを使用するので、BPV が 0 を置換したものであることを検知し、BPV エラーフラグは立てられません。単一の BPV は、11110000 の置換ビットシーケンスとマッチしないため、デバイスの設定によってはエラーを生成します。

E1 ラインの HDB3 エンコーディング方法では、連続 4 つの 0 送信のシーケンスを検知し、単一の BPV（1100）と置換します。B8ZS エンコーディングと同様に、受信デバイスは 0 置換を検知し、BPV エラーを生成しません。

バイトエンコーディング

T1 インターフェースは、1 バイト当たり 8 ビットのバイトエンコーディングを使用します（nx64）。1 バイト当たり 7 ビットの代替バイトエンコーディングを設定できます（nx56）。インターフェースのバイトエンコーディングを構成するには、以下を行います。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: バイトエンコーディングタイプを選択して **Apply** をクリックします。

CLI

set interface *interface* t1-options byte-encoding *option*
save

ラインビルドアウト

WAN インターフェースでは、ラインビルドアウトを構成できます。これは、デバイスと主なオフィスの間のプログラム可能な距離です。T1 インターフェースには、ラインビルドアウト用の 5 つの可能な設定範囲があります。

- 0 ～ 40 m
- 40 ～ 81 m
- 81 ～ 121 m
- 121 ～ 162 m
- 162 ～ 200 m

T3 インターフェースには T3 ラインビルドアウトのための 2 つの設定があります。短い設定は、255 フィート（約 68 メートル）未満であり、長い設定は、255 フィート以上で 450 フィート（約 137 メートル）未満です。

インターフェースライン範囲を設定するには、以下を行います（X は t1 または t3）。

WebUI

Network > Interfaces > List > Edit (*X Interface*) > WAN: ラインビルドアウト範囲を選択して **Apply** をクリックします。

CLI

set interface *interface* t1-options buildout *range*
save

または

set interface *interface* t3-options long-buildout
save

フレーミングモード

T1 インターフェースは、スーパーフレーム（SF）と拡張スーパーフレーム（ESF）の、2 つのタイプのフレーミングを使用します。E1 インターフェースは、G.704 フレーミングまたは CRC4 フレーミングのない G.704 を使用するか、あるいは非フレーミングモードでもかまいません。E3 インターフェースは、G.751 フレーミングを使用するか、あるいは非フレーミングモードでもかまいません。

WAN インターフェースのフレーミングを構成するには、以下を行います（x は t1、e1、t3、または e3）。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: フレーミングモードを選択して **Apply** をクリックします。

CLI

set interface *interface* x-options framing *options*

T1 用のスーパーフレーム

D4 とも呼ばれるスーパーフレーム（SF）は、192 データビットから構成されます。8 ビットチャネルが 24、フレーミングビットが 1 つあります。その 1 つのフレーミングビットは、12 ビットフレーミングシーケンスの一部です。各 T1 フレームの 193 番目のビットがある値に設定され、12 ビット SF のフレーミングビットパターンを決定するため、12 の連続したフレームごとに確認します。受信デバイスは、着信データストリームと同期するため、これらのビットを検出し、いつフレーミングパターンが始まり終わるかを決定します。

T1 用の拡張スーパーフレーム

拡張スーパーフレーム（ESF）では、D4 SF を 12 フレームから 24 フレームまで延長し、またビットを 12 から 24 に増やします。余分なビットは、フレーム同期、エラー検出および施設データリンク（FDL）による保守通信に使用されます。SF シーケンスのフレーム 4、8、12、16、20 および 24 のフレーミングビットだけが使用され、同期パターンを作成します。

T3 用の C ビットパリティフレーミング

C ビットパリティモードは、送信された T3 信号上に存在するフレーミングのタイプを管理します。C ビットパリティモードが有効な場合、C ビットの位置は、ANSI T1.107a-1989 で定義されているように、FEBE（Far End Block Error）、FEAC（Far-End Alarm and Control）、端末データリンク、パスパリティ、およびモードインジケータビットに使用されます。C ビットパリティモードが無効な場合、基本の T3 フレーミングモード（M13）が使用されます。

T3 インターフェースで C ビットパリティモードを無効にし、M13 フレーミングを使用するには、以下を行います。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: フレーミングモードを選択して **Apply** をクリックします。

CLI

```
unset interface interface t3-options cbit-parity
save
```

クロッキング

クロッキングは、ネットワークがどのように送信データをサンプリングするかを決めます。情報のストリームはネットワーク中のルーターによって受信されるので、クロックソースは、いつデータをサンプリングするかを指定します。WAN インターフェースには、次のクロッキング情報を設定できるものがあります。

- クロッキングモード
- クロッキングソース
- 内部クロック速度
- 送信クロックの反転

クロッキングモード

クロッキングモードには 3 つあります。

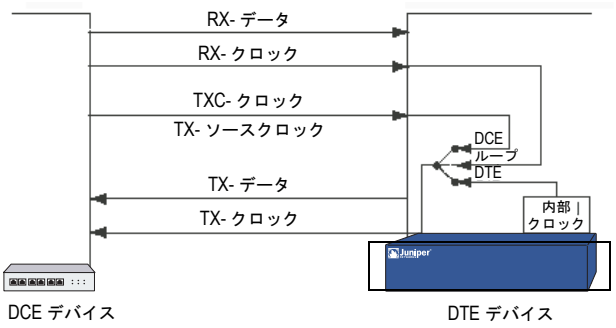
- **ループクロッキングモード**は、DCE から DTE へのデータをクロッキングするのに、DCE 受信（RX）クロックを使用します。
- **DCE クロッキングモード**は、DTE 送信（TX）クロックを使用します。これは、DTE が DTE 用の送信クロックとして使用できるように DCE が生成します。
- **内部クロッキングモード**は、*ラインタイミング*とも呼ばれ、内部で生成されるクロックを使用します。

注： TIA/EIA 530、V.35、RS0232 および RS-449 インターフェースでは、ループ、DCE あるいは内部クロッキングモードを使用するため、各インターフェースを独立して設定できます。X.21 インターフェースについては、ループクロッキングモードだけがサポートされます。

DCE クロッキングモードとループクロッキングモードは、DCE が生成した外部クロックを使用します。

図 3 は、ループ、DCE および内部クロッキングモードのクロックソースを示します。

図 3: シリアルインターフェースのクロッキングモード



シリアルインターフェースのクロッキングモードを構成するには、以下を行います。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN:

Hold Time (保持時間)
Clock Mode

クロッキングモードを選択して **Apply** をクリックします。

CLI

set interface *interface* serial-options clocking-mode { dce | internal | loop }

クロッキングソース

クロックソースは、制御ボードに存在する内部 stratum 3 クロック、または設定しているインターフェースから受信される外部クロックになります。

デフォルトでは、インターフェースのクロッキングソースは内部クロックです。つまり、各インターフェースは内部 stratum 3 クロックを使用することになります異なったクロックソースを使用できるインターフェースでは、ソースは内部（*ラインタイミング*または*ノーマルタイミング*とも呼ばれる）または外部（*ループタイミング*とも呼ばれる）のいずれかになります。

外部クロッを使用するインターフェースのクロックソースを設定するには、以下を行います。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN:

Hold Time
Clocking

クロッキングモードを選択して **Apply** をクリックします。

CLI

set interface *interface* clocking external

内部クロック速度

内部クロック速度は、内部クロッキングモードで通常使用される内部クロックの速度です。

注 : 内部クロッキングモードを設定した RS-232 インターフェースでは、クロック速度は 20 kHz 未満でなければなりません。

クロック速度を設定するには、以下を行います。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: 以下を選択して **Apply** をクリックします。

Hold Time (**保持時間**)
Clock Rate: **速度を選択する**

CLI

set interface *interface* serial-options clock-rate *number*
save

次のインターフェース速度を構成できます。

1.2 KHz	56.0 KHz	250.0 KHz	1.3 MHz
2.4 KHz	64.0 KHz	500.0 KHz	2.0 MHz
9.6 KHz	72.0 KHz	800.0 KHz	4.0 MHz
19.2 KHz	125.0 KHz	1.0 MHz	8.0 MHz
38.4 KHz	148.0 KHz		

WAN インターフェースは 8.0 MHz のデフォルト速度で使用することになっていますが、次の条件のいずれかが該当する場合、より低い速度を使用する必要があるかもしれません。

- 相互接続ケーブルが有効な操作には長すぎる。
- 相互接続ケーブルが外部雑音源にさらされている。これにより、ジェネレータの代わりに用いられた 50 オーム抵抗器により、ケーブルのロード終端の信号コンダクタと回路コモンの間で異なって測定される +1 ボルトを超える不要な電圧が発生する場合があります。
- 他の信号との干渉を最小化する必要があります。
- 1 つ以上の信号を反転する必要があります。

注： 内部クロッキングモードが有効な TIA/EIA 530、V.35、RS-232 および RS-449 インターフェースで、クロック速度を設定できます。内部クロッキングモードの詳細については、14 ページの「クロッキングモード」を参照してください。

信号速度とインターフェース用ケーブル距離との関係に関する詳細は、次の標準を参照してください。

- EIA 422-A, *Electrical Characteristics of Balanced Voltage Digital Interface Circuits*
- EIA 423-A, *Electrical Characteristics of Unbalanced Voltage Digital Interface Circuits*

送信クロックの反転

送信クロックは、WAN インターフェースを通して送信された各発信パケットを整列させます。デバイスが、外部でタイミングを取るクロッキングモード（DCE またはループ）を使用する場合、長いケーブルは、DTE に送信されたクロックとデータの位相シフトを引き起こす場合があります。高速では、この位相シフトがエラーを引き起こす可能性があります。送信クロックの反転は位相シフトを修正し、それによって、誤り率を小さくします。

送信を反転させるには、以下を行います。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: 以下を選択して **Apply** をクリックします。

Serial Options
Transmit clock invert: (**選択**)

CLI

set interface *interface* serial-options transmit-clock invert
save

信号処理

通常の信号処理は次の標準が定義しています。

- TIA/EIA 標準 530
- ITU-T 勧告 V.35
- ITU-T 勧告 X.21

表 2 は、各信号タイプをサポートするシリアルインターフェースのモードを示します。

表 2: シリアルインターフェースタイプによる信号処理

信号	シリアルインターフェース
DCE からの信号 :	
CTS (Clear-to-Send)	TIA/EIA 530、V.35、RS-232、RS-449
DCD (Data-Carrier-Detect)	TIA/EIA 530、V.35、RS-232、RS-449
DSR (Data-Set-Ready)	TIA/EIA 530、V.35、RS-232、RS-449
TM (Test-Mode)	TIA/EIA 530 のみ
DCE への信号 :	
DTR (Data-Transfer-Ready)	TIA/EIA 530、V.35、RS-232、RS-449
RTS (Request-to-Send)	TIA/EIA 530、V.35、RS-232、RS-449

シリアルインターフェースの特性を構成するには、以下を行います。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: 以下を選択して **Apply** をクリックします。

DTE Options
オプションを選択します

CLI

set interface *interface* serial-options dte-options { ... }
save

注 : **ignore-all** が指定されている場合、他の信号処理オプションは構成できません。

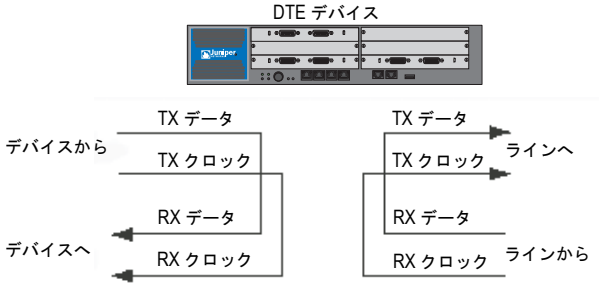
ループバック信号

T1、E1、T3、または E3 のリンク上の制御信号がループバック信号です。ループバック信号を使用すると、ネットワーク制御センターのオペレータは、リンクのリモートエンドにあるデバイスに、送信パス上にその受信信号を再送信して返すように指示できます。次に、送信デバイスは、受信信号が送信信号と一致するか確認でき、リンク上で末端間チェックを実行できます。

リモートループバックとローカルループバック

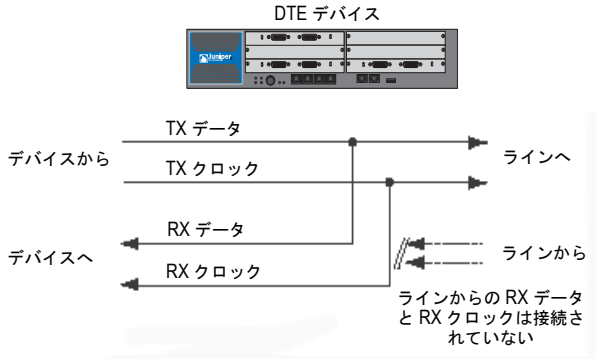
リモートラインインターフェース単位（LIU）ループバックは、受信（RX）データと RX クロックとして、デバイスに送信（TX）データと TX クロックをループします。図 4 に示すように、ラインから、LIU ループバックは、RX データと RX クロックを TX データおよび TX クロックとしてループバックします。

図 4: WAN インターフェースの LIU ループバック



ローカルの DCE とリモートの DCE は、リンクパートナー DCE の上のローカルおよびリモートループバックを有効にするため、TIA/EIA 530 インターフェース特有の信号を制御します。図 5 は、ローカルループバックを示します。

図 5: WAN インターフェースのローカルループバック



ループバックモード

図 6 に示すように、ローカルの T1、T3、E1、E3 または ISDN（bri）インターフェースとリモートのチャネルサービスユニット（CSU）の間でループバックモードを構成できます。ループバックモードは、ローカルまたはリモートに設定できます。ローカルのループバックでは、インターフェースは CSU にパケットを送信できますが、自身の送信を再受信し、CSU からのデータを無視します。リモートのループバックでは、CSU から送信されたパケットは、インター

フェースが受信し、有効なルートがある場合は転送され、CSU に直ちに再送信されます。ローカルおよびリモートのループバック送信は、データとクロッキング情報の両方をループバックします。パケットは、ローカルのルーティングプラットフォームまたはリモートの CSU のいずれかでループを構成できます。

シリアルインターフェースのループバックモードを構成するには、以下を行います。

WebUI

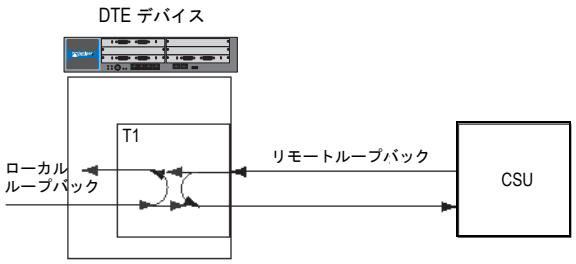
Network > Interfaces > List > Edit (*serial interface*) > WAN: 以下を選択して **Apply** をクリックします。

Diagnosis Options
Loopback Mode:

CLI

set interface *interface* serial-options loopback { dce-local | local | remote }
save

図 6: リモートおよびローカルの WAN インターフェースのループバックトラフィック



E1、E3、または ISDN（bri）インターフェースのループバックモードを構成するには、以下を行います。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: 以下を選択して **Apply** をクリックします。

Diagnosis Options
Loopback Mode: local または remote

CLI

set interface *interface* e1-options loopback { local | remote }
set interface *interface* e3-options loopback { local | remote }
set interface *interface bri*-options loopback { local | remote }
save

WAN インターフェースでは、リモートルーターでクロッキング情報なしでデータをループバックするため、ループバックペイロードオプションを設定できるものがあります。

T1 および T3 インターフェースのループバックモードを構成するには、以下を行います。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: 以下を選択して **Apply** をクリックします。

Diagnosis Options
Loopback Mode: payload

CLI

set interface *interface* t1-options loopback payload
set interface *interface* t3-options loopback payload
save

T3 HDLC ペイロードスクランブリングは、リンクの安定性を向上させます。接続の両側がスクランブルを使用するか、または両側が使用しないか、いずれかにします。

インターフェースの T3 チャネルでスクランブリングを構成するには、以下を行います。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN:

T3 Options
Check the Payload Scrambling checkbox

CLI

set interface *interface* t3-options payload-scrambler
set interface *interface* e3-options payload-scrambler
save

CSU 互換モード

T3 または E3 インターフェースをサブレートすると、HDLC でカプセル化されたペイロードを制限することにより、最大許容ピーク速度が低下します。サブレートモードは、多重化の独自の方法を使用する CSU と接続するようにインターフェースを設定します。

Digital Link、Kentrox、Adtran、Verilink あるいは Larscom の CSU と互換性をもつ T3 インターフェースを構成できます。Digital Link または Kentrox の CSU と互換性をもつ E3 インターフェースを構成できます。

ラインのリモートエンドにある CSU と互換性をもつように T3 インターフェースを設定するには、以下を行います。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN:

T3 Options
CSU Compatibility Mode を選択

CLI

set interface *interface* t3-options compatibility-mode { adtran | digital-link | kentrox | larscom | verilink } *number*
set interface *interface* e3-options compatibility-mode { digital-link | kentrox } *number*
save

T3 または E3 インターフェースのサブレートは、リモート CSU のサブレートと正確に一致しなければなりません。

各 CSU 互換モードには、異なる設定パラメーターがあります。

- Adtran: CSU で設定した値と正確に一致する 1 ～ 588 までの値に、サブレートを指定しなければなりません。588 のサブレート値は、44.2 Mbps、あるいは HDLC でカプセル化されたペイロードの 100 パーセントに相当します。1 のサブレート値は、44.2/588、つまり 75.17 Kbps、あるいは HDLC でカプセル化されたペイロードの 0.17 パーセントに相当します。

- Digital Link: **xKb** または **x.xMb** という形式で CSU で設定したデータ転送速度にサブレートを指定しなければなりません。デジタルリンク CSU では、**xKb** または **x.xMb** という形式で、CSU で設定したデータ転送速度と一致するようサブレート値を指定できます。サポートされる値のリストは、**compatibility-mode digital-link subrate** オプションの後に **?** を入力します。

- Kentrox: CSU で設定した値と正確に一致する 1 ～ 69 までの値に、サブレートを指定しなければなりません。69 のサブレート値は、34.995097 Mbps、あるいは HDLC でカプセル化されたペイロード（44.2 Mbps）の 79.17 パーセントに相当します。1 のサブレート値は、999.958 Kbps、あるいは HDLC でカプセル化されたペイロードの 2.26 パーセントに相当します。サブレート値が 1 増えると、約 0.5 Mbps の速度上昇に相当します。

- Larscom: CSU で設定した値と正確に一致する 1 ～ 14 までの値に、サブレートを指定しなければなりません。14 のサブレート値は、44.2 Mbps、あるいは HDLC でカプセル化されたペイロードの 100 パーセントに相当します。1 のサブレート値は、44.2/14、つまり 3.16 Mbps、あるいは HDLC でカプセル化されたペイロードの 7.15 パーセントに相当します。

- Verilink: CSU で設定した値と正確に一致する 1 ～ 28 までの値に、サブレートを指定しなければなりません。最大許容ピーク速度を計算するには、設定したサブレートに 1.578 Mbps を掛けます。たとえば、28 のサブレート値は、28 に 1.578 Mbps を掛けた値に相当します。これは、44.2 Mbps、つまり HDLC でカプセル化されたペイロードの 100 パーセントになります。1 のサブレート値は、1.578 Mbps、あるいは HDLC でカプセル化されたペイロードの 3.57 パーセントに相当します。20 のサブレート値は、20 掛ける 1.578 Mbps、つまり 31.56 Mbps、あるいは HDLC でカプセル化されたペイロードの 71.42 パーセントに相当します。

リモートループバック応答

T1 施設データリンクのループ要求信号は、作動モニタリングおよび診断の形で、様々なネットワーク情報を通信するために使用されます。拡張スーパーフレーム（ESF）は、施設データリンク（FDL）によって、非侵入シグナリングとコントロールをサポートし、それによってクリアチャネル通信を提供します。リモートループバック要求は、FDL 上でもインバインドにあってもかまいません。リモートループバック要求に応答するようインターフェースを構成するには、以下を行います。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: 以下を選択して **Apply** をクリックします。

T1 Options
Remote Loopback Respond: (**選択**)

CLI

```
set interface interface t1-options remote-loopback-respond
save
```

FEAC 応答

T3 FEAC（far-end alarm and control）信号を使用して、遠端端末から近端端末へアラームまたは状況情報を送信したり、近端端末から遠端端末で T3 ループバックを開始できます。

リモートのチャネルサービスユニット（CSU）がループバックにローカルのルーティングプラットフォームを入れることを可能にするには、CSU の FEAC 要求に応答するようルーティングプラットフォームを構成しなければなりません。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: 以下を選択して **Apply** をクリックします。

T3 Options
Remote Loopback Respond: (**選択**)

CLI

```
set interface interface t3-options feac-loop-respond
save
```

注： T3 **loopback** オプションでリモートまたはローカルのループバックを構成する場合、設定に **feac-loop-respond** オプションを含めても、ルーティングプラットフォームは、CSU からの FEAC 要求に応答しません。ルーティングプラットフォームが応答するには、設定から **loopback** オプションを削除する必要があります。

タイムスロット

タイムスロットは、チャネルまたはコネクタとも呼ばれ、T1 および E1 リンクと使用され、ユーザーは、ピン使用を細分したり、それらすべてを使用して単一のリンクを作成できます。

フラクショナル T1

タイムスロットは自由に組み合わせることができます。T1 インターフェースでは、タイムスロットの範囲は 1 ～ 24 です。

注： タイムスロットの範囲を設定するにはハイフンを使用します。連続しないタイムスロットを設定するにはコンマを使用します。空白を入れないでください。

フラクショナル T1 インターフェースに特定のタイムスロットを割り当てるには、以下を行います。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: 以下を入力して **Apply** をクリックします。

T1 Options
Timeslots: 1-5,10,24

CLI

set interface *interface* t1-options timeslots 1-5,10,24
save

フラクショナル E1

タイムスロットは自由に組み合わせることができます。ScreenOS は、フレーミングのためにショット 1 を予約しているので、フラクショナル E1 インターフェースを設定するのに使用ができません。E1 インターフェースでは、タイムスロットの範囲は 2 ～ 32 です。

注 : タイムスロットの範囲を設定するにはハイフンを使用します。連続しないタイムスロットを設定するにはコンマを使用します。空白を入れないでください。

フラクショナル E1 インターフェースに特定のタイムスロットを割り当てるには、以下を行います。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: 以下を入力して **Apply** をクリックします。

E1 Options
Timeslots: 4-6,11,25

CLI

set interface *interface* e1-options timeslots 4-6,11,25
save

ビット誤り率テスト

ビット誤り率テスト（BERT）は、リンクの品質をチェックし、ユーザーはインターフェースのエラーをトラブルシュートできます。インターフェースがこのテストの実行要求を受信すると BERT を実行するように、WAN インターフェースのいくつかを設定できます。

BERT は、ラインループが、送信デバイスまたは遠端ルーターのいずれかにあることを要求します。ローカルルーターは既知のビットパターンを生成し、送信パスからそれを送信します。それから、受信パターンは、送信されたパターンと比較、確認されます。受信パターンのビット誤り率（BER）が高いほど、物理ライン上の雑音がひどいことになります。遠端ルーターの方向へラインループの位置を少しずつダウンストリームに移動させると、リンクの問題の多い部分を分離できます。

BERT を開始する前に、**set interface** *interface* **disable** CLI コマンドでインターフェースを無効にします。

BERT パラメーターを構成するには、次の手順を行います。

1. 送信パスに送信するビットパターンまたはアルゴリズムを設定します。
2. インバウンドのパターンを受信する場合にモニタする誤り率を設定します。この値を指定するのに 0（デフォルト）～ 7 の整数の形式で指定します。この値は、BER の 10^{-0}（ビットあたり 1 つのエラー）から 10^{-7}（1000 万ビットあたり 1 つのエラー）に相当します
3. テスト時間を設定します。
4. 設定を保存します。
5. BERT を開始します。

この例では、T3 インターフェースの BERT パラメーターを、pseudo-2t35-o151 のアルゴリズム、10^{-4} のエラー率で 60 秒間テストを実行するように設定します。

WebUI

Network > Interfaces > List > Edit (*WAN interface*) > WAN: 以下を入力して **Apply** をクリックします。

BERT Algorithm: pseudo-2e9-o153 (**選択**)
BERT Error Rate: 4
BERT Test Length: 60
Loopback Mode: None (**選択**)

CLI

```
set interface serial1/0 t3-options bert-algorithm pseudo-2t35-o151
set interface serial1/0 t3-options bert-error-rate 4
set interface serial1/0 t3-options bert-period 60
save
exec interface serial1/0 bert-test start
```

注 : テストを早く終了する場合は、**exec interface** *interface* **bert-test stop** CLI コマンドを使用します。

BERT の結果を表示するには、**get counter statistics interface** *interface* **extensive** CLI コマンドを使用します。

注 : ローカルとリモートのルーティングプラットフォームの間で BERT パターンを交換するには、リンクのリモートエンドでインターフェース設定に **loopback remote** オプションを含めます。ローカルのルーティングプラットフォームからは、**exec interface** *interface* **bert-test start** CLI コマンドを発行します。

内部または外部に問題があるかどうかは、**show interface** *interface* **extensive** CLI コマンドを使用して出力のエラーカウンターをチェックすると確認できます。

ISDN オプション

ISDN オプションでは少なくとも ISDN スイッチタイプを設定する必要があります。他のオプションはキャリアが決定します。

スイッチタイプ

サポートされている ISDN スイッチタイプは、ATT5E、NT DMS-100、INS-NET、ETSI および NI1 です。

WebUI

Network > Interfaces > List > Edit (*bri*) > WAN: 以下を入力して **Apply** をクリックします。

Switch Type After Reboot:

CLI

set interface bri0/0 isdn switch-type att5e

SPID

サービスプロファイル識別子（SPID）を必要とする ISP を使用している場合、ご使用の ISDN デバイスは、接続を初期化するためスイッチにアクセスしたとき割り当てられる有効な SPID を ISP に送信するまで、通話を行ったり受信したりできません。

SPID は通常、いくつかのオプション番号を備えた 7 桁の電話番号です。しかし、ISP が異なると、異なる番号付けスキームを使用するかもしれません。DMS-100 スイッチタイプについては、2 つの SPID が B チャネルに 1 つずつ割り当てられます。キャリアが SPID 番号を定義します。

現在、DMS-100 と NI1 のスイッチタイプだけが SPID を必要とします。AT&T 5ESS スイッチタイプは、SPID をサポートできますが、SPID を使用せずに ISDN サービスをセットアップするよう推奨します。さらに、SPID はローカルアクセスの ISDN インターフェースでのみで意味があります。リモートルーターは SPID を受信しません。

WebUI

Network > Interfaces > List > Edit (*bri*) > ISDN: 以下を入力して **Apply** をクリックします。

SPID1: 123456789
SPID2: 987654321

CLI

set interface bri0/0 isdn spid1 123456789

TEI ネゴシエーション

端末エンドポイント識別子（TEI）ネゴシエーションは、アクティブコールがない場合、レイヤ 1 または 2 を非活性化してもよいスイッチで役立ちます。通常、この設定は、ヨーロッパでの ISDN サービスおよび、TEI ネゴシエーションを開始するように設計されている DMS-100 スイッチへの接続で使用します。

WebUI

Network > Interfaces > List > Edit (*bri*) > ISDN: 以下を入力して **Apply** をクリックします。

TEI negotiation: First Call

CLI

set interface bri0/0 isdn tei-negotiation first-call

最初の通話が行われる時（デフォルト）、またはデバイスのスイッチオン時に、TEI ネゴシエーションを実行できます。

発呼者番号

ISDN BRI が ISDN スイッチに供給する、発信コールの番号。ネットワークによっては、この数が示される通話では価格が割り引かれる場合があります。

WebUI

Network > Interfaces > List > Edit (*bri*) > ISDN: 以下を入力して **Apply** をクリックします。

Calling Number: 1234567890

CLI

set interface bri0/0 isdn calling-number 1234567890

発呼者番号は 32 文字未満の文字列でなければなりません。

T310 値

セキュリティデバイスが CALL PROC メッセージを受信した後に ALERT、CONNECT、DISC あるいは PROGRESS メッセージを受信しない場合、T310 タイムアウト値が終了した後、ネットワークに DISC メッセージを送信します。

WebUI

Network > Interfaces > List > Edit (*bri*) > ISDN: 以下を入力して **Apply** をクリックします。

T310 Value: 20

CLI

set interface bri0/0 isdn t310-value 20

5 ～ 100 秒の間の値を入力できます。デフォルトの T310 タイムアウト値は 10 秒です。

送信完了

香港と台湾などの場所では、ISDN スイッチは、全数が含まれることを示す発信コールセットアップメッセージに、送信完了情報要素を追加する必要があります。この IE は通常、他の場所では必要ありません。

WebUI

Network > Interfaces > List > Edit (*bri*) > ISDN: 以下を入力して **Apply** をクリックします。

Send Complete: **チェック**

CLI

```
set interface bri0/0 isdn sending-complete
```

デフォルトの設定では、送信完了情報要素は含まれません。

BRI モード

ISDN インターフェース（bri）は、専用回線モードに、あるいはダイヤラーとして設定できます。

専用回線モード

BRI は、専用回線モードをサポートするように構成できます。このモードでは、D チャネル上のシグナリングを行いません。BRI が専用回線モードに設定されると、BRI はデータの提供だけができるレイヤ 3 インターフェースになります。専用回線モードの BRI があれば、セキュリティデバイスの IP アドレスを提供し、BRI の設定に PPP カプセル化を含めなければなりません。

Q931 ダイアリングは、チャネルをセットアップするには必要ありません。Q931 プロトコルおよび Q921 プロトコルの詳細は、*ScreenOS CLI Reference Guide: IPv4 Command Descriptions* を参照してください。他のすべての ISDN オプションが、専用回線モードで機能するとは限りません。

WebUI

Network > Interfaces > List > Edit (*bri*): 以下を入力して **Apply** をクリックします。

BRI Mode
Leased Line (128kps): **チェック**

CLI

```
set interface bri0/0 isdn leased-line 128kbps
```

Dialer Enable

ISDN BRI がダイアリングを有効にするよう設定されている場合、BRI はダイヤラーインターフェースとして動作できます。BRI をダイヤラーインターフェースとして設定してからしか、ダイヤルオンデマンドルーティング（DDR）を提供できません。デフォルトでは、ISDN BRI はダイヤラー対応ではありません。

WebUI

Network > Interfaces > List > Edit (*bri*): 以下を入力して **Apply** をクリックします。

BRI Mode
Dial using BRI: **チェック**

CLI

set interface bri0/0 isdn dialer-enable

Apply をクリックすると、ダイヤラーオプションが表示されます。ダイヤラーオプションの設定に関する詳細は、「ダイヤラーオプション」を参照してください。

ダイヤラーオプション

ダイヤラーインターフェースの名前は、**dialer*x*** の形式になっています。ここで、*x* は 0 ～ 9 の数字です。ダイヤラーインターフェースがまだ作成されていない場合、指定した数字のダイヤラーインターフェースが自動的に作成されます。

set interface dialer*x* コマンドを使用して、次のダイヤラーオプションを設定できます。

- **主要 / 代替番号**

  主要番号は、セキュリティデバイスがコールするリモートの宛先を提供します。主要番号が接続されていない場合、代替番号が使用されます。主要番号と代替番号は、32 文字未満の文字列です。

- **ロードしきい値**

  このオプションは、追加のオンデマンド帯域幅を提供します。このオプションを設定して、トラフィックが 1 つの B チャネルに指定したロードしきい値を超えると、別の B チャネルが利用されます。B チャネルロードしきい値の範囲は 1 ～ 100（パーセント）です。デフォルトは 80 パーセントです。

- **アイドル時間**

  このオプションを使用して、接続を切る前に、デバイスがトラフィックを待つ時間（秒）を設定します。アイドル時間は 0 ～ 60000 秒に設定できます。0 を設定すると、接続はアイドルになることができません。デフォルトは 180 秒です。

- **リトライ回数**

  このオプションを使用して、セキュリティデバイスが、指定した電話番号をダイヤルする回数を指定します。通話が接続できない場合、その番号は、指定された回数（1 ～ 6 回）リダイヤルされます。デフォルトは 3 回です。

- **間隔**

  このオプションを使用して、未接続によって発生した再ダイヤルのダイヤル間隔（秒）を設定します。1 ～ 60 秒を指定できます。デフォルトは 30 秒です。

- ***ダイヤラープール***

  このオプションを使用して、ダイヤラーインターフェースが使用するダイヤラープールを識別します。ダイヤラープール ID は、32 文字未満の文字列です。

次のコマンドを使用して、ダイヤラーインターフェースを作成します。

WebUI

Network > Interfaces > List > New > Dialer IF: 以下を入力して **Apply** をクリックします。

Interface Name: dialerx
Primary Number: 16900
Alternate Number: 44440
Load Threshold: 80
Idle Time: 100
Retry times: 3
Interval: 30
Dialer Pool:

CLI

set interface dialer*x* primary-number 16900
set interface dialer*x* alternative-number 44440
set interface dialer*x* load-threshold 80
set interface dialer*x* idle-time 100
set interface dialer*x* retry 30

WAN インターフェースの使用不可

WebUI または CLI を使用して、WAN インターフェースを使用不可にできます。

WebUI

Network > Interfaces > Edit (*interface*) > WAN: Enable チェックボックスをオフにして、**Apply** をクリックします。

CLI

set interface *interface* disable
save

WAN インターフェースのカプセル化

WAN インターフェースを設定した後、インターフェースのカプセル化は設定できます。このセクションでは、次の WAN インターフェースカプセル化タイプを説明します。

- 30 ページの「ポイントツーポイントプロトコル」
- 30 ページの「フレームリレー」
- 31 ページの「Cisco ハイレベルデータリンク伝送制御手順（Cisco-HDLC）」

単一インターフェースカプセル化オプション	サポートされるカプセル化タイプ
番号なしインターフェース	PPP、FR および Cisco-HDLC
プロトコル MTU	PPP および FR
静的 IP	PPP および Cisco-HDLC
キープアライブ	PPP、FR および Cisco-HDLC
キープアライブ LMI	FR

ポイントツーポイントプロトコル

ポイントツーポイントプロトコル（PPP）リンクは、全二重、同時、双方向の動作を提供し、さまざまなホスト、ブリッジ、およびルーターを簡単に接続するための一般的なソリューションです。

PPP カプセル化では、異なるネットワーク層プロトコルを、一般に使用される物理リンク上で同時に多重化できます。PPP は、ハイレベルデータリンク伝送制御手順（HDLC）をパケットのカプセル化に使用します。HDLC は、ビット指向の同期データリンク層プロトコルで、フレーム文字とチェックサムを使用して、同期シリアルリンク上でのデータカプセル化方法を指定します。PPP のカプセル化は、RFC 1661, *The Point-to-Point Protocol (PPP)* で定義されています。

PPP 接続を確立するには、PPP リンクの各終端が、リンク制御プロトコル（LCP）パケットを交換してリンクを設定します。LCP は、データリンクオプションを確立、設定、テストするために使用されます。これらのオプションはカプセル化形式のオプションを含んでいます。リンク上のピアの認証、パケットサイズの異なる制限、ループバックされたリンクの検出などの一般的な設定エラーによるエラーの処理、リンクが適切に機能しているか、あるい機能していないかの判断、リンクの終了などです。

PPP は、リンク確立中の認証により、デバイスへの接続を許可または拒否できます。この認証は、RFC 1334, *PPP Authentication Protocols* で説明されているように、パスワード認証プロトコル（PAP）またはチャレンジハンドシェイク認証プロトコル（CHAP）のいずれかを使用して実行できます。これらの認証プロトコルは、主として、交換回路あるいはダイヤルアップライン上のネットワークサーバーに接続するホストとルーターによる使用を意図しています。しかし、専用線でも使用できます。

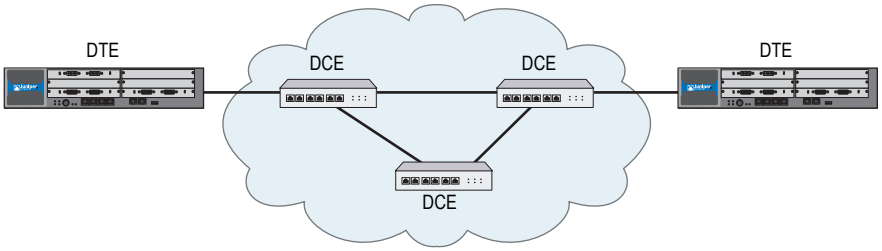
フレームリレー

フレームリレーは、開放型システム間相互接続（OSI）参照モデルのデータリンク層で動作する WAN プロトコルです。フレームリレーのカプセル化は、RFC 1490, *Multiprotocol Interconnect over Frame Relay* および Frame Relay Forum Implementation Agreement FRF3.1/3.2 で定義されています。

フレームリレープロトコルでは、フレームリレーサービスプロバイダーが管理する共有のデータ伝送設備を使用することにより、コストを削減できます。プロバイダーがフレームリレースイッチを維持する、フレームリレーネットワークの各サイトから POP（Point of Presence）までのローカル接続に固定料金を支払います。フレームリレースイッチ間のネットワーク部分は、サービスプロバイダーのすべての顧客によって共有されます。

図 7 は、フレームリレーネットワークのデバイスを示します。

図 7: フレームリレーネットワークのデバイス



2 つのカテゴリのデバイスをフレームリレーネットワークに接続できます。

- **データ端末装置（DTE）**デバイスは、一般に特定のネットワークの終端装置で、通常は顧客の敷地に置かれます。
- **データ回線終端装置（DCE）**デバイスは、ネットワークのスイッチングサービスを提供する、一般にキャリアが所有するインターネット作動デバイスです。DCE は通常、パケット交換機です。

フレームリレーの相手固定接続（PVC）は、フレームリレーネットワークを介して 2 つの DTE デバイス間の論理接続を提供します。多くの PVC は、ネットワークを介して送信するため、単一の実回線に多重化できます。各 PVC には、各顧客が自分のトラフィックだけを受信できるように、独自のデータリンク接続識別子（DLCI）を割り当てます。

Cisco ハイレベルデータリンク伝送制御手順（Cisco-HDLC）

Cisco ルーターとブリッジのシリアルインターフェース用のデフォルトのプロトコルは、Cisco ハイレベルデータリンク伝送制御手順（Cisco-HDLC）です。Cisco-HDLC を使用して、WAN リンク上を転送するためローカルエリアネットワーク（LAN）プロトコルパケットをカプセル化します。

Cisco-HDLC は、国際標準化機構（ISO）が策定した標準 HDLC プロトコルの拡張です。HDLC は、ビット指向の同期データリンク層プロトコルで、フレーム文字とチェックサムを使用して、同期シリアルリンク上でのデータカプセル化方法を指定します。

Cisco-HDLC は、ピアネットワークデバイスとキープアライブメッセージを交換することにより、シリアルインターフェース上のライン状況を監視します。キープアライブメッセージは、最初の端点がまだアクティブであることを示す、ある端点から別の端点までの信号です。キープアライブは、非活動あるいは失敗した接続を識別するために使用されます。キープアライブでは、ピアネットワークデバイスと SLARP（Serial Line Address Resolution Protocol）アドレス要求およびアドレス応答メッセージを交換することにより、ルーターは、隣接ノードの IP アドレスを発見できます。

基本的なカプセル化オプション

AN インターフェースのカプセル化を構成するには、以下を行います。

WebUI

Network > Interfaces > Edit (*WAN interface*): WAN カプセル化タイプおよびセキュリティゾーンを選択し、**Apply** をクリックします。

（オプション）物理リンクのカプセル化オプションを構成します。この手順は、リンクのデフォルトの HDLC オプションを変更する必要がある場合のみ、必要です。

CLI

set interface *interface* encapsulation *type*
set interface *interface* zone *zone*

注： リンクを表すインターフェースを設定することにより、物理リンクを設定します。

番号なしインターフェース

番号なしインターフェースは、自身の IP アドレスを割り当てられませんが、その代わり、他のインターフェースから IP アドレスを借ります。このように、アドレス空間が節約されます。番号なしインターフェースが、機能していない（Interface status UP または Protocol UP が表示されていない）インターフェースをポイントしている場合、番号なしインターフェースも機能しません。ループバックインターフェースが機能しなくなることはないので、番号なしインターフェースがループバックインターフェースをポイントすることを推奨します。

IP 番号なしインターフェースを構成するには、以下を行います。

WebUI

Network > Interface > Edit (*WAN interface*): 番号なしオプションを選択し、ソースインターフェースを選択してから、**Apply** をクリックします。

CLI

set interface *interface* ip unnumbered interface *src interface*
save

プロトコル最大送信単位の構成

PPP またはフレームリレーカプセル化を備えた各物理インターフェースで、プロトコル最大伝送単位（MTU）を設定できます。デフォルトのプロトコル MTU は、シリアル、T1、E1、およびマルチリンクインターフェースでは 1500 バイト、T3 インターフェースでは 4470 バイトです。800 から 8192 バイトまでの値を指定できます。

媒体 MTU はプロトコル MTU に由来します。プロトコル MTU のサイズを大きくした場合、メディア MTU の大きさはプロトコル MTU およびカプセル化オーバーヘッドの合計と同じか、それ以上でなければなりません。

物理インターフェースのプロトコル MTU を構成するには、以下を行います。

WebUI

Network > Interfaces > Edit (*WAN interface*): Maximum Transfer Unit (MTU) フィールドに 800 と 8192 の間の値を入力し、**OK** をクリックします。

CLI

set interface *interface* mtu *number*
save

静的 IP アドレスの構成

WAN インターフェースは、WAN データリンクのもう一方の端にあるサーバーが動的に割り当てた IP アドレスを使用します。あるいは、インターフェースに静的 IP アドレスを明示的に割り当てることができます。

WAN インターフェースに IP アドレスを割り当てるには、以下を行います。

WebUI

Network > Interfaces > Edit (*WAN interface*): IP Address/Netmask フィールドに IP アドレスを入力して、**Apply** をクリックします。

CLI

set interface *interface* ip *ip_addr/mask*
save

キープアライブ

キープアライブメッセージは、最初の端点がまだアクティブであることを示す、ある端点から別の端点までの信号です。キープアライブは、非活動あるいは失敗した接続を識別するために使用されます。WAN カプセル化で設定された物理インターフェースは、10 秒間隔でキープアライブパケットを送信します。

別の間隔でキープアライブパケットを送信するようインターフェースを設定するには、以下を行います。

WebUI

Network > Interfaces > Edit (*WAN interface*) > WAN encapsulation type: **Keepalive Interval** に秒数を入力して、**Apply** をクリックします。

CLI

set interface *interface* keepalives *seconds*
save

物理インターフェースでキープアライブの送信を無効にするには、以下を行います。

WebUI

Network > Interfaces > Edit (*WAN interface*) > WAN Encapsulation type: Keepalive チェックボックスをオフにして、**Apply** をクリックします。

CLI

unset interface *interface* keepalives
save

宛先がキープアライブパケットを受信するかどうかで、リンクが無効か有効かを判断します。デフォルトでは、宛先が 3 つの連続したキープアライブパケットを受信しない場合、ScreenOS は、リンクが無効であると判断します。宛先が 1 つのキープアライブパケットを受信すると、無効なリンクは有効に戻ります。

リンクが無効か有効かを宛先が判断する基準を変更するには、以下を行います。

WebUI

Network > Interfaces > Edit (*wan interface*) > WAN Encapsulation type: **Down Counter** または **Up Counter** に回数を入力し、**Apply** をクリックします。

CLI

set interface *interface* keepalives down-count *number*
set interface *interface* keepalives up-count *number*
save

PPP カプセル化オプション

このセクションでは、いくつかの WAN インターフェースで利用可能なポイントツーポイントプロトコル（PPP）カプセル化オプションについて説明します。MLPPP を構成するには、45 ページの「マルチリンク PPP 構成オプション」を参照してください。

WAN インターフェースをサポートするデバイス上の単一物理リンクで PPP を設定するには、次を行います。

1. 物理リンク上の PPP カプセル化を構成し、セキュリティゾーンにリンクを割り当てます。物理リンク上の IP アドレスを設定します。
2. （オプション）物理リンクの PPP オプションを構成します。この手順は、リンクのデフォルトの PPP オプションを変更する必要がある場合のみ、必要です。
3. PPP アクセスプロファイルを設定し、それをインターフェースにバインドします。認証が PPP データリンク上で使用されない場合でも、この手順は必要です。
4. （オプション）CHAP または PAP 認証が使用されている場合は、デバイスのローカルデータベースでユーザー名とパスワードを構成します。

PPP アクセスプロファイル

PPP アクセスプロファイルには次の情報が含まれます。

- リンク制御プロトコル（LCP）リンクのセットアップ中に、デバイスへの接続を許可するか拒否するため、認証が使用されるかどうか。認証が指定されている場合、選択した認証方法に対するオプションを設定できます。

注： 認証が PPP 接続で使用されなくても、認証方法を指定しないアクセスプロファイルを設定し、それをインターフェースにバインドしなければなりません。

- インターフェースが、既に設定した静的 IP アドレスを使用するかどうか。インターフェースがサーバーによって動的に割り当てられた IP アドレスを使用する場合、IP アドレスのネットマスクを指定できます。

LCP リンクのセットアップ中に、デバイスへの接続を許可するか拒否するために認証を使用することができます。認証が失敗した場合、PPP リンクは終了します。デフォルトでは、PPP 暗号化用に設定されたインターフェースでは、認証は無効になります。明示的にインターフェースの認証を有効にしなければ、インターフェースは認証要求を行わず、受信する認証チャレンジをすべて拒否します。

次の認証プロトコルの 1 つあるいは両方をサポートするよう、インターフェースを設定できます。

- RFC 1334, *PPP Authentication Protocols* で定義されている、パスワード認証プロトコル（PAP）
- RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)* で定義されている、チャレンジハンドシェイク認証プロトコル（CHAP）。

WAN インターフェースのカプセル化を構成するには、以下を行います。

WebUI

Network > PPP > PPP Profile > New: PPP Profile フィールドに *profile_name* を入力して、他のオプションを入力し、**OK** をクリックします。

Network > Interfaces > Edit (*WAN interface*): Binding a PPP Profile ドロップダウンリストで *profile_name* を選択して、**Apply** をクリックします。

CLI

```
set ppp profile profile_name ...
set interface interface ppp profile profile_name
save
```

PPP 認証方法

LCP リンクのセットアップ中に、デバイスへの接続を許可するか拒否するために認証を使用することができます。認証が失敗した場合、PPP リンクは終了します。PPP 認証方法を表示するには、以下を行います。

WebUI

Network > PPP > PPP Profile > Edit (*profile_name*): **Any**、**CHAP**、**PAP**、または **none** を選択して、**OK** をクリックします。

CLI

```
set ppp profile profile_name { chap | pap | any | none }
save
```

アクセスプロファイルで静的 IP アドレスを使用している場合、そのプロファイルは、明示的に設定された IP アドレスを持つインターフェースにしかバインドできません。反対に、インターフェースに静的 IP アドレスがある場合、インターフェースにバインドするアクセスプロファイルは、**static IP** オプションを指定しなければなりません。

インターフェースの IP アドレスがサーバーによって動的に割り当てられる場合、インターフェースのネットマスクは /32（255.255.255.255）です。インターフェースに別のネットマスク値を指定するには、以下を行います。

WebUI

Network > PPP > PPP Profile > Edit (*profile_name*): Netmask フィールドに新しい *mask* 値を入力し、**OK** をクリックします。

CLI

```
set ppp profile profile_name netmask mask
save
```

パスワード

パスワードは、そのピアが存在するインターフェース上の PPP クライアントを確証するために使用されます。パスワードを設定するには、以下を行います。

WebUI

Network > PPP > PPP Profile > Edit (*profile_name*): **Password** に文字列を入力し、**OK** をクリックします。

CLI

```
set ppp profile profile_name auth secret password
save
```

PPP 認証プロトコル

このセクションでは、WAN インターフェースのいくつかで利用可能な PPP 認証プロトコルについて説明します。

チャレンジハンドシェイク認証プロトコル（CHAP）

認証がインターフェース上で有効な場合、チャレンジおよび応答パケットで送信される名前として、インターフェースはシステムホスト名を使用します。インターフェースがチャレンジおよび応答パケットで使用する名前とは異なるものを設定できます。CHAP ローカル名を変更するには、以下を行います。

WebUI

Network > PPP > PPP Profile > Edit (*profile_name*): Local Name フィールドに名前を入力して、**OK** をクリックします。

CLI

```
set ppp profile profile_name auth local-name name
save
```

デフォルトでは、PPP 認証がインターフェース上で有効な場合、インターフェースは常にそのピアにチャレンジし、そのピアからのチャレンジに応答します。そのピアにチャレンジせず、チャレンジされた時だけに応答するようインターフェースを設定できます（この動作は*パッシブモード*と呼ばれています）。

注： パッシブモードは、チャレンジハンドシェイク認証プロトコル（CHAP）でだけ有効です。

パッシブモードを有効にするには、以下を行います。

WebUI

Network > PPP > PPP Profile > Edit (*profile_name*): **Passive** を選択し、**OK** をクリックします。

CLI

```
set ppp profile profile_name passive
save
```

パスワード認証プロトコル

パスワード認証プロトコル（PAP）は、2 ウェイハンドシェイクを使用し、クリアテキストでリンク上にアカウント名とパスワードを送信します。他の認証プロトコルを共通して持たない場合にだけ、システムは一般に PAP を使用します。

認証プロトコルを PAP に接続するには、以下を行います。

WebUI

Network > PPP > Edit (*profile_name*): 認証タイプを選択して **Apply** をクリックします。

CLI

```
set ppp profile profile_name auth type pap
save
```

ローカルデータベースユーザー

CHAP または PAP が PPP リンク上で使用される場合、ピアデバイスは、認証のためにデバイスへユーザー名とパスワードを送信します。デバイスは、受信したユーザー名とパスワードをそのローカルデータベースで設定された WAN ユーザータイプエントリと比較します。ユーザー名とパスワードがローカルデータベースのエントリと一致するピアだけに、デバイスへの接続とデータの送受信が認められます。

WAN ユーザーを設定するには、以下を行います。

WebUI

Objects > Users > Local > New: 次のように入力してから **OK** をクリックします。

WAN User: (**選択**)
User Name: *name_str*
User Password: *pswd_str*
Confirm Password: *pswd_str*

CLI

```
set user name_str password pswd_str
set user name_str type wan
save
```

注 : WAN ユーザーは、ローカルデータベースでのみ設定できます。

フレームリレーカプセル化オプション

このセクションでは、いくつかの WAN インターフェースで利用可能なフレームリレーカプセル化オプションを設定する方法を説明します。MLFR を構成するには、46 ページの「マルチリンクフレームリレー構成オプション」を参照してください。

注： WAN インターフェースの Basic Properties ページで **Main Link** オプションが選択されていることを確認します。

キープアライブメッセージ

フレームリレーのキープアライブメッセージは、ローカル管理インターフェース（LMI）パケットの送信によって実装されます。ScreenOS は、フレームリレーインターフェース上でデフォルトでは LMI キープアライブメッセージを送信します。

対向フレームリレー接続では、接の両側のキープアライブの送信を無効にするか、接続の片側を DTE（デフォルトの ScreenOS 設定）として、もう片側を DCE として設定します。

キープアライブが有効な場合、マルチポイントまたはマルチキャスト接続で可能な DLCI 設定の数は、インターフェースに選択された MTU サイズによって制限されます。利用可能な DLCI を計算するには、次の式を使用します。

(MTU – 12) / 5

可能な DLCI の数を増すためには、キープアライブを無効にします。物理インターフェースでキープアライブの送信を無効にするには、WebUI または CLI を使用します。

WebUI

Network > Interfaces > Edit (*interface*) > FR: **No-Keepalive** を選択して **Apply** をクリックします。

CLI

```
set interface interface frame-relay lmi no-keepalive
save
```

フレームリレー LMI タイプ

デフォルトでは、ScreenOS は、ANSI T1.617 Annex D で指定された LMI を送信します。ITU Q933 Annex A に LMI タイプを変更するには、以下を行います。

WebUI

Network > Interfaces > Edit (*WAN interface*) > FR: **ITU** を選択して **Apply** をクリックします。

CLI

```
set interface interface frame-relay lmi type itu
save
```

次のフレームリレー LMI キープアライブオプションを設定できます。

- **DTE のフルステータスポーリング間隔**（CLI ではキーワード n391-dte で表す）。DTE は、DTE ポーリングタイマーによって指定された間隔で、DCE に状況問い合わせを送信します。ポーリング間隔は、これらの問い合わせが完全な状況報告を受信する頻度を指定します。たとえば、10 の値は、問い合わせの 10 回目ごとに完全な状況報告を受信します。それ以外の問い合わせは、キープアライブの交換のみを要求します。

- **DTE のエラーしきい値**（CLI ではキーワード n392-dte で表す）。DTE が監視するイベントカウントで指定したイベントカウント内で、リンクを無効にするため必要なエラー数。

- **DTE が監視するイベントカウント**（CLI ではキーワード n393-dte で表す）。範囲は 1 ～ 10 で、デフォルト値は 4 です。

- **DTE キープアライブタイマー**（CLI ではキーワード t391-dte で表す）。DTE が DCE にキープアライブ応答要求を送信し、DTE エラーしきい値によっては状況を更新する期間。

フレームリレー LMI オプションを構成するには、以下を行います。

WebUI

Network > Interfaces > Edit (*WAN interface*) > FR: LMI オプションに適切に値を入力して、**Apply** をクリックします。

CLI

set interface *interface* frame-relay lmi *option*
save

PVC の作成と構成

1 つのフレームリレー物理インターフェース内で、サブインターフェースであると見なされる、複数のポイントツーポイント仮想インターフェースを作成できます。各サブインターフェースは、データリンク接続識別子（DLCI）によって識別される、1 つの相手固定接続（PVC）へマッピングされます。各サブインターフェースにつき DLCI は 1 つだけ指定できます。DLCI は 16 ～ 1022 までの値です。（1 ～ 15 の数字は予約されています。）フレームリレーパケット交換網を横断した送信用に、単一の物理リンク上に多くの PVC を多重化するよう選択できます。

注 : 指定する DLCI 値は、ユーザーのローカルプロバイダーがユーザーの PVC に割り当てた DLCI です。

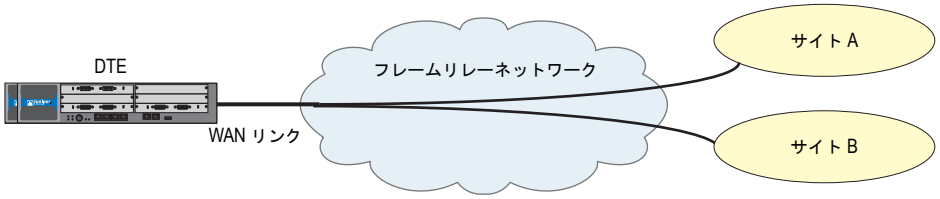
サブインターフェース名は、物理インターフェース名とサブインターフェース数から構成されます。たとえば、物理インターフェースの名前が **serial1/1** の場合、サブインターフェースは **serial1/1.1** または **serial1/1.2** になります。

注 : WebUI では、インターフェース名を選択すると、サブインターフェース数が自動的に加算されます。CLI では、インターフェース名とサブインターフェース数の両方を入力しなければなりません。

同様に、管理 IP アドレス、サービスオプションなどの特性のような、管理機能用のサブインターフェースも設定できます。（インターフェースでの管理 IP およびサービスオプションの構成に関する詳細は、*第 2 部 基本*を参照してください。）

図 8 は、物理インターフェース serial1 に設定した 2 つのポイントツーポイント PVC を示します。各 PVC を異なるセキュリティゾーンに関連させることができます。各 PVC のセキュリティゾーンは、物理インターフェースに割り当てられたセキュリティゾーンと異なってもかまいません。

図 8: ポイントツーポイントフレームリレーのサブインターフェース



ポイントツーポイントフレームリレーのサブインターフェースを構成するには、サブインターフェースを作成して、セキュリティゾーンにそれを割り当て、次にサブインターフェースにフレームリレー DLCI と IP アドレスを割り当てます。

注： 物理インターフェースに割り当てられたものと異なるセキュリティゾーンに、サブインターフェースを割り当てることができます。

WebUI

Network > Interface > New > WAN Sub-IF: 次のように入力してから **OK** をクリックします。

Interface Name: *interface* (**選択**)
Zone Name: (**選択**)
Frame Relay DLCI: (*id_num* **を入力**)
IP Address/Netmask: (*ip_addr* **を入力**)

CLI

set interface *subinterface* zone *zone*
set interface *subinterface* frame-relay dlci *id_num*
set interface *subinterface* ip *ip_addr*
save

逆アドレス解決プロトコル

フレームリレーサブインターフェースは、RFC 2390, *Inverse Address Resolution Protocol* で説明されているように、逆のアドレス解決プロトコル（ARP）をサポートすることができます、逆 ARP が有効な場合、デバイスは、フレームリレー PVC のもう一方の端の要求を発信している装置に IP アドレス情報を提供して、受信した逆フレームリレー ARP の要求に応答します。デバイスは、逆フレームリレー ARP の要求を開始しません。

デフォルトでは、逆フレームリレー ARP は無効になっています。逆フレームリレー ARP の要求に応答するデバイスを設定するには、以下を行います。

WebUI

Network > Interface > Edit (*subinterface*): **Frame Relay Inverse ARP** を選択して、**Apply** をクリックします。

CLI

```
set interface subinterface frame-relay inverse-arp
save
```

マルチリンクカプセル化

このセクションでは、WAN インターフェース上のマルチリンクカプセル化に関する次の情報を提供します。

- 41 ページの「概要」
- 42 ページの「基本的なマルチリンクバンドルの設定」
- 45 ページの「マルチリンク PPP 構成オプション」
- 46 ページの「マルチリンクフレームリレー構成オプション」

概要

WAN インターフェースは、ユーザーからネットワークへのインターフェースに、Frame Relay Forum FRF.16, *Multilink Frame Relay UNI/Network-to-Network Interface (NNI) Implementation Agreement* に基づいた、マルチリンクフレームリレー（MLFR）およびマルチリンクポイントツーポイントプロトコル（MLPPP）をサポートしています。両方のマルチリンクカプセル化タイプは、複数の物理リンクの*バンドル*への集約を可能にすることにより、アプリケーションの帯域幅を増すコスト効率の良い方法を提供します。バンドルの中の各物理リンクは、*バンドルリンク*と呼ばれます。たとえば、アプリケーションが 1 つの T1 ラインで利用可能な帯域幅より多くを必要とする場合、アプリケーションの使用帯域幅を増す 2 つの選択肢があります。

- T3 ラインをリースする
- 複数の T1 リンクをバンドルする

MLFR と MLPPP もフォールトトレランスを提供します。たとえば、バンドル中の 1 つのバンドルリンクが機能しなくなると、バンドルは、残りのバンドルリンクを横断して送信することにより、フレームリレーまたは PPP サービスをサポートし続けます。MLFR と MLPPP も、バンドル内のリンクを横断してロードバランスを提供します。送信のため選択されたバンドルリンクが長いパケットを送信するのに忙しい場合、別のリンクがデータを送信します。

マルチリンクカプセル化のオプション	サポートされるカプセル化タイプ
最小リンク	MLPPP と MLFR
フラグメントしきい値	MLPPP と MLFR
MRRU	MLPPP
ドロップタイムアウト	MLPPP と MLFR
確認リトライ	MLFR
確認時間	MLFR
ハロータイマー	MLFR

基本的なマルチリンクバンドルの設定

バンドルは、作成したマルチリンクインターフェースでアクセスします。マルチリンクインターフェースの名前は、ml*id_num* でなければなりません。たとえば、マルチリンクインターフェース名は、**ml1**, **ml2** などとなります。

注： WebUI では、*id_num* は、新しいマルチリンクインターフェースを作成すると、自動的に加算されます。CLI では、*id_num* 値を指定する必要があります。

デフォルトでは、新しいマルチリンクインターフェースのカプセル化タイプは MLPPP です。フレームリレーをサポートするマルチリンクインターフェース上では、MLFR カプセル化を明示的に設定しなければなりません。

マルチリンクインターフェースを作成し、MLFR カプセル化に設定するには、以下を行います。

WebUI

Network > Interfaces > New > Multilink IF: WAN カプセル化に **Multi-Link Frame Relay** を選択し、**Apply** をクリックします。

CLI

```
set interface interface encapsulation mlfr-uni-nni
save
```

バンドル識別子

バンドル ID は、FRF.16 が指定するように、ローカルと特定のバンドルを持つリモートエンドを関連付けます。ML バンドル中のバンドルリンクはすべて、80 バイト以内の同じバンドル ID を使用しなければなりません。2 つのデバイス間で複数のバンドルを設定している場合、各バンドル ID は一意であることが必要です。たとえば、バンドル ID にネットワークノード識別子、システムのシリアル番号あるいはネットワークアドレスを使用できます。

マルチリンクインターフェースに対して特定のバンドル ID を設定しない場合、マルチリンクインターフェース名（**ml1** または **ml2** など）が使用されます。バンドル ID を構成するには、以下を行います。

WebUI

Network > Interfaces > Edit (*interface*) > Basic: WAN カプセル化に ML Type を入力して、**Apply** をクリックします。

CLI

set interface *interface* bundle-id *name_str*
save

ドロップタイムアウト

マルチリンクバンドルの個々のリンクが 1 つ以上のパケットをドロップする場合に、回復メカニズムを提供するためドロップタイムアウト値を設定することができます。ドロップタイムアウトは、遅延差許容設定ではなく、全般的なレイテンシーを制限しません。リンクを横断して予期される遅延差より著しく大きいドロップタイムアウト値を設定することを推奨します。このようにして、実際のパケット損失があるが、正常なジッタ条件下ではない場合、タイムアウト時間が経過します。

ドロップタイムアウト値を設定するには、以下を行います。

WebUI

Network > Interfaces > Edit (*interface*) > ML Encapsulation Type: **Drop Timeout** にミリ秒単位で数を入力し、**Apply** をクリックしま。

CLI

set interface *interface* drop-timeout *milliseconds*
save

5 ミリ秒未満の設定は推奨しません。0 ではタイムアウトを無効になります。

注 : マルチリンクインターフェースでは、無効なバンドルまたはリンク向けで、ネットワークのエラー条件に遭遇するパケットまたはフラグメントは、バンドルごとの統計で、ドロップされたパケットやフレームカウントには計算されません。ScreenOS は、広域出力バイトあるいは出力パケット計算ではなく、広域エラー統計でパケットを数えます。エラー条件がマルチリンクインターフェースの内部で生成された場合のみ、またパケットがネットワークの他の場所でエラーに遭遇した場合のみ、この通常とは異なる計算状況が起こります。

最小リンク値は 1 ～ 8 です。8 を指定すれば、バンドルを有効にするため、バンドルの設定されたリンクはすべて有効でなければなりません。

フラグメントしきい値

マルチリンク回線内の個々のリンクを横断して送信されるパケットペイロードの最大サイズを設定するため、フラグメントしきい値を設定できます。ScreenOS は、回線サイズにふさわしいより小さな単位にフラグメントしきい値を超える着信パケットを分割します。もう一方の端でフラグメントを再アセンブリしますが、出力トラフィックストリームには影響しません。

フラグメントしきい値を設定するには、以下を行います。

WebUI

Network > Interfaces > Edit (*interface*) > ML Encapsulation Type: **Bundle-link Fragmentation Threshold** の値を入力して、**Apply** をクリックします。

CLI

set interface *interface* mlfr-uni-nni fragment-threshold *number*
save

デフォルトでは、フラグメントしきい値は物理インターフェースの MTU です。（シリアル、T1 および E1 バンドルリンクについては、デフォルトの MTU サイズは 1500 バイトです。T3 バンドルリンクについては、デフォルトの MTU サイズは 4470 バイトです。）最大フラグメントサイズは 128 ～ 16,320 バイトです。設定する値は 64 の倍数（*N*x64）でなければなりません。

注： MLPPP WAN インターフェースに適切なロードバランシングを提供するため、設定でフラグメントしきい値とショートシーケンスオプションの両方を設定しないでください。

MLPPP インターフェースでは、バンドルのリンクの MTU が、バンドル MTU にカプセル化オーバーヘッドを加えたものより小さい場合、フラグメントは自動的に有効になります。ショートシーケンスが有効な MLPPP WAN インターフェースでは、この状況を回避する必要があります。

フラグメントしきい値を設定するには、以下を行います。

WebUI

Network > Interfaces > Edit (*interface*) > ML Encapsulation Type: **Fragment Threshold** の値を入力して、**Apply** をクリックします。

CLI

set interface *interface* fragment-threshold *bytes*
save

最小リンク

バンドル全体が有効になるため有効でなければならないリンクの最小数を設定できます。デフォルトでは、バンドルが有効であると見なされるには、リンクが 1 つだけ有効である必要があります。

バンドルのリンクの最小数を設定するには、以下を行います。

WebUI

Network > Interfaces > Edit (*interface*) > ML Encapsulation Type: **Minimum Links** に新しい数を入力して、**Apply** をクリックします。

CLI

set interface *interface* minimum-links *number*
save

マルチリンク PPP 構成オプション

このセクションでは、いくつかの WAN インターフェースで利用可能な、追加の MLPPP 構成オプションについて説明します。

基本的な設定手順

MLPPP カプセル化をサポートするインターフェースで MLPPP を構成するには、次を行います。

1. バンドルを作成し、MLPPP カプセル化用に設定します。バンドルをセキュリティゾーンに割り当てます。バンドルのバンドル ID または MTU のような、他のオプションも設定できます。

2. （オプション）バンドルの MLPPP オプションを構成します。この手順は、バンドルのデフォルトの MLPPP オプションを変更する必要がある場合のみ、必要です。

3. PPP アクセスプロファイルを設定し、それをインターフェースにバインドします。認証が PPP データリンク上で使用されない場合でも、この手順は必要です。

4. （オプション）CHAP または PAP 認証が使用されている場合は、セキュリティデバイスのローカルデータベースでピアのユーザー名とパスワードを構成します。

5. バンドルリンクをバンドルに割り当てます。

6. （オプション）バンドルの各バンドルリンクの PPP オプションを構成します。この手順は、リンクのデフォルトの PPP オプションを変更する必要がある場合のみ、必要です。

最大受信再構築単位

最大受信再構築単位（MRRU）は、最大転送単位（MTU）に似ていますが、マルチリンクバンドルにのみ関係します。マルチリンクインターフェースが処理できる最大パケット長です。デフォルトでは、MRRU は 1500 バイトに設定されています。ピア装置が許可する場合は、異なる MRRU 値を設定できます。MRRU は、オリジナルのペイロードに加えて、2 バイトの PPP ヘッダーを含んでいます。しかし、個々のマルチリンクパケットがバンドル中の個別のリンクを横断している間に適用される、追加の MLPPP ヘッダーを含んでいません。

異なる MRRU を構成するには、以下を行います。

WebUI

Network > Interfaces > Edit (*interface*) > MLPPP: **Maximum Received Reconstructed Unit** にバイト数を入力して、**Apply** をクリックします。

CLI

```
set interface interface mrru bytes
save
```

シーケンスヘッダーの形式

シーケンスヘッダー形式は、12 あるいは 24 ビットに設定できますが、24 ビットが、ほとんどのネットワークについてより強固な値であると考えられます。

12 ビットのシーケンスヘッダー形式を設定するには、以下を行います。

WebUI

Network > Interfaces > Edit (*interface*) > MLPPP: **Short-Sequence MLPPP Number** を選択して **Apply** をクリックします。

CLI

```
set interface interface short-sequence
save
```

マルチリンクフレームリレー構成オプション

このセクションでは、いくつかの WAN インターフェースで利用可能な、追加の MLFR 構成オプションについて説明します。

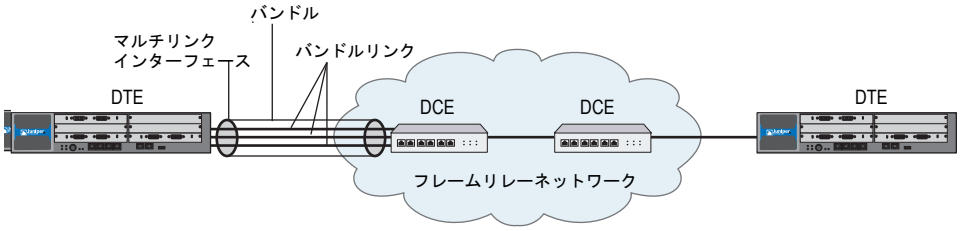
基本的な設定手順

MLFR カプセル化をサポートするインターフェースで MLFR を構成するには、次を行います。

1. バンドルを作成し、MLFR カプセル化用に設定します。バンドルをセキュリティゾーンに割り当てます。バンドルのバンドル ID または MTU のような、他のオプションも設定できます。
2. （オプション）バンドルのフレームリレーオプションを構成します。この手順は、バンドルのデフォルトのフレームリレーオプションを変更する必要がある場合のみ、必要です。
3. バンドルリンクをバンドルに割り当てます。
4. （オプション）バンドルの各バンドルリンクの MLFR オプションを構成します。この手順は、リンクのデフォルトの MLFR オプションを変更する必要がある場合のみ、必要です。
5. バンドルには 1 つ以上の PVC を作成し、各 PVC にフレームリレー DLCI と IP アドレスを割り当てます。

図 9 は、MLFR により、複数の T1 バンドルリンクが単一のバンドルに集約される仕組みを示します。

図 9: マルチリンクフレームリレーバンドル



フレームリレー機能は、各バンドルリンク上でではなくマルチリンクインターフェース上で構成されます。（バンドルリンクは、ピア DTE と DCE デバイスには見えますが、フレームリレーデータリンク層には見えません。) ローカルのデバイスとピアデバイスは、どのバンドルリンクが作動状態か判断するために、また、どのバンドルリンクが各バンドルと関連づけられているか同期するために、リンク保全性プロトコル（LIP）制御メッセージを交換します。

リンク管理については、バンドルリンクの端はそれぞれ MLFR LIP に従い、バンドルリンクのもう片方の端にそのピアとリンク制御通報を交換します。バンドルリンクを呼び出すため、リンクの両端は、ADD_LINK と ADD_LINK_ACK のメッセージの交換を終えなければなりません。リンクを維持するため、両端は周期的に HELLO と HELLO_ACK のメッセージを交換します。ハローメッセージの交換と確認は、リンクのキープアライブメカニズムの役目を果たします。デバイスがハローメッセージを送信するが、肯定応答を受信しない場合、設定された最大リトライ回数までハローメッセージを再送信します。肯定応答を受信せずに、デバイスがリトライの最大回数送信した場合、ScreenOS はバンドルリンクを無効であると見なします。

ピアデバイスが、リンクをバンドルに使用すると応答すると、ScreenOS はバンドルリンクを呼び出します。ピアデバイスがローカルデバイスからのハローメッセージに肯定応答すると、リンクは有効なままになります。ローカル管理インターフェース（LMI）が有効なとき、ローカルデバイスとピアデバイスのフレームリレーデータリンク層が LMI を使用して同期していると、バンドルリンク状況は有効であると見なされます、LMI キープアライブが成功している限り、バンドルリンクは有効なままになります。

MLFR のリンク割り当て

MLFR インターフェースは、DCE または DTE になることができます（デフォルトの ScreenOS 設定)。DTE は、マスターの役目を果たし、リンクの DCE 部分から状況を要求します。

MLFR カプセル化用に設定された物理リンクでは、バンドルの各リンク端点は、リンク追加メッセージの送信により、バンドルのそのピアとの動作の要求を開始します。ハローメッセージは、ローカルの端点が有効であることを、ピア端点に通知します。リンクの両端は、ハローメッセージを周期的にまたはハロータイマーで指定したように生成します。リンク削除メッセージは、ローカルエンド管理がバンドル動作からリンクを削除していることをピアに通知します。端点は、肯定応答メッセージを送信して、リンク追加、リンク削除、およびハローの各メッセージに応答します。

確認リトライ

バンドルリンクでは、確認応答タイマーの終了後に連続したハローまたはリンク削除メッセージに対して、再送信を試行する回数を設定できます。再送信の試行を設定するには、以下を行います。

WebUI

Network > Interfaces > Edit (*interface*) > MLFR: **Line Interface Protocol (LIP) Retransmission Count before Link-Down** の値を入力して、**Apply** をクリックします。

CLI

set interface *interface* mlfr-uni-nni acknowledge-retries *number*
save

肯定応答タイマー

リンク追加肯定応答、ハロー肯定応答、あるいはリンク削除肯定応答を待つ最大期間を設定できます。肯定応答時間を設定するには、以下を行います。

WebUI

Network > Interfaces > Edit (*interface*) > MLFR: **Maximum Period to Wait for an Acknowledgement** の値を入力して、**Apply** をクリックします。

CLI

set interface *interface* mlfr-uni-nni acknowledge-timer *seconds*
save

ハロータイマー

ハローメッセージが送信される速度を設定するには、以下を行います。

WebUI

Network > Interfaces > Edit (*interface*) > MLFR: **LIP Hello Keepalive Interval** の値を入力して、**Apply** をクリックします。

CLI

set interface *interface* mlfr-uni-nni hello-timer *seconds*
save

指定された期間 (ミリ秒) が経過した後、ハローメッセージが送信されます。ハロータイマーが終了すると、リンク端点はリンク追加メッセージを生成します。

WAN インターフェース構成例

このセクションには、以下の WAN 設定例があります。

- 49 ページの「シリアルインターフェースの構成」
- 49 ページの「T1 インターフェースの構成」
- 50 ページの「E1 インターフェースの構成」
- 51 ページの「T3 インターフェースの構成」
- 51 ページの「E3 インターフェースの構成」
- 52 ページの「ISDN 接続用のデバイスの構成」

シリアルインターフェースの構成

この例は、シリアルインターフェースの WAN プロパティを設定します。WAN インターフェースのプロパティを構成したら、59 ページの「カプセル化設定例」を参照して、WAN カプセル化を構成します。

WebUI

Network > Interfaces > Edit (serial6/0) > WAN: 以下を選択して **Apply** をクリックします。

Hold Time (保持時間)
    Clock Mode Internal (選択)
    Clock Rate: 8.0 (選択)
DTE Options
    Line Encoding: Non-Return-To-Zero (選択)

CLI

1. **クロッキング情報を設定します。**
   set interface serial6/0 serial-options clocking-mode internal
   set interface serial6/0 serial-options clock-rate 8.0
2. **ラインエンコーディングを設定します。**
   set interface serial6/0 serial-options encoding nrz
   save

T1 インターフェースの構成

この例は、T1 インターフェースの WAN プロパティを設定します。WAN インターフェースのプロパティを構成したら、59 ページの「カプセル化設定例」を参照して、WAN カプセル化を構成します。

WebUI

Network > Interfaces > Edit (serial3/0) > WAN: 以下を選択して **Apply** をクリックします。

Hold Time (保持時間)
    Clock Mode: External (選択)
T1 Options
    Line buildout: 0 - 132 (選択)
    Line Encoding: 8-bits Zero Suppression (選択)
    Byte Encoding: 8-bits per byte (選択)
    Frame Checksum: 16-bits (選択)
    Framing Mode: Extended Super Frame (選択)
    Transmitting Flag in Idle Cycles: 0x7E (選択)
    Start/End Flags on Transmission: Filler (選択)
    Invert Data: (選択解除)

CLI

1. **クロッキングソースを設定します。**
   set interface serial3/0 clocking external
2. **ラインビルドアウトを設定します。**
   set interface serial3/0 t1-options buildout 0-132
3. **ラインエンコーディングを設定します。**
   set interface serial3/0 t1-option line-encoding b8zs
   unset interface serial3/0 t1-option invert-data
4. **バイトエンコーディングを設定します。**
   set interface serial3/0 t1-option byte-encoding nx56
5. **フレーミングオプションを設定します。**
   set interface serial3/0 t1-options fcs 16
   set interface serial3/0 t1-options framing esf
6. **フラグオプションを設定します。**
   set interface serial3/0 t1-options idle-cycle-flag flags
   set interface serial3/0 t1-options start-end-flag filler
   save

E1 インターフェースの構成

この例は、E1 インターフェースの WAN プロパティを設定します。WAN インターフェースのプロパティを構成したら、59 ページの「カプセル化設定例」を参照して、WAN カプセル化を構成します。

WebUI

Network > Interfaces > Edit (serial6/1) > WAN: 以下を選択して **Apply** をクリックします。

Hold Time (保持時間)
Clock Mode: External (選択)
E1 Options
Frame Checksum: 16-bits (選択)
Framing Mode: with CRC4 (選択)
Transmitting Flag in Idle Cycles: 0x7E (選択)
Start/End Flags on Transmission: Filler (選択)
Invert Data: (選択解除)
(オプション) Time slots: 2-32

CLI

1. **クロッキングソースを設定します。**
   set interface serial6/1 clocking external
2. **フレーミングオプションを設定します。**
   set interface serial6/1 e1-options fcs 16
   set interface serial6/1 e1-options framing g704
3. **フラグを設定します。**
   set interface serial6/1 e1-options idle-cycle-flag flags
   set interface serial6/1 e1-options start-end-flag filler
   unset interface serial6/1 e1-options invert-data
4. **(オプション) タイムスロットを設定します。**
   set interface serial6/1 e1-options timeslots 2-32
   save

T3 インターフェースの構成

この例は、T3 インターフェースの WAN プロパティを設定します。WAN インターフェースのプロパティを構成したら、59 ページの「カプセル化設定例」を参照して、WAN カプセル化を構成します。

WebUI

Network > Interfaces > Edit (serial4/0) > WAN: 以下を選択して **Apply** をクリックします。

Hold Time (保持時間)
Clock Mode: External (選択)
T3 Options
Frame Checksum: 16-bits (選択)
Transmitting Flag in Idle Cycles: 0x7E (選択)
Start/End Flags on Transmission: Filler (選択)

CLI

1. **クロッキングソースを設定します。**
set interface serial4/0 clocking external
2. **フレーミングオプションを設定します。**
set interface serial4/0 t3-options fcs 16
3. **フラグを設定します。**
set interface serial4/0 t3-options idle-cycle-flag flags
set interface serial4/0 t3-options start-end-flag filler
save

E3 インターフェースの構成

この例は、E3 インターフェースの WAN プロパティを設定します。WAN インターフェースのプロパティを構成したら、59 ページの「カプセル化設定例」を参照して、WAN カプセル化を構成します。

WebUI

Network > Interfaces > Edit (serial4/0) > WAN: 以下を選択して **Apply** をクリックします。

Hold Time (保持時間)
Clock Mode: External (選択)
E3 Options
Frame Checksum: 16-bits (選択)
Transmitting Flag in Idle Cycles: 0x7E (選択)
Start/End Flags on Transmission: Filler (選択)

CLI

1. **クロッキングソースを設定します。**
set interface serial4/0 clocking external
2. **フレーミングオプションを設定します。**
set interface serial4/0 e3-options fcs 16
3. **フラグを設定します。**
set interface serial4/0 e3-options idle-cycle-flag flags
set interface serial4/0 e3-options start-end-flag filler
save

ISDN 接続用のデバイスの構成

次の手順は、デフォルトのオプションを使用して、ISDN 用にユーザーのデバイスを設定するのに必要な最小セットアップを要約しています。

構成手順	詳細は、
1. ISDN スイッチタイプを選択します。	52 ページ
2. PPP プロファイルを構成します。	52 ページ
3. ISDN インターフェース（BRI）をセットアップします。	53 ページ
4. ISDN BRI を通るようにトラフィックをルーティングします。	58 ページ

手順 1: ISDN スイッチタイプの選択

構成するべき最小の ISDN オプションは、ユーザーのデバイスが接続される ISDN スイッチのタイプを選択することです。ISDN オプションの詳細については、25 ページの「ISDN オプション」を参照してください。

WebUI

Network > Interfaces > List > Edit (*bri*): **WAN** を選択して、適用可能なオプション値を選択し、**Apply** をクリックします。

Switch type after Reboot: etsi

CLI

```
set in bri0/0 isdn switch-type etsi
```

ISDN スタックの構成を表示するには、**get int bri2/0 isdn** コマンドを使用します。

手順 2: PPP プロファイルの構成

静的または動的 IP アドレスを使用して、PPP プロファイルを構成します。

WebUI

Network > PPP > PPP Profile > New: 適用可能なオプション値を入力し、**OK** をクリックします。

PPP Profile: isdn-ppp
Authentication: CHAP
Passive: Check
Local Name: 169
Password: 169

CLI

```
set ppp profile isdn-ppp
set ppp profile isdn-ppp auth local-name 169
set ppp profile isdn-ppp auth secret 169
set ppp profile isdn-ppp auth type chap
set ppp profile isdn-ppp passive
```

手順 3: ISDN BRI インターフェースのセットアップ

このセクションでは、ISDN サポート用に ISDN BRI を設定する 3 つの方法を説明します。

ISDN BRI の構成	詳細は、
ISDN BRI をダイヤラーとして使用	53 ページの「1 つの宛先のみのダイヤルアウト」
ダイヤルアウトにダイヤラーインターフェースを使用	54 ページの「ダイヤラーインターフェースを使用したダイヤルアウト」
専用回線モードの使用	57 ページの「専用回線モードの使用」

ISDN サポート用にユーザーのデバイスを設定する例は、それぞれのセクションを参照してください。

1 つの宛先のみのダイヤルアウト

この例では、支店（5 ページの図 2 を参照）にある端点を本社に接続するためのダイヤラーとして、ISDN インターフェース（BRI）を設定します。2 つのサイト間で断続的なトラフィックがあるときだけに 1 つの宛先へダイヤルアウトしている場合は、この設定をセットアップします。トラフィックがないと、接続はドロップします。

10.1.1.1 ネットワーク上の支店 A は、bri0/0 インターフェースを通って 10.2.2.2/16 ネットワーク上の支店 B、または 11.0.0.0/16 ネットワーク上の本社にダイヤルアウトします。

WebUI

Network > Interfaces > List > Edit (*bri*): **Basic** を選択して、適用可能なオプション値を選択し、**Apply** をクリックします。

BRI Mode: Dial Using BRI
Dialer Enable Options
Primary Number: 16900
WAN Encapsulation: PPP

Apply をクリックします。

Binding a PPP Profile: isdn-ppp

CLI

```
set in bri0/0 dialer-enable
set in bri0/0 encap ppp
set in bri0/0 ppp profile isdn-ppp
set in bri0/0 primary-number 16900
```

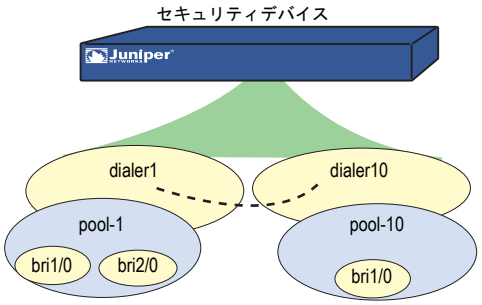
ダイヤラーインターフェースを使用したダイヤルアウト

この例では、ダイヤラーインターフェースを使用してダイヤルアウトします。宛先の数が利用可能な物理ラインの数を超える場合、複数の宛先へダイヤルアウトするのに、この方法を使用します。この設定は、ダイヤルオンデマンドルーティング（DDR）とオンデマンド帯域幅をサポートします。

ダイヤラープールは、ダイヤラーインターフェース経由で論理的なダイヤルピアを使用することにより、ISDN BRI を利用します。これにより、すべての潜在的な宛先から実際の物理リンクが分離されます。宛先の数が利用可能な物理ラインの数を超える場合、物理インターフェースは、ダイヤラープールのメンバーとして設定できます。物理インターフェースは、複数のプールに所属することもでき、1 本のラインを複数の宛先へダイヤルするのに使用できます。

図 10 は、ダイヤラーインターフェース、ダイヤラープールおよび ISDN BRI の関係を示します。

図 10: ダイヤラーインターフェースを使用したダイヤルアウト



デフォルトでは、ISDN BRI はどのダイヤラープールにもありません。同様に、各 ISDN BRI をいくつかのダイヤラープールに追加できます。

次のセクションは、54 ページの図 10 に示すように、WebUI および CLI を使用して dialer1 と dialer10 の設定についてステップ毎に説明しています。構成の終わりに、支店 A（5 ページの図 2 を参照）にある 2 つのステーションは、ダイヤラーインターフェース dialer1 を使用して支店 B に接続できます。同時に、支店 A の別のワークステーションは、dialer10 を使用して、本社へダイヤルアウトできます。

1. dialer1 および dialer10 インターフェースを構成します。

   a. ダイヤラーインターフェースを作成し構成します。

   b. PPP プロファイル（isdn-ppp）をダイヤラーインターフェースにバインドします。

2. ダイヤラープール pool-1 および pool-10 を構成します。

   a. 2 つのダイヤラープールを作成します。

   b. ダイヤラープールをそれぞれのダイヤラーインターフェースにバインドします。pool-1 を dialer1 に、pool-10 を dialer10 にバインドします。

3. ダイヤラープールに ISDN インターフェース（BRI）を追加します。

   dialer pool-1 に bri1/0 と bri2/0 を追加します。
   dialer pool-10 に bri1/0 を追加します。

BRI の他のオプションを設定するには、27 ページの「BRI モード」を参照してください。

WebUI

1. dialer1 インターフェースの構成

Network > Interface > List > New > Dialer IF: 次のように入力してから **OK** をクリックします。

Interface Name: dialer1
Primary Number: 16900
WAN Encapsulation: Multi-link PPP
Zone Name: Untrust
MTU: 1500

Apply をクリックします。

Binding a PPP Profile: isdn-ppp

Network > Interfaces > List > Edit (*dialer1*) > Dialer Pool: 適用可能なオプション値を入力し、**Apply** をクリックします。

Dialer pool: pool-1

Add をクリックします。

Network > Interfaces > List > Edit (*bri1/0*):

Basic を選択して、適用可能なオプション値を入力し、**Apply** をクリックします。

BRI Mode:
Leased Line Mode(128kbps): **チェック解除**
Dial Using BRI: **チェック解除**

Dialer Pool を選択して、適用可能なオプション値を入力し、**Apply** をクリックします。

pool-1 に優先順位を設定し、Select as Member ボックスをチェックします。

Priority: 1
Select as Member: **チェック**

Network > Interfaces > List > Edit (*bri2/0*):

Basic を選択して、適用可能なオプション値を入力し、**Apply** をクリックします。

BRI Mode:
Leased Line Mode(128kbps): **チェック解除**
Dial Using BRI: **チェック解除**

Dialer Pool を選択して、適用可能なオプション値を入力し、**Apply** をクリックします。

pool-1 に優先順位を設定し、Select as Member ボックスをチェックします。

Priority: 1
Select as Member: **チェック**

2. **dialer10 インターフェースの構成**
Network > Interface > List > New > Dialer IF: 次のように入力してから **OK** をクリックします。

Interface Name: dialer10
Primary Number: 16900
WAN Encapsulation: Multi-link PPP
Zone Name: Untrust
MTU: 1500

Apply をクリックします。

Binding a PPP Profile: isdn-ppp

Network > Interfaces > List > Edit (*dialer10*) > Dialer Pool: 適用可能なオプション値を入力し、**Apply** をクリックします。

Dialer pool: pool-10

Add をクリックします。

Network > Interfaces > List > Edit (*bri1/0*):

Basic を選択して、適用可能なオプション値を入力し、**Apply** をクリックします。

BRI Mode:
Leased Line Mode(128kbps): **チェック解除**
Dial Using BRI: **チェック解除**

Dialer Pool を選択して、適用可能なオプション値を入力し、**Apply** をクリックします。

pool-10 に優先順位を設定し、Select as Member ボックスをチェックします。

Priority: 1
Select as Member: **チェック**

CLI

1. **dialer1 インターフェースの構成**

```
set interface dialer1 zone Untrust
set interface dialer1 primary-number 16900
set interface dialer1 encap mlppp
set interface dialer1 mtu 1500
set interface dialer1 ppp profile isdn-ppp

set dialer pool name pool-1
set interface dialer1 dialer-pool pool-1

set dialer pool pool-1 member-interface bri2/0 priority 1
```

2. dialer10 インターフェースの構成

```
set interface dialer10 zone Untrust
set interface dialer10 primary-number 16900
set interface dialer10 encap mlppp
set interface dialer10 mtu 1500
set interface dialer10 ppp profile isdn-ppp

set dialer pool name pool-1
set interface dialer10 dialer-pool pool-10

set dialer pool pool-10 member-interface bri1/0 priority 1
```

5 ページの図 2 に示すように、支店 A の 2 つのステーションが、ダイヤラーインターフェース dialer1 を使用して、支店 B に接続できます。同時に、支店 A の別のワークステーションは、dialer10 を使用して、本社へダイヤルアウトできます。

専用回線モードの使用

この例では、専用回線を使用して ISDN 接続を確立します。BRI が専用回線モードに設定されると、BRI はデータの提供だけができるレイヤ 3 インターフェースになります。ゆえに、D チャネルは必要ありません。合計データ速度が 128 Kbps の 1 本のチャネル（B＋B）だけがサポートされます。Q931 ダイアリングは、チャネルをセットアップするには必要ありません。Q931 プロトコルおよび Q921 プロトコルの詳細は、*ScreenOS CLI Reference Guide: IPv4 Command Descriptions* を参照してください。

この構成方法を使用して、コスト効率が良く、信頼できる高速接続で 2 つのサイトを接続します。

WebUI

Network > Interfaces > List > Edit (*bri*): **Basic** を選択して、適用可能なオプション値を選択し、**OK** をクリックします。

BRI Mode: リース回線
WAN Encapsulation: PPP

Apply をクリックします。

Binding a PPP Profile: isdn-ppp

CLI

```
set in bri0/0 isdn leased-line 128kbps
set in bri0/0 encap ppp
set in bri0/0 ppp profile isdn-ppp
```

手順 4: 宛先へのトラフィックのルーティング

ISDN インターフェース（BRI）とダイヤラーインターフェースを通ってトラフィックをルーティングするように、支店 A のセキュリティデバイスで次を設定します。

WebUI

Network > Routing > Destination > New: 適用可能なオプション値を選択し、**OK** をクリックします。

IP Address/Netmask: 10.2.2.2/16
Next Hop: Gateway
Interface: bri1/0

Network > Routing > Destination > New: 適用可能なオプション値を選択し、**OK** をクリックします。

IP Address/Netmask: 11.0.0.0/16
Next Hop: Gateway
Interface: bri1/0

Network > Routing > Destination > New: 適用可能なオプション値を選択し、**OK** をクリックします。

IP Address/Netmask: 10.2.2.2/16
Next Hop: Gateway
Interface: bri2/0

Network > Routing > Destination > New: 適用可能なオプション値を選択し、**OK** をクリックします。

IP Address/Netmask: 11.0.0.0/16
Next Hop: Gateway
Interface: bri2/0

CLI

```
set route 10.2.2.2/16 interface bri1/0
set route 10.2.2.2/16 interface bri2/0
set route 11.0.0.0/16 interface bri1/0
set route 11.0.0.0/16 interface bri2/0
```

WebUI

Network > Routing > Destination > New: 適用可能なオプション値を選択し、**OK** をクリックします。

IP Address/Netmask: 10.2.2.2/16
Next Hop: Gateway
Interface: dialer1

Network > Routing > Destination > New: 適用可能なオプション値を選択し、**OK** をクリックします。

IP Address/Netmask: 11.0.0.0/16
Next Hop: Gateway
Interface: dialer1

Network > Routing > Destination > New: 適用可能なオプション値を選択し、**OK** をクリックします。

IP Address/Netmask: 10.2.2.2/16
Next Hop: Gateway
Interface: dialer10

Network > Routing > Destination > New: 適用可能なオプション値を選択し、**OK** をクリックします。

IP Address/Netmask: 11.0.0.0/16
Next Hop: Gateway
Interface: dialer10

CLI

```
set route 10.2.2.2/16 interface dialer1
set route 11.0.0.0/16 interface dialer1

set route 10.2.2.2/16 interface dialer10
set route 11.0.0.0/16 interface dialer10
```

支店 A の 2 つのステーションが、ダイヤラーインターフェース dialer1 を使用して、支店 B に接続できます。同時に、支店 A の別のワークステーションは、dialer10 を使用して、本社へダイヤルアウトできます。

カプセル化設定例

このセクションには、以下の WAN 設定例があります。

- 59 ページの「PPP カプセル化の構成」
- 60 ページの「MLPPP カプセル化の構成」
- 62 ページの「フレームリレーカプセル化の構成」
- 62 ページの「MLFR カプセル化の構成」
- 64 ページの「Cisco HDLC カプセル化の構成」

注 : カプセル化情報を構成する前に WAN インターフェースのプロパティを構成します。

PPP カプセル化の構成

この例では基本的な PPP カプセル化構成を示します。

WebUI

1. PPP アクセスプロファイルを設定します。

Network > PPP > Edit > New: 以下を入力して **Apply** をクリックします。

PPP Profile: juniper1
Authentication: CHAP (選択)
Static IP: (選択)
Local Name: local-firewall
Password: abcd1234#B

2. **ユーザー情報を設定します。**
   Objects > User > Local > New: 以下を入力して **Apply** をクリックします。

   User Name: router
   WAN User: (選択)
   Authentication User: (選択)
   User Password: abcd1234#C
   Confirm Password: abcd1234#C

3. **WAN インターフェースに juniper1 アクセスプロファイルを割り当てます。**
   Network > Interfaces > List > Edit（serial2/0): 以下を選択して **Apply** をクリックします。

   WAN Encapsulation: PPP (選択)
   Binding a PPP Profile: juniper1 (選択)
   Zone Name: untrust (選択))
   Fixed IP: (選択)
   IP Address/Netmask: 192.168.100.1/24
   Manageable: (選択)

CLI

1. **PPP アクセスプロファイルを設定します。**
   set ppp profile juniper1 auth type chap
   set ppp profile juniper1 auth local-name local-firewall
   set ppp profile juniper1 auth secret abcd1234#B
   set ppp profile juniper1 static-ip

2. **ユーザー情報を設定します。**
   set user router password abcd1234#C
   set user router type wan

3. **WAN インターフェースに juniper1 アクセスプロファイルを割り当てます。**
   set interface serial2/0 untrust zone
   set interface serial2/0 encap ppp
   set interface serial2/0 ppp profile juniper1
   set interface serial2/0 ip 192.168.100.1/24
   set interface serial2/0 manage
   save

MLPPP カプセル化の構成

この例では基本的な MLPPP カプセル化構成を示します。

WebUI

1. **PPP アクセスプロファイルを設定します。**
   Network > PPP > Edit > New: 以下を入力して **Apply** をクリックします。

   PPP Profile: juniper-mlppp
   Authentication: CHAP (選択)
   Static IP: (選択)
   Local Name: local-firewall
   Password: abcd1234

2. ユーザー情報を設定します。
Objects > User > Local > New: 以下を入力して **Apply** をクリックします。

User Name: router
WAN User: (選択)
Authentication User: (選択)
User Password: abcd1234
Confirm Password: abcd1234

3. マルチリンクインターフェースを設定します。
Network > Interfaces > List > New Multilink IF: 以下を入力して **Apply** をクリックします。

Interface Name: ML.1
WAN Encapsulation: Multi-Link PPP (選択)
Zone Name: Untrust (選択)

Edit (ml1 interface): 以下を入力して **Apply** をクリックします。

Binding a PPP Profile: juniper-mlppp (選択)
Fixed IP: (選択)
IP Address/Netmask: 192.168.100.1/24
Manageable: (選択解除)
Service Options
Other Services: ping (選択)

4. マルチリンクバンドルに WAN インターフェースを設定します。
Network > Interfaces > List > Edit (serial1/0): Member link オプションの ml1 Multilink Interface オプションを選択し、**Apply** をクリックします。

Network > Interfaces > List > Edit（serial2/0): Member link オプションの ml1 Multilink Interface オプションを選択し、**Apply** をクリックします。

CLI

1. PPP アクセスプロファイルを設定します。
```
set ppp profile juniper-mlppp auth type chap
set ppp profile juniper-mlppp auth local-name local-firewall
set ppp profile juniper-mlppp auth secret abcd1234
set ppp profile juniper-mlppp static-ip
```

2. ユーザー情報を設定します。
```
set user router password abcd1234
set user router type wan
```

3. マルチリンクインターフェースを設定します。
```
set interface ml1 zone untrust
set interface ml1 encap mlppp
set interface ml1 ppp profile juniper-mlppp
```

4. マルチリンクバンドルに WAN インターフェースを設定します。
```
set interface serial1/0 bundle ml1
set interface serial2/0 bundle ml1
set interface ml1 ip 192.168.100.1/24
set interface ml1 manage ping
save
```

フレームリレーカプセル化の構成

この例では基本的なフレームリレーカプセル化構成を示します。

WebUI

1. **フレームリレーカプセル化を設定します。**
   Network > Interfaces > List > Edit（serial2/0): WAN カプセル化には Frame Relay を選択して、**Apply** をクリックします。

   Edit（serial2/0） > FR: ITU タイプを選択して **Apply** をクリックします。

2. **PVC を設定します。**
   Network > Interfaces > List > New WAN Sub-IF: 以下を入力して **Apply** をクリックします。

   Interface Name: serial2/0 (選択).1
   Zone Name: Untrust (選択)
   Frame Relay DLCI: 200
   Fixed IP: (選択)
   IP Address/Netmask: 192.168.100.1/24
   Manageable: (選択解除)
   Service Options
   Other Services: ping (選択)

注： 指定する DLCI 値は、ユーザーのローカルプロバイダーがユーザーの PVC に割り当てた DLCI です。

CLI

1. **フレームリレーカプセル化を設定します。**
   set interface serial2/0 encap frame-relay
   set interface serial2/0 frame-relay lmi type itu

2. **PVC を設定します。**
   set interface serial2/0.1 zone untrust
   set interface serial2/0.1 frame-relay dlci 200
   set interface serial2/0.1 ip 192.168.100.1/24
   set interface serial2/0.1 manage ping
   save

MLFR カプセル化の構成

この例では基本的なマルチリンクフレームリレー（MLFR）カプセル化構成を示します。

WebUI

1. **マルチリンクインターフェースを作成します**
   Network > Interfaces > List > New: Multilink IF: 以下を入力して **Apply** をクリックします。

   Interface Name: ML 1
   WAN Encapsulation: Multi-Link FR (選択)
   Zone Name: Untrust (選択)

Network > Interfaces > List > Edit (serial2/0): WAN カプセル化には Frame Relay を選択して、**Apply** をクリックします。

Edit (serial2/0) > FR: ITU タイプを選択して **Apply** をクリックします。

2. **バンドルに WAN インターフェースを設定します。**
Network > Interfaces > List > Edit (serial1/0): Member link オプションの ml1 Multilink Interface オプションを選択し、**Apply** をクリックします。

Network > Interfaces > List > Edit (serial2/0): Member link オプションの ml1 Multilink Interface オプションを選択し、**Apply** をクリックします。

3. **バンドル PVC を設定します。**
Network > Interfaces > List > New WAN Sub-IF: 以下を入力して **Apply** をクリックします。

Interface Name: ml (選択).1
Zone Name: Untrust (選択)
Frame Relay DLCI: 200
Frame Relay Inverse ARP: (選択)
Fixed IP: (選択)
IP Address/Netmask: 192.168.100.1/24
Manageable: (選択解除)
Service Options
Other Services: ping (選択)

注 : 指定する DLCI 値は、ユーザーのローカルプロバイダーがユーザーの PVC に割り当てた DLCI です。

CLI

1. **マルチリンクインターフェースを作成します**
set interface ml1 zone untrust
set interface ml1 encap mlfr-uni-nni
set interface ml1 frame-relay lmi type itu

2. **バンドルに WAN インターフェースを設定します。**
set interface serial1/0 bundle ml1
set interface serial2/0 bundle ml1

3. **バンドル PVC を設定します。**
set interface ml1.1 zone untrust
set interface ml1.1 frame-relay dlci 200
set interface ml1.1 frame-relay inverse-arp
set interface ml1.1 ip 192.168.100.1/24
set interface ml1.1 manage ping
save

Cisco HDLC カプセル化の構成

この例では基本的な Cisco HDLC カプセル化構成を示します。

WebUI

デバイス A

Network > Interfaces > List > Edit（serial2/0): 以下を入力して **Apply** をクリックします。

WAN Encapsulation: Cisco HDLC (選択)
Zone Name: Trust (選択)
Fixed IP: (選択)
IP Address/Netmask: 192.168.3.1/24

デバイス B

Network > Interfaces > List > Edit（serial2/0): 以下を入力して **Apply** をクリックします。

WAN Encapsulation: Cisco HDLC (選択)
Zone Name: Trust (選択)
Fixed IP: (選択)
IP Address/Netmask: 192.168.3.2/24

CLI

デバイス A

1. **WAN インターフェースをセキュリティ ゾーンへバインドします**
   set interface serial2/0 zone trust
2. **カプセル化タイプを設定します。**
   set interface serial2/0 encap cisco-hdlc
3. **インターフェースの IP アドレスを設定します。**
   set interface serial2/0 ip 192.168.3.1/24
   save

デバイス B

1. **WAN インターフェースをセキュリティ ゾーンへバインドします**
   set interface serial2/0 zone trust
2. **カプセル化タイプを設定します。**
   set interface serial2/0 encap cisco-hdlc
3. **インターフェースの IP アドレスを設定します。**
   set interface serial2/0 ip 192.168.3.2/24
   save

第 2 章
デジタル加入者線

ScreenOS では、非対称デジタル加入者回線（ADSL）および G. 対称高速デジタル加入者線（G.SHDSL）接続を構成でき、これは統合インターネットプロトコルセキュリティ仮想プライベートネットワーク (IPSec VPN) とファイアウォールサービスを、ブロードバンド使用の在宅勤務者、支店または販売店に提供しています。このセクションは利用可能な DSL インターフェースを説明し、設定例を示します。

ご利用できるデータ転送レートは、サービスプロバイダの DSL サービスのタイプによります。ほとんどのサービスプロバイダは複数のレートレベルを提供しており、高速転送の方が低速転送より価格が高くなります。

注： セキュリティデバイス上の IPSec VPN およびファイアウォール機能の設定については、*第 5 部: 仮想プライベート ネットワーク* を参照してください。

本章のセクションは、以下のようになります。

- 65 ページの「デジタル加入者線の概要」
- 74 ページの「ADSL インターフェース」
- 75 ページの「G.SHDSL インターフェース」
- 77 ページの「ADSL 設定例」

デジタル加入者線の概要

従来の電話線は、ツイストペア銅線上にアナログ信号で音声を運びます。しかしながら、アナログ転送は利用できる帯域幅のほんの一部分しか使用しません。サービスプロバイダは、同じ媒体を使って、より広い帯域幅を利用するデジタル転送を可能にします。サービスプロバイダは、音声を送信するために使っている帯域幅のほんの一部を利用して、アナログとデジタル転送を分離することができます。電話とコンピュータが同じ線を同時に使用できるのはこのためです。サービスプロバイダの中央オフィスでは、DSL access multiplexer (DSLAM) が非同期転送モード (ATM) ネットワークなどの高速ネットワークに多くの DSL ラインを接続します。

adsl1 インターフェースのために設定する情報は、ADSL 接続の DSLAM 設定と対応しなければならないので、インターフェースを設定する前に、次の情報をサービスプロバイダから入手する必要があります。

- DSLAM の VC を識別する、仮想パス識別子および仮想チャンネル識別子 (VPI/VCI) 。
- ATM カプセル化方式。ScreenOS は次の ATM カプセル化方式をサポートします。
  - 仮想回路 (VC) ベースの複合方式（各プロトコルは個別の ATM VC に引き継がれる）。
  - 論理リンク制御 (LLC) 。複数のプロトコルを同一 ATM VC に引き継ぐことができる。これはデフォルトのカプセル化方式です。

注： DSL 接続で利用できる複合方式のタイプについては、サービスプロバイダに確認してください。

- ポイントツーポイントプロトコル (PPP) は ATM 相手固定接続 (PVC) などのシリアルポイントツーポイントリンク上に IP パケットを転送する際の標準プロトコルです。ScreenOS は次の PPP パケットの転送方式をサポートします。
  - PPP over Ethernet (PPPoE) - RFC 2516 では PPP packets over Ethernet のカプセル化を説明しています。PPPoE に関する詳細については、**2**-219 ページ の「システムパラメータ」を参照してください。
  - PPP over ATM (PPPoA) - RFC 1483 では ATM でのネットワークトラフィックのカプセル化を説明しています。PPPoA に関する詳細については、68 ページの「Point-to-Point Protocol over ATM」を参照してください。

注： サービスプロバイダのネットワークが PPPoE または PPPoA を使用する場合、サービスプロバイダは接続のためのユーザー名とパスワード、使用している認証方式そしてそのほかのプロトコル固有のパラメータを提供する必要があります。

- サービスプロバイダはネットワークに静的 IP アドレスまたは IP アドレスの範囲を提供します。サービスプロバイダは DNS 名およびアドレス解決のために使用する DNS (ドメイン名システム) サーバーのアドレスも提供する必要があります。

非同期転送モード

DSL インターフェースは、Transport Layer として ATM を使用します。ATM 仮想回路 (VC) には 2 つのタイプがあります。スイッチ仮想回路 (SVC) は一時的な論理ネットワーク接続で、個々のデーター転送セッションのために作成、維持されます。他方、永続的仮想回路 (PVC) は継続的にネットワークに対して利用できる論理接続です。DSL インターフェースは単一の物理ラインに対して、複数の PVC をサポートします。

ユーザーの物理ラインで PVC を設定するには、以下を行います。

WebUI

Network > Interfaces > Edit (adsl または shdsl interface): **次のように入力してから OK をクリックします。**

Zone Name: Untrust (**選択**)
VPI/VCI: 8/35
Multiplexing Method: LLC (**選択**)
RFC1483 Protocol Mode: Bridged (**選択**)

CLI

set interface *interface* pvc 8 35 mux llc protocol bridge zone untrust
save

ATM 通信品質

ATM のサービス品質（QoS）は、ユーザーが送信速度を制限して送信する ATM トラフィックを形成します。ATM QoS には多くの利点があります。

- 1 つの VC からのトラフィックがインターフェースの全帯域幅を消費して、他の VC に影響を与えデータが損失する、ということがないようにします。
- ある VC の速度が平均して一定の速度を超過しないとポリシーが指示する場合、帯域幅アクセスを制御します。
- リモートターゲットインターフェースの速度にローカルインターフェースの伝送速度を一致させます。たとえば、リンクの片方の端が 256 Kbps で送信し、もう片方の端が 128 Kbps で送信する、と仮定します。均一のエンドツーエンドのパイプがなければ、中間のスイッチは、より低速の端でパケットをドロップしなければならず、そのリンクを使用しているアプリケーションを混乱させる場合があります。

Juniper Networks は、ADSL mini-PIM で 3 つの ATM QoS サービスをサポートしています。

- **固定ビットレート (CBR):** 固定速度非圧縮ビデオを送信するときにしばしば利用されるサービス。
- **未指定ビットレート (UBR):** 遅延を許容できるデータを送信するときにしばしば利用されるサービス。
- **可変ビットレート非リアルタイム (VBR-NRT):** テレビ会議のような、圧縮しパケット化された音声およびビデオデータを送信するとき、しばしば利用されるサービス。

ATM QoS を設定するには、以下を行います。

WebUI

Network > Interfaces > Edit (adsl interface): **次のように入力してから OK をクリックします。**

Zone Name: Untrust (**選択**)
VPI/VCI: 8/35
QoS: UBR (**選択**)
RFC1483 Protocol Method: Bridged (**選択**)

CLI

```
set interface adsl1/0 qos ubr
save
```

Point-to-Point Protocol over ATM

Point-to-Point Protocol over ATM (PPPoA) は DSL インターフェースがあるセキュリティデバイス上で終了する PPP セッションに通常使われます。PPPoA はデスクトップクライアントを必要としないので、主にビジネスクラスのサービスに利用されます。

次に示すのは、PPPoA クライアントインスタンスの設定パラメータです。

- PPPoA 接続のユーザー名およびパスワード
- PPPoA インスタンスがバンドされているインターフェース（DSL インターフェースまたはサブインターフェース）およびインターフェースのネットマスク（デフォルトは 255.255.255.255 ）。
- 認証方法 : チャレンジハンドシェイク式認証プロトコル (CHAP) 、パスワード認証プロトコル (PAP) または任意の認証プロトコル（任意がデフォルト設定です）。
- 自動接続 : 接続終了後、自動的に再開するまでの秒数。デフォルトを 0 にすると、この機能は無効になります。
- 接続終了時にクリア : 接続終了時に IP 情報がクリアされることを指定します。これはデフォルトで無効になっています。
- アイドル間隔 : セキュリティデバイスが接続を終了するまでの、接続アイドル時間（分）を指定します。デフォルトは 30 分です。
- LCP-Echo 要求を送信する際の PPP Link Control Protocol (LCP) パラメータ。

PPPoA 接続が開始されると、PPPoA サーバーは Untrust ゾーンインターフェースおよび DNS サーバーの IP アドレスを自動的に提供します。PPPoA から DNS サーバーアドレスが受信されると、デバイスは、これらの DNS サーバーアドレスでデバイス上の DHCP サーバーを更新します。DHCP サーバーの DNS サーバーアドレスを更新したくない場合は、PPPoA 接続で受信した DNS パラメータの自動更新を無効にすることができます。

PPPoA インスタンスの状態を表示するには、WebUI （ネットワーク > PPPoA ）または **get pppoa all** コマンドを使用します。**get pppoa all** コマンドは物理インターフェースの状態も表示します。

セキュリティデバイス上の PPP セッションのデフォルトタイムアウト値は 1800 秒（ 30 分）です。この値は LCP-Echo 要求が再試行された数 (10) を要求間の間隔（ 180 秒）で掛け算した、デフォルトの回数に基づいています。LCP-Echo 要求が再試行される回数および要求間の間隔は設定することができます。

LCP-Echo 要求が再試行される回数を 12 、そして要求間の間隔を 190 にするには、以下のようにします。

WebUI

Network > PPP > PPPoA Profile > Edit (PPPoA インスタンス): 次のように入力してから **OK** をクリックします。

PPP Lcp Echo Retries: 12
PPP Lcp Echo Timeout: 190

CLI

```
set pppoa name poa1 ppp lcp-echo-retries 12
set pppoa name poa1 ppp lcp-echo-timeout 190
save
```

マルチリンクポイントツーポイントプロトコル

ScreenOS では、1 つの高速 DSL 接続に 2 つ以上の DSL チャネルをバンドルするために使用される、ADSL 上のマルチリンクポイントツーポイントプロトコル（MLPPP）の設定が可能です。このバンドルにより、ダウンストリームおよびアップストリームの帯域幅は 2 倍になります。DSL インターフェースが活動している間に、2 つの DSL インターフェースをマルチリンク（ML）インターフェースへバンドルすると、リンク制御プロトコル（LCP）が起動します。LCP ネゴシエーションが正常に終了するまで、ML インターフェースは活動状況に変化しません。ML インターフェースが静的 IP アドレスを使用しない場合、LCP ネゴシエーションが終了した後、ML インターフェースは動的 IP アドレスを取得します。

MLPPP が ADSL インターフーイスと連携する場合、次の制限が適用されます。

- 2 つの PIM は、同じ BRAS に接続しなければなりません
- MLPPP にバンドルできるのは、2 つのインターフェースだけです
- DSL インターフェースは ML インターフェースと同じセキュリティゾーンになければなりません

DSL インターフェースの Discrete Multitone

Discrete multitone (DMT) はデジタルデータをアナログ信号にコード化するための方式です。デフォルトでは、ADSL インターフェースは DMT 動作モードについてサービスプロバイダの DSLAM と自動的にネゴシエートします。ADSL インターフェースのモードを変更して、インターフェースが次の DMT 標準のみを使用するように設定できます。

- American National Standards Institute (ANSI) TI.413 Issue 2 は最大 8 Mbps ダウンストリームおよび 1 Mbps アップストリームのデータレートをサポートします。
- International Telecommunications Union (ITU) G.992.1（G.dmt としても知られている）は 6.144 Mbps ダウンストリームおよび 640 kbps アップストリームのデータレートをサポートしています。
- ITU 992.2 （*G.lite* としても知られている）は最高 1.536 Mbps のダウンストリームおよび 512 kbps のアップストリームのデータレートをサポートしています。この標準は*スプリッターレス DSL* としても知られています。これは ADSL ラインに信号スプリッターを取り付ける必要がなく、サービスプロバイダの装置が遠隔から信号を分割するからです。

- ITU 992.3 （ADSL2 としても知られている）は最高 1.2 Mbps のアップストリームおよび 12 Mbps のダウンストリームのデータレートをサポートしています。
- ITU 992.5 （ADSL2 + としても知られている）は最高 1.2 Mbps のアップストリームおよび 24 Mbps のダウンストリームのデータレートをサポートしています。

ADSL DMT の動作モードを ADSL2 + に設定するには、以下を行います。

WebUI

Network > Interfaces > Edit (adsl interface): **次のように入力してから OK をクリックします。**

Operating Mode: ADSL2+ (**選択**)

CLI

```
set interface adsl1/0 phy operating-mode adsl2plus
save
```

G.SHDSL インターフェースの DMT は、ITU G.991.2、シングルペア高速デジタル加入者回線（SHDSL）のトランシーバとして定義されます。

注： 動作モードの互換性については、ISP にご連絡ください。どの動作モードが接続でサポートされているか判断するため、自動モードの使用を推奨します。

アネックスモード

アネックスモードは、単純な従来の電話サービス（POTS）に DSL ネットワークを接続するために、システム参照モデルを定義します。

ScreenOS は、次のアネックスモードをサポートします。

- Annex A: 北米のネットワーク実装で使用されます。
- Annex B: ヨーロッパのネットワーク実装で使用されます

アネックスモード B モードを使用するよう ADSL インターフェースを構成するには、以下を行います。

WebUI

Network > Interfaces > Edit (adsl1/0 interface): **次のように入力してから OK をクリックします。**

Operating Mode: NON-UR2 (**選択**)

CLI

```
set interface adsl1/0 phy operating-mode non-ur2
save
```

アネックスモード A モードを使用するよう G.SHDSL インターフェースを構成するには、以下を行います。

WebUI

Network > Interfaces > Edit (shdsl1/0 interface): **次のように入力してから OK をクリックします。**

Operating Mode
Annex: Annex-A (**選択**)

CLI

```
set interface shdsl1/0 operating-mode annex-a
save
```

仮想回路

仮想回路を追加するには、ADSL または G.SHDSL インターフェースにサブインターフェースを作成します。サブインターフェースは最大 10 個まで作成できます。たとえば、定義済みのゾーン **Untrust** にバインドされた新しいサブインターフェース **adsl1/0.1** を作成するには、以下を行います。

WebUI

Network > Interfaces > List > New ADSL Sub-IF: 以下を入力して **Apply** をクリックします。

Interface Name: adsl1/0.1
VPI/VCI: 0/35
Zone Name: Untrust (**選択**)

CLI

```
set interface adsl 1/0.1 pvc 0 35 zone Untrust
save
```

サブインターフェースは、71 ページの「VPI/VCI および複合方式」に説明のあるように、VPI/VCI 値の設定を含むメインのインターフェースと同様に構成する必要があります。サブインターフェースは、メインのインターフェースとは個別に構成します。つまり、メインのインターフェースとは異なる複合方式、VPI/VCI および PPP クライアントをサブインターフェースに構成することができるのです。また、メインのインターフェースに静的 IP アドレスがなくても、サブインターフェースに静的 IP アドレスを構成することができます。

VPI/VCI および複合方式

サービスプロバイダは、各仮想接続に VPI/VCI ペアを割り当てます。たとえば、VPI/VCI のペアとして 1/32 を受信したとすると、これは、VPI 値が 1、VCI 値が 32 であることを意味しています。この値は、サービスプロバイダが DSLAM (Digital Subscriber Line Access Multiplexer) の加入者側で構成する値と一致していなければなりません。

adsl1/0 インターフェースで VPI/VCI ペアを 1/32 に構成するには、以下の手順を実行します。

WebUI

Network > Interfaces > List > Edit（adsl1/0 インターフェース): VPI/VCI フィールドに **1/32** と入力して、**Apply** をクリックします。

CLI

```
set interface adsl1/0 pvc 1 32
save
```

デフォルトで SSG 20 は仮想回路ごとに論理リンク制御（LLC）方式の多重化を使用します。

adslx/0 インターフェース上で VPI/VCI を 1/32 に構成し、仮想回路で LLC カプセル化を使用するには、以下の手順を実行します。

WebUI

Network > Interfaces > List > Edit（adsl1/0 インターフェース): 以下を入力して **Apply** をクリックします。

VPI/VCI: 1 / 32
Multiplexing Method: LLC (**選択**)

CLI

```
set interface adsl1/0 pvc 1 32 mux llc
save
```

PPPoE または PPPoA

PPPoE は ADSL および G.SHDSL カプセル化のもっとも一般的な形式であり、ネットワーク上の各ホストの終端に利用されます。PPP セッションは SSG 20 で終了できるため、PPPoA は主にビジネスクラスのサービスに利用します。SSG 20 をサービスプロバイダのネットワークに接続するには、サービスプロバイダに割り当てられたユーザー名とパスワードを構成する必要があります。PPPoA の構成は、PPPoE の構成に似ています。

注 : SSG 20 がサポートするのは、仮想回路ごとに 1 つの PPPoE セッションです。

PPPoE にユーザー名 **roswell** とパスワード **area51** を構成して、PPPoE の構成を adsl1/0 インターフェースにバインドするには、以下の手順を実行します。

WebUI

Network > PPP > PPPoE Profile > New: 次のように入力してから **OK** をクリックします。

PPPoE Instance: poe1
Bound to Interface: adsl1/0 (**選択**)
UserName: roswell
Password: area51

CLI

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1/0
save
```

SSG 20 では、ほかにも構成可能な PPPoE パラメータや PPPoA パラメータがあります。たとえば認証方法（デフォルトサポートは、チャレンジハンドシェイク式認証プロトコルかパスワード認証プロトコルのいずれか)、アイドルタイムアウト（デフォルトでは 30 分）などがあります。サービスプロバイダのサーバーと適切な通信を行うために構成する必要のある他の PPPoE や PPPoA のパラメータについては、ご利用のサービスプロバイダにお尋ねください。

静的 IP アドレスおよびネットマスク

ネットワーク用の固定 IP アドレスとネットマスクがサービスで割り当てられている場合、そのネットワークに IP アドレスとネットマスクを構成し、SSG 20 に接続したルーターポートの IP アドレスを構成してください。また、デバイスが静的 IP アドレスを使用するよう指定する必要があります（通常、SSG 20 は PPPoE または PPPoA クライアントとして動作し、PPPoE サーバーまたは PPPoA サーバーとのネゴシエーションで ADSL インターフェースの IP アドレスを受け取ります)。

72 ページの「PPPoE または PPPoA」にあるように、PPPoE インスタンスまたは PPPoA インスタンスを構成して adsl1/0 インターフェースにバインドしてください。**Obtain IP using PPPoE** または **Obtain IP using PPPoA** を選択し、PPPoE インスタンスまたは PPPoA インスタンスの名前を選択してください。

ネットワークに静的 IP アドレス 1.1.1.1/24 を設定するには、以下の手順を実行します。

WebUI

Network > Interfaces > List > Edit（adsl1/0 インターフェース): 以下を入力して **Apply** をクリックします。

IP Address/Netmask: 1.1.1.1/24
Static IP: (選択)

CLI

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

または

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoa name poa1 static-ip
save
```

ADSL インターフェース

Asymmetric digital subscriber line (ADSL) はデジタル加入者線 (DSL) 技術で、既存の電話線で音声電話サービスと高速デジタル通信を同時に行うことを可能にします。ADSL サービスを家庭やビジネス顧客に提供しているサービスプロバイダは増えつつあります。

データ転送は*非対称*です。というのは、データ送信レート（*アップストリームレート*）はデータ受信レート（*ダウンストリームレート*）よりかなり低いからです。インターネットに送信するほとんどのメッセージは小さく、アップストリーム帯域幅を要しませんが、グラフィック、ビデオやオーディオなど、インターネットから受信するデータは、より大きいダウンストリーム帯域幅を必要とするので、インターネットアクセスには最適です。

セキュリティデバイスに付属している ADSL ケーブルは、デバイス上の ADSL ポートを電話線に接続します。ADSL モデムは必要ではありません。サービスプロバイダから信号スプリッタやマイクロフィルタを入手して、取り付けることもできます。

非同期転送モード (ATM) 仮想回路でサービスプロバイダのネットワークに接続するとき、ネットワークでは ADSL2/2 + インターフェース **adslx/0** を使用します。ここで x は PIM スロットを表します。ADSL2/2 + サブインターフェースを作成すれば、さらに仮想回路を追加構成できます。詳細については、71 ページの「仮想回路」を参照してください。

SSG 20 の現在のインターフェース一覧については、WebUI で Network > Interfaces > List ページを参照してください。Telnet またはコンソールセッションを使用している場合は、**get interface** CLI コマンドを入力します。これで、adslx/0 インターフェースがアントラステッドゾーンにバインドされていることが分かります。

ADSL2/2 + インターフェースでプロバイダのサービスプロバイダに接続している場合は、adsl(x/0) インターフェースを構成してください。そのためには、サービスプロバイダから以下の情報を入手してください。

- VPI/VCI (仮想パス識別子および仮想チャネル識別子) の値
- 以下のいずれかの AAL5 (ATM Adaptation Layer 5) 複合方式
  - 仮想回路方式の多重化。各プロトコルは各 ATM 仮想回路に引き継がれます。
  - 論理リンク制御 (LLC) カプセル化。複数のプロトコルを同じ ATM VC に引き継ぐことができます（デフォルト多重化方式)。
- PPPoE (Point-to-Point Protocol over Ethernet) または PPPoA (Point-to-Point Protocol over ATM) によるサービスプロバイダのネットワークへの接続用にサービスプロバイダから割り当てられたユーザー名およびパスワード
- 認証方法 (PPPoE または PPPoA 接続のいずれかがある場合)
- オプションで、ご使用のネットワークの静的 IP アドレスおよびネットマスク値

G.SHDSL インターフェース

G. 対称高速デジタル加入者線（SHDSL）インターフェースは、1 人の顧客構内設備（CPE）加入者と中央局（CO）の間のデータ転送用の、マルチレート、高速、対称デジタル加入者線技術をサポートします。上りより下りにより多くの帯域幅を提供するよう設計された ADSL と異なり、SHDSL は対称的で、2.3 Mbps の帯域幅を両方向に提供します。G.SHDSL インターフェースは ATM-over-SHDSL モードのみをサポートします。

G.SHDSL インターフェースは、DSLAM へのポイントツーポイント接続によってネットワークトラフィックを送信するため、ATM インターフェースを使用できます。DSL 接続を通じて接続するよう、PPPoE（Point-to-Point Protocol over Ethernet）または PPPoE（PPP over ATM）を構成できます。回線速度

ScreenOS では、1 秒あたりのキロバイト単位で、利用可能な回線速度を指定できます。G.SHDSL インターフェースで構成できる 2 つの PIC モードがあります。各インターフェースに 1 つのモードだけを構成できます。

- 2 ポート 2 線モード - 回線速度の自動検出または固定回線速度をサポートし、64 Kbps 単位で 192 Kbps から 2.3 Mbps までのネットワーク速度を提供します。2 線モードは、2 つの独立したより遅い SHDSL インターフェースを提供します。
- 1 ポート 4 線モード - 固定回線速度のみをサポートし、128 Kbps 単位で 384 Kbps から 4.6 Mbps までのネットワーク速度を提供します。4 線モードは、単一のより速い SHDSL インターフェースを提供します。

G.SHDSL の回線速度を構成するには、以下を行います。

WebUI

Network > Interfaces > Edit (shdsl): 次のように選択してから **OK** をクリックします。

Operating Mode
Line Rate: auto (**選択**)

CLI

```
set interface shdsl1/0 phy operating-mode line-rate auto
save
```

ループバックモード

ループバックテストは、信号が送信され、ネットワークまたは回線のすべてまたは一部を通過した後に送信側デバイスに戻される、診断手順です。返された信号は、装置または通信経路の保全性を評価するために、送信された信号と比較されます。

ScreenOS では、G.SHDSL インターフェースのループバックテストのタイプを指定できます。G.SHDSL インターフェースのループバックモードを構成するには、以下を行います。

WebUI

Network > Interfaces > Edit (shdsl): 次のように選択してから **OK** をクリックします。

Operating Mode
Loopback: local (**選択**)

CLI

```
set interface shdsl1/0 phy operating mode loopback local
save
```

操作、管理、および保守

ScreenOS では、ATM 仮想回路上で、liveness とも呼ばれる、OAM（操作、管理および保守）F5 ループバックセルのしきい値を設定できます。OAM ループバックは、特定の PVC の接続を確認するために使用されます。さらに、OAM セルが ATM 仮想回路上で送信される、秒単位の間隔である、OAM 期間を設定することもできます。

OAM liveness を設定するには、以下を行います。

WebUI

Network > Interfaces > Edit (shdsl): 次のように選択してから **OK** をクリックします。

Operating Mode
Oam-Liveness: Down **5** Up **5**

CLI

```
set interface shdsl1/0 phy operating-mode oam-liveness 5
save
```

OAM 期間を設定するには、以下を行います。

WebUI

Network > Interfaces > Edit (shdsl): 次のように選択してから **OK** をクリックします。

Operating Mode
Oam-Period: Period **5**

CLI

```
set interface shdsl1/0 phy operating-mode oam-period 5
save
```

信号対雑音比

信号対雑音比（SNR）は、ネットワークチャンネル上の伝送チャネルまたはオーディオ信号の質を測定します。SNR の設定により、しきい値より高い SNR マージンで回線トレーンを作ることにより、より安定した G.SHDSL 接続が形成されます。しきい値より下の外部雑音が回線に流れている場合、ラインは安定しています。さらに、SNR マージンしきい値を使用不可にすることもできます。SNR が 0 であれば、信号は不要な雑音と判別不能であることを示します。

ScreenOS では、次のしきい値のいずれかまたは両方を構成できます。

- **current:** 現在の雑音マージンに SNR しきい値を加えた値より高い回線トレーン。範囲は 0 ～ 10 db で、デフォルト値は **0** です。
- **snext:** 自己近端漏話（SNEXT）しきい値より高い回線トレーン。デフォルトは **disabled** です。

SNR しきい値を構成するには、以下を行います。

WebUI

Network > Interfaces > Edit (shdsl): 次のように選択してから **OK** をクリックします。

Operating Mode
Snr-margin: Current **0** Snext **11**

CLI

```
set interface shdsl1/0 phy operating-mode snr-margin current 0
set interface shdsl1/0 phy operating-mode snr-margin snext 11
save
```

ADSL 設定例

このセクションには、以下の設定例があります。

- 78 ページの「例 1:（小規模なビジネス / 自宅）ADSL インターフェース上の PPPoA」。セキュリティデバイスを PPPoA （または PPPoE ）を持つ ADSL インターフェースを使ったインターネット接続がある、ファイアウォールとして設定します。
- 81 ページの「例 2:（小規模なビジネス / 自宅）ADSL インターフェース上の 1483 ブリッジング」。セキュリティデバイスを 1483 ブリッジングを持つ ADSL インターフェースを使ったインターネット接続がある、ファイアウォールとして設定します。
- 83 ページの「例 3:（小規模なビジネス）ADSL インターフェース上の 1483 ブリッジング」。セキュリティデバイスを RFC 1483 ルーティング使用して、ADSL インターフェースを介したインターネット接続がある、ファイアウォールとして設定します。
- 85 ページの「例 4:（小規模なビジネス / 自宅）ダイヤルアップバックアップ」。セキュリティデバイスを PPPoE を持つ ADSL インターフェースを使った主要インターネット接続がある、ファイアウォールとして設定します。バックアップ接続はダイヤルアップです。

- 88 ページの「例 5:（小規模なビジネス / 自宅）Ethernet バックアップ」。セキュリティデバイスを PPPoE を持つ ADSL インターフェースを使った主要インターネット接続がある、ファイアウォールとして設定します。バックアップ接続は ethernet です。
- 91 ページの「例 6:（小規模なビジネス / 自宅）ADSL バックアップ」。セキュリティデバイスを PPPoE を使用した ADSL インターフェースを使った主要インターネット接続がある、ファイアウォールとして設定します。バックアップ接続は別の ADSL インターフェースです。
- 94 ページの「例 7:（小規模なビジネス）MLPPP ADSL」。セキュリティデバイスをマルチリンク PPP ADSL 接続を使ったインターネット接続がある、ファイアウォールとして設定します。
- 96 ページの「例 8:（小規模なビジネス）ローカルサーバーへのアクセスを許可」。セキュリティデバイスを ADSL インターフェースを使ったインターネット接続がある、ファイアウォールとして設定します。ローカル web サーバーにインターネットアクセスを許可し、同時に他の内部のホストが直接インターネットからアクセスできないようにします。
- 99 ページの「例 9:（支店）ADSL を通した VPN トンネル」。セキュリティデバイスを ADSL インターフェースを使った、本社への VPN トンネルがあるファイアウォールとして設定します。ローカル web サーバーにインターネットアクセスを許可し、同時に他の内部のホストが直接インターネットからアクセスできないようにします。
- 103 ページの「例 10:（支社）2 次 VPN トンネル」。セキュリティデバイスを ADSL インターフェースを使った、本社とインターネットに接続があるファイアウォールとして設定します。2 次接続として、本社へインターネットを通して VPN トンネルを設定します。

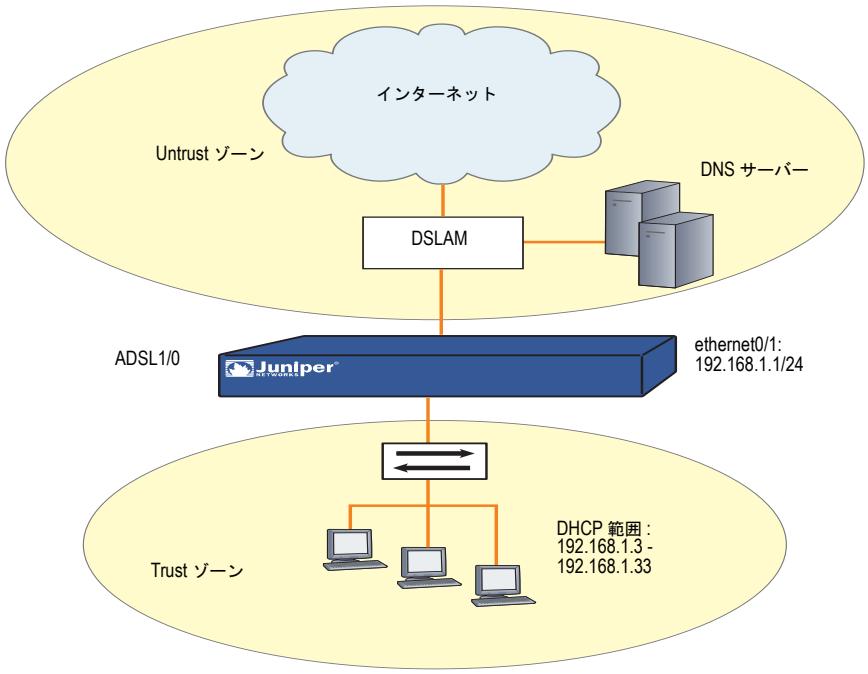
例 1:（小規模なビジネス / 自宅）ADSL インターフェース上の PPPoA

この例は、図 11 に示すように、PPPoA を利用して、セキュリティデバイスを ADSL インターフェースを使ったインターネット接続がある、ファイアウォールとして設定する方法を示します。セキュリティデバイスには PPPoA クライアントおよび DHCP サーバーの役割を同時に果たすものがあります。

ADSL インターフェース上の PPPoA を設定するには、次を行います。

1. ethernet0/1 インターフェースを Trust ゾーンに割り当て、DHCP サーバーに設定します。セキュリティデバイスが Trust ゾーンのホストに IP アドレスを割り当てると、同時にホストに対して、サービスプロバイダから入手した DNS サーバーアドレスを提供します。
2. ADSL インターフェース上に PVC を設定し、ここでは LLC カプセル化を使用するペアの値が 0/35 である VPI/VCI および、「poa1」という名前の PPPoA インスタンスを設定します。poa1 は ADSL インターフェースにバインドされています。セキュリティデバイスが ADSL インターフェースに対して IP アドレスを受信すると、同時に DNS サーバーに対して 1 つまたは 1 つ以上のアドレスを受信します。
3. セキュリティデバイス上での PPPoA を起動します。セキュリティデバイスは PPPoA を介してサービスプロバイダから ADSL インターフェース (adsl1/0) に対して動的に割り当てられた IP アドレスを受信し、また Trust ゾーンのホストに対して IP アドレスを動的に割り当てます。
4. 内部ネットワーク上で DHCP を起動します。

図 11: PPPoA を利用した ADSL インターフェース



WebUI

1. **イーサネットインターフェースおよび DHCP サーバー**
   Network > Interfaces > ethernet0/1 > Edit: 次のように入力してから **OK** をクリックします。

   Zone: Trust
   Static IP: (選択)
   IP Address/Netmask: 192.168.1.1/24

   Network > DHCP > Edit (ethernet2/1) > DHCP Server: Apply をクリックします。

   > Addresses > New: 次のように入力してから **OK** をクリックします。

   Dynamic: (選択)
   IP Address Start: 192.168.1.3
   IP Address End: 192.168.1.33

2. **ADSL インターフェースおよび PPPoA**
   Network > Interfaces > Edit (for adsl 1/0): 次のように入力してから **OK** をクリックします。

   VPI/VCI: 0/35
   Encapsulation: LLC (選択)
   Zone Name: Untrust

Network > PPP > PPPoA Profile > New: 次のように入力してから **OK** をクリックします。

PPPoA Instance:poa1
Bound to Interface: adsl1/0 (選択)
UserName: alex
Password:tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
Automatic Update of DHCP Server's DNS Parameters: (選択)

3. **セキュリティデバイス上での PPPoA の起動**
Trust ゾーンのセキュリティデバイスおよびワークステーションの電源をオフにします。

セキュリティデバイスの電源をオンにします。

セキュリティデバイスは DSLAM に PPPoA 接続を確立し、ADSL インターフェースの IP アドレスおよび DNS サーバーの IP アドレスを取得します。

4. **インターネットネットワーク上での DHCP の起動**
ワークステーションの電源をオンにします。

ワークステーションは、TCP/IP 接続を試行する際に、DNS サーバーの IP アドレスを自動的に受信し、ワークステーション自身の IP アドレスを取得します。

CLI

1. **Trust インターフェースおよび DHCP サーバー**

```
set interface ethernet0/1 zone trust
set interface ethernet0/1 ip 192.168.1.1/24
set interface ethernet0/1 dhcp server service
set interface ethernet0/1 dhcp server ip 192.168.1.3 192.168.1.33
```

2. **ADSL インターフェースおよび PPPoA**

```
set interface adsl2/1 pvc 0 35 mux llc zone untrust
set pppoa name poa1 username alex password
    tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
set pppoa name poa1 interface adsl1/0
set pppoa name poa1 update-dhcpserver
save
```

3. **セキュリティデバイス上での PPPoA の起動**
Trust ゾーンのセキュリティデバイスおよびワークステーションの電源をオフにします。

セキュリティデバイスの電源をオンにします。

セキュリティデバイスは DSLAM に PPPoA 接続を確立し、ADSL インターフェースの IP アドレスおよび DNS サーバーの IP アドレスを取得します。

4. **インターネットネットワーク上での DHCP の起動**
ワークステーションの電源をオンにします。

ワークステーションは、TCP/IP 接続を試行する際に、DNS サーバーの IP アドレスを自動的に受信し、ワークステーション自身の IP アドレスを取得します。

例 2:（小規模なビジネス / 自宅）ADSL インターフェース上の 1483 ブリッジング

RFC 1483 は AAL5 リンク上でブリッジされたプロトコルデータユニット（PDU）を転送する方法を説明しています。ブリッジされた PDU は IPSec 処理というオーバーヘッドを要求しないので、データトラフィックに利用できる帯域幅が多くなります。このようなトラフィックは IP パケット l レイヤーではセキュアされないので、プライベート VC がある場合にのみ利用します（サービスプロバイダは ADSL インターフェースに対して静的 IP アドレスを割り当てます）。

この例は、図 12 に示すように、1483 ブリッジングを利用して、セキュリティデバイスを ADSL インターフェースを使ったインターネット接続がある、ファイアウォールとして設定する方法を示します。サービスプロバイダは、ネットワークに対して静的 IP アドレス 1.1.1.1/32 を割り当て、DNS サーバーに対して IP アドレスを割り当てます。

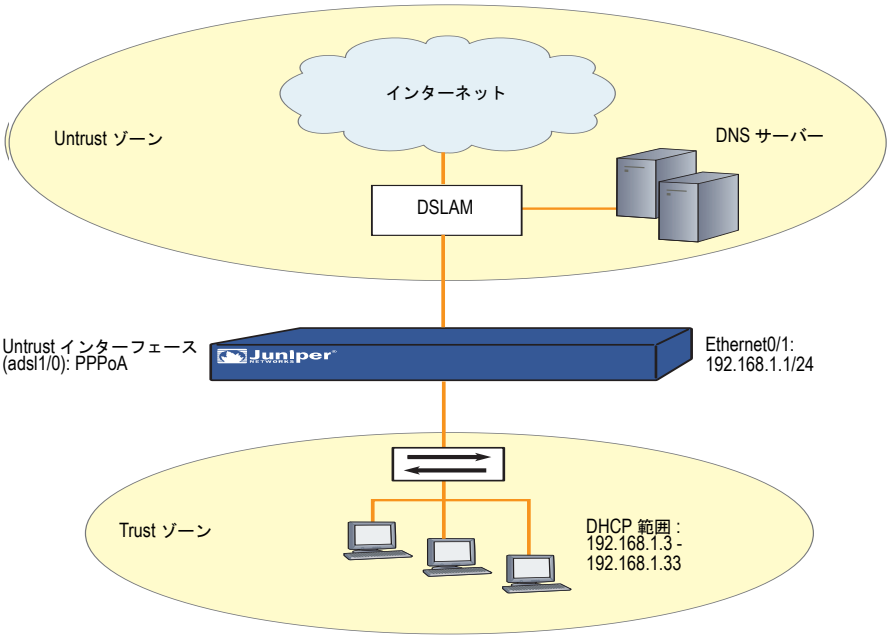
ADSL インターフェース上の 1483 ブリッジングを設定するには、次を行います。

1. trust インターフェースを構成し、それを DHCP サーバーとして設定します。

2. ADSL インターフェースに PVC を設定します。このときの設定は VPI/VCI ペア 0/35 および静的 IP アドレス 1.1.1.1/32 で、サービスプロバイダにより割り当てられます。

3. 内部ネットワーク上で DHCP を起動します。セキュリティデバイスはまた、Trust ゾーンのホストに対して IP アドレスを動的に割り当てます。セキュリティデバイスが Trust ゾーンのホストに IP アドレスを割り当てると、同時にサービスプロバイダからの DNS サーバーアドレスを提供します。

図 12: RFC 1483 ブリッジングを利用したインターフェース



WebUI

1. **イーサネットインターフェースおよび DHCP サーバー**
   Network > Interfaces > Edit (ethernet0/1): 次のように入力してから **OK** をクリックします。

   Zone: Trust
   Static IP: (選択)
   IP Address/Netmask: 192.168.1.1/24
   Interface Mode: NAT

   Network > DHCP > Edit (trust インターフェース) > DHCP Server: 以下を入力して **Apply** をクリックします。

   Gateway: 1.1.1.1
   Netmask: 255.255.255.0
   DNS#1: 1.1.1.221

   > Addresses > New: 次のように入力してから **OK** をクリックします。

   Dynamic: (選択)
   IP Address Start: 192.168.1.3
   IP Address End: 192.168.1.33

2. **ADSL インターフェース**
   Network > Interfaces > Edit (adsl1/0 interface): 以下を入力して **Apply** をクリックします。

   VPI/VCI: 0/35
   Zone Name: Untrust
   Static IP: (選択)
   IP Address/Netmask: 1.1.1.1/32

3. インターネットネットワーク上での DHCP の起動
ワークステーションの電源をオフにします。

ワークステーションは、TCP/IP 接続を試行する際に、DNS サーバーの IP アドレスを自動的に受信し、ワークステーション自身の IP アドレスを取得します。

CLI

1. Trust インターフェースおよび DHCP サーバー
```
set interface ethernet0/1 zone trust
set interface ethernet0/1 ip 192.168.1.1/24
set interface ethernet0/1 dhcp server service
set interface ethernet0/1 dhcp server ip 192.168.1.3 192.168.1.33
```

2. ADSL インターフェース
```
set interface adsl1/0 pvc 0 35 mux llc zone untrust
set interface adsl1/0 ip 1.1.1.1/32
save
```

3. インターネットネットワーク上での DHCP の起動
ワークステーションの電源をオフにします。

ワークステーションは、TCP/IP 接続を試行する際に、DNS サーバーの IP アドレスを自動的に受信し、ワークステーション自身の IP アドレスを取得します。

例 3:（小規模なビジネス）ADSL インターフェース上の 1483 ブリッジング

RFC 1483 は AAL5 リンク上でルーティングされたプロトコルデータユニット（PDU）を転送する方法を説明します。この構成で、デバイスが ADSL インターフェースを通してルーティング情報を他のルーターと交換できるようにします。

この例は、図 13 に示すように、1483 ルーティングおよび LLC カプセル化を利用して、セキュリティデバイスを ADSL インターフェースを使ったインターネット接続がある、ファイアウォールとして設定する方法を示します。

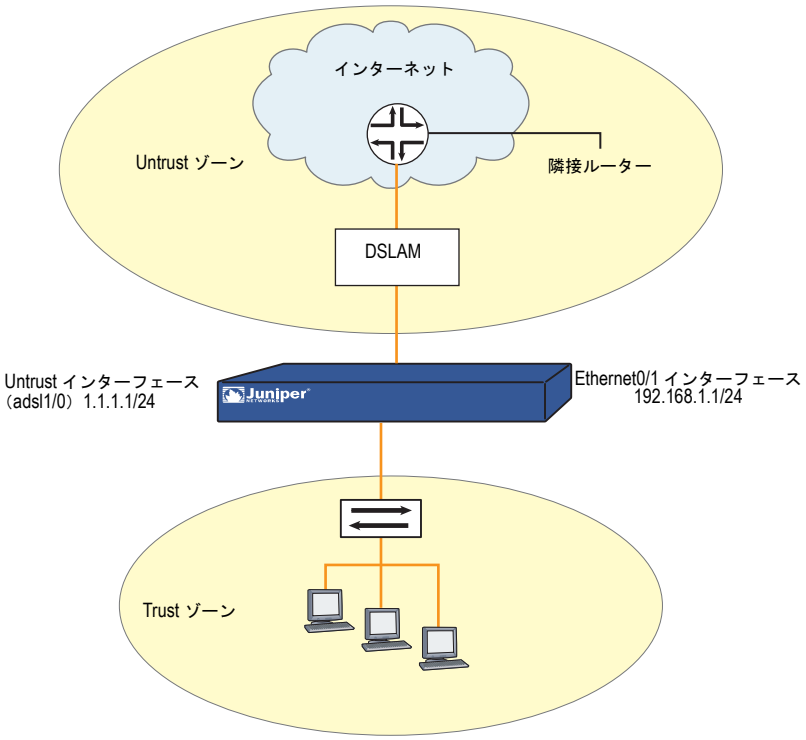
ADSL インターフェース上の 1483 ルーティングを設定するには、次を行います。

1. ADSL インターフェースの構成 ADSL インターフェースに PVC を設定します。このときの設定は VPI/VCI ペア 0/35 および静的 IP アドレス 1.1.1.1/24 です。また ADSL インターフェースを、隣接するルーターで作動している DHCP サーバーから IP アドレスを受け取る DHCP クライアントになるように設定することもできます。

2. イーサネットインターフェースを構成します。IP アドレスを 192.168.1.1/24 に、インターフェースモードを route に設定します。

3. trust-vr 仮想ルーターおよび ADSL と trust インターフェース上の動的ルーティングプロトコル（RIP 、OSPF または BGP）を有効にします。この例では動的ルーティングプロトコルは RIP です。隣接するルーターのインターフェースもまた LLC カプセル化おおび 1483 ルーティングの設定がされています。

図 13: ADSL インターフェース上の 1483 ルーティング



WebUI

1. **ADSL インターフェース**
   Network > Interfaces > Edit (adsl1/0 interface): 次のように入力してから **OK** をクリックします。

   VPI/VCI: 0/35
   Multiplexing Method: LLC (選択)
   RFC1483 Protocol Mode: Routed (選択)
   Zone: Untrust
   Static IP: (選択)
   IP Address/Netmask: 1.1.1.1/24

2. **Ethernet Interface**
   Network > Interfaces > Edit (Ethernet0.1): 次のように入力してから **OK** をクリックします。

   Zone: Trust
   Static IP: (選択)
   IP Address/Netmask: 192.168.1.1/24
   Interface Mode: Route

3. **動的ルーティングプロトコル**
   Network > Routing > Virtual Router (trust-vr) > Edit: Select **Create RIP Instance**.

   Enable RIP を選択して **OK** をクリックします。

Network > Interface > Edit (adsl1 インターフェース) > RIP: **Protocol RIP Enable** を選択し、**Apply** をクリックします。

Network > Interface > Edit (trust インターフェース) > RIP: **Protocol RIP Enable** を選択し、**Apply** をクリックします。

CLI

1. **ADSL インターフェース**
   set int adsl1/0 pvc 0 35 mux llc protocol routed zone untrust
   set int adsl1/0 ip 1.1.1.1/24
2. **Trust インターフェース**
   set interface ethernet0/1 zone trust
   set interface ethernet0/1 ip 192.168.1.1/24
   set interface ethernet0/1 route
3. **動的ルーティングプロトコル**
   set vr trust-vr protocol rip
   set vr trust-vr protocol rip enable
   set interface adsl1/0 protocol rip
   set interface adsl1/0 protocol rip enable
   set interface ethernet0/1 protocol rip
   set interface ethernet0/1 protocol rip enable
   save

例 4:（小規模なビジネス / 自宅）ダイヤルアップバックアップ

この例は、図 14 で示すように、セキュリティデバイスをファイアウォールとして設定する方法を示します。この場合、主要インターネット接続は PPPoE で ADSL インターフェースを使い、バックアップインターネット接続はダイヤルアップ接続を使います。

注 : デバイスにはバックアップ機能をサポートしないものもあります。

ADSL インターフェースによる主要接続とダイヤルアップによるバックアップ接続を設定するには、次を行います。

1. ADSL インターフェースおよび PPPoE を構成します。ADSL インターフェース上に PVC を設定し、ここでは LLC カプセル化を使用するペアの値が 0/35 である VPI/VCI および、「poa1」という名前の PPPoE インスタンスを設定します。poa1 は ADSL インターフェースにバインドされています。
2. モデムポートでシリアルインターフェースを使用して、インターネットへのバックアップ接続を構成します。ADSL とシリアルインターフェースが両方とも Untrust ゾーンにバインドされている場合、インターフェースフェールオーバーが自動的に設定されます。つまり、ADSL インターフェースが利用できなくなった場合、セキュリティデバイスは自動的に外向きトラフィックをシリアルインターフェースに送信し、Integrated Services Digital Network

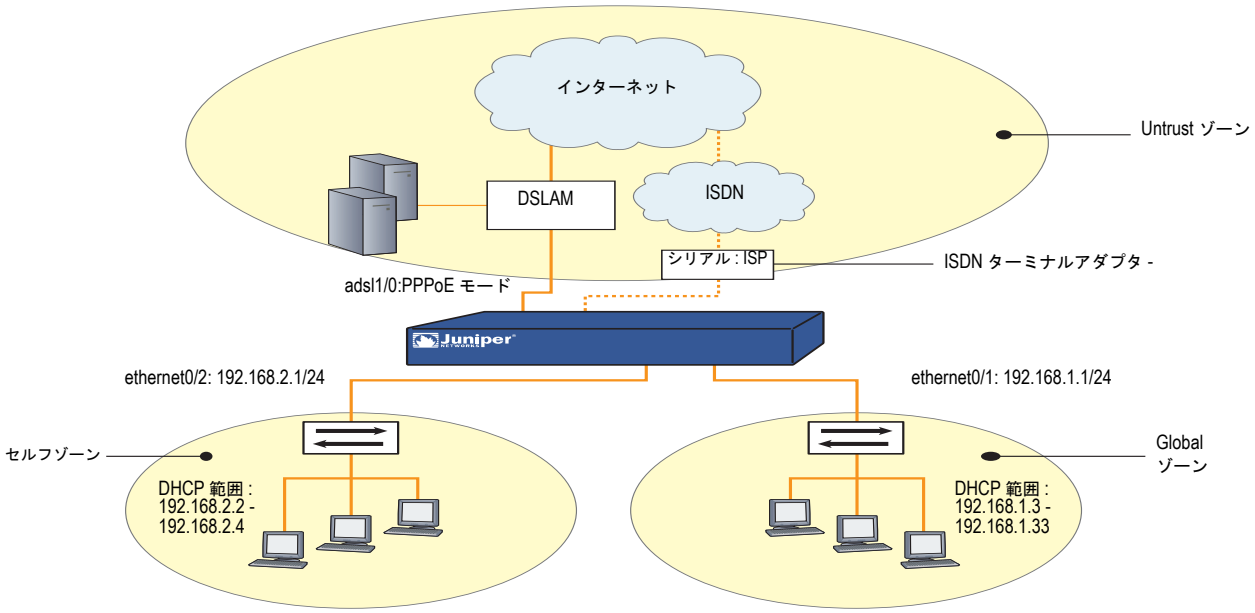
(ISDN) ターミナルアダプタまたはお使いの ISP アカウントのモデムを使ってダイヤルします。ADSL インターフェースが再度利用できるようになると、セキュリティデバイスは自動的に外向きトラフィックを adsl1 インターフェースに送信します。インターフェースフェールオーバーについては、**11**-87 ページ の「Failover」を参照してください。DNS 構成については、109 ページの「ISP フェールオーバーとダイヤル回復」を参照してください。

3. Global ゾーンを構成します。Global ゾーンの静的 IP を 192.168.1.1/24 に設定し、インターフェースモードを NAT に設定します。

4. Self ゾーンを構成します。Self ゾーンの静的 IP を 192.168.2.1/24 に設定し、インターフェースモードを NAT に設定します。

5. Self ゾーンおよび Global ゾーンで DHCP を起動します。

図 14: ダイアルバックアップ付き ADSL



シリアルインターフェースを設定するには、次の情報が必要です。

- ダイヤルアップサービスプロバイダのアカウントへのログインとパスワード
- アカウントへダイヤルするための主要電話接続
- モデム初期化文字列

WebUI

1. **ADSL インターフェースおよび PPPoE**
   Network > Interfaces > Edit (adsl1/0 interface): 次のように入力してから **OK** をクリックします。

   VPI/VCI: 0/35
   Encapsulation: LLC (選択)
   Zone Name: Untrust

Network > PPP > PPPoE Profile > New: 次のように入力してから **OK** をクリックします。

PPPoE Instance: poe1
Bound to Interface: adsl1/0 (選択)
UserName: alex
Password: tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
Automatic Update of DHCP Server's DNS Parameters: (選択)

2. **バックアップダイヤルアップインターフェース**
Network > Interfaces > Backup: 次のように入力してから **OK** をクリックします。

Primary Interface: adsl1/0
Backup Interface: serial0/0
Type: track ip

Network > Interfaces > Edit > Monitor (adsl1/0 インターフェース用に): 次のように入力してから **OK** をクリックします。

Enable Track IP: (選択)
Threshold: 1
Weight: 255

Network > Interfaces > Edit > Monitor > Track IP > Click **ADD**: 次のように入力してから OK をクリックします。

Dynamic: (選択)

3. **LAN Interface**
Network > Interfaces > Edit (ethernet1 インターフェース用に): 次のように入力してから **OK** をクリックします。

Zone: Work (選択済み)
Static IP: (選択)
IP Address/Netmask: 192.168.1.1/24
Interface Mode: NAT

Network > DHCP > Edit (ethernet0/1 インターフェース用に) > DHCP Server: **Apply** をクリックします。

> Addresses > New: 次のように入力してから **OK** をクリックします。

Dynamic: (選択)
IP Address Start: 192.168.1.3
IP Address End: 192.168.1.33

4. **Self インターフェース**
Network > Interfaces > Edit (ethernet0/2 インターフェース用に): 次のように入力してから **OK** をクリックします。

Zone: Home (選択済み)
Static IP: (選択)
IP Address/Netmask: 192.168.2.1/24
Interface Mode: NAT

Network > DHCP > Edit (ethernet2 インターフェース用に) > DHCP サーバー : **Apply** をクリックします。

> Addresses > New: 次のように入力してから **OK** をクリックします。

Dynamic: (選択)
IP Address Start: 192.168.2.2
IP Address End: 192.168.2.5

5. **Home と Work ゾーンでの DHCP の起動**
ワークステーションの電源をオフにします。

ワークステーションは、TCP/IP 接続を試行する際に、DNS サーバーの IP アドレスを自動的に受信し、ワークステーション自身の IP アドレスを取得します。

CLI

1. **ADSL インターフェースおよび PPPoE**
```
set interface adsl1/0 pvc 0 35 mux llc zone untrust
set pppoe name poe1 username alex password
    tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
set pppoe name poe1 interface adsl1/0
```

2. **バックアップダイヤルアップインターフェース**
```
set interface adsl1/0 backup interface serial0/0 type track-ip
set interface adsl1/0 monitor track ip
set interface adsl1/0 monitor track-ip dynamic
```

3. **LAN インターフェース**
```
set interface ethernet0/1 ip 192.168.1.1/24
set interface ethernet0/1 dhcp server service
set interface ethernet0/1 dhcp server ip 192.168.1.3 192.168.1.33
```

4. **Self インターフェース**
```
set interface ethernet0/2 ip 192.168.2.1/24
set interface ethernet0/2 dhcp server service
set interface ethernet0/2 dhcp server ip 192.168.2.2 192.168.2.5
save
```

5. **Home と Work ゾーンでの DHCP の起動**
ワークステーションの電源をオフにします。

ワークステーションは、TCP/IP 接続を試行する際に、DNS サーバーの IP アドレスを自動的に受信し、ワークステーション自身の IP アドレスを取得します。

例 5:（小規模なビジネス / 自宅）Ethernet バックアップ

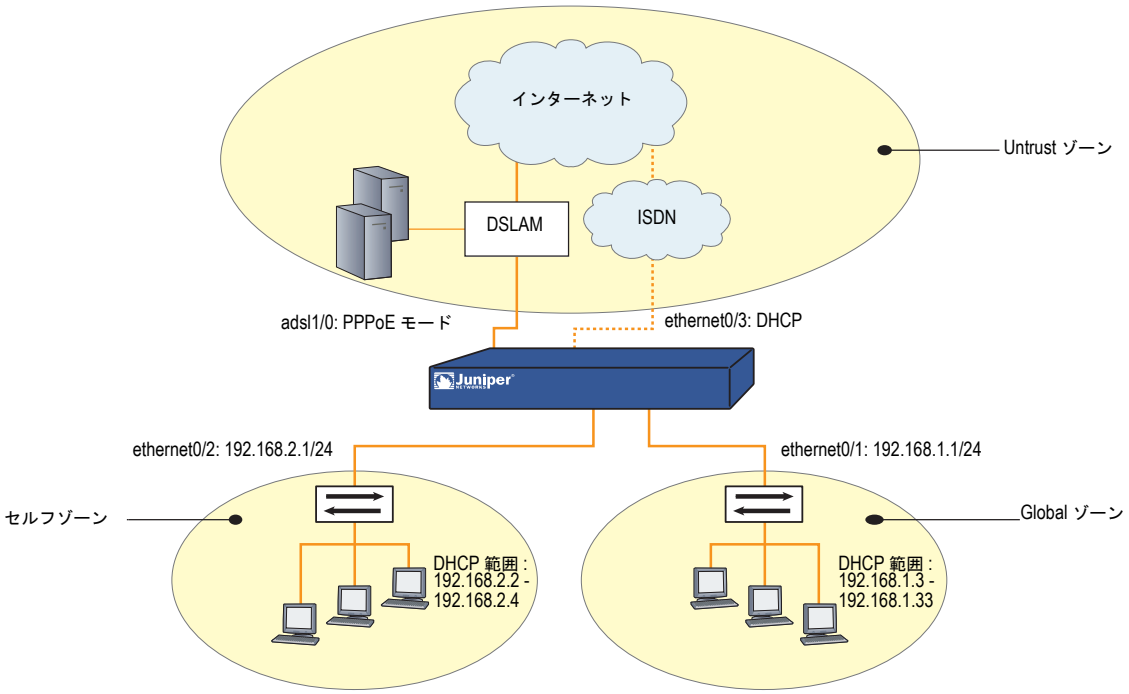
この例は、図 15 で示すように、セキュリティデバイスをファイアウォールとして設定する方法を示します。この場合、主要インターネット接続は PPPoE で ADSL インターフェースを使い、バックアップインターネット接続は Ethernet 接続を使います。

注 : この例は、85 ページの「例 4:（小規模なビジネス / 自宅）ダイヤルアップバックアップ」で示した構成と類似のものですが、インターネットへのバックアップ接続に アントラステッド Ethernet ポートを使用している点が異なります。

ADSL インターフェースによる主要接続と Ethernet 接続によるバックアップ接続を設定するには、次を行います。

1. ADSL インターフェースを PPPoE で構成します。ADSL インターフェース上に PVC を設定し、ここでは LLC カプセル化を使用するペアの値が 0/35 である VPI/VCI および、「poa1」という名前の PPPoE インスタンスを設定します。poa1 は ADSL インターフェースにバインドされています。
2. バックアップインターフェースに ethernet3 を設定します。
3. Global ゾーンを構成します。
4. Self ゾーンを構成します。

図 15: イーサネットバックアップ付き ADSL



WebUI

1. **ADSL インターフェースおよび PPPoE**

   Network > Interfaces > Edit (for adsl1/0): 次のように入力してから **OK** をクリックします。

   VPI/VCI: 0/35
   Encapsulation: LLC (選択)
   Zone: Untrust

   Network > PPP > PPPoE Profile > New: 次のように入力してから **OK** をクリックします。

   PPPoE Instance: poe1
   Bound to Interface: adsl1/0 (選択)
   UserName: alex

Password: tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
Automatic Update of DHCP Server's DNS Parameters: (選択)

2. バックアップ Ethernet インターフェース

Network > Interfaces > Edit (for ethernet0/3): 次のように入力してから **OK** をクリックします。

Zone Name: Untrust (選択)
Obtain IP using DHCP: (選択)
自動的に DHCP サーバーパラメータを更新 : (選択)

3. Global ゾーンの VIP

Network > Interfaces > Edit (for ethernet0/1): 次のように入力してから **OK** をクリックします。

Zone: Global
Static IP: (選択)
IP Address/Netmask: 192.168.1.1/24
Interface Mode: NAT

Network > DHCP > Edit (for ethernet0/1) > DHCP Server: Apply をクリックします。

> Addresses > New: 次のように入力してから **OK** をクリックします。

Dynamic: (選択)
IP Address Start: 192.168.1.3
IP Address End: 192.168.1.33

4. セルフゾーン

Network > Interfaces > Edit (ethernet0/2): 次のように入力してから **OK** をクリックします。

Zone: Self
Static IP: (選択)
IP Address/Netmask: 192.168.2.1/24
Interface Mode: NAT

Network > DHCP > Edit (for ethernet 0/2) > DHCP Server: Apply をクリックします。

> Addresses > New: 次のように入力してから **OK** をクリックします。

Dynamic: (選択)
IP Address Start: 192.168.2.2
IP Address End: 192.168.2.5

CLI

1. ADSL インターフェースおよび PPPoE

```
set interface adsl1/0 pvc 0 35 mux llc zone untrust
set pppoe name poe1 username alex password
    tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
set pppoe name poe1 interface adsl1/0
```

2. バックアップ Ethernet インターフェース

```
set interface ethernet0/3 zone untrust
set interface ethernet0/3 dhcp client
```

```
set interface ethernet0/3 update-dhcpserver
```

3. **Global ゾーンの VIP**

```
set interface ethernet0/1 ip 192.168.1.1/24
set interface ethernet0/1 dhcp server service
set interface ethernet0/1 dhcp server ip 192.168.1.3 192.168.1.33
```

4. **セルフゾーン**

```
set interface ethernet0/2 ip 192.168.2.1/24
set interface ethernet0/2 dhcp server service
set interface ethernet0/2 dhcp server ip 192.168.2.2 192.168.2.5
save
```

例 6:（小規模なビジネス / 自宅）ADSL バックアップ

この例は、図 16 で示すように、セキュリティデバイスをファイアウォールとして設定する方法を示します。この場合、主要インターネット接続は PPPoE で ADSL インターフェースを使い、バックアップインターネット接続は別の ADSL 接続を使います。

ADSL インターフェースによる主要接続と Ethernet 接続によるバックアップ接続を設定するには、次を行います。

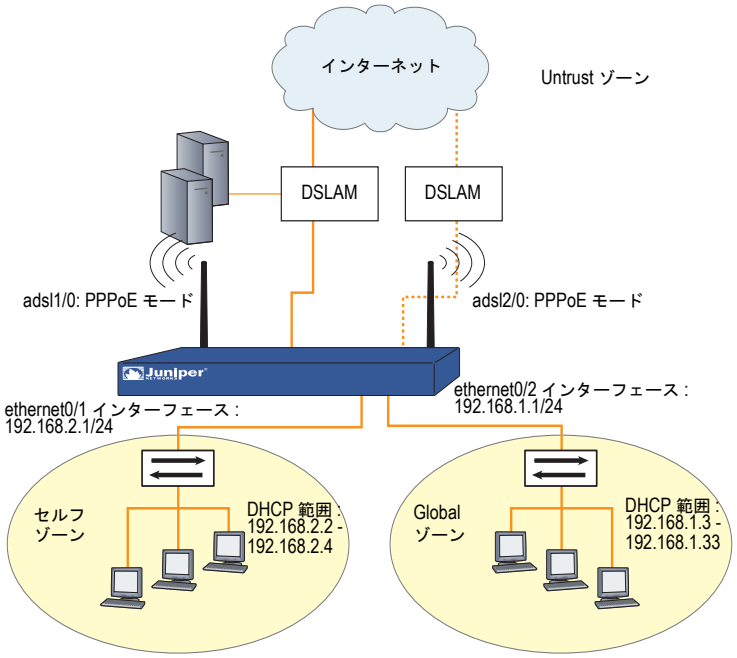
1. ADSL インターフェースを PPPoE で構成します。ADSL インターフェース上に PVC を設定し、ここでは LLC カプセル化を使用するペアの値が 0/35 である VPI/VCI および、「poa1」という名前の PPPoE インスタンスを設定します。poa1 は ADSL インターフェースにバインドされています。

2. バックアップ ADSL インターフェースを adsl2/0 に設定します。

3. Global ゾーンを構成します。

4. Self ゾーンを構成します。

図 16: ADSL アップバックアップ付きの ADSL



WebUI

1. **ADSL インターフェースおよび PPPoE**
   Network > Interfaces > Edit (for adsl1/0): 次のように入力してから **OK** をクリックします。

   VPI/VCI: 0/35
   Encapsulation: LLC (選択)
   Zone: Untrust

   Network > PPP > PPPoE Profile > New: 次のように入力してから **OK** をクリックします。

   PPPoE Instance: poe1
   Bound to Interface: adsl1/0 (選択)
   UserName: alex
   Password: tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
   Automatic Update of DHCP Server's DNS Parameters: (選択)

2. **バックアップ ADSL インターフェース**
   Network > Interfaces > Edit (for adsl2/0): 次のように入力してから **OK** をクリックします。

   VPI/VCI: 8/35
   Encapsulation: LLC (選択)
   Zone: Untrust

Network > PPP > PPPoE Profile > New: 次のように入力してから **OK** をクリックします。

PPPoE Instance: poe2
Bound to Interface: adsl2/0 (選択)
UserName: alex
Password: tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
Automatic Update of DHCP Server's DNS Parameters: (選択)

Network > Interfaces > Backup: 次のように入力してから **OK** をクリックします。

Primary Interface: adsl1/0
Backup Interface: adsl2/0
Type: track ip

Network > Interfaces > Edit > Monitor (adsl1/0 interface): 次のように入力してから **OK** をクリックします。

Enable Track IP: (選択)
Threshold: 1
Weight: 255

3. **Global ゾーンの VIP**

Network > Interfaces > Edit (ethernet0/2): 次のように入力してから **OK** をクリックします。

Zone: Global
Static IP: (選択)
IP Address/Netmask: 192.168.1.1/24
Interface Mode: NAT

Network > DHCP > Edit (for ethernet0/2) > DHCP Server: Apply をクリックします。

> Addresses > New: 次のように入力してから **OK** をクリックします。

Dynamic: (選択)
IP Address Start: 192.168.1.3
IP Address End: 192.168.1.33

4. **セルフゾーン**

Network > Interfaces > Edit (ethernet0/1): 次のように入力してから **OK** をクリックします。

Zone: Self
Static IP: (選択)
IP Address/Netmask: 192.168.2.1/24
Interface Mode: NAT

Network > DHCP > Edit (ethernet0/1) > DHCP Server: **Apply** をクリックします。

> Addresses > New: 次のように入力してから **OK** をクリックします。

Dynamic: (選択)
IP Address Start: 192.168.2.2
IP Address End: 192.168.2.5

CLI

1. **ADSL インターフェースおよび PPPoE**
   set interface adsl1/0 pvc 0 35 mux llc zone untrust
   set pppoe name poe1 username alex password
   tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
   set pppoe name poe1 interface adsl1/0

2. **バックアップ ADSL インターフェース**
   set interface adsl2/0 pvc 8 35 mux llc zone untrust
   set pppoe name poe1 username alex password
   tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
   set pppoe name poe2 interface adsl2/0
   set interface adsl1/0 backup interface adsl2/0 type track-ip
   set interface adsl1/0 monitor track ip
   set interface adsl1/0 monitor track-ip dynamic

3. **Global ゾーンの VIP**
   set interface ethernet0/2 ip 192.168.1.1/24
   set interface ethernet0/2 dhcp server service
   set interface ethernet0/2 dhcp server ip 192.168.1.3 192.168.1.33

4. **セルフゾーン**
   set interface ethernet0/1 ip 192.168.2.1/24
   set interface ethernet0/1 dhcp server service
   set interface ethernet0/1 dhcp server ip 192.168.2.2 192.168.2.5
   save

例 7:（小規模なビジネス）MLPPP ADSL

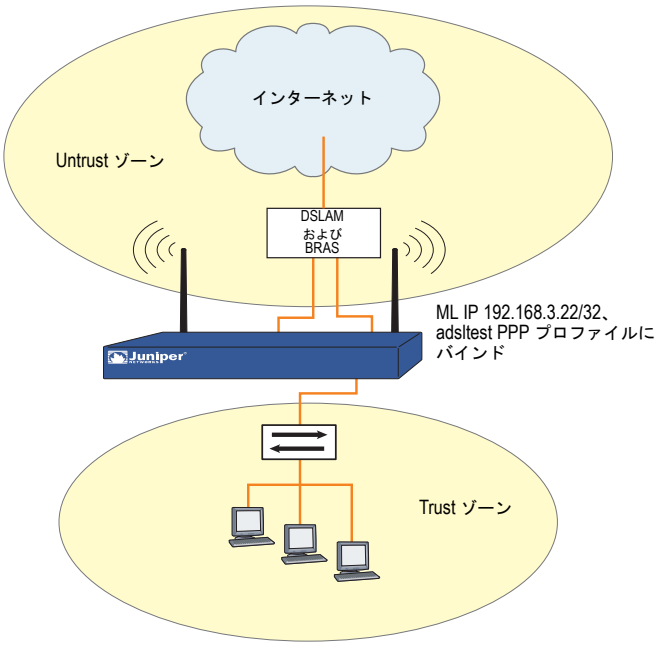
この例は、図 14 に示すように ADSL インターフェース上に PVC を設定し、ここでは MLPPP カプセル化を使用するペアの値が 8/35 である VPI/VCI および、「 adsltest 」という名前の PPP プロファイルが設定され、adsltest は ML インターフェースにバインドされています。

注 : デバイスには MLPP カプセル化をサポートしないものもあります。

ADSL で MLPPP を設定するには、次を行います。

1. マルチリンクインターフェースを構成します。
2. 動的 IP アドレスを使用して、PPP プロファイルを構成します。
3. PPP プロファイルをマルチリンクインターフェースにバインドします。
4. ADSL インターフェースをマルチリンクインターフェースへバンドルします。

図 17: ADSL 上の MLPPP



WebUI

1. **マルチリンクインターフェース**
   Network > Interfaces > New (multilink interface): 次のように入力してから **OK** をクリックします。

   Interface Name: 1
   WAN Encapsulation: Multi-Link PPP (選択)
   Zone Name: Untrust (選択)

2. **動的 IP アドレスを使った PPP プロファイル**
   Network > PPP Profile > Edit: 次のように入力してから **OK** をクリックします。

   PPP Profile: adsltest
   Authentication: CHAP (選択) および PAP (選択)
   Static IP: (選択解除)
   Netmask: 255.255.255.255
   Passive: Don't challenge peer (選択解除)
   Local Name: root
   Password: 123456 (表示しない)

   静的 IP アドレスを使った PPP プロファイル（オプション）
   Static IP: (選択)

3. **PPP プロファイルを ml インターフェースへのバインド**
   Network > Interfaces > Edit (ml1 interface) > Basic properties: 次のように入力してから **OK** をクリックします。

   WAN Encapsulation: Multi-Link PPP (選択)
   Binding a PPP Profile: adsltest (選択)
   Fixed IP: (選択)
   IP Address/Netmask: 192.168.3.22/24

Manage IP: 0.0.0.0
Interface Mode: Route (選択)
Maximum Transfer Unit (MTU): 1500

4. **ADSL インターフェースを ml インターフェースへバンドル**
   Network > Interfaces > Edit (adsl1/0 interface): 次のように入力してから **OK** をクリックします。

   VPI/VCI: 8/35
   QoS Options: UBR (選択)
   Multiplexing Method: LLC (選択)
   RFC1483 Protocol Mode: Bridged (選択)
   Operating Mode: Auto (選択)
   Bind to a multilink interface: ml1 (選択)
   DNS Proxy: (選択)

CLI

1. **マルチリンクインターフェース**
   set interface ml1 zone untrust
   set interface ml1 encap mlppp

2. **動的 IP アドレスを使った PPP プロファイル**
   set ppp profile adsltest
   set ppp profile adsltest auth type any
   set ppp profile adsltest auth local-name root
   set ppp profile adsltest auth secret 123456

   静的 IP アドレスを使った PPP プロファイル（オプション）
   set ppp profile adsltest static-ip
   set interface ml1 ip 192.168.3.22/32

3. **PPP プロファイルを ml インターフェースへのバインド**
   set interface ml1 ppp profile adsltest

4. **ADSL インターフェースを ml インターフェースへバンドル**
   set interface adsl1/0 pvc 8 35 zone untrust
   set interface adsl2/0 pvc 8 35 zone untrust
   set interface adsl1/0 bundle ml1
   set interface adsl2/0 bundle ml1

5. **バンドルからメンバーリンクを削除**
   unset interface adsl1/0 bundle
   unset interface adsl2/0 bundle

例 8:（小規模なビジネス）ローカルサーバーへのアクセスを許可

図 18 で示すように、内部ホストが ADSL インターフェースを利用してインターネットにアクセスし、他の内部ホストを保護しながら、インターネットユーザーのローカル web サーバーへのアクセスを許可するためのセキュリティデバイスの設定方法を示します。

ユーザーの内部ネットワークの他の部分から web サーバーへのトラフィックフローを分離するためには、次を行います。

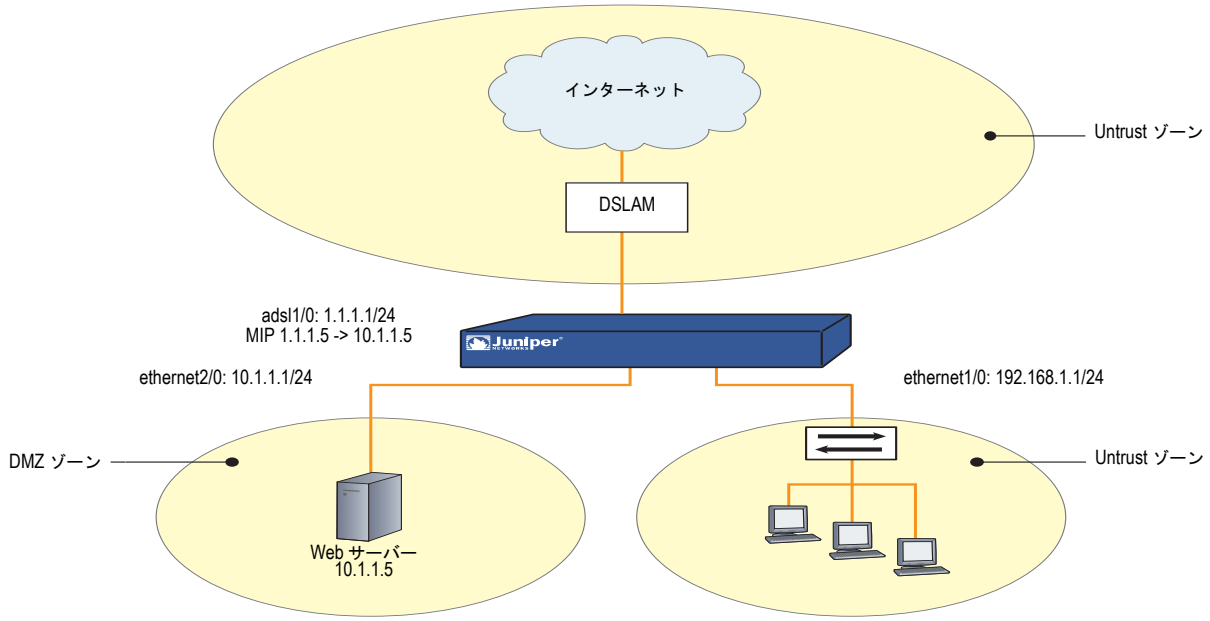
1. trust インターフェースおよび dmz インターフェースを構成します。

2. ADSL インターフェースおよびマップ IP（MIP）を構成します。ADSL インターフェースに PVC を設定します。このときの設定は VPI/VCI ペア 0/35 および静的 IP アドレス 1.1.1.1/24 で、サービスプロバイダにより割り当てられます。Trust インターフェースを Trust ゾーンにバインドし、IP アドレス 192.168.1.1/24. を割り当てます。ホスト 1.1.1.5 向けの HTTP トラフィックを、DMZ ゾーンの 10.1.1.5 が割り当てられた Web サーバーに向ける MIP を設定します。

3. web サーバーが置かれているゾーンに対して HTTP トラフィックのみを許可するポリシーを作成します。

   （デフォルトのポリシーは、Trust ゾーンから Untrust ゾーンへのすべてのトラフィックを許可し、Untrust ゾーンから Trust ゾーンへのすべてのトラフィックをブロックします。）

図 18: ローカルサーバーへのアクセスを許可する ADSL インターフェース



WebUI

1. **イーサネットインターフェース**

   Network > Interfaces > Edit (ethernet1/0): 次のように入力してから **OK** をクリックします。

   Static IP: (選択)
   IP Address/Netmask: 192.168.1.1/24
   Interface Mode: NAT

   Network > DHCP > Edit (ethernet1/0) > DHCP Server: Apply をクリックします。

   > Addresses > New: 次のように入力してから **OK** をクリックします。

   Dynamic: (選択)
   IP Address Start: 192.168.1.3
   IP Address End: 192.168.1.33

Network > Interfaces > Edit (ethernet2/0): 次のように入力してから **OK** をクリックします。

Static IP: (選択)
IP Address/Netmask: 10.1.1.1/24
Interface Mode: NAT

2. ADSL インターフェースおよび MIP

Network > Interfaces > Edit (for adsl1/0): 以下を入力して **Apply** をクリックします。

VPI/VCI: 0/35
Zone Name: Untrust
Static IP: (選択)
IP Address/Netmask: 1.1.1.1/24

> MIP > New: 次のように入力してから **OK** をクリックします。

Mapped IP: 1.1.1.5
Netmask: 255.255.255.255
Host IP Address: 10.1.1.5
Host Virtual Router Name: trust-vr

3. ポリシー

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択) Any
Destination Address:
Address Book Entry: (選択), MIP (1.1.1.5)
Service: HTTP
Action: Permit

CLI

1. Trust および DMZ インターフェース

```
set interface ethernet1/0 ip 192.168.1.1/24
set interface ethernet1/0 nat
set interface ethernet1/0 dhcp server service
set interface ethernet1/0 dhcp server ip 192.168.1.3 192.168.1.33
set interface ethernet2/0 ip 10.1.1.1/24
set interface ethernet2/0 nat
```

2. ADSL インターフェースおよび MIP

```
set interface adsl1 pvc 0 35 zone untrust
set interface adsl1/0 ip 1.1.1.1/24
set interface adsl1/0 mip 1.1.1.5 host 10.1.1.5 netmask 255.255.255.255
    vrouter trust-vr
```

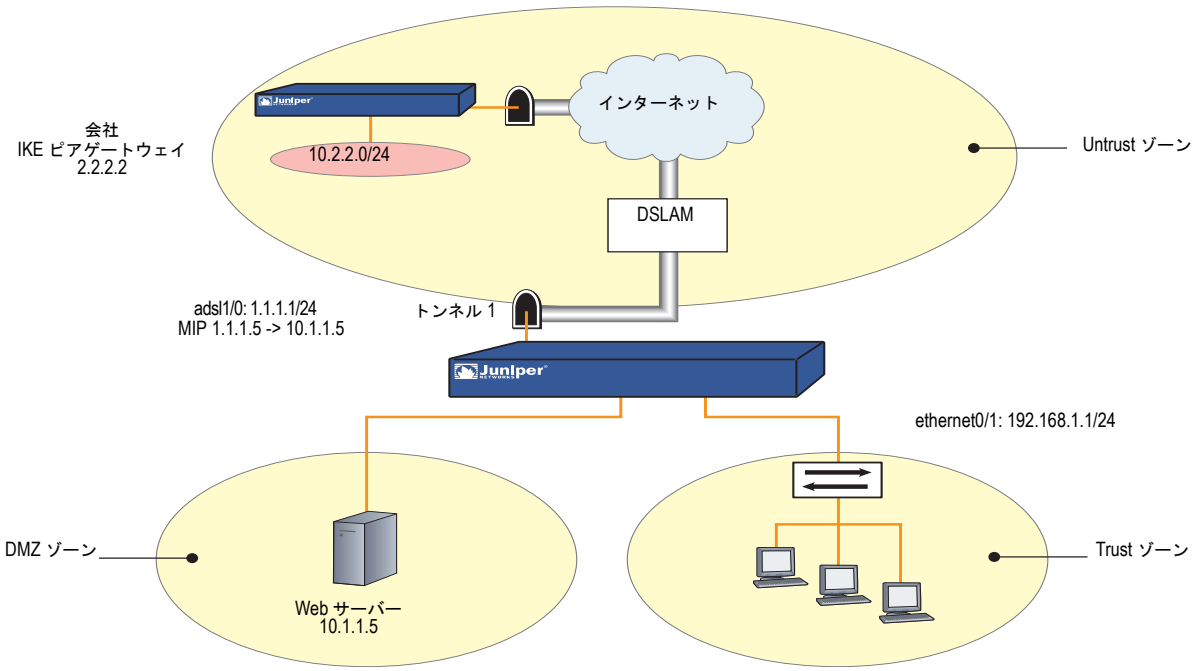
3. ポリシー

```
set policy from untrust to dmz any MIP (1.1.1.5) http permit
save
```

例 9:（支店）ADSL を通した VPN トンネル

この例は、図 19 で示すように、セキュリティデバイス上の ADSL インターフェースを通って本社への VPN トンネルを設定する方法、およびインターネットから直接アクセスできないように他の内部ホストを保護しながら、ローカルの web サーバーへのインターネットアクセスを許可する方法を説明します。94 ページの「例 7:（小規模なビジネス）MLPPP ADSL」を参照してください。

図 19: ADSL インターフェースを通しての VPN トンネル



この例では、ルートベースの AutoKey IKE トンネルを事前共有の秘密を使用して設定する方法も説明します。フェーズ 1 およびフェーズ 2 セキュリティレベルに対しては、フェーズ 1 プロポーザルには pre-g2-3des-sha 、フェーズ 2 には事前に定義されている「互換性のある」一連のプロポーザルを設定します。ADSL インターフェースを通って VPN トンネルを設定するには、次を行います。

1. trust インターフェースおよび dmz インターフェースを構成します。

2. ADSL インターフェースおよびマップ IP（MIP）を構成します。ADSL インターフェースに PVC を設定します。このときの設定は VPI/VCI ペア 0/35 および静的 IP アドレス 1.1.1.1/24 で、サービスプロバイダにより割り当てられます。Trust インターフェースを Trust ゾーンにバインドし、IP アドレス 192.168.1.1/24. を割り当てます。ホスト 1.1.1.5 向けの HTTP トラフィックを、DMZ ゾーンの 10.1.1.5 が割り当てられた Web サーバーに向ける MIP を設定します。

3. トンネルインターフェースを作成し、Untrust セキュリティゾーンにバインドします。トンネルを作成するには、次を行います。

a. トンネルインターフェースを設定して、adsl1 インターフェースから IP アドレスを借ります。このアドレスは Untrust セキュリティゾーンにもバインドされています（「番号なし」インターフェースとしても知られています）。

b. VPN トンネルを構成し、Untrust ゾーンにおいて出力インターフェースを adsl1 インターフェースに指定し、トンネルインターフェースにバインドしてから、プロキシ ID を構成します。

c. トンネルインターフェースを通して、企業 LAN にルートを入力します。

d. VPN トラフィックにポリシーを設定し、支社と本社間に VPN トラフィックが通るようにします。

4. web サーバーが置かれているゾーンに対して HTTP トラフィックのみを許可するポリシーを作成します。

（デフォルトのポリシーは、Trust ゾーンから Untrust ゾーンへのすべてのトラフィックを許可し、Untrust ゾーンから Trust ゾーンへのすべてのトラフィックをブロックします。）

WebUI

1. Trust および DMZ インターフェース

Network > Interfaces > Edit (ethernet0/1): 次のように入力してから **OK** をクリックします。

Static IP: (選択)
IP Address/Netmask: 192.168.1.1/24
Interface Mode: NAT

Network > DHCP > Edit (ethernet0/1) > DHCP Server: Apply をクリックします。

> Addresses > New: 次のように入力してから **OK** をクリックします。

Dynamic: (選択)
IP Address Start: 192.168.1.3
IP Address End: 192.168.1.33

Network > Interfaces > Edit (ethernet0/2): 次のように入力してから **OK** をクリックします。

Static IP: (選択)
IP Address/Netmask: 10.1.1.1/24
Interface Mode: NAT

2. ADSL インターフェースおよび MIP

Network > Interfaces > Edit (for adsl1/0): 以下を入力して **Apply** をクリックします。

VPI/VCI: 0/35
Zone Name: Untrust
Static IP: (選択)
IP Address/Netmask: 1.1.1.1/24

> MIP > New: 次のように入力してから **OK** をクリックします。

Mapped IP: 1.1.1.5
Netmask: 255.255.255.255
Host IP Address: 10.1.1.5
Host Virtual Router Name: trust-vr

3. VPN トンネル

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (**選択**)
Interface: adsl1 (trust-vr)

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: To_Corp
Security Level: Custom
Remote Gateway Type:
Static IP Address: (**選択**), IP Address/HostName: 2.2.2.2
Preshared Key: h1p8A24nG5

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Main (ID Protection)

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: Branch1_Corp
Security Level: Compatible
Remote Gateway:
Predefined: (**選択**), To_Corp

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Security Level: Compatible
Bind to: Tunnel Interface, tunnel.1
Proxy-ID: (**選択**)
Local IP/Netmask: 192.168.1.1/24
Remote IP/Netmask: 10.2.2.0/24
Service: ANY

Network > Routing > Destination > trust vr > New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.2.2.0/24
Gateway: (**選択**)
Interface: Tunnel.1

4. ポリシー

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**) Any
Destination Address:
Address Book Entry: (**選択**), MIP (1.1.1.5)
Service: HTTP
Action: Permit

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Name: To_Corp
Source Address: 192.168.1.1/24
Destination Address: 10.2.2.0/24
Service: ANY
Action: Permit
Position at Top: (選択)

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Name: From_Corp
Source Address: 10.2.2.0/24
Destination Address: 192.168.1.1/24
Service: ALL
Action: Permit
Position at Top: (選択)

CLI

1. **Trust および DMZ インターフェース**
```
set interface ethernet0/1 ip 192.168.1.1/24
set interface ethernet0/1 nat
set interface ethernet0/1 dhcp server service
set interface ethernet0/1 dhcp server ip 192.168.1.3 192.168.1.33
set interface ethernet0/2 ip 10.1.1.1/24
set interface ethernet0/2 nat
```

2. **ADSL インターフェースおよび MIP**
```
set interface adsl1/0 pvc 0 35 zone untrust
set interface adsl1/0 ip 1.1.1.1/24
set interface adsl1/0 mip 1.1.1.5 host 10.1.1.5 netmask 255.255.255.255
    vrouter trust-vr
```

3. **VPN トンネル**
```
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface adsl1
set ike gateway To_Corp address 2.2.2.2 main outgoing-interface adsl1/0
    preshare hlp8A24nG5 proposal pre-g2-3des-sha
set vpn Branch1_Corp gateway To_Corp sec-level compatible
set vpn Branch1_Corp bind interface tunnel.1
set vpn Branch1_Corp proxy-id local-ip 192.168.1.1/24 remote-ip 10.2.2.0/24
    any
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
```

4. **ポリシー**
```
set policy from untrust to dmz any mip(1.1.1.5) http permit
set policy top name "To Corp" from trust to untrust 192.168.1.1/24 10.2.2.0/24
    any permit
set policy top name "From Corp" from untrust to trust 10.2.2.0/24
    192.168.1.1/24 any permit
save
```

例 10:（支社）2 次 VPN トンネル

この例は、図 20 で示すように、セキュリティデバイスを ADSL インターフェースを使った、本社とインターネットに接続があるファイアウォールとして設定します。この例は 99 ページの「例 9:（支店）ADSL を通した VPN トンネル」に示されている設定と似ていますが、2 つの PVC を作成するという点で異なります。一つはインターネット用に、そして他方は本社用です。また 2 次接続として、本社へインターネットを通して VPN トンネルを設定します。

ADSL を通る 1 次および 2 次 VPN トンネルを設定するには、次を行います。

1. trust インターフェースおよび dmz インターフェースを構成します。

2. ADSL インターフェースおよびマップ IP（MIP）を構成します。ADSL インターフェースに PVC を設定します。このときの設定は VPI/VCI ペア 0/35 および静的 IP アドレス 1.1.1.1/24 で、サービスプロバイダにより割り当てられます。Trust インターフェースを Trust ゾーンにバインドし、IP アドレス 192.168.1.1/24. を割り当てます。ホスト 1.1.1.5 向けの HTTP トラフィックを、DMZ ゾーンの 10.1.1.5 が割り当てられた Web サーバーに向ける MIP を設定します。

3. 本社（HQ）カスタムゾーンを設定します。

4. ADSL サブインターフェースを設定します。ADSL サブインターフェース adsl1.1 の作成により、セキュリティデバイス上で追加の PVC を設定します。adsl1.1 サブインターフェースを設定し、ここでは LLC カプセル化を使用するペアの値が 1/35 である VPI/VCI および、「poe1」という名前の PPPoE インスタンスが設定され、これらはサブインターフェースにバインドされています。次にポリシーを定義して、トラフィックが HQ ゾーンに行き来するようにします。

注 : ADSL サブインターフェースをカスタムゾーン「HQ」にバインドします（主 ADSL インターフェースは、デフォルトでは Untrust ゾーンにバインドされます）。

---

5. トンネルインターフェースを作成し、Untrust セキュリティゾーンにバインドします。トンネルを作成するには、次を行います。

   a. トンネルインターフェースを設定して、adsl1 インターフェースから IP アドレスを借ります。このアドレスは Untrust セキュリティゾーンにもバインドされています（「番号なし」インターフェースとしても知られています）。

   b. IKE ゲートウェイを設定します。

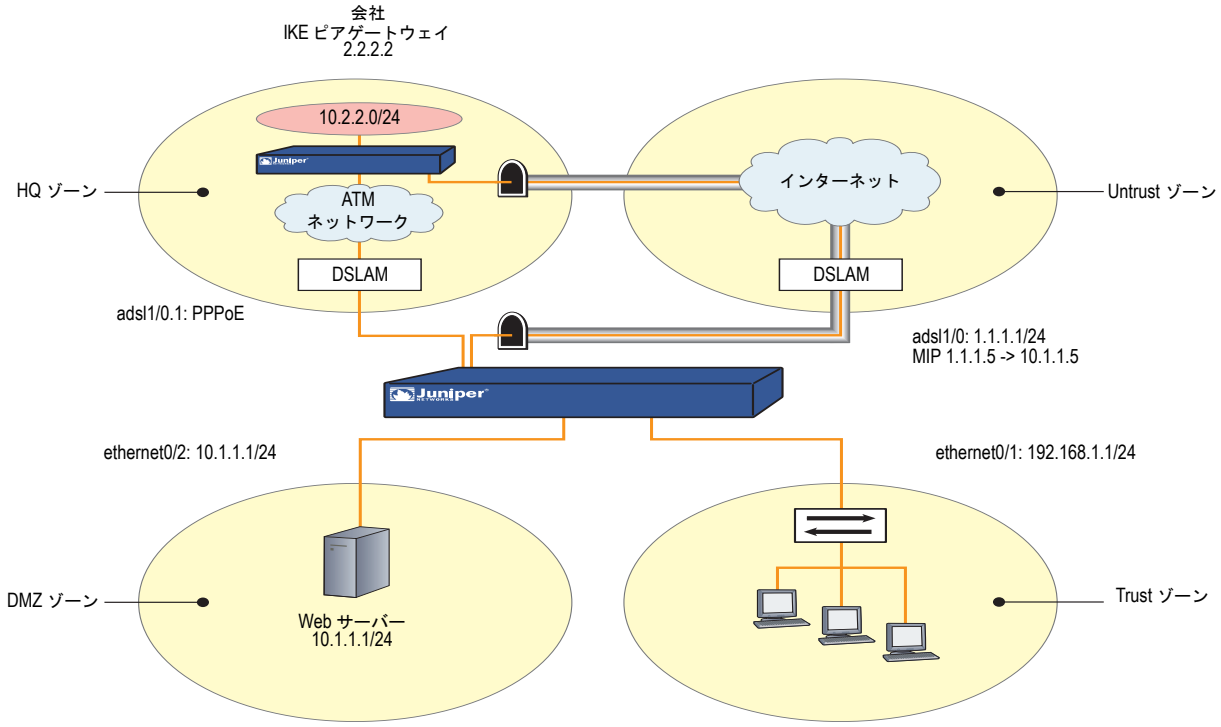
   c. VPN トンネルを構成し、Untrust ゾーンにおいて出力インターフェースを adsl1 インターフェースに指定し、トンネルインターフェースにバインドしてから、プロキシ ID を構成します。

6. 仮想ルート (trust-vr) を作成します。

7. VPN トラフィックにポリシーを設定し、支社と本社間に VPN トラフィックが通るようにします。

（デフォルトのポリシーは、Trust ゾーンから Untrust ゾーンへのすべてのトラフィックを許可し、Untrust ゾーンから Trust ゾーンへのすべてのトラフィックをブロックします。）

図 20: 2 次トンネル付きの ADSL インターフェース



Trust ゾーンのワークステーションと本社との間で 2 つの異なるルートがあるので（一つは adsl1.1 インターフェースを使用、そして他方は VPN トンネルインターフェースを使用）、どのルートを「優先」したいか指定する必要があります。VPN トンネルを通るルートのメトリックを adsl1.1 インターフェースを通るルートのものより高くします。

WebUI

1. **Trust および DMZ インターフェース**
   Network > Interfaces > Edit (ethernet0/1): 次のように入力してから **OK** をクリックします。

   Static IP: (選択)
   IP Address/Netmask: 192.168.1.1/24
   Interface Mode: NAT

   Network > DHCP > Edit (ethernet0/1) > DHCP Server: Apply をクリックします。

   > Addresses > New: 次のように入力してから **OK** をクリックします。

   Dynamic: (選択)
   IP Address Start: 192.168.1.3
   IP Address End: 192.168.1.33

Network > Interfaces > Edit (ethernet0/2): 次のように入力してから **OK** をクリックします。

Static IP: (選択)
IP Address/Netmask: 10.1.1.1/24
Interface Mode: NAT

2. ADSL インターフェースおよび MIP

Network > Interfaces > Edit (for adsl1/0): 以下を入力して **Apply** をクリックします。

VPI/VCI: 0/35
Zone Name: Untrust
Static IP: (選択)
IP Address/Netmask: 1.1.1.1/24

> MIP > New: 次のように入力してから **OK** をクリックします。

マップ IP: 1.1.1.5
Netmask: 255.255.255.255
Host IP Address: 10.1.1.5
Host Virtual Router Name: trust-vr

3. HQ ゾーン

Network > Zones > New: 次のように入力してから **OK** をクリックします。

Zone Name: HQ
Block Intra-Zone Traffic: (選択)

4. ADSL サブインターフェース

Network > Interfaces > New ADSL Sub-IF: 次のように入力してから **OK** をクリックします。

Interface Name: adsl1/0.1
VPI/VCI: 1/35
Encapsulation: LLC (選択)
Zone: HQ (選択)

Network > PPPoE > New: 次のように入力してから **OK** をクリックします。

PPPoE Instance: poe1
Bound to Interface: adsl1/0.1 (選択)
UserName: felix
Password: ioP936QNlwab48Rc

5. VPN トンネル

Network > Interfaces > New Tunnel IF: 次のように入力してから **OK** をクリックします。

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (選択)
Interface: adsl1 (trust-vr)

VPNs > AutoKey Advanced > Gateway > New: 次のように入力してから **OK** をクリックします。

Gateway Name: To_Corp
Security Level: Custom
Remote Gateway Type:
Static IP Address: (**選択**), IP Address/HostName: 2.2.2.2
Preshared Key: h1p8A24nG5

> Advanced: 次の高度な設定を入力してから **Return** をクリックして基本 Gateway 構成ページに戻ります。

Security Level: Custom
Phase 1 Proposal (Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Main (ID Protection)

VPNs > AutoKey IKE > New: 次のように入力してから **OK** をクリックします。

VPN Name: Branch1_Corp
Security Level: Compatible
Remote Gateway:
Predefined: (**選択**), To_Corp

> Advanced: 次の詳細設定を入力してから **Return** をクリックし、基本 AutoKey IKE 構成ページに戻ります。

Security Level: Compatible
Bind to: Tunnel Interface, tunnel.1
Proxy-ID: (**選択**)
Local IP/Netmask: 192.168.1.1/24
Remote IP/Netmask: 10.2.2.0/24
Service: ANY

6. ルート

Network > Routing > Destination > trust vr > New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.2.2.0/24
Gateway: (**選択**)
Interface: adsl1.1
Metric: 1

Network > Routing > Destination > trust vr > New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 10.2.2.0/24
Gateway: (**選択**)
Interface: Tunnel.1
Metric: 5

7. ポリシー

Policies (From: Trust, To: HQ) > New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (**選択**) Any
Destination Address:

Address Book Entry: (選択) Any
Service: ANY
Action: Permit

Policies (From: HQ, To: Trust) > New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択) Any
Destination Address:
Address Book Entry: (選択) Any
Service: ANY
Action: Permit

Policies (From:DMZ, To:HQ) > New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択) Any
Destination Address:
Address Book Entry: (選択) Any
Service: ANY
Action: Permit

Policies (From: HQ, To: DMZ) > New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択) Any
Destination Address:
Address Book Entry: (選択) Any
Service: ANY
Action: Permit

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択) Any
Destination Address:
Address Book Entry: (選択), MIP (1.1.1.5)
Service: HTTP
Action: Permit

Policies > (From: Trust, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Name: To_Corp
Source Address: 192.168.1.1/24
Destination Address: 10.2.2.0/24
Service: ANY
Action: Permit
Position at Top: (選択)

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Name: From_Corp
Source Address: 10.2.2.0/24
Destination Address: 192.168.1.1/24

Service: ALL
Action: Permit
Position at Top: (選択)

CLI

1. **Trust および DMZ インターフェース**
   set interface ethernet0/1 ip 192.168.1.1/24
   set interface ethernet0/1 nat
   set interface ethernet0/1 dhcp server service
   set interface ethernet0/1 dhcp server ip 192.168.1.3 192.168.1.33
   set interface ethernet0/2 ip 10.1.1.1/24
   set interface ethernet0/2 nat

2. **ADSL インターフェースおよび MIP**
   set interface adsl1/0 pvc 0 35 zone untrust
   set interface adsl1/0 ip 1.1.1.1/24
   set interface adsl1/0 mip 1.1.1.5 host 10.1.1.5 netmask 255.255.255.255 vrouter trust-vr

3. **HQ ゾーン**
   set zone name HQ
   set zone HQ block
   set zone HQ vrouter trust-vr

4. **ADSL サブインターフェース**
   set interface adsl1/0.1 pvc 1 35 mux llc zone HQ
   set pppoe name poe1 username felix password ioP936QNlwab48Rc
   set pppoe name poe1 interface adsl1/0.1

5. **VPN トンネル**
   set interface tunnel.1 zone untrust
   set interface tunnel.1 ip unnumbered interface adsl1/0
   set ike gateway To_Corp address 2.2.2.2 main outgoing-interface adsl1/0 preshare hIp8A24nG5 proposal pre-g2-3des-sha
   set vpn Branch1_Corp gateway To_Corp sec-level compatible
   set vpn Branch1_Corp bind interface tunnel.1
   set vpn Branch1_Corp proxy-id local-ip 192.168.1.1/24 remote-ip 10.2.2.0/24 any

6. **ルート**
   set vrouter trust-vr route 10.2.2.0/24 interface adsl1/0.1 metric 1
   set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1 metric 5

7. **ポリシー**
   set policy from trust to HQ any any any permit
   set policy from HQ to trust any any any permit
   set policy from dmz to HQ any any any permit
   set policy from HQ to dmz any any any permit
   set policy from untrust to dmz any mip(1.1.1.5) http permit
   set policy top name “To Corp” from trust to untrust 192.168.1.1/24 10.2.2.0/24 any permit
   set policy top name "From Corp" from untrust to trust 10.2.2.0/24 192.168.1.1/24 any permit
   save

第 3 章

ISP フェールオーバーとダイヤル回復

ISP フェールオーバーおよびダイヤル回復をサポートするデバイスには、Aux シリアルポート（外部 V.92 モデム用）または ISDN BRI ポート、あるいは組み込み V.92 アナログモデムポートのいずれかがあります。モデルによっては、これらの機能が mini-PIM オプションとして利用可能です。1 次リンク（イーサネットポート）に障害が発生すると、これらのポートは一般にバックアップポートとして使用されます。1 次リンクは通常、セキュリティデバイスへのイーサネット接続を持つ、ISP への ADSL モデムです。VPN 監視または物理ポートの障害は、バックアップインターフェースへのフェールオーバーが発生する典型的な原因です。

本章のセクションは、以下のようになります。

- 109 ページの「フェールオーバーの ISP 優先順位の設定」
- 110 ページの「ISP フェールオーバーの条件の定義」
- 111 ページの「ダイヤルアップ回復ソリューションの構成」

フェールオーバーの ISP 優先順位の設定

ルート管理者（委託管理者としてではなく）として、合計 4 つの ISP を設定できます。各 ISP の優先順位は、固有の番号でなければなりません。またテスト（監視）目的で、1 つまたは複数の ISP エントリを優先順位ゼロで設定することもできます。ただし、ゼロが割り当てられた ISP エントリは、フェールオーバーには使われません。

モデム接続をお使いのときは、委託管理者が手動で ISP 優先順位を変えることができます。フェールオーバーが起きたとき、ISP に割り当てられた優先順位が、他の ISP に対して特定の ISP に連絡が来る順位を示します。値が低ければ低いほど、ISP の優先順位が高くなります委託管理者はまた、優先順位設定がゼロの ISP が利用できるかどうかチェックします。

WebUI

Home > Interface link status: **Edit** をクリックします。次にシリアルインターフェースの **ISP** をクリックします。

CLI

```
set interface serial0/0 modem isp pac-bell-1 priority 1
set interface serial0/0 modem isp pac-bell-1 primary-number 555-55-55
    alternative-number 666-66-66
```

```
set interface serial0/0 modem isp pac-bell-1 account login rbrockie password
    !2007ah
set interface serial0/0 modem isp pac-bell-2 priority 2
set interface serial0/0 modem isp pac-bell-2 primary-number 777-77-77
    alternative-number 888-88-88
set interface serial0/0 modem isp pac-bell-2 account login rbrockie password
    !2007ah
save
```

ISP フェールオーバーの条件の定義

ISP 情報および優先順位を設定したら、監視しているルートが untrust-vr ルーティング表から消えたときに、次に高い優先順位の ISP （次に低い優先順位の番号）のフェールオーバーをトリガーする untrust-vr のルートを選択的に監視できます。ISP 2 へのフェールオーバーが起きても、必ずしも ISP 1 がダウン状態または故障したとは限りません。ISP 1 より先にある、アクセスしたい特定のルートが利用できないことを意味しており、あきらめてバックアップ ISP を呼び出す前に、指定された秒数の間、デバイスに待ってもらう必要があります。

この機能を利用するには、特定ルートに対して現在 untrust-vr に表示されている IP アドレスを指定します。オプションとして、デバイスがバックアップ ISP を呼び出すまでに待つ秒数を指定することもできます。デフォルトのホールドダウンタイムは 30 秒です。

先の例では、ルート管理者として優先順位 1 の ISP およびバックアップ ISP を設定しました。この例ではセキュリティデバイスがルート 1.1.1.1/24 を監視するように設定します。このルートは興味ある、または重要なルートであるとします。このルートは現在 untrust-vr にあります。ホールドダウンタイマーを 100 秒に設定します。CLI を使用して、Untrust-vr で監視したいルートを設定します。指定したルートが利用できなくなると、次の ISP （優先順位 2 ）へのフェールオーバーが起きます。

WebUI

Home > Interface link status: **Edit** をクリックします。次にシリアルインターフェースの **ISP Failover** をクリックします。

CLI

```
set interface serial0/0 modem isp-failover holddown 100
set interface serial0/0 modem isp-failover type route vrouter untrust-vr 1.1.1.1/24
save
```

ダイヤルアップ回復ソリューションの構成

次の項目を設定して、ネットワークのダイヤルアップ障害回復ソリューションを設定します。

- セキュリティデバイス
- モデムまたは ISDN ターミナルアダプター (TA)
- インターフェースフェールオーバートリガーメカニズム
- 遠くにあるデバイス（他のルーターまたはファイアウォールデバイス）が送信デバイスへのリターンパスを識別する方法

インターフェースフェールオーバーをトリガーするには、3 つのうちから 1 つフェールオーバーメカニズムを選びます。

- **Track IP** は特定の IPv4 アドレスがフェールオーバーを決定するために利用できるかどうかを監視します。IP トラッキングを使用するには、**set interface *interface* backup interface serial0/0 type track-ip** コマンドを入力します（ここで、***interface*** は、メインのインターフェース）。
- **Tunnel tracking** はフェールオーバーを決定するために、VPN トンネルステータスを監視します。トンネルステータスによりトラッキングするには、**set interface *interface* backup interface serial0/0 type tunnel-if** コマンドを入力します（ここで、***interface*** は、メインのインターフェース）。
- **Route tracking** は知られているルートのステータスを監視します。ルートエントリは BGP または OSPF などの動的ルーティングプロトコルで設定同期することができます。BGP の隣接性が失われた場合、セキュリティデバイスはその BGP ピアから学習したすべてのルートを削除します。ルートエントリがホールドダウンタイムより長い時間アクティブでなかった場合、セキュリティデバイスはバックアップインターフェースへのインターフェースフェールオーバーをトリガーします。この機能では、フェールオーバーを回避するため、指定された vrouter のルーティングテーブルのアクティブなルートにアドレスが正確に一致する必要があります。ルートによるフェールオーバーを可能にするには、**set interface *interface* backup interface serial0/0 type route vroute untrust 1.1.1.1/24** コマンドを入力します（ここで *interface* はメインのインターフェース、1.1.1.1 は監視ルートの IP アドレス）。

図 21 では、カルフォルニア州サンノゼのビジネス街にあるコンピュータが、サンノゼの他の場所にあるリモートオフィスのサーバーにネットワークされています。セキュリティデバイスはいつも ethernet3 (e3) にバインドされている VPN トンネルである tunnel.1 を使って、コンピュータ (PC) からインターネットを使って、リモートサーバーにアクセスするためにファイアウォールにトラフィックを送信します。トラフィックは静的ルートと VPN 監視を使います（デフォルト設定）。Tunnel.1 のメトリックは 1 で、これにより必ずファイアウォールへの優先ルートとなります。tunnel.2 のメトリックはより高い 180 なので、優先ルートとはなりません。

tunnel.1 がダウンすると、セキュリティデバイスはシリアルインターフェースにバインドされている tunnel.2 がファイアウォールに連絡するようにします。この例では IP トラッキングよりトンネルトラッキングが優先され、インターフェースフェールオーバーを可能にしています。IP トラッキングでは、リンクがダウンするとフェールオーバーが起こりますが、VPN トンネルがダウンして

いるかどうかわからないので、フェールオーバーが起きたかわかりません。トンネルトラッキング機能は主要 Untrust インターフェースにバインドされているトンネルインターフェースがダウンしたときのみフェールオーバーが起きます。主要 Untrust インターフェースはケーブルが外されたり、VPN モニターがトリガーされているときも障害が起きることがあり、これはトンネルに障害が起きていることを意味します。

セキュリティデバイス tunnel.2 （シリアル）インターフェースは ISP に割り当てられた IP アドレスを使用して、ファイアウォールに ISDN を介して接続します。

フェールオーバーは「自動」に設定してあり、インターフェースが再び利用できるようになると、tunnel.1 へのフェールバックが起きます。

set vpn *name* **monitor rekey** コマンドを入力すると、VPN 監視はアクティブになります。必要に応じて **set vpnmonitor { interval | threshold }** コマンドを入力して、デフォルトの間隔およびしきい値設定を変更することができます。**get vpnmonitor** コマンドを入力すると VPN 監視設定を表示することができます。

図 21: ダイヤル回復設定

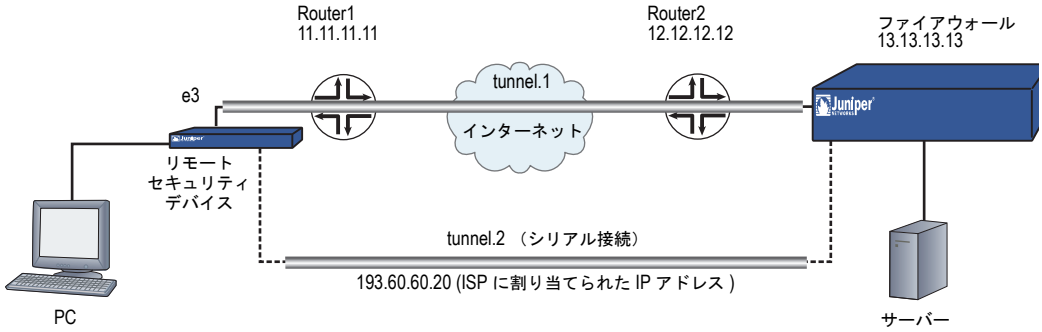


図 21 にあるように、以下にリモートのセキュリティデバイスの設定を示します。

WebUI

シリアルおよびトンネルインターフェースの設定

Network > Interfaces: シリアルインターフェースの **Edit** を選択し、インターフェースを Untrust ゾーンにバインドします。**Apply** をクリックします。

Network > Interfaces: トンネルインターフェース (tunnel.1) の **New** を選択し、インターフェースを Untrust ゾーンにバインドします。必要に応じて設定をし、**Apply** をクリックします。

Network > Interfaces: トンネルインターフェース (tunnel.2) の **New** を選択し、インターフェースを Untrust ゾーンにバインドします。必要に応じて設定をし、**Apply** をクリックします。

静的ルートとメトリックの設定

Network > Routing > Destination: untrust-vr の **New** ルートを選択し、IP アドレス、ゲートウェイ情報、メトリックを設定し、**OK** をクリックします。

Network > Routing > Destinations: untrust-vr, の **New** ルートを選択し、ISP がシリアル接続用に割り当てた IP アドレスに設定し、ゲートウェイ情報（該当する場合）、メトリック（先のエントリより大きい番号）を設定し、**OK** をクリックします。

IKE ゲートウェイの設定

VPNs > AutoKey IKE > Edit: IKE 要求事項を入力してから **OK** をクリックします。

VPN を IKE ゲートウェイにバインド

VPNs > AutoKey IKE > Edit: **Advanced** を選択し、VPN を tunnel.1 の IKE ゲートウェイにバインドします。**OK** をクリックする。

VPNs > AutoKey IKE > Edit: **Advanced** を選択し、VPN を tunnel.2 の IKE ゲートウェイにバインドします。**OK** をクリックする。

インターフェースフェールオーバーの構成

CLI から構成します。

インバンドモデムポート設定の構成

Network > Interface (Modem)

Set the primary ISP account

Network > Interface (ISP)

CLI

シリアルおよびトンネルインターフェースの設定

```
set interface serial0/0 zone untrust
set interface ethernet0/3 zone untrust
set interface ethernet0/3 ip 111.11.11.10/24
set interface tunnel.1 ip unnumbered interface ethernet0/3
set interface serial0/0 ip 193.60.60.19/24
set interface tunnel.2 ip unnumbered interface serial0/0
```

静的ルートとメトリックの設定

```
set route 0.0.0.0/0 interface ethernet0/3 metric 1
set route 0.0.0.0/0 interface serial0/0 metric 180
```

IKE ゲートウェイの設定

```
set ike gateway eth address 13.13.13.13 Main outgoing-interface ethernet0/3
    preshare 123qwe! sec-level standard

set ike gateway serial address 13.13.13.13 Main outgoing-interface serial0/0
    preshare 123qwe! sec-level standard
```

VPN を IKE ゲートウェイにバインド

```
set vpn eth gateway eth no-replay tunnel idletime 0 sec-level standard
set vpn eth monitor rekey
set vpn eth id 1 bind interface tunnel.1

set vpn serial gateway serial no-replay tunnel idletime 0 sec-level standard
set vpn serial monitor rekey
set vpn serial id 2 bind interface tunnel.2
```

インターフェースフェールオーバーの構成

```
set interface ethernet0/3 backup interface serial0/0 type tunnel-if
set interface ethernet0/3 backup deactivation-delay 5
set interface ethernet0/3 backup activation-delay 5
set interface ethernet0/3 backup auto
set vpn eth backup-weight 100
```

インバンドモデムポート設定の構成

```
set interface serial0/0 modem settings port-1 init-strings AT&F
set interface serial0/0 modem settings port-1 active
```

主要 ISP アカウントの設定

```
set interface serial0/0 modem isp isp-1 priority 1
set interface serial0/0 modem isp isp-1 primary-number 555-55-55
    alternative-number 666-66-66
set interface serial0/0 modem isp isp-1 account login rbrockie pass !2007ah
```

第 4 章

ワイヤレス ローカル エリア ネットワーク

Juniper Networks ワイヤレスデバイスおよびシステムは、統合インターネットプロトコルセキュリティ仮想プライベートネットワーク（IPSec VPN）でワイヤレスローカルエリアネットワーク（WLAN）接続を提供し、在宅勤務者、支社または小売店などのワイヤレスクライアントにファイアウォールサービスを提供します。

本章では、無線インターフェースを設定する方法について説明し、構成例を提供します。

本章のセクションは、以下のようになります。

- 116 ページの「概要」
- 118 ページの「基本的なワイヤレスネットワーク機能の構成」
- 122 ページの「SSID への認証と暗号化の設定」
- 131 ページの「アンテナ使用の指定」
- 131 ページの「国コード、チャネルおよび周波数の設定」
- 132 ページの「拡張チャネルの使用」
- 132 ページの「サイト調査の実行」
- 133 ページの「利用可能なチャネルの発見」
- 133 ページの「アクセス制御リストエントリの設定」
- 134 ページの「Super G の構成」
- 135 ページの「Atheros XR（拡張範囲）の構成」
- 136 ページの「Wi-Fi マルチメディアサービス品質の構成」
- 140 ページの「詳細なワイヤレスパラメーターの設定」
- 146 ページの「ワイヤレスインターフェースでの作業」
- 148 ページの「ワイヤレス構成情報の表示」
- 149 ページの「設定例」

概要

無線セキュリティデバイスとシステムは、有線または無線のネットワークに無線ユーザーあるいは他のワイヤレスデバイスを接続します。ワイヤレスデバイスがローカルエリアネットワークにアクセスすることを可能にするデバイスは、ワイヤレスアクセスポイント（AP）です。本章に記載された機能は、内蔵の無線通信インターフェースを備えたセキュリティデバイスあるいはシステムを必要とします。

注： 無線プラットフォームはすべて、4 つまでのアクティブな無線通信インターフェースを同時にサポートできます。

ScreenOS は無線セキュリティデバイス上で動作し、既存のまたは計画中の有線ネットワークと接続するためのルーティングおよびファイアウォールのサービスを提供します。

有線インターフェースと同様、ワイヤレスインターフェースでは次の項目を構成できます。

- IP アドレス / ネットマスクおよび管理 IP アドレス
- WebUI、SNMP、Telnet、SSH、あるいは SSL のような管理オプション
- アドレス変換
- DNS（ドメイン名サーバー）プロキシ
- WebAuth
- ダイナミックホスト構成プロトコル（DHCP）のサーバー機能（DHCP クライアントまたはリレー機能はサポートされません）

注： *第 2 部 : 基本*および*第 8 部 : アドレス変換*を参照してください。.

次のワイヤレス ScreenOS 機能によって、WLAN の管理およびセキュリティ保護ができます。

- システム当たり 4 つまでの WLAN
- 16 個までのサービスセット識別子（SSID）

- 認証
  - オープン
  - 有線と同等のプライバシー（WEP）（共有鍵）
  - WEP（802.1X)
  - Wi-Fi プロテクテッドアクセス（WPA）（事前共有鍵）
  - WPA（802.1X)
  - WPA2 (事前共有鍵)
  - WPA2（802.1X)
- 暗号化
  - AES (次世代標準暗号)AES
  - 一時鍵保全プロトコル（TKIP）
  - WEP
- Wi-Fi™ マルチメディア（WMM）サービス品質機能
- ラジオバンドについてほぼ 2 倍のパフォーマンスを発揮するターボモード

注 : 性能の記述については製品に付属するデータシートを参照してください。

ワイヤレス製品によるインターフェース名指定の違い

ワイヤレス製品は 4 つまでの WLAN をサポートします。WebUI および CLI に入力するコマンドは製品によって異なります。

ワイヤレス製品によってはトランシーバが 2 台あります。

- 2.4GHz (WAN 0)
- 5GHz (WAN 1)

トランシーバ独自のパラメーターが、自動的に WebUI または CLI に表示されます。

基本的なワイヤレスネットワーク機能の構成

設定が必要なワイヤレス機能があります。他の機能はオプションです。しかし、ワイヤレスインターフェースに変更を加えるごとに、WLAN を再起動しなければなりません（詳細は 122 ページの「WLAN 構成の再起動」を参照してください）。

このセクションには、以下のトピックがあります。

- 118 ページの「サービスセット識別子の作成」
- 119 ページの「2.4 GHz トランシーバへの操作モードの設定」
- 120 ページの「5GHz トランシーバへの操作モードの設定」
- 122 ページの「WLAN 構成の再起動」

サービスセット識別子の作成

ワイヤレスネットワークは、サービスセット識別子（SSID）によって識別されます。SSID では、1 つのワイヤレスセキュリティデバイスを使用して、複数の WLAN を維持できます。ワイヤレスインターフェースに SSID をバインドします。ワイヤレスインターフェースはセキュリティゾーンにバインドできます。SSID は、長さが 32 テキスト文字までの一意の名前です。名前の中でスペースを使用するには、名前を二重引用符で囲まなければなりません。

注： SSID を作成するとき、セキュリティデバイスのワイヤレスインターフェースの数による制限はありません。ワイヤレスインターフェースの数より多くの SSID を作成できます。最高 4 つの SSID をワイヤレスインターフェースにバインドできます。ユーザーのネットワークニーズが変わるのに応じて、SSID をワイヤレスインターフェースへバインドしたりバインドを解除することによって、サイトまたは時間特有の WLAN を有効にできます。

次の例では、名前が「My Home Network」の SSID を設定します。セキュリティ向上のため、名前を推測が困難なものにし、SSID 名にデバイスの所在地を含まないようにできます。

WebUI

Wireless > SSID > New: SSID フィールドに名前を入力し、**OK** をクリックします。

CLI

```
set ssid name “My Home Network”
```

SSID ブロードキャストの抑制

SSID を作成した後、セキュリティデバイスが通知するビーコンで SSID のブロードキャストを無効にできます。SSID ブロードキャストが無効な場合、SSID のことを知っているワイヤレスクライアントだけが関連付けが可能です。デフォルトでは、SSID はビーコンでブロードキャストされます。

SSID ブロードキャストを抑制するには、次の手順のいずれかを実行します。

WebUI

Wireless > SSID > Edit (*name_str*): **Disable SSID Broadcast** を選択し、**OK** をクリックします。

CLI

set ssid *name_str* ssid-suppression

クライアントの分離

クライアントの分離によって、同じサブネットのワイヤレスクライアントが互いに直接通信することを禁止します。これにより、各クライアントはファイアウォールを通じて通信することになります。デフォルトでは、このオプションは無効です。

同じサブネットのワイヤレスクライアントが互いに直接に通信することを禁止するには、次のいずれかの手順を使用します。

WebUI

Wireless > SSID > Edit (*name_str*): **SSID Client Isolation** を選択して、**OK** をクリックします。

CLI

set ssid *name_str* client-isolation enable

2.4 GHz トランシーバへの操作モードの設定

次のモードのいずれかで動作するよう WLAN 0 を設定できます。

- 802.11b モード（11b）
- 802.11b 互換の 11g モード（11g）
- 802.11b 非互換の 11g モード（11g-only）
- ターボ静的 11g-only モード

802.11b 非互換の **11g** モード（**11g-only**）は、セキュリティデバイスが 802.11b クライアントと関連付けを妨げます。**11g** オプションを選択すると、デバイスは 802.11b および 802.11g クライアントとの関連付けを許可します。**11b** オプションでは、デバイスは 802.11b クライアントとのみ関連付けできます。**Turbo** モードは、高性能オプションです。

注 : ターボモードがセキュリティデバイスに有効な場合、11g ターボをサポートするクライアントだけが接続できます。

デフォルトのモードは 802.11g に設定されています。このモードは 802.11g および 802.11b クライアントだけを許可します。

動作モードを 802.11g に設定するには、次の手順の 1 つを使用します。

WebUI

Wireless > WLAN > General Settings: Operation Mode リストから **802.11g** を選択して **Apply** をクリックします。（セキュリティデバイスに複数のトランシーバがある場合、2.4 GHz トランシーバについて選択します。）

CLI

1 つのトランシーバを持つセキュリティデバイスで動作モードを 802.11g に設定するには、以下のコマンドを入力します。

```
set wlan mode 11g
```

2 つのトランシーバを持つセキュリティデバイスで動作モードを 802.11g に設定するには、以下のコマンドを入力します。

```
set wlan 0 mode 11g
```

5GHz トランシーバへの操作モードの設定

802.11a モードまたはターボモードで動作するように 5 GHz トランシーバ、WLAN 1 を設定できます。802.11a モードは、5GHz の周波数帯内で動作し、デフォルトの動作モードです。

注 : ターボモードがセキュリティデバイスで有効な場合、11a ターボをサポートするクライアントだけが関連づけできます。

ターボモードを有効にすると、ダウンロード性能を上げることができます。

次の例では、WLAN 1 でターボモードを有効にします。

WebUI

Wireless > WLAN > General Settings: Operation Mode リストから **Turbo** を選択して **Apply** をクリックします。

CLI

WLAN 1 にターボモードを有効にするには、以下のコマンドを入力します。

```
set wlan 1 mode turbo
```

データ送信最低速度の構成

フレーム送信のデータ送信最低速度をメガビット / 秒（Mbps）で設定できます。データ送信速度はトランシーバのタイプにより、次のいずれかになります。

- 802.11a: 6, 9, 12, 18, 24, 36, 48, 54
- XR が有効な 802.11a: 0.25, 0.5, 3, 6, 9, 12, 18, 24, 36, 48, 54
- 802.11b: 1, 2, 5.5, 11
- 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
- XR が有効な 802.11g: 0.25, 0.5, 1, 2, 3, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54
- ターボモードが有効な場合 : 12, 18, 24, 36, 48, 72, 96, 108

デフォルト値の **auto** 速度は、最初に最高速度を使用し、送信が失敗すると次の速度に自動的に落とします。

データ送信速度を設定するには、次の手続の 1 つを使用します。

WebUI

Wireless > General Settings: Transmit Data Rate リストから速度を選択します（セキュリティデバイスに複数のトランシーバがある場合は、希望のトランシーバ用に選択します）。

CLI

1 つのトランシーバを持つセキュリティデバイスでデータ送信速度を 11 Mbps に設定するには、以下のコマンドを入力します。

```
set wlan transmit rate 11
```

2 つのトランシーバを持つセキュリティデバイスで、5 GHz トランシーバでデータ送信速度を 54 Mbps に設定するには、以下のコマンドを入力します。

```
set wlan 1 transmit rate 54
```

送信パワーの設定

送信パワーを設定し、セキュリティデバイスの周波数範囲を調節できます。パワーレベルを最大送信パワーの 1/8、フル、1/2、最小、または 1/4 に設定できます。最大送信パワーとは、セキュリティデバイスが動作している国で許可されている最大パワーのことです。デフォルトはフルパワーです。

送信パワーを設定するには、次の手続の 1 つを使用します。

WebUI

Wireless > General Settings: Transmit Power リストからパワーレベルを選択します（セキュリティデバイスに複数のトランシーバがある場合は、希望のトランシーバ用に選択します）。

CLI

1 つのトランシーバを持つセキュリティデバイスで送信パワーを 1/2 に設定するには、以下のコマンドを入力します。

```
set wlan transmit power half
```

2 つのトランシーバを持つセキュリティデバイスで、5 GHz トランシーバで送信パワーを 1/2 に設定するには、以下のコマンドを入力します。

```
set wlan 1 transmit power half
```

WLAN 構成の再起動

WLAN 構成に変更を加えたら、デバイス内の WLAN サブシステムを再起動します。これにより、ワイヤレスインターフェースが再起動されます。サブシステムを再度アクティブにして始めて、すべての WLAN 関連の構成変更は有効になります。

ネットワークによっては、再起動プロセスが完了するのに 60 秒以上かかる場合があります。ワイヤレストラフィックは中断され、ワイヤレスクライアントセッションはすべて終了します。ワイヤレスクライアントは、接続を再確立するため、ワイヤレスネットワークに再接続しなければなりません。

システムを再起動するには、次の手順のいずれかを実行します。

WebUI

トランシーバが 1 つのセキュリティデバイス :

Wireless > Activate Changes: Activate Changes ボタンをクリックします。

トランシーバが 2 つのセキュリティデバイス :

ワイヤレスページのトップにある Activate Changes ボタンをクリックします。

CLI

WLAN を再起動するには、以下のコマンドを入力します。

```
exec wlan reactivate
```

SSID への認証と暗号化の設定

認証と暗号化の設定はそれぞれの SSID で固有です。各 SSID について、異なる認証と暗号化の設定を行うことができます。

ScreenOS は、WLAN について次の認証および暗号化メカニズムをサポートします。

- 認証
  - オープン
  - WEP（共有鍵）
  - WEP（802.1X)
  - WPA (事前共有鍵)
  - WPA（802.1X)
  - WPA2 (事前共有鍵)
  - WPA2（802.1X)

- 暗号化
  - AES (次世代標準暗号)AES
  - 一時鍵保全プロトコル（TKIP）
  - WEP

次のセクションでは、WEP、WPA および WPA2 を説明し、SSID でそれらを設定する方法について説明します。EAP および 802.1X に関する詳細は、**9**-87 ページの「ワイヤレスおよびイーサネットインターフェース用の拡張認証」を参照してください。

WEP（有線と同等のプライバシー）の構成

Wired Equivalent Privacy (WEP) はワイヤレス通信に機密性を提供します。Rivest Cipher 4 (RC4) ストリーム暗号化アルゴリズムを使って、データがワイヤレスリンクを移動するときにデータを暗号化・復号化します。WEP 鍵をローカルに格納するか、あるいは外部認証サーバーと鍵を動的にネゴシエートできます。ワイヤレスクライアントはこの鍵を自分のシステム上に保存します。

ScreenOS は 2 つの WEP 鍵長をサポートします。それは 40 と 104 ビットです。鍵は 24 ビット初期ベクター（IV）と連結されているので、結果として長さは 64 と 128 ビットになります。

注 : いくつかの第三者のワイヤレスクライアントは、WEP 鍵の長さを指定する際に、IV からの 24 ビットを含めます。接続問題を避けるため、ワイヤレスデバイスで 40 または 104 ビットとされている同じ WEP 鍵の長さが、実はクライアント側の 64 または 128 ビットとされている鍵と同じ長さである可能性があります。

複数の WEP 鍵

1 つの SSID 当たり 4 個までの WEP 鍵を作成できます。

WEP 鍵を 1 つだけ作成した場合、ワイヤレスデバイスは、その SSID でワイヤレスクライアントを認証し、かつ自身とクライアントとの間で送信されたトラフィックの暗号化と解読を行うのに、その鍵を使用します。

また、ワイヤレスデバイス上に複数の WEP 鍵を定義することもでき、一つの SSID に対して最高 4 つの鍵を定義することができます。複数の鍵を使用することで、同じ SSID 内の異なるワイヤレスクライアントに対して、セキュリティのレベルを調整することができます。あるトラフィックには長い鍵を使用してセキュリティを向上し、あまり重要ではないトラフィックに対しては、短い鍵を使用して、処理のオーバーヘッドを少なくします。ワイヤレスデバイスは暗号化用に **default** 指定されている WEP 鍵を使用し、他の鍵（または再度デフォルトの鍵）を認証および復号化に使います。鍵にデフォルト指定をしないと、最初に定義した鍵がデフォルトとなります。

WEP 鍵の保存および鍵 ID ナンバーについて、次の点に注意してください。

- クライアントが外部 RADIUS サーバーから、固有の、動的に作成された WEP 鍵を使用する際、ワイヤレスデバイスは双方向コミュニケーションの

ために、この固有の鍵を使います（この鍵も RADIUS サーバーから受け取ります)。

- ワイヤレスクライアントがワイヤレスデバイス上に、ローカルに保存された、静的に定義された WEP 鍵を使う場合、デバイスはデフォルト鍵を使用して、送信するすべてのワイヤレストラフィックを暗号化します。クライアントは、ワイヤレスデバイスからのトラフィックを復号化するために、この鍵をロードしておく必要があります。

- 複数の WEP 鍵をワイヤレスデバイスに保存する場合、デフォルト ID 鍵は 1、2、3 または 4 となります。

- いくつかの WEP 鍵をワイヤレスデバイスに保存し、外部 RADIUS サーバーから動的に作成された WEP 鍵を使う場合、ワイヤレスデバイス上のデフォルト WEP 鍵の ID を 1 とすることができません。これは RADIUS サーバーがすべての鍵の ID として 1 を使うからです。ワイヤレスデバイスは暗号化に鍵 ID が 2 、3 または 4 のデフォルト WEP 鍵を使うことができます。そして認証および復号化のためにが ID が 1 、2 、3 または 4 の、静的に定義された WEP 鍵を使うことができます。

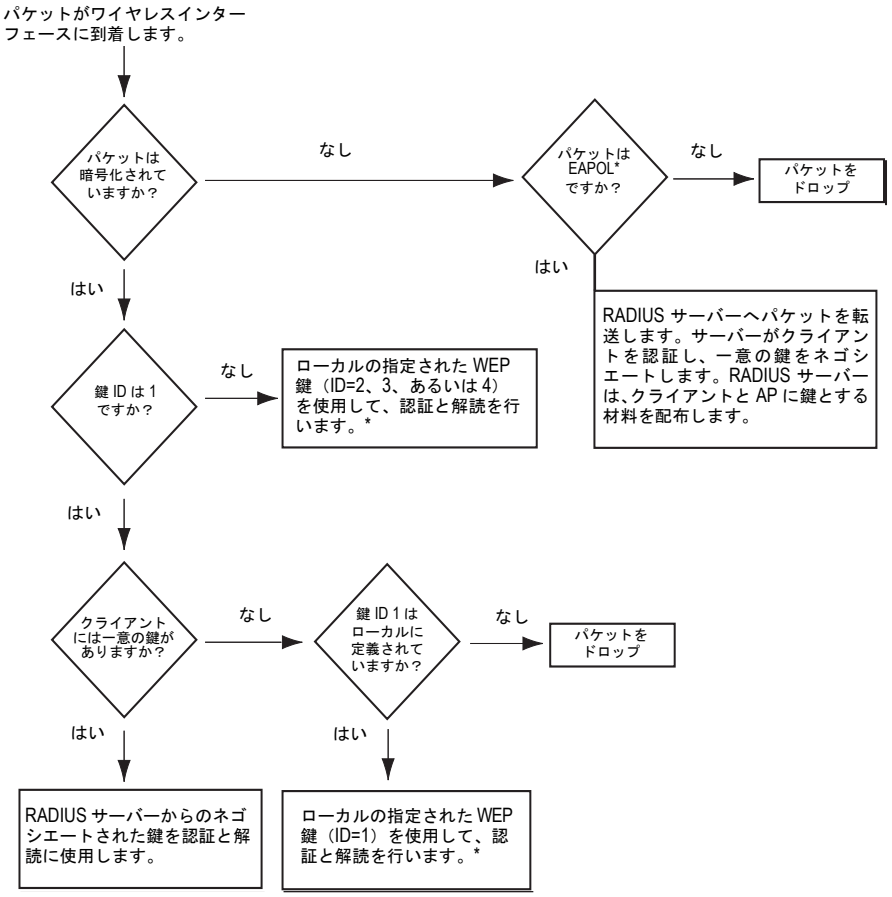
- RADIUS サーバーからの WEP 鍵を専有的に使う場合、サーバーはすべての鍵に対して鍵 ID 1 を使用します。RADIUS は各クライアントに対して、セッション毎に異なる鍵を作成・配布します。

- ワイヤレスクライアントから受信したトラフィックの認証・暗号化をするときは、ワイヤレスデバイス用にローカル保存された異なる鍵を指定することができます。クライアントは、自身を認証し、デバイスに送信されたトラフィックを暗号化するために、この鍵と ID ナンバーをロードしておく必要があります。（クライアントが ID 鍵を供給しない場合、デバイスはデフォルトの WEP 鍵を使用して、クライアントを認証し、トラフィックを復号化しようとします。）

注： クライアントが暗号化、復号化および認証に一つの鍵だけを使用する場合は、デフォルトの WEP 鍵を使う必要があります。

図 22 は WEP 鍵がローカルに保存されており、RADIUS サーバーからもらったものである場合、ワイヤレスデバイスがどのようにしてワイヤレス接続要求を処理しているかを示します。

図 22: RADIUS サーバー上の WEP による接続性プロセス



* 指定した鍵はデフォルトキーと同じまはた異なるものでもかまいません。

オープン認証の設定

認証を実行しないと指定する、オープン認証を設定できます。ワイヤレスクライアントは SSID を提供し、ワイヤレスネットワークに接続されます。オープン認証を使用する場合、次の暗号鍵オプションを指定できます。

- 暗号化なし
- WEP 暗号化
  - Local key source: WEP 鍵はセキュリティデバイス上に格納されます。デフォルトの鍵を指定しなければなりません。
  - Server: WEP 鍵は、RADIUS サーバーからネゴシエートされた動的な鍵です。
  - Both: トランシーバが 1 つのセキュリティデバイスのみで利用可能。WEP 鍵は、デバイスおよび RADIUS サーバー上に格納されます。デフォルトの鍵を指定しなければなりません。

1 つの SSID 当たり 4 個までの WEP 鍵を指定できます。

RADIUS サーバーからの WEP 鍵を使ったオープン認証の設定

次の例では、hr という名前の SSID に次のパラメーターを使用します。

- オープン認証
- WEP 暗号化
- rs1 という名前の RADIUS サーバーから取得した、動的に生成された WEP 鍵

WebUI

トランシーバが 1 つセキュリティデバイスの場合は、次の手続を使用します。

Wireless > SSID > Edit: 次のように入力してから **OK** をクリックします。

WEP Based Authentication and Encryption Methods: Open, WEP Encryption
Key Source: Server
Auth Server: rs1（RADIUS サーバーがまだ存在しない場合、**Create new Auth Server** をクリックして定義します）

トランシーバが 2 つセキュリティデバイスの場合は、次の手続を使用します。

Wireless > SSID > Edit: 次のように入力してから **OK** をクリックします。

802.1X Based Authentication and Encryption Methods: 802.1X
Auth Server: rs1（RADIUS サーバーがまだ存在しない場合、**Create new Auth Server** をクリックして定義します）

CLI

トランシーバが 1 つのセキュリティデバイスの場合は、次のコマンドを使用します。

```
set ssid hr authentication open encryption wep key-source server rs1
```

トランシーバが 2 つセキュリティデバイスの場合は、次のコマンドを使用します。

```
set ssid hr authentication 802.1x auth-server rs1
```

ローカルの WEP 鍵を使ったオープン認証の設定

次の例では、hr という名前の SSID に次のパラメーターを使用します。

- オープン認証
- WEP 暗号化
- WEP 鍵はセキュリティデバイス上にローカルに格納
- Key ID: 1
- Key length: 40-bit
- ASCII テキスト : 1a2i3
- ID が 1 の鍵がデフォルトの鍵

WebUI

トランシーバが 2 つセキュリティデバイスの場合は、次の手続を使用します。

Wireless > SSID > Edit: 次のように入力してから **OK** をクリックします。

WEP Based Authentication and Encryption Methods: Open, WEP Encryption

WEP Key をクリックし、以下のように入力してから、**Add** をクリックします。

Key ID: 1
Key Length: 40
Key String: **ASCII を選択して、1a2i3 を入力します**（Confirm フィールドにもう 1 度入力)
Default Key (選択)

CLI

トランシーバが 2 つセキュリティデバイスの場合は、次のコマンドを使用します。

```
set ssid hr key-id 1 length 40 method asciitext 1a2i3 default
set ssid hr authentication open encryption wep
```

WEP 共有鍵認証の設定

クライアントの認証に使用されるセキュリティデバイス上に格納されている静的な WEP 鍵を設定できます。クライアントは、各自のワイヤレスデバイス上に静的な WEP 鍵を保持しています。1 つの SSID 当たり 4 個までの WEP 鍵を作成できます。

5 つの ASCII 文字からなる 5 桁の 16 進数あるいは文字列を提供して、40 ビットの暗号化を指定できます。26 桁の ASCII 文字からなる 16 進数または 13 個の ASCII 文字からなる文字列を提供して、104 ビットの暗号化を指定できます。

次の例では、hr という名前の SSID に次のパラメーターを使用します。

- WEP 共有鍵
- Key ID: 1
- Key length: 40-bit
- ASCII テキスト : 1a2i3
- ID が 1 の鍵がデフォルトの鍵

WebUI

Wireless > SSID > Edit: 次のように入力してから **OK** をクリックします。

WEP Based Authentication and Encryption Methods: WEP Shared Key

WEP Key をクリックし、以下のように入力してから、**Add** をクリックします。

Key ID: 1
Key Length: 40

Key String: **ASCII** を選択して、**1a2i3** を入力します（Confirm フィールドにもう 1 度入力）
Default Key (選択)

CLI

```
set ssid hr authentication shared-key
set ssid hr key-id 1 length 40 method asciitext 1a2i3 default
```

ScreenOS は、ワイヤレスクライアントが WEP 共有鍵で自身を認証するかどうか自動的にネゴシエートするメカニズムを提供しています。このオプションを使って、異なる WEP 実装をサポートするさまざまなオペレーティングシステムを使用しているワイヤレスクライアントにアクセスしたい場合、互換性を改善することができます。

自動ネゴシエートを有効にするには、次のいずれかを実行します。

WebUI

Wireless > SSID > Edit (*name_str)*: **Auto** を選択します。

CLI

```
set ssid name_str authentication auto
```

注： すべての SSID に対して WEP を構成できますが、デバイスは意図的に同時に 1 つの BSS しか使用できないように制限します。このため、WPA または WPA2 の使用を推奨します。

Wi-Fi 保護アクセスの構成

Wi-Fi 保護アクセス（WPA）は、WLAN 認証および暗号化に対するセキュリティがより高いソリューションで、WEP のさまざまな短所に対応して設計されたものです。ScreenOS は WPA と WPA2 をサポートしています。

WPA および WPA2 は 802.1X 認証をサポートしています。802.1X 認証は、RADIUS サーバーによる認証のために、拡張可能認証プロトコル（EAP）方法を使用します。EAP はカプセル化プロトコルで、認証に使われ、データリンクレイヤー（レイヤー 2）で動作します。詳細は RFC 2284, *PPP Extensible Authentication Protocol (EAP)* を参照してください。

ScreenOS は、Juniper Networks 社の Steel-Belted RADIUS サーバー や Microsoft 社の Internet Authentication Service（IAS）RADIUS サーバーのような、802.1X 準拠の RADIUS サーバーと連携します。

RADIUS サーバーと WPA あるいは WPA2 を使用する場合、セキュリティデバイスは、ワイヤレスクライアントと RADIUS サーバーとの間の認証要求や応答を転送します。クライアントの認証に成功すると、RADIUS サーバーはクライアントとセキュリティデバイスの両方に暗号鍵を送信します。それ以降、セキュリティデバイスは暗号化タイプ（Temporal key Integrity Protocol（TKIP）または 次世代標準暗号 (AES)）を含む暗号化プロセスおよび鍵更新間隔を管理します。TKIP についての情報は IEEE Standard 802.11 を参照してください。AES についての情報は RFC 3268, *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)* を参照してください。

事前共有鍵と WPA または WPA2 を使用することもできます。事前共有鍵は、セキュリティデバイスとクライアントのデバイスで設定される静的な鍵です。両方のデバイスが、その鍵を使用して、そのセッション用の一意の鍵（グループ鍵）を生成します。ASCII パスフレーズ（パスワード）の使用により、あるいは 16 進数の形式で、事前共有鍵を指定できます。802.1X 認証と同じ暗号化タイプ、TKIP または AES も使用します。

認証タイプとして WPA と WPA2 を許可したい場合、認証方法として 802.1X を使用していれば、wpa-auto キーワード（または WebUI オプション）、認証方法として事前共有鍵を使用していれば wpa-auto-psk キーワード（または WebUI オプション）を指定できます。

WPA と WPA2 の 802.1X 認証の構成

WPA と WPA2 に 802.1X 認証を構成するには、次を指定します。

- RADIUS サーバー
- 暗号化タイプ : TKIP または AES の他に、auto を指定できます。auto は、暗号化タイプとして TKIP と AES を指定します。
- 鍵更新間隔 : クライアント用のグループ鍵が更新されるまでに経過する時間。デフォルトでは、再入力間隔は 1800 秒（30 分）です。値の範囲は 30 ～ 4294967295 秒です。鍵更新間隔を無効にするには、**disable** CLI キーワードを使用するか、WebUI で 0 を指定します。

認証タイプとして WPA または WPA2 を指定するのに加えて、auto オプションを指定できます。このオプションは、認証タイプとして WPA および WPA2 を許可します。

次の例では、hr という名前の SSID に次のパラメーターを使用します。

- WPA（auto オプション）
- rs1 という名前の RADIUS サーバー
- 3600 秒の鍵更新間隔
- 暗号化タイプは AES

WebUI

Wireless > SSID > (**hr SSID** を選択): 以下を入力して **OK** をクリックします。

WPA Based Authentication and Encryption Methods: WPA Auto Pre-shared Key
Auth Server: rs1（RADIUS サーバーがまだ存在しない場合、**Create new Auth Server** をクリックして定義します）
Rekey Interval: 3600
Encryption Type: AES

CLI

```
set ssid hr authentication wpa-auto rekey-interval 3600 encryption aes auth-server
    rs1
```

WPA と WPA2 のため事前共有鍵認証の構成

WPA と WPA2 に事前共有鍵を構成するには、次を指定します。

- 事前共有鍵
  - 16 進形式 : 256 ビット（64 文字）の 16 進値を、そのままの形式で鍵に指定します。
  - ASCII パスフレーズ : SSID にアクセスするために、8 ～ 63 の ASCII 文字からなるパスフレーズを指定します。
- 暗号化タイプ : TKIP または AES の他に、auto を指定できます。auto は、暗号化タイプとして TKIP と AES を指定します。
- 鍵更新間隔 : クライアント用のグループ鍵が更新されるまでに経過する時間。デフォルトでは、再入力間隔は 1800 秒（30 分）です。値の範囲は 30 ～ 4294967295 秒です。鍵更新間隔を無効にするには、**disable** CLI キーワードを使用するか、WebUI で 0 を指定します。

認証タイプとして WPA または WPA2 を指定するのに加えて、auto オプションを指定できます。このオプションは、認証タイプとして WPA および WPA2 を許可します。

次の例では、hr という名前の SSID に次のパラメーターを使用します。

- WPA2
- $FKwinnisJamesTown8fg4 という ASCII パスフレーズを使用する、事前共有鍵
- 3600 秒の鍵更新間隔
- 暗号化タイプは TKIP

WebUI

Wireless > SSID > (**hr SSID** を選択): 以下を入力して **OK** をクリックします。

WPA Based Authentication and Encryption Methods: WPA2 Pre-shared Key
Key by Password: $FKwinnisJamesTown8fg4（Confirm Key by Password フィールドにパスフレーズを再入力）
Rekey Interval: 3600
Encryption Type: TKIP

CLI

```
set ssid hr authentication wpa2-psk passphrase $FKwinnisJamesTown8fg4
    encryption tkip rekey-interval 3600
```

アンテナ使用の指定

ワイヤレスセキュリティデバイスでは、特定のアンテナを選択したり、アンテナダイバーシティーを使用可能にできます。ダイバーシティーが選択されている場合、アンテナ A またはアンテナ B で信号の強い方が使用されます。デフォルトの設定は「ダイバーシティー」です。ダイバーシティー設定は、ほとんどの状況に適応します。外部の単向性アンテナを使用するため、アンテナ A またはアンテナ B を指定できます。セキュリティデバイスによっては、アンテナ A は電源コネクタに最も近いアンテナになります。セキュリティデバイスによっては、アンテナ A と B にラベルが付いています。詳細はハードウェアのマニュアルを参照してください。

アンテナ設定を変更するには、次の手順のいずれかを実行します。

WebUI

Wireless > General Settings: Antenna Diversity リストからアンテナ設定を選択し、**OK** をクリックします。

CLI

トランシーバが 1 つのセキュリティデバイスでアンテナ A を選択するには、以下のコマンドを入力します。

```
set wlan antenna a
```

トランシーバが 2 つのセキュリティデバイスで 5GHz トランシーバにアンテナ A を選択するには、以下のコマンドを入力します。

```
set wlan 1 antenna a
```

国コード、チャネルおよび周波数の設定

チャネル割り当て用に使用される規制されているドメインは、FCC（米国）、TELEC（日本）、ETSI（ヨーロッパ）または WORLD（すべての国）にプリセットされています。ETSI 規制ドメインは、2 つのトランシーバを備えたセキュリティデバイスでのみ利用可能です。事前設定された規制ドメインは変更できません。規制されているドメインが FCC または TELEC にプリセットされている場合、国を選択できません。規制ドメインが WORLD または ETSI である場合、国を選択しなければなりません。WORLD または ETSI にプリセットされたデバイスに対して国を設定しなければ、警告メッセージが表示され、ワイヤレス機能は動作しません。

ワイヤレスセキュリティデバイスは、1 台のトランシーバで同じチャネルと周波数をすべての SSID に使用します。デバイスは、入力した国コードに従い、適切なチャネルを選択します（特定のチャネルを手動で指定した場合を除く）。使用中のチャネルが、WebUI のチャネルリストに現れます。設定を auto にしておくと、デバイスはチャネルを選択できます。

利用可能な国コード、チャネルおよび周波数のリストについては、A-I　の「Wireless Information 」を参照してください。

国コードおよびチャネルを設定するには、次手続の 1 つを使用します。

WebUI

Wireless > General Settings: ドロップダウンリストから国、チャネルおよび周波数を選択し、**Apply** をクリックします。

CLI

set wlan country-code *country_abbreviation*
set wlan { 0 | 1 } channel { auto | 1 | 2 | 3 | ... }

拡張チャネルの使用

セキュリティデバイスが、チャネル 12 と 13 の使用を認める、規制されたドメインに位置する場合、2.4GHz トランシーバはそれらを使用できます。

WebUI

Wireless > General Settings: Extended Channel Mode チェックボックスを選択します。

CLI

トランシーバが 1 つのセキュリティデバイスには、以下のコマンドを入力します。

set wlan extended-channel

トランシーバが 2 つのセキュリティデバイスには、以下のコマンドを入力します。

set wlan 0 extended-channel

サイト調査の実行

他のアクセスポイントが近くでブロードキャストしているかどうか確かめるため、近辺を調査できます。サイト調査の実行により、悪質なアクセスポイントがその領域にあるかどうか確認できます。サイトの調査は、エリア内でビーコンを出しているアクセスポイントを検出して、検出した各アクセスポイントに対して、次の詳細を記録します。

- サービスセット識別子 (SSID)
- MAC アドレス
- 受信した信号の強度を示す指標 (RSSI)

  RSSI はデシベル（dB）単位で示されており、信号 / ノイズ比（SNR）を示します。SNR は信号レベルをノイズレベルで割った数値で、信号の強度を表します。

- ブロードキャストチャンネル

最初にサイトの調査を行ってからも、エリア内に悪質なアクセスポイントがないことを確かめるために、時々調査を行うことがあるかもしれません。サイト調査は次のように行います。

WebUI

Wireless > Statistics > Site Survey

CLI

exec wlan site-survey

注 : ネットワークによっては、サイト調査の完了に最高 60 秒 かかる場合があり、ワイヤレスネットワークトラフィックが中断されます。

利用可能なチャネルの発見

CLI を使用して、送信に使用するデバイスに最適なチャネルを見つけることができます。自動的にチャネルを選択するデフォルトの設定を使用せずに、干渉が最小のチャネルを見つけたい場合、このコマンドを使用します。

利用可能な最良のチャネルを発見するには、以下のコマンドを使用します。

exec wlan find-channel

注 : この機能は WebUI では使用できません。

アクセス制御リストエントリの設定

アクセス制御リスト (ACL) を使って、どのワイヤレスクラインアントがネットワークにアクセスできるかを制御できます。ACL はクライアントを MAC アドレスで識別し、それぞれのアドレスに対してワイヤレスデバイスがアクセスを許可あるいは拒否するかどうかを指定します。ACL は次のつ 3 のアクセスモードのうちの 1 つで動作します。

- Disabled: ワイヤレスデバイスは MAC アドレスをフィルターしません。これはデフォルトモードです。
- Enabled: ワイヤレスデバイスは、Deny アクションで指定したクライアント以外のすべてのクライアントへのアクセスを許可します。
- Strict: ワイヤレスデバイスは、Allow アクションで指定したクライアント以外のすべてのクライアントへのアクセスを拒否します。

注 : ACL 設定はすべての SSID に対して適用されます。

最高 64 の拒否クライアントおよび 64 の許可クライアントまで設定できます。

MAC アドレスを ACL に追加するには、次のいずれかの手順を行います。

WebUI

Wireless > MAC Access List: 次のように入力してから **Add** をクリックします。

Access Mode: (**リストから 3 つのモードのうち 1 つを選択**)
Input a new MAC address: (**ワイヤレスクライアントの MAC アドレスを入力**)
Control Status: (**Allow** または **Deny** を選択)

WebUI では、Select a learned MAC address リストから MAC アドレスを選択することもできます。ワイヤレスクライアントがワイヤレスデバイスと関連したとき、このリストにエントリが表示されます。所属している SSID に関わらず、現在関連しているすべてのワイヤレスクライアントの動的ディスプレイのリストです。

注 : Wireless > General Settings ページの MAC Address Access Control リストからアクセスモードを設定することもできます。

CLI

```
set wlan acl mode { disable | enable | strict }
set wlan acl mac_addr { deny | allow }
```

Super G の構成

Super G® 機能を備えた Atheros Communications 社製チップセットを持つワイヤレスデバイスでは、Super G を有効にできます。これにより、次の方法を使用して、ユーザーのデータスループット速度が 802.11a および 802.11g クライアントでは 4 Mbps まで向上します。

- バースト : デバイスは、各フレームの後に休止するのではなく、連続して複数フレームを送信できます。
- 高速フレーム : 標準より大きなフレームサイズを許可することにより、フレーム当たりより多くの情報を送信できます。
- 圧縮 : リンクレベルのハードウェア圧縮は、内蔵のデータ圧縮エンジンによって実行されます。

デフォルトでは、この機能は無効です。

ワイヤレスクライアントが Super G をサポートしておらず、セキュリティデバイスで Super G が有効な場合、ワイヤレスクライアントは、ワイヤレスネットワークに接続できますが、Super G 機能は利用できません。

注 : Atheros Communications Super G チップセットに関する詳細は、www.atheros.com を参照してください。

Super G を有効にするには、次の手順のいずれかを実行します。

WebUI

Wireless > General Settings: Super-G チェックボックスを選択します（セキュリティデバイスに複数のトランシーバがある場合は、希望のトランシーバ用に選択します）。

CLI

トランシーバが 1 つのセキュリティデバイスで Super G を有効にするには、以下のコマンドを入力します。

```
set wlan super-g
```

トランシーバが 2 つのセキュリティデバイスで 5GHz トランシーバに Super G を有効にするには、以下のコマンドを入力します。

```
set wlan 1 super-g
```

Atheros XR（拡張範囲）の構成

Atheros Communications eXtended Range（XR）技術を有効にできます。XR は、通常よりワイヤレスネットワークの「デッドスポット」が少なく、範囲が広くなるように、IEEE 802.11a および 802.11g の標準によって定義されている、802.11 信号を処理します。XR は弱い信号をより効果的に処理し、到達範囲を拡大します。XR では、データ転送速度が低いほど、到達範囲は拡大します。

各トランシーバの最初のアクティブな SSID だけが XR をサポートできます。XR が有効な場合、各トランシーバの最初のアクティブな SSID が XR 機能を使用します。

XR を有効にするには、次の手順のいずれかを実行します。

WebUI

Wireless > General Settings: XR Support チェックボックスを選択します（セキュリティデバイスに複数のトランシーバがある場合は、希望のトランシーバ用に選択します）。

CLI

トランシーバが 1 つのセキュリティデバイスで XR を有効にするには、以下のコマンドを入力します。

```
set wlan xr
```

トランシーバが 2 つのセキュリティデバイスで 5GHz トランシーバに XR を有効にするには、以下のコマンドを入力します。

```
set wlan 1 xr
```

Wi-Fi マルチメディアサービス品質の構成

Wi-Fi マルチメディア（WMM）サービス品質（QoS）機能によって、ワイヤレスネットワークの性能を向上させることができます。これは、各アプリケーションの異なるレイテンシーとスループット要件に適応するため、オーディオ、ビデオおよび音声アプリケーションの伝送優先順位を調節することによって行われます。デフォルトでは、WMM は無効です。

WMM は、802.11e で定義されているように、EDCA（Enhanced Distributed Channel Access）に基づきます。WMM の詳細は http://www.wi-fi.org を参照してください。

この機能が利用できないセキュリティデバイスがあります。

WMM を有効にする

2.4 GHz ラジオ (WLAN 0) または 5GHz ラジオ (WLAN 1) で WMM を有効にできます。

WMM を有効にするには、次の手順のいずれかを実行します。

WebUI

Wireless > WMM Settings: トランシーバの Enable ラジオボタンを選択し、**Apply** をクリックします。

CLI

```
set wlan [ 0 | 1 ] wmm enable
```

WMM サービス品質の構成

WMM を有効にした後、ユーザーのネットワーク要件に適応するように、WMM パラメーターを設定できます。接続の末端であるアクセスポイント（ap）およびステーション（sta）から動作するように WMM を設定します。

- *ap* はセキュリティデバイスのための WMM 設定です。
- *sta* は、クライアント用の WMM 設定です。クライアントは、4 つの AC に従ってトラフィックを内部の待ち行列に入れ、設定したパラメーターに基づいて送信機会を検知すると、パケットを送信します。

セキュリティデバイスあるいはクライアント（ステーション）がパケットを送信する場合に限り、WMM 設定が使用されます。

アクセスのカテゴリ

IETF（Internet Engineering Task Force）の DSCP（Differentiated Services Code Point）ヘッダーに基づき、セキュリティデバイスとクライアントは、4 つのアクセスカテゴリ（AC）の 1 つにトラフィックを分類します。

- Best effort (0) ー QoS レベルを処理できないトラフィックおよびレイテンシーにそれほど敏感でないが、長い遅延によって影響される場合があるトラフィック。
- Background priority (1) ー優先度が低いトラフィック
- Video (2) ービデオトラフィックは他のデータトラフィックより優先度が高くなります
- Voice (3) ー音声トラフィックは優先度が最高になります。

表 3 は、アクセスカテゴリとサービスのタイプ（TOS）の間のマッピングを示しています。

表 3: アクセスカテゴリと TOS のマッピング

アクセスのカテゴリ	TOS 値
音声	0xC0、0xB8、0xE0
ビデオ	0x80、0xA0、0x88
ベストエフォート	0x00、0x60 など
バックグラウンド	0x40、0x20

注 : 802.1d タグはサポートされていません。

具体的な優先度および設定は各 AC に関連付けられていますが、WebUI または CLI によってこれらの設定を無効にできます。

デフォルトの WMM 設定

次の用語は、構成可能な WMM パラメーターを表し、表 4 と表 5 に列の見出しとして現れます。また、これらの表は、アクセスポイント（セキュリティデバイス）とステーション（クライアント）設定のデフォルト設定を示しています。

- *aifs*

  AIFSN（Arbitrary Inter-Frame Space Number）は、SIFS 期間の後に、スロットの数を指定します。この期間中に、AC のためのセキュリティデバイスまたはクライアントは、送信またはバックオフ実行の前に、媒体のアイドル状態をチェックします。

- *logcwmin* と *logcwmax*

  WMM は、コンテンションウィンドウ（CW）を定義します。これは、ランダムなバックオフ期間と等しくなります。

  CWmin パラメーターは、特定の AC がバックオフ用の乱数を生成するため、セキュリティデバイスまたはクライアントが使用するコンテンションウィンドウのスロットの最小数を指定します。logcwmin が x の場合、CWmin は 2^x-1 です。

  CWmax パラメーターは、特定の AC がバックオフ用の乱数を生成するため、セキュリティデバイスまたはクライアントが使用するウィンドウのスロットの最大数を指定します。logcwmax が x の場合、CWmax は 2^x-1 です。

  ScreenOS は、コンテンションのないアクセスまたはスケジュールされたアクセスをサポートしません。

- *txoplimit*

  Transmit Opportunity は、セキュリティデバイスまたはクライアントが送信を開始できる最長時間を指定します。txoplimit を x に設定すれば、最長時間は 32*x マイクロ秒です。

- *ackpolicy*

  アクセスポイントの肯定応答ポリシーを有効または無効にできます。このパラメーターはクライアントには適用されません。

表 4 は、アプリケーションタイプが WMM のセキュリティデバイスについて、すべてのサポートされるワイヤレスモードのデフォルト値を示しています。デフォルトでは *ackpolicy* は、すべてのワイヤレスモードについて無効です。

表 4: AC 別アクセスポイント WMM のデフォルト値

AC	ワイヤレスモード	aifs	logcwmin	logcwmax	txoplimit
Best Effort（0）	802.11a	3	4	6	0
	802.11a Turbo	2	3	5	0
	802.11b	3	5	7	0
	802.11g	3	4	6	0
	802.11g Turbo	2	3	5	0
	XR	0	3	3	0
Background (1)	802.11a	7	4	10	0
	802.11a Turbo	7	3	10	0
	802.11b	7	5	10	0
	802.11g	7	4	10	0
	802.11g Turbo	7	4	10	0
	XR	0	3	3	0
Video (2)	802.11a	1	3	4	94
	802.11a Turbo	1	2	3	94
	802.11b	1	4	5	188
	802.11g	1	3	4	94
	802.11g Turbo	1	2	3	94
	XR	0	3	3	0
Voice (3)	802.11a	1	2	3	47
	802.11a Turbo	1	2	2	47
	802.11b	1	3	4	102
	802.11g	1	2	3	47
	802.11g Turbo	1	2	2	47
	XR	0	3	3	0

表 5 は、クライアント（sta）の WMM 構成について、すべてのサポートされるワイヤレスモードのデフォルト値を示しています。

表 5: AC 別ステーション WMM のデフォルト値

AC	ワイヤレスモード	aifs	logcwmin	logcwmax	txoplimit
Best Effort	802.11a	3	4	10	0
	802.11a Turbo	2	3	10	0
	802.11b	3	5	10	0
	802.11g	3	4	10	0
	802.11g Turbo	2	3	10	0
	XR	0	3	3	0
Background	802.11a	7	4	10	0
	802.11a Turbo	7	3	10	0
	802.11b	7	5	10	0
	802.11g	7	4	10	0
	802.11g Turbo	7	4	10	0
	XR	0	3	3	0
Video	802.11a	2	3	4	94
	802.11a Turbo	2	2	3	94
	802.11b	2	4	5	188
	802.11g	2	3	4	94
	802.11g Turbo	2	2	3	94
	XR	0	3	3	0
Voice	802.11a	2	2	3	47
	802.11a Turbo	1	2	2	47
	802.11b	2	3	4	102
	802.11g	2	2	3	47
	802.11g Turbo	1	2	2	47
	XR	0	3	3	0

例

次の例では、5GHz トランシーバで WMM のステーション設定を使用し、音声トラフィック（A = 0）の設定を以下のように変更します。

- logcwmin: 0
- logcwmax: 15
- aifs: 4
- txoplimit: 10

これらの設定で WMM を構成するには、次のように行います。

WebUI

Wireless > WMM Settings: 希望の設定を入力して **Apply** をクリックします。

CLI

```
set wlan 1 wmm sta 0 logcwmin 0
set wlan 1 wmm sta logcwmax 15
set wlan 1 aifs 4
set wlan 1 txoplimit 10
save
```

詳細なワイヤレスパラメーターの設定

このセクションは、詳細なワイヤレスパラメーターに関する情報を含んでいます。あるタイプのワイヤレス配備では、性能を向上させるため、小さな変更を加える必要があるかもしれません。

次の詳細なワイヤレス機能についてこのセクションで説明します。

- 140 ページの「エージング間隔の構成」
- 141 ページの「ビーコン間隔の設定」
- 142 ページの「DTIM（Delivery Traffic Indication Message）期間の構成」
- 142 ページの「バーストしきい値の構成」
- 143 ページの「フラグメントしきい値の構成」
- 143 ページの「送信要求しきい値の構成」
- 144 ページの「送信可モードの構成」
- 144 ページの「送信可速度の構成」
- 144 ページの「送信可タイプの構成」
- 145 ページの「スロット時間の設定」
- 145 ページの「プリアンブル長の構成」

エージング間隔の構成

クライアントとのトラフィックのやり取りがない場合にワイヤレスクライアントが切断される前に経過する時間を指定できます。この値は 60 秒と 1,000,000 秒の間の値になります。デフォルト値は 300 秒です。エージングを無効にするには、**set wlan advanced aging-interval disable** コマンドを使用します。

エージング間隔が経過し、クライアントが切断された後、その MAC 情報はセキュリティデバイスの MAC テーブルから削除されます。各トランシーバの MAC テーブルには、60 までのクライアント MAC アドレスを含めることができます。MAC テーブルがいっぱいの場合、新しいクライアントとの接続は拒否されるので、タイミングよく、接続を使用していない既存のクライアントが切断され、MAC アドレスが MAC テーブルから削除されるように、エージング間隔を設定します。

2.4 GHz トランシーバに 500 秒のエージング間隔を設定するには、次の手続の 1 つを使用します。

WebUI

Wireless > General Settings > Advanced: 次のように入力してから **Return** をクリックします。

Aging Interval: 500（**トランシーバが 2 つのデバイスについては、WLAN0 にエージング間隔を指定します**）

CLI

トランシーバが 1 つのセキュリティデバイスでエージング間隔を変更にするには、以下のコマンドを入力します。

```
set wlan advanced aging-interval 500
```

2 つのトランシーバを持つセキュリティデバイスで、2.4 GHz トランシーバのエージング間隔を 500 秒に設定するには、以下のコマンドを入力します。

```
set wlan 0 advanced aging-interval 500
```

ビーコン間隔の設定

ビーコンが送信される間隔を設定できます。値の範囲は、20 〜 1,000 タイムユニット (1 タイムユニットは 1024 μs) です。デフォルト値は 100 タイムユニットです。

2.4 GHz トランシーバで 200 タイムユニット (2048 μs) にビーコン間隔を設定するには、次の手続の 1 つを使用します。

WebUI

Wireless > General Settings > Advanced: 次のように入力してから **Return** をクリックします。

Beacon Interval: 200（**トランシーバが 2 つのデバイスについては、WLAN0 にビーコンを指定します**）

CLI

トランシーバが 1 つのセキュリティデバイスでビーコン間隔を変更にするには、以下のコマンドを入力します。

```
set wlan advanced beacon-interval 200
```

2 つのトランシーバを持つセキュリティデバイスで、2.4 GHz トランシーバのビーコン間隔を変更するには、以下のコマンドを入力します。

```
set wlan 0 advanced beacon-interval 200
```

DTIM（Delivery Traffic Indication Message）期間の構成

DTIM（delivery traffic indication map）が送信される前に送信されるビーコンの数を設定できます。DTIM 期間を長くすると、クライアントに送信されるブロードキャストの数が減ります。値の範囲は 1 ～ 255 です。デフォルト値は 1 ビーコン間隔です。

DTIM 期間を 2 に設定するには、次の手順の 1 つを使用します。

WebUI

Wireless > General Settings > Advanced: 次のように入力してから **Return** をクリックします。

DTIM Period: 2 (トランシーバが 2 つのデバイスについては、WLAN0 に DTIM 期間を指定します)

CLI

トランシーバが 1 つのセキュリティデバイスで DTIM 期間を変更にするには、以下のコマンドを入力します。

```
set wlan advanced dtim-period 2
```

2 つのトランシーバを持つセキュリティデバイスで、2.4 GHz トランシーバの DTIM 期間を変更するには、以下のコマンドを入力します。

```
set wlan 0 advanced dtim-period 2
```

バーストしきい値の構成

バーストの中のフレームの最大値を設定できます。有効な範囲は 2 と 255 との間です。デフォルト値は 3 です。この機能が利用できないセキュリティデバイスがあります。

バーストしきい値を 5 に変更するには、次の手順の 1 つを使用します。

WebUI

Wireless > General Settings > Advanced: 次のように入力してから **Return** をクリックします。

Burst Threshold: 5

CLI

```
set wlan advanced burst-threshold 5
```

フラグメントしきい値の構成

送信前に複数フレームにフラグメント化されないフレームの最大長を設定できます。値の範囲は 256 と 2346 の間の偶数です。デフォルト値は 2346 です。

2.4 GHz トランシーバに 500 のフラグメントしきい値を設定するには、次の手順の 1 つを使用します。

WebUI

Wireless > General Settings > Advanced: 次のように入力してから **Return** をクリックします。

Fragment Threshold: 500（トランシーバが 2 つのデバイスについては、WLAN0 にフラグメントしきい値を指定します）

CLI

トランシーバが 1 つのセキュリティデバイスでフラグメントしきい値を変更にするには、以下のコマンドを入力します。

```
set wlan advanced fragment-threshold 500
```

2 つのトランシーバを持つセキュリティデバイスで、2.4 GHz トランシーバのフラグメントしきい値を設定するには、以下のコマンドを入力します。

```
set wlan 0 advanced fragment-threshold 500
```

送信要求しきい値の構成

フレームを送信するため送信要求（RTS）方法を使用する前に、フレームの最大長を設定できます。値の範囲は 256 ～ 2346 です。デフォルト値は 2346 です。

2.4 GHz トランシーバに 500 の RTS しきい値を設定するには、次の手順の 1 つを使用します。

WebUI

Wireless > General Settings > Advanced: 次のように入力してから **Return** をクリックします。

RTS Threshold: 500（トランシーバが 2 つのデバイスについては、WLAN0 に RTS しきい値を指定します）

CLI

トランシーバが 1 つのセキュリティデバイスで RTS しきい値を変更にするには、以下のコマンドを入力します。

```
set wlan advanced rts-threshold 500
```

2 つのトランシーバを持つセキュリティデバイスで、2.4 GHz トランシーバの RTS しきい値を設定するには、以下のコマンドを入力します。

```
set wlan 0 advanced rts-threshold 500
```

送信可モードの構成

送信可（CTS）保護は、802.11 を実行するのに必要なオーバーヘッドを減らすため、肯定応答（ACK）パケットをブロックします。デフォルトの設定は *auto* です。デフォルトでは、セキュリティデバイスは、クライアントの CTS の設定を検知します。常に CTS を使用するには **on** を、決して CTS を使用しない場合は **off** を、選択することもできます。

注： この機能は、802.11b ワイヤレスモードでは機能せず、利用できないセキュリティデバイスがあります。

セキュリティデバイスのデフォルトの活動を変更する場合、「送信可速度の構成」および「送信可タイプの構成」で説明するように、CTS の速度とタイプも変更しなければならない場合があります。

CTS 保護をオフにするには、次の手続の 1 つを使用します。

WebUI

Wireless > General Settings > Advanced: 次のように選んでから **Return** をクリックします。

CTS Mode: Off

CLI

```
set wlan advanced cts-mode off
```

送信可速度の構成

CTS フレームが送信される速度（Mbps）を設定できます。この機能は、802.11b ワイヤレスモードでは機能せず、利用できないセキュリティデバイスがあります。有効な値は 1、2、5.5 および 11 Mbps です。デフォルトは 11 Mbps です。

CTS 速度を 5.5 に設定するには、次の手順の 1 つを使用します。

WebUI

Wireless > General Settings > Advanced: 次のように選んでから **Return** をクリックします。

CTS Rate: 5.5

CLI

```
set wlan advanced cts-rate 5.5
```

送信可タイプの構成

ScreenOS は、CTS のみおよび CTS-RTS という、2 つの送信可（CTS）保護タイプを提供します。CTS の目的は、2 つの無線クライアント間のコリジョンを減少させることです。CTS のみオプション（デフォルト）では、セキュリティデバイスは、データを転送する前に CTS フレームを待たなければなりません。CTS-RTS（送信要求）オプションでは、データを転送する前にセキュリティデバイスは RTS-CTS ハンドシェイクを完了しなければなりません。

この機能が利用できないセキュリティデバイスがあります。

CTS タイプを CTS のみに設定するには、次の手順の 1 つを使用します。

WebUI

Wireless > General Settings > Advanced: 次のように選んでから **Return** をクリックします。

CTS Type: CTS Only

CLI

set wlan advanced cts-type cts-only

スロット時間の設定

スロット時間を **long** に設定している場合、セキュリティデバイスは、長いスロット時間だけを使用します。デフォルトでは、セキュリティデバイスは短いスロット時間を使用します。この機能は 802.11g モードでのみ使用されます。

2.4GHz トランシーバで長いスロット時間を有効にするには、次の手順の 1 つを使用します。

WebUI

Wireless > General Settings > Advanced: Long Slot Time チェックボックスを選択して、**Return** をクリックします。

CLI

トランシーバが 1 つのセキュリティデバイスで長いスロット時間を有効にするには、以下のコマンドを入力します。

set wlan advanced slot-time long

2 つのトランシーバを持つセキュリティデバイスで、2.4 GHz トランシーバについて長いスロット時間を有効にするには、以下のコマンドを入力します。

set wlan 0 advanced slot-time long

プリアンブル長の構成

送信プリアンブルを短いものから長いものへと変更できます。長いプリアンブルに設定していると、長いプリアンブルだけが使用されます。短いプリアンブルが有効な場合、短いプリアンブルと長いプリアンブルが使用されます。デフォルトは短いプリアンブルです。2.4 GHz トランシーバを 802.11b および 802.11g モードに設定している場合のみ、このコマンドは適用されます。

WebUI

Wireless > General Settings > Advanced: Long Transmit Preamble チェックボックスを選択して、**Return** をクリックします。

CLI

トランシーバが 1 つのセキュリティデバイスで長いプリアンブルを有効にするには、以下のコマンドを入力します。

set wlan advanced long-preamble

2 つのトランシーバを持つセキュリティデバイスで、2.4 GHz トランシーバについて長いプリアンブルを有効にするには、以下のコマンドを入力します。

set wlan 0 advanced long-preamble

ワイヤレスインターフェースでの作業

このセクションでは、ワイヤレスインターフェースで実行できる次のタスクを説明します。

SSID のワイヤレスインターフェースへのバインド

セキュリティデバイスが最初にブートしたとき、いくつかのワイヤレスインターフェースが存在しますが、それらは SSID に関連付けられていません。SSID を作成した後、インターフェースをアクティブにするには、インターフェースを SSID にバインドする必要があります。

トランシーバが 1 つのセキュリティデバイスについては、SSID を作成した後、特定のセキュリティゾーンにバインドされているワイヤレスインターフェースに SSID をバインドしなければなりません。トランシーバが 2 つのセキュリティデバイスについては、ワイヤレスインターフェースは、ゾーンにバインドするか、またはブリッジグループ（bgroup）に配置できます。ブリッジグループの詳細については、147 ページの「ワイヤレスブリッジグループの作成」を参照してください。

SSID をワイヤレスインターフェースにバインドするには、次の手順のいずれかを行います。

WebUI

Wireless > SSID > Edit (インターフェースにバインドしたい SSID): Wireless Interface Binding リストからインターフェースを選択し、**OK** をクリックします。

または

トランシーバが 1 つのセキュリティデバイスでは、次を行います。

Network > Interfaces > Edit: Bind to SSID リストから SSID を選択し、**OK** をクリックします。

トランシーバが 2 つのセキュリティデバイスでは、次を行います。

Network > Interfaces > List > Edit: Bind to SSID リストから SSID を選択し、**OK** をクリックします。

CLI

set ssid *name_str* interface *interface*

ワイヤレスインターフェースのトランシーバへのバインド

セキュリティデバイスによっては、ワイヤレスインターフェースが使用するトランシーバを指定できます。デフォルトでは、ワイヤレスインターフェースは 2 つのトランシーバにバインドされ、802.11a、802.11b あるいは 802.11g モードで動作できます。

以下のオプションを指定できます。

- 0、802.11b および 802.11g の 2.4 GHz トランシーバだけを有効にします。
- 1、802.11a の 5GHz のトランシーバだけを有効にします。

- both、インターフェース（802.11a/b/g）で両方のトランシーバ（2.4 GHz と 5GHz）を有効にします。

たとえば、**set wlan mode** コマンドで、操作モードに **802.11b** を指定し、**0** オプションを選択すれば、802.11b だけがワイヤレスインターフェースに利用可能です。

wireless0/0 インターフェースが 2.4 GHz トランシーバを使用するように指定するには、次の手続の 1 つを使用します。

WebUI

Network > Interface > List > Edit (wireless interface): Wlan リストから **2.4G(802.11b/g)** を選択し、**OK** をクリックします。

CLI

set interface wireless0/0 wlan 0

ワイヤレスブリッジグループの作成

セキュリティデバイスにはブリッジグループ（bgroups）をサポートするものがあります。bgroup では、ネットワークユーザーは、コンピュータを再構成またはリブートしなくても、有線 / ワイヤレストラフィック間のスイッチができます。1 つの bgroup を操作するために複数の SSID を構成したり、有線サブネットと同じサブネットで動作するように 1 つの SSID を構成できます。

ブリッジグループをサポートするワイヤレスセキュリティデバイスでは、ブリッジグループは bgroup0 ～ bgroup3 によって識別されます。

同じ bgroup にイーサネットとワイヤレスインターフェースを設定するには、次の手続の 1 つを使用します。

WebUI

Network > Interfaces > List > Edit (bgroup) > Bind Port: インターフェースに **Bind to Current Bgroup** を選択し、**Apply** をクリックします。

CLI

同じブリッジグループインターフェースにイーサネットとワイヤレスインターフェースを設定するには、次を行います。

set interface *bgroup_name* port *wireless_interface*
set interface *bgroup_name* port *ethernet_interface*

注 : *bgroup_name* には、bgroup0 ～ bgroup3 を使用できます。
ethernet_interface には、ethernet0/0 ～ ethernet0/4 を使用できます。
wireless_interface には、wireless0/0 ～ wireless0/3 を使用できます。

ワイヤレスインターフェースの使用不可

WebUI または CLI から特定のワイヤレスインターフェースを使用不可にできます。デフォルトでは、インターフェースを SSID にバインドすると、そのインターフェースが有効になります。この機能が利用できないプラットフォームがあります。

ワイヤレスインターフェースを使用不可にするには、次の手順のいずれかを実行します。

WebUI

Network > Interfaces > List > Deactivate（使用不可にするワイヤレスインターフェース）

CLI

set interface *wlan_if_name* shutdown

ワイヤレス構成情報の表示

ワイヤレスの構成と統計の詳細を表示できます。これらのコマンドは CLI から利用可能です。WebUI では利用できません。

WLAN 構成を表示するには、以下のコマンドを入力します。

```
device-> get wlan
AP software version: 5.0
AP bootrom version: 1..1
    Regulatory Domain is World,  Country Code is China
    ACL mode is disabled

WLAN   Mode   Antenna   Channel   Rate   Power  Super G
0      b/g    Diversity AUTO      11     full   Enabled
1      a      a         116 (5580)54     full   Disabled
```

ワイヤレスインターフェース関連付け情報を表示するには、以下のコマンドを入力します。

get interface *wlan_if_name* association [*mac_addr*]

WLAN のアクセス制御リスト（ACL）を表示するには、以下のコマンドを入力します。

get wlan acl

WLAN インターフェースのインターフェース詳細を表示するには、以下のコマンドを入力します。

get interface *wlan_if_name*

設定例

このセクションには、以下の構成例があります。

- 149 ページの「例 1: オープン認証および WEP 暗号化」
- 150 ページの「例 2: パスフレーズおよび自動暗号化を持っている WPA-PSK 認証」
- 150 ページの「例 3: 透過モードの WLAN」
- 154 ページの「例 4: 複数および差別化されたプロファイル」

例 1: オープン認証および WEP 暗号化

この例では、トランシーバが 1 つのセキュリティデバイスについて、**openwep** という名前の SSID が付いた BSS を作成し、それを wireless2 インターフェースにバインドします。この設定で WEP key-id が 1 に設定され、入力 ASCII 文字列は 40 ビットとなります。これにより誰でも認証できるようになりますが、WEP 鍵でコミュニケーションを暗号化するようになります。

WebUI

Wireless > SSID > New: 次のように入力してから **OK** をクリックします。

SSID: openwep

> WEP Key: 次のように入力してから **Back to SSID Edit** をクリックします。

Key ID: 1
Key Length: 40
Key String
ASCII: (**選択**), abcde
Add: (**選択**)

> WEP ベース認証および暗号化方式

Open: (**選択**)
WEP **暗号化** : (**選択**); Key Source: Local
Wireless Interface Binding: wireless2

Wireless > Activate Changes: Activate Changes ボタンをクリックします。

CLI

```
set ssid name openwep
set ssid openwep key-id 1 length 40 method ascii abcde
set ssid openwep authentication open encryption wep
set ssid openwep interface wireless2
exec wlan reactivate
```

例 2: パスフレーズおよび自動暗号化を持っている WPA-PSK 認証

この例では、トランシーバが 1 つのセキュリティデバイスについて、**wpapsk** という名前の SSID を作成し、それを wireless2 インターフェースにバインドします。これにより事前共有鍵と自動暗号化を持った Wi-Fi 保護アクセス認証 (WPA) を設定します。ネットワークにアクセスするために wireless2 インターフェースに接続したいワイヤレスクライアントは、ワイヤレス接続を確立する際に WPA パスフレーズ i7BB92-5o23iJ を使う必要があります。

WebUI

Wireless > SSID > New: 次のように入力してから **OK** をクリックします。

SSID: wpapsk

> WPA ベース認証方式

WPA Pre-shared Key: (**選択**)
Key by Password: (**選択**) i7BB92-5o23iJ
Confirm key by Password: i7BB92-5o23iJ
Encryption Type: Auto
Wireless Interface Binding: wireless2

Wireless > Activate Changes: Activate Changes ボタンをクリックします。

CLI

```
set ssid name wpapsk
set ssid wpapsk authentication wpa-psk passphrase i7BB92-5o23iJ encryption
    auto
set ssid wpapsk interface wireless2
exec wlan reactivate
```

例 3: 透過モードの WLAN

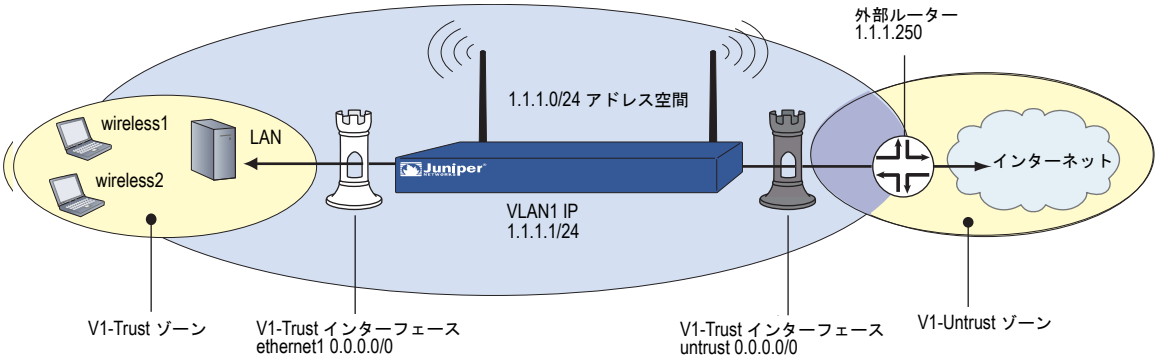
この例では、1 つの WLAN が、トランシーバが 1 つある透過モードのセキュリティデバイスに保護されています。管理トラフィックのセキュリティを高めるには、次のことを行います。

1. WebUI 管理のポート番号を 80 から 5555 に変え、CLI 管理の Telnet ポート番号を 23 から 4646 に変えます。

2. また、VLAN1 の IP アドレス 1.1.1.1/24 を使って、V1-Trust セキュリティゾーンからセキュリティデバイスを管理します。

3. さらに、外部ルーター向けのデフォルトルートを 1.1.1.250 と設定して、セキュリティデバイスからこの外部ルーター宛のアウトバウンド VPN トラフィックを送信できるようにします (V1-Trust ゾーン上のホストもすべて、デフォルトゲートウェイは 1.1.1.250 となります。)

図 23: 透過モードの WLAN デバイス



WebUI

1. **VLAN1 インターフェース**
   Network > Interfaces > Edit (VLAN1 インターフェース): 次のように入力してから **OK** をクリックします。

   IP Address/Netmask: 1.1.1.1/24
   Management Services: WebUI, Telnet (**選択**)
   Other Services: Ping (**選択**)

2. **ポートモード**
   Configuration > Port Mode: Port Mode ドロップダウンメニューで **Trust-Untrust** を選択します。

3. **HTTP ポート**
   Configuration > Admin > Management: HTTP Port フィールドに **5555** を入力してから、**Apply** をクリックします。

注 : デフォルトのポート番号は 80 です。不正アクセスを防ぐため、1,024 ～ 32,767 の範囲の適当な番号に変更するよう推奨します。変更後は、デバイス管理用にログインする際、Web ブラウザの URL フィールドに http://1.1.1.1:5555 を入力してください。

---

4. **インターフェース**
   Network > Interfaces > Edit (trust): 次のように入力してから **OK** をクリックします。

   Zone Name: V1-Trust
   IP Address/Netmask: 0.0.0.0/0

   Network > Interfaces > Edit (for untrust): 次のように入力してから **OK** をクリックします。

   Zone Name: V1-Untrust
   IP Address/Netmask: 0.0.0.0/0

Network > Interfaces > Edit (wireless1): 次のように入力してから **OK** をクリックします。

Zone Name: V1-Trust
IP Address/Netmask: 0.0.0.0/0

Network > Interfaces > Edit (wireless2): 次のように入力してから **OK** をクリックします。

Zone Name: V1-Trust
IP Address/Netmask: 0.0.0.0/0

5. **ゾーン**

V1-Trust 、V1-Untrust および VLAN ゾーンのデフォルト仮想ルーターは trust-vr です。

6. **SSID**

Wireless > SSID > New: 次のように入力してから **OK** をクリックします。

SSID: xparent-wpa

> WPA ベース認証方式

WPA Pre-shared Key: (**選択**)
Key by Password: (**選択**), 12345678
Confirm key by Password: 12345678
Encryption Type: TKIP
Wireless Interface Binding: wireless2

Wireless > SSID > New: 次のように入力してから **OK** をクリックします。

SSID: xparent-share

> WEP ベース認証および暗号化方式

> WEP Key: 次のように入力してから **Back to SSID Edit** をクリックします。

Key ID: 1
Key Length: 40
Key String
ASCII: (**選択**), abcde
Default Key: (**選択**)
Add: (**選択**)

> WEP ベース認証および暗号化方式

WEP Shared Key: (**選択**)
Wireless Interface Binding: wireless1

7. **ルート**

Network > Routing > Destination > trust-vr New: 次のように入力してから **OK** をクリックします。

Network Address/Netmask: 0.0.0.0/0
Gateway: (**選択**)
Interface: vlan1(trust-vr)
Gateway IP Address: 1.1.1.250
Metric: 1

8. ポリシー

Policies > (From: V1-Trust, To: V1-Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), Any
Service: ANY
Action: Permit

9. WLAN 構成をアクティブにする

Wireless > Activate Changes: Activate Changes ボタンをクリックします。

CLI

1. VLAN1

```
set interface vlan1 ip 1.1.1.1/24
set interface vlan1 manage web
set interface vlan1 manage telnet
set interface vlan1 manage ping
```

2. ポートモード

```
exec port-mode trust-untrust
```

3. HTTP ポート

```
set admin telnet port 4646
```

注 : デフォルトのポート番号は 23 番。不正アクセスを防ぐため、1,024 ～ 32,767 の範囲の適当な番号に変更するよう推奨します。Telnet を介してデバイス管理用に後にログインする際、次のアドレスを入力してください。1.1.1.1 4646.

---

4. インターフェース

```
set interface trust ip 0.0.0.0/0
set interface trust zone v1-trust
set interface untrust ip 0.0.0.0/0
set interface untrust zone v1-untrust
set interface wireless1 ip 0.0.0.0/0
set interface wireless1 zone v1-trust
set interface wireless2 ip 0.0.0.0/0
set interface wireless2 zone v1-trust
```

5. ゾーン

```
set zone V1-Trust vrouter trust-vr
set zone V1-Untrust vrouter trust-vr
set zone VLAN vrouter trust-vr
```

6. SSID

```
set ssid name xparent-wpa
set ssid xparent-wpa authentication wpa-psk passphrase 12345678 encryption
    tkip
set ssid xparent-wpa interface wireless2
set ssid name xparent-share
set ssid xparent-share key-id 1 length 40 method asciitext abcde default
set ssid xparent-share authentication shared-key
set ssid xparent-share interface wireless1
exec wlan reactivate
```

7. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway 1.1.1.250 metric 1

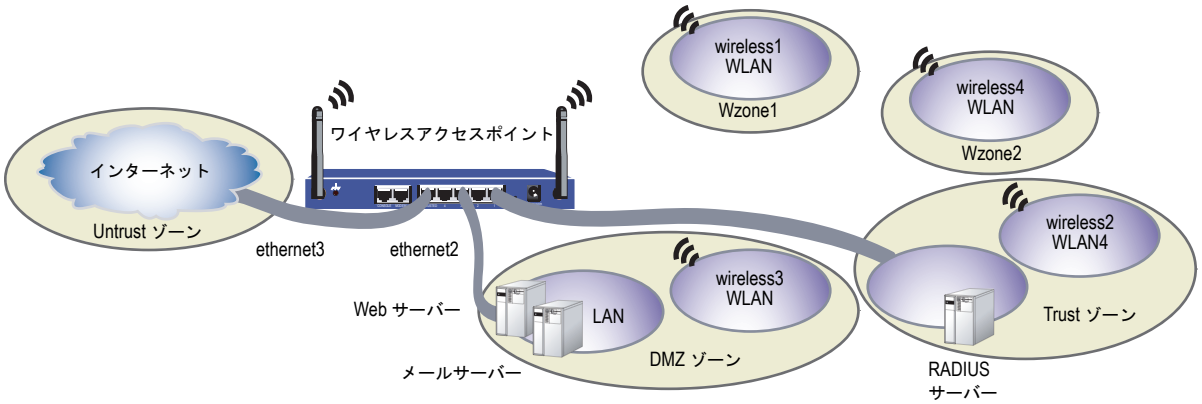
8. **ポリシー**
   set policy from v1-trust to v1-untrust any any any permit
   save

例 4: 複数および差別化されたプロファイル

この例では、それぞれが異なる名前、認証および暗号化スキームの 4 つの SSID を作成します。これらは、トランシーバが 1 つの拡張ポートモードのセキュリティデバイス用です。このモードでは以下のポート、インターフェース、ゾーンバインディングを備えています。

インターフェース	セキュリティゾーン	ベーシックサービスセット名
ethernet1 （ポート 1 と 2 ）	Trust	なし
ethernet2 （ポート 3 と 4 ）	DMZ	なし
ethernet3 (Untrust ポート)	Untrust	なし
wireless1	Wzone1	SSID: WPA 事前共有鍵付きの wzone1-wpa
wireless2	Trust	SSID: RADIUS サーバーを使った WPA 付きの trust-wpa
wireless3	DMZ	SSID: WEP 共有鍵付きの dmz-share
wireless4	Wzone2	SSID: WEP open/no 暗号化付きの wzone2-open

図 24: 複数および差別化されたプロファイル付きのワイヤレス



この例では次のことを行います。

1. ベーシックサービスセット (BSS) を設定します。これには SSID 名前の割り当て、暗号化と認証方式の設定およびのワイヤレスインターフェースを SSID にバインドすることが含まれています。

2. 各ワイヤレスインターフェースを DHCP サーバーの役割を果たすように設定し、それぞれの SSID のワイヤレスクライアントに対してアドレスを動的に割り当てるようにします。

3. wireless1 インターフェースに対して、ワイヤレスデバイス管理を使用可能にします。

4. ワイヤレスデバイスを構成して、WPA 暗号化のために RADIUS サーバーを使用するようにします。

5. それぞれのワイヤレスインターフェースに対して、ポリシーを作成します。

6. WLAN を再度アクティブにします。

この例では WebUI または CLI のどちらでも設定することができます。

WebUI

1. ベーシックサービスセットの設定

Wireless > SSID > New: 次のように入力してから **OK** をクリックします。

SSID: wzone1-wpa

> WPA ベース認証方式

WPA Pre-shared Key: (**選択**)
Key by Password: (**選択**), 12345678
Confirm key by Password: 12345678
Encryption Type: Auto
Wireless Interface Binding: wireless1

Wireless > SSID > New: 次のように入力してから **OK** をクリックします。

SSID: trust-wpa

> WPA ベース認証方式

WPA: (**選択**)
Encryption Type: Auto
Wireless Interface Binding: wireless2

Wireless > SSID > New: 次のように入力してから **OK** をクリックします。

SSID: dmz-share

> WEP ベース認証および暗号化方式

WEP Key: 次のように入力してから **Back to SSID Edit** をクリックします。

Key ID: 1
Key Length: 40
Key String
ASCII: (**選択**), abcde
Add: (**選択**)
WEP Shared Key: (**選択**)
Wireless Interface Binding: wireless3

Wireless > SSID > New: 次のように入力してから **OK** をクリックします。

SSID: wzone2-open

> WEP ベース認証および暗号化方式

Open: (選択)
No Encryption: (選択)
Wireless Interface Binding: wireless4

2. インターフェース

Network > Interfaces > Edit (ethernet3): 次のように入力してから **OK** をクリックします。

Obtain IP using DHCP: (選択)
Automatic update DHCP server parameters: (選択)

Network > Interfaces > Edit (wireless1): 次のように入力してから **OK** をクリックします。

IP Address/Netmask: 192.168.5.1/24

> Management Option

Management Services: WebUI, Telent, SSH, SNMP, SSL
Other Services: Ping

Network > DHCP > Edit (wireless1) > DHCP Server: 次のように入力してから **OK** をクリックします。

DHCP Server: (選択)
DHCP Server Mode: Enable
Lease: Unlimited
DNS#1: 192.168.5.30

> Addresses > New: 次のように入力してから **OK** をクリックします。

Dynamic: (選択)
IP Address Start: 192.168.5.2
IP Address End: 192.168.5.22

注 : デフォルトでは、デバイス管理は wireless2 に対して使用可能で、デフォルト IP アドレスは 192.168.2.1/24 です。

Network > DHCP > Edit (wireless2) > DHCP Server: 次のように入力してから **OK** をクリックします。

DHCP Server: (選択)
DHCP Server Mode: Enable
Lease: Unlimited

> Addresses > New: 次のように入力してから **OK** をクリックします。

Dynamic: (選択)
IP Address Start: 192.168.2.2
IP Address End: 192.168.2.22

Network > Interfaces > Edit (wireless3): IP Address/Netmask フィールドに **192.168.3.1/24** と入力し、**OK** をクリックします。

Network > DHCP > Edit (wireless3) > DHCP Server: 次のように入力してから **OK** をクリックします。

DHCP Server: (選択)
DHCP Server Mode: Enable
Lease: Unlimited

> Addresses > New: 次のように入力してから OK をクリックします。

Dynamic: (選択)
IP Address Start: 192.168.3.2
IP Address End: 192.168.3.22

Network > Interfaces > Edit (wireless4): IP Address/Netmask フィールドに **192.168.4.1/24** と入力し、**OK** をクリックします。

Network > DHCP > Edit (wireless4) > DHCP Server: 次のように入力してから **OK** をクリックします。

DHCP Server: (選択)
DHCP Server Mode: Enable
Lease: Unlimited

> Addresses > New: 次のように入力してから **OK** をクリックします。

Dynamic: (選択)
IP Address Start: 192.168.4.2
IP Address End: 192.168.4.22

3. RADIUS 認証サーバー

Configuration > Auth > Servers > New: 次のように入力してから **OK** をクリックします。

Name: radius1
IP/Domain Name: 192.168.1.50
Backup1: 192.168.1.60
Backup2: 192.168.1.61
Timeout: 30
Account Type: 802.1X
RADIUS: (選択)
Shared Secret: 456htYY97kl

4. ポリシー

Policies > (From: Wzone1, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), Any

Service: ANY
Action: Permit

Policies > (From: Wzone1, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), Any
Service: ANY
Action: Permit

Policies > (From: Wzone2, To: Untrust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), Any
Service: ANY
Action: Permit

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), Any
Service: HTTP
Action: Permit

Policies > (From: Untrust, To: DMZ) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), Any
Service: MAIL
Action: Permit

5. WLAN 構成をアクティブにする

Wireless > Activate Changes: Activate Changes ボタンをクリックします。

CLI

1. ベーシックサービスセット

```
set ssid name wzone1-wpa
set ssid wzone1-wpa authentication wpa-psk passphrase 12345678 encryption
    auto
set ssid wzone1-wpa interface wireless1

set ssid name trust-wpa
set ssid trust-wpa authentication wpa encryption auto
set ssid trust-wpa interface wireless2

set ssid name dmz-share
```

```
set ssid dmz-share key-id 1 length 40 method ascii abcde
set ssid dmz-share authentication shared-key
set ssid dmz-share interface wireless3

set ssid name wzone2-open
set ssid wzone2-open authentication open encryption none
set ssid wzone2-open interface wireless4
```

2. **インターフェース**

```
set interface ethernet3 dhcp client settings update-dhcp server
set interface ethernet3 dhcp client

set interface wireless1 ip 192.168.5.1/24
set interface wireless1 route
set interface wireless1 ip manageable
set interface wireless1 dhcp server service
set interface wireless1 dhcp server enable
set interface wireless1 dhcp server option gateway 192.168.5.1
set interface wireless1 dhcp server option netmask 255.255.255.0
set interface wireless1 dhcp server option dns1 192.168.5.30
set interface wireless1 dhcp server ip 192.168.5.2 to 192.168.5.22

set interface wireless2 dhcp server ip 192.168.2.2 to 192.168.2.22

set interface wireless3 ip 192.168.3.1/24
set interface wireless3 dhcp server ip 192.168.3.2 to 192.168.3.22

set interface wireless4 ip 192.168.4.1/24
set interface wireless4 dhcp server ip 192.168.4.2 to 192.168.4.22
```

3. **RADIUS 認証サーバー**

```
set auth-server radius1 server-name 192.168.1.50
set auth-server radius1 type radius
set auth-server radius1 account-type 802.1X
set auth-server radius1 backup1 192.168.1.60
set auth-server radius1 backup2 192.168.1.61
set auth-server radius1 timeout 30
set auth-server radius1 radius secret A56htYY97kl
```

4. **ポリシー**

```
set policy from wzone1 to untrust any any any permit
set policy from wzone1 to dmz any any any permit
set policy from wzone2 to untrust any any any permit
set policy from untrust to dmz any any http permit
set policy from untrust to dmz any any mail permit
```

5. **WLAN 構成をアクティブにする**

```
exec wlan reactivate
```

索引

A

AAL5 カプセル化 66
AAL5 複合 74
ACL 133
ADSL
    VPN トンネル 99
    インターフェースの構成 74
    概要 74
ATM 67
ATM Adaptation Layer 5 74

C

C ビットパリティモード 13
CSU 互換性、T3 インターフェース 20

D

Discrete multitone
    DMT を参照
DMT 69, 70

I

IP トラッキング 111
ISP
    Priority 109
    フェールオーバーホールドダウンタイマー 110
ISP IP アドレスとネットマスク 73

P

Point-to-Point Protocol over ATM
    PPPoA を参照
Point-to-Point Protocol over Ethernet
    PPPoE を参照
PPP 66
PPPoA 66, 68, 74
PPPoE 66, 74

R

route tracking 111

S

SSID
    ワイヤレスインターフェースへのバインド 146
Super G 134

T

T3 インターフェース
    C ビットパリティモード 13
    CSU 互換性 20
tunnel tracking 111

V

VC 66
VCI 66
VPI 66
VPI/VCI
    値 74
    構成 71
VPN 監視 112

W

WEP 123
Wired Equivalent Privacy （有線と同等のプライバシー）
    WEP を参照
WLAN
    DTIM 142
    Super G の構成 134
    WMM 136
    XR 135
    アクセス制御リスト 133
    暗号化と認証 122
    エージング間隔 140
    拡張チャネル 132
    国コードおよびチャネル 131
    構成、再起動 134
    サイトの調査 132
    詳細なパラメーター 140
    スロット時間 145
    送信可速度 144
    送信可タイプ 144
    送信可モード 144
    送信要求しきい値 143
    バーストしきい値 142
    ビーコン間隔 141
    フラグメントしきい値 143
    プリアンブル長 145
    ブリッジグループ 147
    利用可能なチャネルの発見 133
    ワイヤレス構成情報の表示 148

WLAN WAP 動作モード
802.11b クライアント、構成 119, 120
802.11g クライアント、構成 119
WLAN、ワイヤレスインターフェース
バインド 146
WMM
アクセスのカテゴリ 136
サービス品質の構成 136
使用可能 136
デフォルトの設定 137

X

XR、構成 135

あ

アクセス制御リスト
ACL を参照
暗号化と認証
Wi-Fi Protected Access （Wi-Fi 保護アクセス）
WPA を参照
Wired Equivalent Privacy （有線と同等のプライバシー）
WEP を参照
複数の WEP 鍵 123

い

委託管理者 109

か

拡張チャネル、WLAN 用の設定 132
仮想回路
VC を参照
仮想チャンネル識別子
VCI を参照
VPI を参照
仮想パス識別子 / 仮想チャネル識別子
VPI/VCI を参照

く

国コードおよびチャネル 131
国コードとチャネル、規制されているドメインの 131

こ

構成
ADSL 2/2 + PIM 74
VPI/VCI ペア 71
仮想回路 71
互換性モードのオプション
T3 インターフェース 20

さ

サービスプロバイダ、からの情報 65
サイトの調査 132
サブレートオプション 20

せ

静的 IP アドレス 74

ち

チャネル、利用可能なものの発見 133
チャレンジハンドシェイク式認証プロトコル 36

に

認証と暗号化、RADIUS サーバーを使用した 124

ひ

非同期転送モード
ATM を参照

ふ

複合、構成 71
物理インターフェース
C ビットパリティモード 13
CSU 互換性 20

わ

ワイヤレスインターフェース
SSID のバインド 146
構成 146
使用不可 148
トランシーバへのバインド 146
ワイヤレスブリッジグループ 147
ワイヤレス ローカル エリア ネットワーク
WLAN を参照

概念と用例
ScreenOS リファレンス ガイド

第 13 部 :
ジェネラルパケットラジオサービス

リリース 6.0.0、改訂 02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

品番 : 530-017779-01-JP, 改訂 02

Copyright Notice

Copyright © 2007 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

目次

本編について v

ドキュメントの規則 v
Web ユーザーインターフェースの規則 v
コマンドラインインターフェースの規則 vi
ネーミング規則および文字タイプ vi
説明図の規則 vii
技術ドキュメンおよびテクニカルサポート viii

第 1 章 GPRS 1

GPRS トンネリングプロトコルファイアウォールとしてのセキュリティデバイス 2
Gp と Gn インターフェース 3
Gi インターフェース 3
動作モード 4
仮想システムサポート 5
ポリシーベースの GPRS トンネリングプロトコル 5
例 : GTP 検査を使用可能にするポリシーの構成 6
GPRS トンネリングプロトコル検査オブジェクト 7
例 : GTP 検査オブジェクトの作成 8
GTP メッセージフィルタリング 8
パケットサニティチェック 9
メッセージ長のフィルタリング 9
例 : GTP メッセージ長の設定 9
メッセージタイプのフィルタリング 10
例 : メッセージタイプの許可および拒否 10
サポートされているメッセージタイプ 11
メッセージレートの制限 12
例 : レート制限の設定 13
シーケンス番号検証 13
例 : シーケンス番号検証を使用可能にする 13
IP フラグメント化 14
GTP-in-GTP パケットフィルタリング 14
例 : GTP-in-GTP パケットフィルタリングを使用可能にする 14
徹底監視 (Deep Inspection) 14
例 : 徹底監視を TEID で使用可能にする 14
GTP 情報要素 15
アクセスポイント名のフィルタリング 15
例 : APN と選択モードの設定 16
IMSI プレフィックスフィルタリング 17
例 : IMSI プレフィックスとフ APN フィルタを組み合わせて設定する 17
無線アクセス技術 18
例 : RAT および APN フィルタの設定 18

GTP 情報要素（続き）
ルーティングエリアアイデンティティとユーザーロケーション情報 ... 18
例 : RAI および APN フィルタの設定 ... 19
例 : ULI および APN フィルタの設定 ... 19
APN Restriction ... 19
IMEI-SV ... 19
例 : IMEI-SV および APN フィルタの設定 ... 20
プロトコルおよびシグナリング要件 ... 20
IE フィルタリングの組み合わせのサポート ... 21
サポートされる R6 情報要素 ... 22
3GPP R6 IE の排除 ... 24
例 : R6 の排除 ... 24
GTP トンネル ... 24
GTP トンネル制限 ... 24
例 : GTP トンネル制限の設定 ... 24
パケット状態監視 ... 25
GTP トンネル確立および終了 ... 25
SGSN 間ルーティングエリアの更新 ... 25
高可用性のためのトンネルフェールオーバー ... 26
放置された GTP トンネルのクリーンアップ ... 26
例 : GTP トンネルのタイムアウトの設定 ... 26
SGSN と GGSN 転送 ... 27
過大請求攻撃の回避 ... 27
過大請求攻撃の説明 ... 27
過大請求攻撃の防御 ... 29
例 : 過大請求攻撃を回避するための設定 ... 30
GTP トラフィック監視 ... 32
トラフィックロギング ... 32
例 : GTP パケットロギングを使用可能にする ... 33
トラフックカウンティング ... 34
例 : GTP トラリフィックカウンティングを使用可能にする ... 34
法に順守した傍受 ... 35
例 : 法に順守した傍受を使用可能にする ... 35

索引 ... IX-I

本編について

第 13 部: ジェネラルパケットラジオサービス は GPRS テクノロジーに関して、高度な知識をお持ちの GPRS ネットワークオペレータ用です。

本編では ScreenOS の GTP 機能を説明し、GTP 機能性を Juniper Networks セキュリティデバイスで構成する方法を示します。以下の章があります。

- 第 1 章「GPRS」、では ScreenOS の GPRS トンネリングプロトコル (GTP) 機能を説明し、GTP 機能性を Juniper Networks セキュリティデバイスで構成する方法を示します。

ドキュメントの規則

このドキュメントは、次のセクションで説明されている規則を使用しています。

- v ページの「Web ユーザーインターフェースの規則」
- vi ページの「コマンドラインインターフェースの規則」
- vi ページの「ネーミング規則および文字タイプ」
- vii ページの「説明図の規則」

Web ユーザーインターフェースの規則

WebUI（Web ユーザーインターフェース）では、各作業の操作指示は、操作手順と構成設定値に分かれています。構成設定を入力できる WebUI ページを開くには、画面の左側にあるナビゲーション ツリーのメニュー項目をクリックして、そのページに移動します。先へ進むと、ナビゲーション パスが画面の上部に表示されます。各ページは角括弧で分離されています。

WebUI のパスおよびアドレスを定義するためのパラメータは、以下のとおりです。

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

```
Address Name: addr_1
IP Address/Domain Name:
    IP/Netmask: ( 選択 ), 10.2.2.5/32
Zone: Untrust
```

構成設定のオンラインヘルプを開くには、画面の左上にある疑問符（?）をクリックします。

ナビゲーションツリーにも、Help > Config Guide 構成ページがあり、セキュリティポリシーおよび IPSec （インターネットプロトコルセキュリティ）の構成に役立ちます。ドロップダウンメニューからオプションを選択して、そのページの指示に従います。構成設定のオンラインヘルプを開くには、左上にある **?** 文字をクリックします。

コマンドラインインターフェースの規則

次の規則は、例とテキストにおいて、コマンドラインインターフェース（CLI）コマンドの構文を示すために使用されます。

例においては、次のように使用されます。

- 角括弧 [ ] 内にあるものはすべてオプションです。
- 中括弧 { } 内にあるものはすべて必須です。
- 選択肢が複数ある場合、各選択肢はパイプ (|) で区切られています。例えば、次のように表示されます。

  set interface { ethernet1 | ethernet2 | ethernet3 } manage

- 変数は*斜体*で表示されます。

  set admin user *name1* password *xyz*

テキストにおいては、コマンドは**太字**で、変数は*斜体*で表示されます。

注 : キーワード入力時には、単語を間違いなく識別できる数の文字を入力すれば十分です。**set admin user wheezer j12fmt54** というコマンドを入力する際には、**set adm u whee j12fmt54** と入力するだけで十分です。ただし、本編に記載されたコマンドはすべて本来の形式で記載されています。

ネーミング規則および文字タイプ

ScreenOS はオブジェクトの名前 (アドレス、管理ユーザー、認証サーバー、IKE ゲートウェイ、仮想システム、VPN トンネルおよびゾーンなど、ScreenOS 構成に定義されているもの) に関して、次の規則に従います。

- 名前文字列に 1 つまたは複数のスペースが含まれる場合、文字列全体を二重引用符で囲む必要があります。例 :

  set address trust “local LAN” 10.1.1.0/24

- 二重引用符で囲まれた文字列の先頭または末尾のスペースを取り除きます。たとえば、「 **local LAN** 」は「**local LAN**」となります。
- 連続した複数のスペースは、一つのスペースとして扱われます。
- CLI キーワードの多くはケースセンシティブではありませんが、名前文字列はケースセンシティブです。たとえば、「**local LAN**」は「**local lan**」とは異なります。

ScreenOS は、次の文字タイプをサポートします。

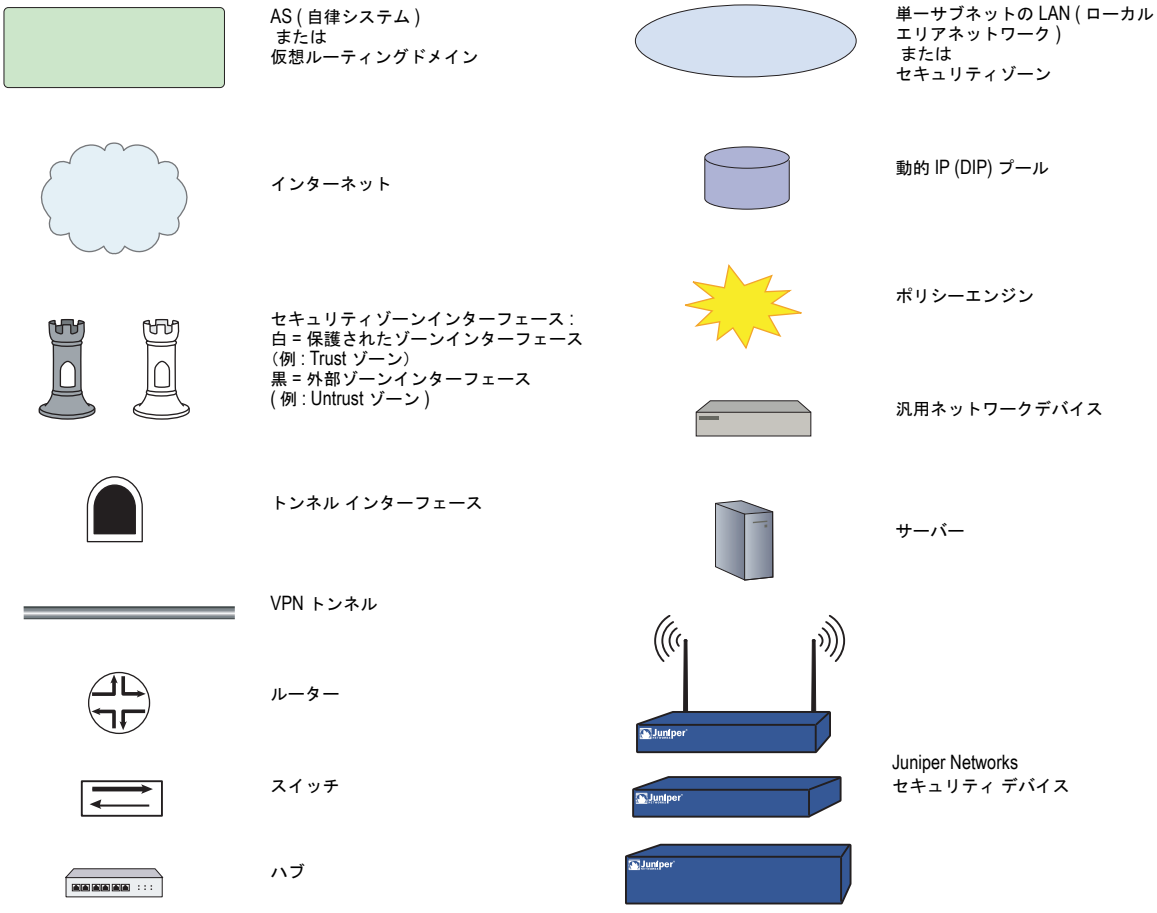
- 1 バイト文字セット (SBCS) およびマルチバイト文字セット (MBCS)。SBCS の例に、ASCII、欧州言語、およびヘブライ語があります。2 バイト文字セット (DBCS) とも呼ばれる MBCS の例に、中国語、韓国語、および日本語があります。
- ASCII 文字の 32（16 進数の 0x20）から 255（0xff)。ただし二重引用符 (") は、スペースを含む名前文字列の先頭と末尾を示す特殊な意味をもつため、例外とします。

注： コンソール接続では、SBCS のみがサポートされます。ご利用のブラウザがサポートする文字セットに応じて、WebUI は SBCS および MBCS の両方をサポートします。

説明図の規則

次の図は、本編を通して説明図に使用されている画像の基本的なものです。

図 1: 説明図の画像



技術ドキュメンおよびテクニカルサポート

Juniper Networks 製品のいずれかの技術ドキュメントを入手するには、www.juniper.net/techpubs/ をご覧になってください。

テクニカルサポートについては、http: //www.juniper.net/customers/support/ にある Case Manager を使って事例サポートを開くか、1-888-314-JTAC (米国内) か 1-408-745-9500 (その他の国) までお問い合わせください。

本書に間違いや欠落があった場合は、techpubs-comments@juniper.net までお知らせください。

第 1 章
GPRS

ジェネラルパケットラジオサービス (GPRS) ネットワークは複数の外部ネットワークに接続し、その中にはローミングパートナー、企業顧客、GPRS ローミングエクスチェンジ (GRX) プロバイダそしてパブリックインターネットが含まれています。GPRS ネットワークのオペレータは、自分のネットワークを保護すると同時に、これらの外部ネットワークを行き来する際のアクセスを提供しながらコントロールするという難題に直面しています。Juniper Networks では GPRS ネットワークオペレータの障害となっているセキュリティ問題の多くに対して、ソリューションを提供しています。

GPRS アーキテクチャにおいて、オペレータのネットワークへのセキュリティ脅威の基本的原因は、GPRS トンネリングプロトコル (GTP) 固有のセキュリティの欠如にあります。GTP は GPRS サポートノード間で使用されるプロトコル (GSN) です。異なる GPRS ネットワーク間でのコミュニケーションはセキュアではありません、というのは GTP が認証、データの信頼性あるいは機密保護をまったく提供しないからです。ローミングパートナー間の接続にインターネットプロトコルセキュリティ (IPSec) を実施し、トラフィックレートを制限し、状態監視を使用することにより GTP のセキュリティリスクの大半を取り除くことができます。Juniper Networks セキュリティデバイスは Gp 、Gn および Gi インターフェース上のさまざまな攻撃を軽減します。ScreenOS の GTP ファイアウォールの機能は、移動するオペレータのネットワークの主なセキュリティ問題に対応しています。

注 : ISG 2000 デバイスのみが GTP 機能をサポートしています。

この章では ScreenOS がサポートしている GTP 機能を説明し、Juniper Networks セキュリティデバイス上での設定のしかたについて示します。本章のセクションは、以下のようになります。

- 2 ページの「GPRS トンネリングプロトコルファイアウォールとしてのセキュリティデバイス」
- 5 ページの「ポリシーベースの GPRS トンネリングプロトコル」
- 7 ページの「GPRS トンネリングプロトコル検査オブジェクト」
- 8 ページの「GTP メッセージフィルタリング」
- 15 ページの「GTP 情報要素」
- 27 ページの「SGSN と GGSN 転送」
- 27 ページの「過大請求攻撃の回避」
- 32 ページの「GTP トラフィック監視」

GPRS トンネリングプロトコルファイアウォールとしてのセキュリティデバイス

GPRS トンネリングプロトコル（GTP）は、個々の移動式端末（MS）、サービング GPRS サポートノード（SGSN）とゲートウェイ GPRS サポートノード（GGSN）間に、GTP トンネルを確立するために使用されます。GTP トンネルは GSN 間のセキュアなチャンネルで、2 つのホストがデータを交換できます。SGSN は MS からパケットを受け取り GTP トンネルを通して GGSN に転送する前に GTP ヘッダー内にカプセル化します。GGSN がパケットを受け取ると、脱カプセル化し、外部ホストに転送します。

Juniper Networks GTP ライセンス セキュリティデバイスは次のタイプの GPRS インターフェースに対して、ファイアウォールによる保護を提供します。

- Gn - Gn インターフェースは、同じ PLMN (Public Land Mobile Network) 内の SGSN と GGSN 間のインターフェースです。
- Gp - Gp インターフェースは、2 つの PLMN (Public Land Mobile Network) 間の接続部です。
- Gi - Gi インターフェースは GGSN とインターネットまたは PLMN に接続されている宛先ネットワークとの接続部です。

注： *インターフェース*という用語は ScreenOS および GPRS テクノロジーにおいては、異なる意味を持ちます。ScreenOS では、インターフェースはセキュリティゾーンへの出入口のようなもので、トラフィックのゾーンへの出入りを許可します。GPRS では、インターフェースは GPRS インフラの 2 つのコンポーネント間の接続部あるいは参照点のことを指します（ SGSN や GGSN など）。

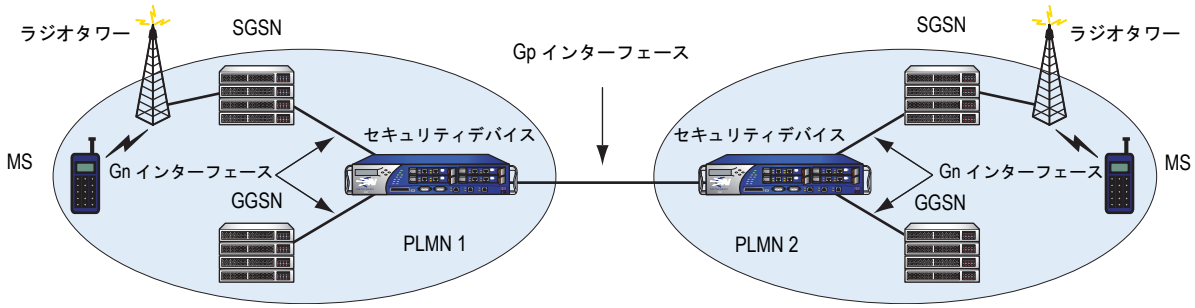
Gp と Gn インターフェース

Gn インターフェースにセキュリティデバイスを実装すると、SGSN や GGSN といった主要なネットワーク資産を保護することができます。Gn インターフェースの GTP トンネルをセキュアにするには、共通の PLMN 内にセキュリティデバイスを SGSN と GGSN の間に置きます。

Gp インターフェースにセキュリティデバイスを実装すると、PLMN を他の PLMN から保護することができます。Gp の GTP トンネルをセキュアにするには、PLMN の SGSN と GGSN をセキュリティデバイスの後に置きます。こうすることによって、行き来するすべてのトラフィックはファイアウォールを通ることになります。

図 2 は Gp インターフェースおよび Gn インターフェースにおいて、PLMN を保護するために Juniper Networks セキュリティデバイスを実装した図です。

図 2: Gp と Gn インターフェース



Gi インターフェース

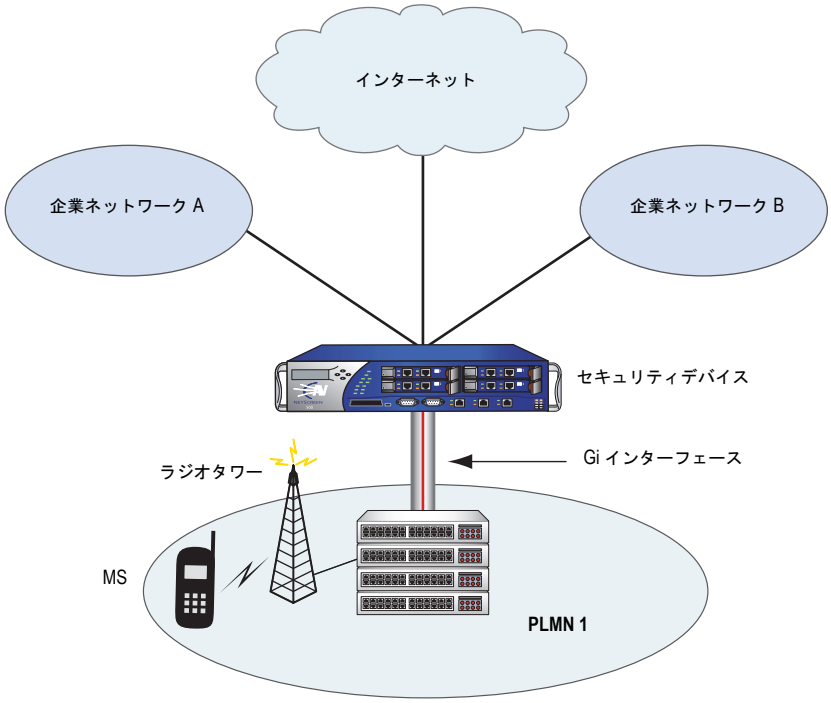
Gi インターフェースにセキュリティデバイスを実装すると、複数のネットワークに対して同時にトラフィックを制御し、PLMN をインターネットおよび外部ネットワークから保護し、移動ユーザーをインターネットやその他のネットワークから守ります。ScreenOS は多数の仮想ルーターを提供するので顧客ネットワークごとに 1 つの仮想ルーターを使用することが可能となり、それによりそれぞれの顧客ネットワークのトラフィックを分離することができます。

セキュリティデバイスは、IPSec バーチャルプライベートネットワーク（VPN）トンネル用のレイヤー 2 トンネリングプロトコル（L2TP）を使用して、パケットをインターネットや宛先ネットワークにセキュアな状態で転送できます。（ただし、Juniper Networks セキュリティデバイスは、full L2TP はサポートしていません。）

仮想ルーターの機能や能力の詳細は、*第 7 部: ルーティング* を参照してください。

図 3 は Gi インターフェースの PLMN を守るためのセキュリティデバイスの実装を示す図です。

図 3: Gi インターフェース



動作モード

ScreenOS は GTP において 2 つのインターフェース動作モードをサポートします。透過モードとルートモードです。セキュリティデバイスをネットワークのルーティングインフラに参加させたい場合、ルートモードで使用することができます。これにはネットワークのデザイン変更がいくらか必要となります。代わりに、ネットワーク全体を再設定することなく、既存のネットワークにおいてセキュリティデバイスを透過モードで実装することもできます。透過モードでは、セキュリティデバイスはレイヤー 2 スイッチまたはブリッジの役割を果たし、インターフェースの IP アドレスは 0.0.0.0 に設定され、セキュリティデバイスはユーザーに対して見えない、つまり*透明*になります。

GTP 検査が使用可能になっていないインターフェースおよびポリシーに対して、ScreenOS はネットワークアドレス変換 (NAT) をサポートします。

ScreenOS では現時点において、透過モードはアクティブ ñ パッシブ高可用性 (HA) のみをサポートします。これはアクティブ パッシブおよびアクティブ アクティブ HA をサポートするルートモードとは違います。

動作モードおよび高可用性の詳細については、「第 2 部 : 基本」と 「第 11 部 : 高可用性」をそれぞれ参照してください。

仮想システムサポート

Juniper Networks セキュリティデバイスは仮想システム (vsys) において GTP 機能を完全にサポートします。しかしながら、リソースを節約するために、10 を超える vsys はお使いにならないことをお奨めします。

ポリシーベースの GPRS トンネリングプロトコル

デフォルトでは、セキュリティデバイスが保護している PLMN は Trust ゾーンにあります。セキュリティデバイスは Trust ゾーンの PLMN を他のゾーンの PLMN から守ります。守ろうとしているご自分の PLMN が対象としている PLMN すべてを Untrust ゾーンに入れることもできますが、それぞれの PLMN に対して、ユーザー定義のゾーンを作成することもできます。PLMN は 1 つまたは複数のセキュリティゾーンを占めることができます。

ポリシーを作成して、ゾーンと PLMN の間をトラフィックがフローできるようにします。ポリシーにはトラフィックを許可、拒否またはトンネルするルールが含まれています。セキュリティデバイスは GTP トラフィックを制御する GTP ポリシーに対して、すべての GTP パケットを点検して GTP ポリシーフィルターを行い、これらのポリシーに従い、パケットを転送、ドロップまたはトンネルします。

ポリシーの GTP サービスを選択して、セキュリティデバイスが GTP トラフィックを許可、拒否またはトンネルするようにします。しかしながら、これではデバイスは GTP トラフィックを検査しません。セキュリティデバイスが GTP トラフィックを検査するには、ポリシーに対して *GTP 検査オブジェクト*とも呼ばれている GTP 設定を適用します。

ポリシーに GTP 設定を適用する前に、まず GTP 検査オブジェクトを作成する必要があります（7 ページの「GPRS トンネリングプロトコル検査オブジェクト」を参照）。1 つのポリシーに対して 1 つの GTP 検査オブジェクトしか適用できません。ただし 1 つの GTP 検査オブジェクトを複数のポリシーに適用することはできます。ポリシーを使って、SGSN などの特定のピアから GTP トンネルの確立を許可または拒否できます。

ソースまたは宛先ゾーンを「Any」としてポリシーを設定することもできます (これによりゾーン内のすべてのホストが含まれます)。また、複数のソースおよび宛先アドレスを指定するポリシーを設定することもできます。

トラフィックロギングやトラフィックカウントなどの機能をポリシーで使用可能にすることもできます。ポリシーの詳細については、「第 2 部 : 基本」を参照してください。

例: GTP 検査を使用可能にするポリシーの構成

この例ではインターフェースを設定し、アドレスおよび 2 つのポリシーを作成し、同じ PLMN 内の 2 つのネットワーク間の双方向トラフィックを許可します。またポリシーに対して GTP 検査オブジェクトを適用します。

WebUI

1. **GTP 検査オブジェクト**
   Objects > GTP > New: 以下を入力して **Apply** をクリックします。

   GTP Name: GPRS1

2. **インターフェース**
   Network > Interfaces > Edit (ethernet1/1): 以下を入力して **Apply** をクリックします。

   Zone Name: Trust
   IP Address/Netmask: 10.1.1.1/24

   Network > Interfaces > Edit (ethernet1/2): 次のように入力してから **OK** をクリックします。

   Zone Name: Untrust
   IP Address/Netmask: 1.1.1.1/24

3. **アドレス**
   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: local-GGSN
   IP Address/Domain Name:
   IP/Netmask: (選択), 10.1.1.0/24
   Zone: Trust

   Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

   Address Name: remote-SGSN
   IP Address/Domain Name:
   IP/Netmask: (選択), 1.2.2.5/32
   Zone: Untrust

4. **ポリシー**
   Policies > (From: Trust, To: Untrust) > New: 次のように入力してから **OK** をクリックします。

   Source Address:
   Address Book Entry: (選択), local-GGSN
   Destination Address:
   Address Book Entry: (選択), remote-SGSN
   Service: GTP
   GTP Inspection Object: GPRS1 (選択)
   Action: Permit

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), remote-SGSN
Destination Address:
Address Book Entry: (選択), local-GGSN
Service: GTP
GTP Inspection Object: GPRS1 (選択)
Action: Permit

CLI

1. **GTP 検査オブジェクト**
   set gtp configuration gprs1
   (gtp:gprs1)-> exit
   save

2. **インターフェース**
   set interface ethernet1/1 zone trust
   set interface ethernet1/1 ip 10.1.1.1/24
   set interface ethernet1/2 zone untrust
   set interface ethernet1/2 ip 1.1.1.1/24

3. **アドレス**
   set address trust local-ggsn 10.1.1.0/32
   set address untrust remote-sgsn 2.2.2.5/32

4. **ポリシー**
   set policy from trust to untrust local-ggsn remote-sgsn gtp permit
   システムはポリシー ID を返します、例えば : policy id = 4.

   set policy id 4 gtp gprs1
   set policy from untrust to trust remote-sgsn local-ggsn gtp permit

   システムはポリシー ID を返します、例えば : policy id = 5.

   set policy id 5 gtp gprs1
   save

GPRS トンネリングプロトコル検査オブジェクト

セキュリティデバイスが GPRS トンネリングプロトコル (GTP) トラフィックの検査を行うには、GTP 検査オブジェクトを作成し、ポリシーに適用します。GTP 検査オブジェクトは柔軟性が高く、異なる設定を実施する複数のポリシーを設定することができます。セキュリティデバイスがソース、宛先ゾーン、アドレス、アクションなどに基づいて GTP トラフィックを異なる方法で制御するように構成できます。

GTP 機能を構成するには、最初に GTP 構成のコンテキストを入力する必要があります。CLI の設定を保存するには、最初に GTP 構成を終了し、**save** コマンドを入力します。

例: GTP 検査オブジェクトの作成

この例では LA-NY という名前の GTP 検査オブジェクトを作成します。デフォルト値のほとんどはそのままにしますが、シーケンス番号検証と GTP-in-GTP Denied 機能を使用可能にします。

WebUI

Objects > GTP > New: 以下を入力して **Apply** をクリックします。

GTP Name: LA-NY
Sequence Number Validation: (**選択**)
GTP-in-GTP Denied: (**選択**)

CLI

```
set gtp configuration la-ny
(gtp:la-ny)-> set seq-number-validated
(gtp:la-ny)-> set gtp-in-gtp-denied
(gtp:la-ny)-> exit
save
```

GTP メッセージフィルタリング

セキュリティデバイスが GTP パケットを受け取ると、デバイスで設定したポリシーとパケットを照合します。パケットがポリシーに適合すると、デバイスはポリシーに適用されている GTP 構成に従ってパケットを検査します。パケットが GTP 構成パラメータに一つでも合致しない場合、デバイスはパケットをドロップします。

このセクションでは GTP 構成の機能を説明し、それを使ってセキュリティデバイスがどのようにして GTP トラフィック検査を行うか説明します。本章のセクションは、以下のようになります。

- 「パケットサニティチェック」
- 9 ページの「メッセージ長のフィルタリング」
- 10 ページの「メッセージタイプのフィルタリング」
- 12 ページの「メッセージレートの制限」
- 13 ページの「シーケンス番号検証」
- 14 ページの「IP フラグメント化」
- 14 ページの「GTP-in-GTP パケットフィルタリング」
- 14 ページの「徹底監視 (Deep Inspection)」

パケットサニティチェック

セキュリティデバイスは各パケットについて GTP サニティチェックを行い、パケットが有効な UDP および GTP パケットであるか判断します。サニティチェックは、GPRS サポートノード (GSN) リソースが不正な GTP パケットを処理することを防いで、GSN リソースを保護します。

GTP パケットサニティチェックを行う際、セキュリティデバイスは次の項目に対して各 GTP パケットのヘッダーを確認します。

- GTP リリースバージョン番号 - ScreenOS はバージョン 0 と 1 をサポートします（GTP を含む）。
- 事前定義されたビットの適切な設定 - どの事前定義されたビットを確認するかは、GTP リリース バージョン番号によります。
- プロトコルタイプ - バージョン 1 用（ GTP を含む）
- UDP/TCP パケット長

パケットが UDP 基準および GTP 基準に合わない場合は、セキュリティデバイスはパケットをドロップするので、不正なトラフィックあるいは偽造されたトラフィックの転送が防止されます。セキュリティデバイスは自動的に GTP パケットサニティチェックを行うので、この機能を設定する必要はありません。

注 : Juniper Networks は 3GPP（3rd Generation Partnership Project) により確立された GTP 基準を満たします。これらの基準の詳細は、次の技術仕様ドキュメントを参照してください。

- 3GPP TS 09.60 v6.9.0 (2000-09)
- 3GPP TS 29.060 v3.8.0 (2001-03)
- 3GPP TS 32.015 v3.9.0 (2002-03)

メッセージ長のフィルタリング

指定した最小または最長メッセージ長に満たないパケットをセキュリティデバイスがドロップするように設定できます。GTP ヘッダーにおいて、メッセージ長フィールドには GTP ペイロードの長さがオクテットで示してあります。GTP ヘッダー自体の長さ、UDP ヘッダーおよび IP ヘッダーは含まれていません。GTP メッセージ長のデフォルト最小、最大値はそれぞれ 0 と 1452 です。

例 : GTP メッセージ長の設定

この例では、GPRS GTP 検査オブジェクトに対して最小 GTP メッセージ長を 8 オクテットとし、最大 GTP メッセージ長を 1200 オクテットに設定します。

WebUI

Objects > GTP > Edit (GPRS1): 以下を入力して **Apply** をクリックします。

```
Minimum Message Length: 8
Maximum Message Length: 1200
```

CLI

```
set gtp configuration gprs1
(gtp:gprs1)-> set min-message-length 8
(gtp:gprs1)-> set max-message-length 1200
(gtp:gprs1)-> exit
save
```

メッセージタイプのフィルタリング

セキュリティデバイスを設定して、GTP パケットをフィルタし、メッセージタイプに基づいて許可または拒否することができます。デフォルトとして、セキュリティデバイスはすべての GTP メッセージタイプを許可します。

GTP メッセージタイプには 1 つまたは多くのメッセージが含まれています。あるメッセージタイプを許可または拒否すると、自動的に指定したタイプのすべてのメッセージが許可または拒否されます。たとえば、**sgsn-context** メッセージタイプをドロップするように選択すると、**sgsn context request** 、**sgsn context response** 、**gsn context acknowledge** メッセージがドロップされます。メッセージタイプの詳細については、11 ページの「サポートされているメッセージタイプ」を参照してください。

GTP バージョン番号に基づいてメッセージタイプを許可または拒否します。例えば、あるバージョンのメッセージタイプを拒否する一方、他のバージョンのメッセージタイプを許可することができます。

例 : メッセージタイプの許可および拒否

この例では、GPRS1 GTP 構成に対してセキュリティデバイスがバージョン 1 に関しては error-indication と failure-report メッセージタイプの両方をドロップするように設定します。

WebUI

Objects > GTP > Edit (GPRS1) > Message Drop: バージョン 1 列で次の項目を選択し、**Apply**をクリックします。

Tunnel Management:
    Error Indication: (**選択**)
Location Management:
    Failure Report Request/Response: (**選択**)

CLI

```
set gtp configuration gprs1
(gtp:gprs1)-> set drop error-indication
(gtp:gprs1)-> set drop failure-report
(gtp:gprs1)-> exit
save
```

サポートされているメッセージタイプ

表 1 は GTP リリース 1997 および 1999 （ GTP のチャージングメッセージを含む）でサポートされている GPRS トンネリングプロトコル (GTP) メッセージおよび、GTP メッセージタイプフィルタリングを設定するために使用できるメッセージタイプをリストしています。

表 1: GPRS トンネリングプロトコル (GTP) メッセージ

メッセージ 12	メッセージタイプ	バージョン 0	バージョン 1
create AA pdp context request	create-aa-pdp	✓	
create AA pdp context response	create-aa-pdp	✓	
create pdp context request	create-pdp	✓	✓
create pdp context response	create-pdp	✓	✓
Data record request	data-record	✓	✓
Data record response	data-record	✓	✓
delete AA pdp context request	delete-aa-pdp	✓	
delete AA pdp context response	delete-aa-pdp	✓	
delete pdp context request	delete-pdp	✓	✓
delete pdp context response	delete-pdp	✓	✓
echo request	echo	✓	✓
echo response	echo	✓	✓
error indication	error-indication	✓	✓
failure report request	failure-report	✓	✓
failure report response	failure-report	✓	✓
forward relocation request	fwd-relocation		✓
forward relocation response	fwd-relocation		✓
forward relocation complete	fwd-relocation		✓
forward relocation complete acknowledge	fwd-relocation		✓
forward SRNS context	fwd-srns-context		✓
forward SRNS context acknowledge	fwd-srns-context		✓
identification request	identification	✓	✓
identification response	identification	✓	✓
node alive request	node-alive	✓	✓
node alive response	node-alive	✓	✓
note MS GPRS present request	note-ms-present	✓	✓
note MS GPRS present response	note-ms-present	✓	✓
pdu notification request	pdu-notification	✓	✓

メッセージ 12	メッセージタイプ	バージョン 0	バージョン 1
pdu notification response	pdu-notification	✓	✓
pdu notification reject request	pdu-notification	✓	✓
pdu notification reject response	pdu-notification	✓	✓
RAN info relay	ran-info		✓
redirection request	redirection	✓	✓
redirection response	redirection	✓	✓
relocation cancel request	relocation-cancel		✓
relocation cancel response	relocation-cancel		✓
send route info request	send-route	✓	✓
send route info response	send-route	✓	✓
sgsn context request	sgsn-context	✓	✓
sgsn context response	sgsn-context	✓	✓
sgsn context acknowledge	sgsn-context	✓	✓
supported extension headers notification	supported-extension		✓
g-pdu	gtp-pdu	✓	✓
update pdp context request	update-pdp	✓	✓
updated pdp context response	update-pdp	✓	✓
version not supported	version-not-supported	✓	✓

メッセージレートの制限

セキュリティデバイスを設定して、GSN に送信されるネットワークトラフィックのレートを制限することができます。GTP-Control (GTP-C) メッセージでは、秒単位でパケットに対して異なるしきい値を設定することができます。GTP-C メッセージは処理と応答が必要なので、GSN を圧倒する可能性があります。GTP-C メッセージにレート制限を設定して、GSN を次のようなサービス拒否 (DoS) 攻撃からを守ることができます。

- **境界ゲートウェイ帯域幅の飽和 :** PLMN と同じ GRX に接続されている悪質なオペレータがボーダーゲートウェイに対して多量のネットワークトラフィックを差し向けることにより、PLMN との間の正当なトラフィック用の帯域が不足し、これによりネットワークへのローミングアクセスまたはネットワークからのローミングアクセスが拒否される可能性があります。

- **GTP フラッド :** GTP トラフィックは GSN をフラッドさせ、CPU サイクルが不正なデータを処理させることができます。これにより加入者がローミングしたり、外部ネットワークにデータを転送したり、また GPRS がネットワークに接続できなくなります。

この機能は Juniper Networks ファイアウォールからそれぞれの GSN に送信されるトラフィックのレートを制限します。デフォルトのレートは「無制限」です。

例 : レート制限の設定

次の例では、受信 GTP-C メッセージのレートを毎秒 300 パケットに制限します。

WebUI

Objects > GTP > Edit (GPRS1): 以下を入力して **Apply** をクリックします。

Control Plane Traffic Rate Limit: 300

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set limit rate 300
(gtp:gprs1)-> exit
save
```

シーケンス番号検証

セキュリティデバイスを構成して、シーケンス番号検証を行うことができます。

GTP パケットのヘッダーにはシーケンス番号フィールドがあります。この番号は GTP パケットを受信している GGSN に対して、パケットの順序を示します。パケットデータプロトコル（PDP）コンテキストアクティブ化段階において、送信 GGSN はトンネルを通して他の GGSN に送信する最初の G-PDU に対してゼロ (0) をシーケンス番号値とします。送信 GGSN は、その後に送信する各 G-PDU に対して、シーケンス番号を 1 つずつ増やしていきます。65535 に到達すると、値はゼロにリセットします。

PDP コンテキスト アクティブ化段階において、受信側 GGSN は自身のカウンターをゼロにリセットします。そのため、受信側 GGSN が有効な G-PDU を受け取るたびに、GGSN はカウンターを 1 つ増します。65535 に到達すると、カウンターはゼロにリセットします。

通常、受信側 GGSN は受け取ったパケットのシーケンス番号をカウンターのシーケンス番号と比較します。番号が一致する場合、GGSN はパケットを転送します。番号が異なる場合、GGSN はパケットをドロップします。GGSN 間にセキュリティデバイスを実装すると、デバイスは GGSN のためにこの検証を実行することができ、番号順に届かなかったパケットはドロップします。この機能は無効なパケットを不必要に処理することを防ぎ、GGSN リソースを節約します。

例 : シーケンス番号検証を使用可能にする

この例では、シーケンス番号検証を使用可能にします。

WebUI

Objects > GTP > Edit (GPRS1): **Sequence Number Validation** を選択して **Apply** をクリックします。

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set seq-number-validated
(gtp:gprs1)-> exit
save
```

IP フラグメント化

GTP パケットはメッセージ本体と、GTP ヘッダー、UDP ヘッダーおよび IP ヘッダーの 3 つのヘッダーで構成されています。最終的な IP パケットが転送リンクのメッセージ送信単位（MTU）より大きい場合、送信 SGSN または GGSN が IP フラグメント化を行います。

デフォルトでは、セキュリティデバイスは完全な GTP メッセージを受信するまで IP フラグメントをバッファし、それから GTP メッセージの検査を始めます。

GTP-in-GTP パケットフィルタリング

セキュリティデバイスを構成して、メッセージ本体に他の GTP パケットを含む GTP パケットを検出して、それをドロップするようにできます。

例 : GTP-in-GTP パケットフィルタリングを使用可能にする

この例では、セキュリティデバイスがメッセージ本体に GTP パケットを含む GTP パケットを検出してドロップするようにできます。

WebUI

Objects > GTP > Edit (GPRS1): **GTP-in-GTP Denied** を選択して **Apply** をクリックします。

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set gtp-in-gtp-denied
(gtp:gprs1)-> exit
save
```

徹底監視 (Deep Inspection)

G-PDU データメッセージ内のトンネル端点識別子（TEID）の徹底監視（徹底監視）を行うよう、セキュリティデバイスを設定できます。

例 : 徹底監視を TEID で使用可能にする

この例では、G-PDU データメッセージの TEID の DI（徹底監視）を行うよう、セキュリティデバイスを設定します。DI の設定は、CLI 以外からはできません。

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set teid-di
(gtp:gprs1)-> exit
save
```

GTP 情報要素

情報要素（IE）は、すべての GTP コントロールメッセージパケットに含まれています。IE は、GTP トンネルの作成、変更、削除、ステータス等の GTP トンネルに関する情報を提供します。ScreenOS は 3 GPP Release 6 に一致する IE をサポートしています。それ以前のリリースを実行する場合、またはオペレータとの間で、3GPP の以前のリリースを実行するよう契約により合意している場合、サポートされていない IE を含むコントロールメッセージを制限することで、ネットワークオーバーヘッドを減らすことが可能です。

このセクションでは、IE に基づきスクリーニングを行うようセキュリティデバイスを設定するため、コントロールメッセージに含まれる IE について説明します。本章のセクションは、以下のようになります。

- 15 ページの「アクセスポイント名のフィルタリング」
- 17 ページの「IMSI プレフィックスフィルタリング」
- 18 ページの「無線アクセス技術」
- 18 ページの「ルーティングエリアアイデンティティとユーザーロケーション情報」
- 19 ページの「APN Restriction」
- 19 ページの「IMEI-SV」
- 20 ページの「プロトコルおよびシグナリング要件」
- 21 ページの「IE フィルタリングの組み合わせのサポート」
- 22 ページの「サポートされる R6 情報要素」
- 24 ページの「3GPP R6 IE の排除」

アクセスポイント名のフィルタリング

アクセスポイント名 (APN) は、ネットワークに到達する方法に関する情報を提供する、GTP パケットのヘッダーに含まれている情報要素 (IE) です。APN は 2 つの要素から成ります。

- **ネットワーク ID** - 「mobiphone.com」などの外部ネットワークの名前を識別する ID。
- **オペレータ ID** - 「mnc123.mcc456」などのオペレータの PLMN を一意的に識別する ID。

デフォルトでは、セキュリティデバイスはすべての APN を許可します。しかしながらデバイスを設定して、ローミング加入者が外部ネットワークにアクセスするのを制限する APN フィルタリングを行うこともできます。最高 2,000 の APN を設定することができます。

APN フィルタリングを使用可能にするには、1 つまたは複数の APN を指定する必要があります。APN を指定するには、ネットワークのドメイン名（たとえば mobiphone.com など）、および任意でオペレータ ID を知っておく必要があります。APN のドメイン名 (ネットワーク ID) の部分は大変長く、多くの文字を含む可能性があるため APN の最初の文字として、ワイルドカードである「*」を使用することができます。ワイルドカードは、APN には mobiphone.com だけではなくそれらの文字の前に他の文字も含まれることを意味します。

また、APN 用に*選択モード*を設定する必要があります。選択モードは APN の元の場所、そして Home Location 登録 (HLR) が user-subscription を検証したかどうかを示します。ネットワークのセキュリティニーズに従って、選択モードを設定します。選択モードとして以下のものが考えられます。

- **移動端末** - 移動端末が提供する APN、加入は検証されていない

  この選択モードは、移動端末 (MS) が APN を提供し、HLR がネットワークに対してユーザー加入を検証しなかったことを示します。

- **ネットワーク** - ネットワーク提供の APN、加入は検証されていない

  この選択モードは、MS が指定しなかったので、ネットワークがデフォルトの APN を提供したことを示し、HLR がネットワークに対してユーザー加入を検証しなかったことを示します。

- **検証済み** - MS またはネットワーク提供の APN、加入は検証済み

  この選択モードは、MS またはネットワークが APN を提供し、HLR がネットワークに対してユーザー加入を検証したことを示します。

APN フィルタリングは **create pdp request** メッセージに対してのみ適用されます。APN フィルタリング実行時、セキュリティデバイスは ATP パケットを検査して、設定された APN と一致する APN を探します。GTP パケットの APN が、指定した APN と一致する場合、セキュリティデバイスは次に選択モードを検証し、APN および選択モードが指定した APN および選択モードと一致する場合にのみ、GTP パケットを転送します。APN フィルタリングは完全一致に基づいているので、APN サフィックスを設定するときにワイルドカード「 * 」を使用すると、認定するはずの APN が不注意に排除されることを防ぎます。セキュリティデバイスは一致しない他のすべての APN を自動的に拒否します。

さらに、セキュリティデバイスは国際移動端末 ID（IMSI）プレフィックスと APN の組み合わせに基づいて GTP パケットをフィルタすることもできます。

例 : APN と選択モードの設定

この例では **mobiphone.com.mnc123.mcc456.gprs** を APN として設定し、ワイルドカード「*」を使用します。また選択モードとして **Network** を設定します。

WebUI

Objects > GTP > Edit (GPRS1) > APN + IMSI > New: 次のように入力してから **OK** をクリックします。

Access Point Name: *mobiphone.com.mnc123.mcc456.gprs
Selection Mode: Network (選択）

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set apn *mobiphone.com.mnc123.mcc456.gprs selection net
(gtp:gprs1)-> exit
save
```

IMSI プレフィックスフィルタリング

GPRS サポートノード (GSN) は国際移動端末 ID（IMSI) により移動端末（MS）を識別します。IMSI は、移動国コード (MCC)、移動ネットワークコード (MNC) および移動加入者 ID 番号 (MSIN) の 3 種類のコードで構成されます。MCC と MNC はいっしょに IMSI プレフィックスを成し、移動加入者ホームネットワークまたは公衆移動端末網 (PLMN) を識別します。

IMSI プレフィックスを設定して、ローミングパートナーからのトラフィックではない GTP トラフィックを拒否するように、セキュリティデバイスを設定することができます。デフォルトでは、セキュリティデバイスは GTP パケットに IMSI プレフィックスフィルタリングを行いません。IMSI プレフィックスを設定すると、セキュリティデバイスは **create pdp request** メッセージだけをフィルタし、指定した IMSI プレフィックスと一致する GTP パケットだけを許可します。セキュリティデバイスは、指定した IMSI プレフィックスと一致しない IMSI プレフィックスを持った GTP パケットを許可します。指定した IMSI プレフィックスと一致しない IMSI プレフィックスを持つ GTP パケットをブロックするには、IMSI フィルタの明白なワイルドカードを使用します。**drop** アクションは最後の IMSI プレフィックスフィルタリングポリシーです。最高 1,000 までの IMSI プレフィックスを設定することができます。

IMSI プレフィックスにより GTP パケットをフィルタリングする場合、APN も指定しなければなりません。「例 : IMSI プレフィックスとフ APN フィルタを組み合わせて設定する」を参照してください。

例 : IMSI プレフィックスとフ APN フィルタを組み合わせて設定する

この例では **mobiphone.com.mnc123.mcc456.gprs** を APN として設定し、ワイルドカード「*」を使用します。この APN には、すべての選択モードを許可します。また、知られている PLMN の IMSI プレフィックスを 246565 に設定します。MCC-MNC ペアは 5 または 6 桁です。

WebUI

Objects > GTP > Edit (GPRS1) > APN + IMSI: 次のように入力してから **OK** をクリックします。

Access Point Name: *mobiphone.com.mnc123.mcc456.gprs
Mobile Country-Network Code: 246565
Selection Mode: Mobile Station, Network, Verified（選択）

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set mcc-mnc 246565 apn *mobiphone.com.mnc123.mcc456.gprs
    pass
(gtp:gprs1)-> exit
save
```

注： CLI の変数 **pass** を選択することは、WebUI の 3 つの選択モード全部を選択することに相当します。この変数を使用すると、指定した APN のすべての選択モードからのトラフィックが許可されます。

無線アクセス技術

「無線アクセス技術」（RAT）情報要素は、Wideband Code Division Multiple Access （WCDMA）を刺激する方法を提供し、また、請求情報システムを介してレポートを実行します。

以前は、第 3 世代無線移動通信技術（3G）システムと第 2 世代無線移動通信技術（2G）システムを区別するために、SGSN IP アドレスを使用していました。しかし、2G/3G SGSN の組み合わせが導入されたことから、セキュリティデバイスにこの区別をさせるためには、RAT 情報要素を設定しなければなりません。RAT IE を設定したら、APN も指定する必要があります。「例 : RAT および APN フィルタの設定」を参照してください。

例 : RAT および APN フィルタの設定

この例では **mobiphone.com.mnc123.mcc456.gprs** を APN として設定し、ワイルドカード「*」を使用します。この APN には、すべての選択モードを許可します。RAT IE が文字列 123 と一致する場合に、セキュリティデバイスが GPT メッセージをドロップするよう設定します。

WebUI

現在のところ、RAT と APN の組み合わせは、コマンドラインインターフェイス（CLI）からしか設定できません。

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set rat 123 apn *mobiphone.com drop
(gtp:gprs1)-> exit
save
```

ルーティングエリアアイデンティティとユーザーロケーション情報

特定の国においては、加入者が特定の種類のネットワークコンテンツにアクセスすることを制限している場合があります。これらの規制要件を満たすため、ネットワークオペレータは、コンテンツのダウンロードを許可する前に、加入者が要求しているコンテンツを監視する能力がなければなりません。ScreenOS では、ネットワークオペレータが、ルーティングエリアアイデンティティ（RAI）とユーザーロケーション情報（ULI）IE に基づきコンテンツをスクリーニングできます。現在の 3GPP Call Detail Record（CDR）フォーマットおよびリアルタイム課金インターフェースにはこれらの属性が欠如しているので、請求課金システムは、決済するローミングパートナーと請求側エンドユーザーを判断するため、SGSN IP アドレスを調べる必要があります。ScreenOS では、ネットワークオペレータは、RAI と ULI に基づきコントロールメッセージをスクリーニングできます。RAT IE または ULI IE を設定したら、APN も指定する必要があります。「例 : RAI および APN フィルタの設定」および「例 : ULI および APN フィルタの設定」を参照してください。

例 : RAI および APN フィルタの設定

この例では **mobiphone.com** を APN として設定し、ワイルドカード「*」を使用します。この APN には、すべての選択モードを許可します。RAI IE が文字列 12345* と一致する場合に、セキュリティデバイスが GPT メッセージをドロップするよう設定します。

WebUI

現在のところ、RAI と APN の組み合わせは、コマンドラインインターフェイス（CLI）からしか設定できません。

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set rai 12345* *mobiphone.com drop
(gtp:gprs1)-> exit
save
```

例 : ULI および APN フィルタの設定

この例では **mobiphone.com** を APN として設定し、ワイルドカード「*」を使用します。この APN には、すべての選択モードを許可します。ULI IE が文字列 123456 と一致する場合に、セキュリティデバイスが GPT メッセージをドロップするよう設定します。

WebUI

現在のところ、ULI と APN の組み合わせは、コマンドラインインターフェイス（CLI）からしか設定できません。

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set uli 123456 apn mobiphone.com drop
(gtp:gprs1)-> exit
save
```

APN Restriction

複数同時プライマリパケット データプロトコル（PDP）コンテキストと、これらの 2 つのアクセスポイント間をルーティングできる MS/UE は、プライベート APN とパブリック APN の両方を有する企業ユーザーの IP のセキュリティを脅かします。GTP **create PDP context** 応答メッセージに APN Restriction IE を追加することで、GGSN から要求された場合（またはこの条件が満たされず拒否された場合）の PDP コンテキストの相互排除性が確保され、これによりセキュリティが脅かされることが回避されます。

IMEI-SV

International Mobile Equipment Identity-Software Version (IMEI-SV）IE は、コンテンツを端末タイプとクライアントアプリケーションに合わせるためのプロキシサーバーが存在しないときにいつでも、そのための方法を提供します。この IE は、GGSN、AAA および（または）ワイヤレスアプリケーションプロトコルゲートウェイ（WAP GW）から生成されるレポートにおいて有用です。疑わしくないトラフィックとしての扱いまたは分類（これは、GPRS トラフィックや GPRS ローミングトラフィックにとって害になる場合がある）を避けるため、GTP 対応のセキュリティデバイスは、GTP 属性の RAT、RAI、ULI、APN Restriction および

IMEI-SV をサポートしています。これらの属性は、特定の GPRS トラフィックや GPRS ローミングトラフィックのブロックに使用される有効フィルタ属性セットに含まれています。IMEI-SV IE を設定したら、APN も指定する必要があります。「例 : IMEI-SV および APN フィルタの設定」を参照してください。

例 : IMEI-SV および APN フィルタの設定

この例では **mobiphone.com** を APN として設定し、ワイルドカード「*」を使用します。この APN には、すべての選択モードを許可します。IMEI-SV IE が文字列 87652 と一致する場合に、セキュリティデバイスが GPT メッセージをパスするよう設定します。

WebUI

現在のところ、RAI と APN の組み合わせは、コマンドラインインターフェイス（CLI）からしか設定できません。

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set imei-sv 87652* apn mobiphone.com pass
(gtp:gprs1)-> exit
save
```

プロトコルおよびシグナリング要件

セキュリティデバイスは、GTP **Create PDP Context Request** メッセージ内の以下の属性をサポートしています。

- RAT
- RAI
- ULI
- APN Restriction
- IMEI-SV

セキュリティデバイスは、GTP **Update PDP Context Request** メッセージ内の以下の属性をサポートしています。

- RAT
- RAI
- ULI

セキュリティデバイスは、GTP **Update PDP Context Response** メッセージ内の APN Restriction 属性をサポートしています。

上述のセキュリティデバイス上の GTP シグナリングメッセージは、以下のように設定できます。

- 透過的にパス
- 以下に基づいて（個別に）ブロック

- RAT
- RAI（123* 等の範囲指定付き）
- ULI（範囲指定付き）
- IMEI-SV（範囲指定付き）

IE フィルタリングの組み合わせのサポート

情報要素（IE）の R6 フィルタリングに関する同時サポートについては、以下のルールが適用されます。

- デフォルトでは、セキュリティデバイスは GTP パケットに IE フィルタリングを行いません。
- 各コマンドラインには、以下の優先順位に従い属性が added 演算されます。
  1. RAT
  2. RAI
  3. ULI
  4. IMEI
  5. MCC-MNC
- 属性制限 を設定したら、APN も指定する必要があります。

  たとえば、セキュリティデバイスに RAT 1 *および* RAI 567* *および* MCC-MNC 56789 を含む GTP メッセージをパスさせたい、*または* RAI 123* を含むメッセージをパスさせたいが、APN 値を含むパケットはすべてドロップさせたい場合は、以下のように設定するとその目的を達成することができます。

  ```
  set rat 1 rai 567* mcc-mnc 56789 apn * pass
  set rai 123* apn * pass
  set apn * drop
  ```

  1 行目は、セキュリティデバイスに RAT 1、RAI 567*、MCC-MNC 56789 *および* APN を含む GTP メッセージをパスさせる設定です。2 行目は、RAI 123* および APN を含むメッセージをパスさせる設定です。3 行目は、APN を含むパケットをドロップさせる設定です。

サポートされる R6 情報要素

ScreenOS は、表 2 にリストされているすべての GTP の 3GPP R6 IE をサポートしています。

表 2: サポートされている情報要素

IE タイプ値	情報要素
1	原因
2	International Mobile Subscriber Identity (IMSI)
3	Routing Area Identity (REI)
4	Temporary Logical Link Identity (TLLI)
5	パケット TMSI（P-TMSI）
8	必要な再順序付け
9	Authentication Triplet
11	MAP 原因
12	P-TMSI 署名
13	MS 認証済み
14	リカバリ
15	選択モード
16	トンネル端点識別子データ 1
17	トンネル端点識別子コントロールプレーン
18	トンネル端点識別子データ 2
19	Teardown ID
20	NSAPI
21	RANAP 原因
22	RAB コンテキスト
23	Radio Priority SMS
24	Radio Priority
25	パケットフロー ID
26	課金特性
27	トレースリファレンス
28	トレースタイプ
29	MS 到達不能の理由
127	課金 ID
128	エンドユーザーアドレス
129	MM コンテキスト
130	PDP コンテキスト
131	アクセスポイント名
132	プロトコル構成オプション
133	GSN アドレス
134	MS 国際 PSTN/ISDN ナンバー（MSISDN）
135	通信品質プロファイル

IE タイプ値	情報要素
136	Authentication Quintuplet
137	トラフィックフローテンプレート
138	ターゲット識別
139	UTRAN Transparent Container
140	RAB セットアップ情報
141	エクステンションヘッダータイプリスト
142	トリガー ID
143	OMC アイデンティティ
144	RAN Transparent Container
145	PDP コンテキスト優先化
146	追加 RAB セットアップ情報
147	SGSN 番号
148	共通フラグ
149	APN Restriction
150	Radio Priority LCS
151	RAT タイプ
152	ユーザーロケーション情報
153	MS タイムゾーン
154	IMEI-SV
155	CAMEL Charging Information Container
156	MBMS UE コンテキスト
157	Temporary Mobile Group Identity (TMGI)
158	RIM ルーティングアドレス
159	MBMS プロトコル構成オプション
160	MBMS サービスエリア
161	ソース TNC PDCP コンテキスト情報
162	追加トレース情報
163	ホップカウンタ
164	選択された PLMN ID
165	MBMS セッション識別子
166	MBMS2G/3G インジケータ
167	強化された NSAPI
168	MBMS セッション時間
169	追加 MBMS トレース情報
251	課金ゲートウェイアドレス
255	Private Extension

3GPP R6 IE の排除

3GPP R6 IE 排除機能は、2GPP ネットワークと 3GPP ネットワーク間のローミングの相互運用性を維持することができます。パケットが 2GPP ネットワーク内にパスされる時に、PLMN と GRX の境界上に置かれ、Gp ファイアウォールの役割を果たす GTP 対応のセキュリティデバイスに、3GPP 特有の属性を GTP パケットヘッダーから取り除かせるよう、設定することができます。GTP メッセージが GGSN に転送される前に、メッセージから RAT、RAI、ULI、IMEI-SV および APN Restriction IE を外すよう、セキュリティデバイスを設定することができます。

例 : R6 の排除

この例では、新たに追加された R6 IE（RAT、ULI、IMEI - SV および APN Restriction）を GTP メッセージから外すよう、セキュリティデバイスの GP インターフェースを設定します。

WebUI

Objects > GTP > New: 以下を選択して **Apply** をクリックします。

Remove R6 EI: (選択)

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set  remove-r6
(gtp:gprs1)-> exit
save
```

GTP トンネル

GTP トンネルは、GPRS トンネリングプロトコル (GTP) を使用して、GSN 間の GTP トラフィックの送信を有効にします。トンネルには次の 2 種類があります : GTP-U メッセージ（ユーザーデータ）のトンネルと GTP-C（シグナリングと制御）メッセージのトンネルです。

GTP トンネル制限

セキュリティデバイスを構成して、GTP トンネルの数を制限することができます。この制限が適用される GSN は、GTP 検査オブジェクトが後に追加されるポリシーに指定されています。これにより、GSN の容量を超えることはありません。

例 : GTP トンネル制限の設定

次の例では GPRS1 GTP 検査オブジェクトに対して、ローミング GTP トンネルの数を 800 に制限します。

WebUI

Objects > GTP > Edit (GPRS1): 以下を入力して **Apply** をクリックします。

Maximum Number of Tunnels
Limited to tunnels: (選択), 800

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set limit tunnel 800
(gtp:gprs1)-> exit
save
```

パケット状態監視

GTP パケット検証の一連を経て（ 8 ページの「GTP メッセージフィルタリング」を参照）、セキュリティデバイスは次に GTP パケットを現在の GTP トンネル状態と検証します。セキュリティデバイスはかつて受信した GTP パケットに基づいて、GTP パケットを転送あるいはドロップするかを決めます。例えば、要求メッセージは応答メッセージに先行します。ですからセキュリティデバイスは **create pdp context request** メッセージを受信しなかったのに、**create pdp context response** メッセージを受信した場合、セキュリティデバイスは応答メッセージをドロップします。

基本的に、現在の GTP 状態モデルに所属していない GTP パケットを受信すると、セキュリティデバイスはパケットをドロップします。次に示されているのは、GTP 状態モデルの簡潔化された例です。

GTP トンネル確立および終了

移動端末は外部ネットワーク（www.buygadgets.com）に到達するために、GTP トンネル確立を開始するために SGSN を持った GPRS 接続を実施します。SGSN は GGSN に **create pdp context request** メッセージを送信します。CGSN が接続を受け入れると（認証、リソース割り当て、通信品質（QoS）保証）、**create pdp context response** メッセージで応答します。SGSN と GGSN の間のメッセージ交換により、GGSN は GTP トンネルを確立し、これを通して MS は GTP-U メッセージを外部ネットワークに送信できます。

コミュニケーションを終了するには、MS は GPRS 切り離しを行い、SGSN が GTP トンネル終了を開始します。SGSN は GGSN に「 pdp コンテキスト要求を削除」メッセージを送信します。GGSN は「 pdp コンテキスト応答を削除」メッセージで応答し、記録から GTP トンネルを削除します。SGSN が応答を受信すると、SGSN も記録から GTP トンネルを削除します。

セキュリティデバイスは複数の要求を受信して、同時に異なる GSN に対して GTP トンネルを確立できます。すべてのトンネルのトラッキング（異なるトンネルに対すトンネルの状態とログメッセージ）を容易にするために、セキュリティデバイスは作成時にそれぞれのトンネルに対して、一意的なインデックスを割り当てます。このトンネルインデックスは、ログに残された各 GTP トンネルメッセージに対して表示されます。

SGSN 間ルーティングエリアの更新

MS が現在の SGSN の範囲から出て、新しい SGSN エリアに入った場合、新しい SGSN は古い SGSN に対して「 sgsn コンテキスト要求」を送信し、MS に関して持っているすべての情報を転送するように要求します。古い SGSN は「 sgsn コンテキスト応答」メッセージで返信し、新しい SGSN に MS に関して持っているすべての情報を送信します。この応答と情報を受信すると、新しい SGSN は「 sgsn コンテキスト承認」メッセージを古い SGSN に送信して受信を確認します。

これ以降、古い SGSN は新しい SGSN に対して MS に関して受信するすべての新しい T-PDU を転送します。この「引渡し」手順を終了するために、新しい SGSN は GGSN に「 pdp コンテキスト要求を更新」メッセージを送る必要があり、これに対して GGSN は「 pdp コンテキスト応答を更新」メッセージで返信します。

SGSN が異なる PLMN に配置されている場合、すべての GTP メッセージはセキュリティデバイスを通ります。2 つのが同じ PLMN に配置されており、GGSN が異なる PLMN に存在する場合、「 pdp コンテキスト要求 / 応答を更新」メッセージだけがセキュリティデバイスを通ります。

高可用性のためのトンネルフェールオーバー

ScreenOS は 2 つの HA （高可用性）モードをサポートします。セキュリティモードがルートモードのときは active-active をサポート、そしてセキュリティデバイスがルートまたは透過モードのときは active-passive をサポートします。実質的に、HA 構成の 2 つのセキュリティデバイスがマスターとバックアップデバイスの役割を果たします。バックアップデバイスはマスターの構成（既存の GTP トンネルを含む）をミラーし、マスターに障害が起きた場合、マスターデバイスの仕事を代わりに行います。マスターとバックアップ間のフェールオーバーはすばやく行われ、ユーザーには見えません。

フェールオーバーが起きると、確立された GTP トンネルはアクティブでそのままの状態を維持しますが、確立中の GTP トンネルは失われます。この場合、フェールオーバーの後で GTP トンネル確立を再開する必要があります。また、終了途上の GTP トンネルが確認メッセージを逃してしまい、セキュリティデバイス上に放置される場合もあります。GTP トンネルの放置はさまざまな原因で起きます。HA に関しては、トンネルの一端にある GSN がトンネルのもう一端の GSN に「pdp コンテキスト要求を削除」メッセージを送信し、その応答を待っている間に障害が起きて、コミュニケーションが中断され、GSN がもう一つの GSN から「pdp コンテキスト応答を削除」メッセージ（削除を確認）を受信できないため、GTP トンネルが放置される場合があります。確認メッセージを送信した GSN は同時に pdp コンテキストを削除し、GTP トンネルの他方にある GSN は、削除確認を待ちながら、放置したままになります。

セキュリティデバイスを構成して、放置された GTP トンネル削除することができます。詳細については、26 ページの「放置された GTP トンネルのクリーンアップ」を参照してください。

HA の詳細および高可用性のためにセキュリティデバイスを構成するには、「第 11 部 : 高可用性」を参照してください。

放置された GTP トンネルのクリーンアップ

この機能により、セキュリティデバイス上に放置されている GTP トンネルを削除します。GTP トンネルが放置される原因はいくつかあります。例えば「pdp コンテキスト応答を削除」メッセージがネットワーク上で失われたり、GSN がきちんとシャットダウンしない場合などに起こります。セキュリティデバイスを構成して、放置された GTP トンネルを自動的に検出して削除することができます。

GTP トンネルタイムアウト値を設定すると、セキュリティデバイスはタイムアウト値により指定された期間アイドルである GTP トンネルを「放置されている」とし、削除します。デフォルトの GTP トンネルタイムアウト値は 24 時間です。

例 : GTP トンネルのタイムアウトの設定

この例では、「GPRS1」GTP 検査オブジェクトの GTP トンネルタイムアウトを 12 時間に設定します。

WebUI

Objects > GTP > Edit (GPRS1): 以下を入力して **Apply** をクリックします。

Tunnel Inactivity Timeout: 12

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set timeout 12
(gtp:gprs1)-> exit
save
```

SGSN と GGSN 転送

Juniper Networks セキュリティデバイスは SGSN と GGSN との間の GTP トラフィック転送をサポートしています。

- **SGSN 転送** - SGSN (A) は create-pdp-context 要求を送信し、それにより後続の GTP-C と GTP-U メッセージに対して、異なる SGSN IP アドレス（ SGSN B と SGSN C ）を指定できます。そのため A の代わりに GGSN は、後続の GTP-C と GTP-U メッセージを SGSN B と C に送信します。

- **GGSN 転送** - GGSN (X) は create-pdp-context 要求を送信し、それにより後続の GTP-C と GTP-U メッセージに対して、異なる GGSN IP アドレス（ GGSN Y と GGSN Z ）を指定できます。そのため A の代わりに SGSN は、後続の GTP-C と GTP-U メッセージを GGSN Y と Z に送信します。

過大請求攻撃の回避

セキュリティデバイスを構成して GPRS 過大請求攻撃を回避することができます。次のセクションでは過大請求攻撃を説明し、次に回避策について述べます。

過大請求攻撃の説明

過大請求攻撃について理解するには、移動端末 (Mobile Station 以下 MS) が IP アドレスを IP プールから取得することを理解しておく必要があります。過大請求攻撃にはさまざまな手口があります。例えば、正当な加入者が自分の IP アドレスを IP プールに返却する際をとらえて、そのアドレスを乗っ取る、という手法があります。こうするとセッションが開いたままになってしまいます。攻撃者が IP アドレスを意のままに操り、検知、報告されることもなければ、料金を支払うことなく (正確には乗っ取られた加入者の負担で) データをダウンロードしたり他の加入者に送信したりできます。

過剰請求攻撃は IP アドレスが利用できるようになり、他の MS に再度割り当てられたときにも起こります。そのため、先の MS が開始したトラフィックが新しい MS に転送され、新しい MS が意図しないトラフィックに対して請求を受けることになります。図 4, 図 5、および 図 6 は、こういった手口の状況を詳しく図示しています。

図 4 では、MS1 が IP アドレスを取得し、GGSN への GTP トンネルの確立を要求します。SGSN (Serving GPRS Support Node、GPRS ユーザーの位置管理などを行うノード) は MS1 の要求に応じて GTP トンネルを作成します。MS1 はサーバーとのセッションを開始します。

図 4: セッションの開始

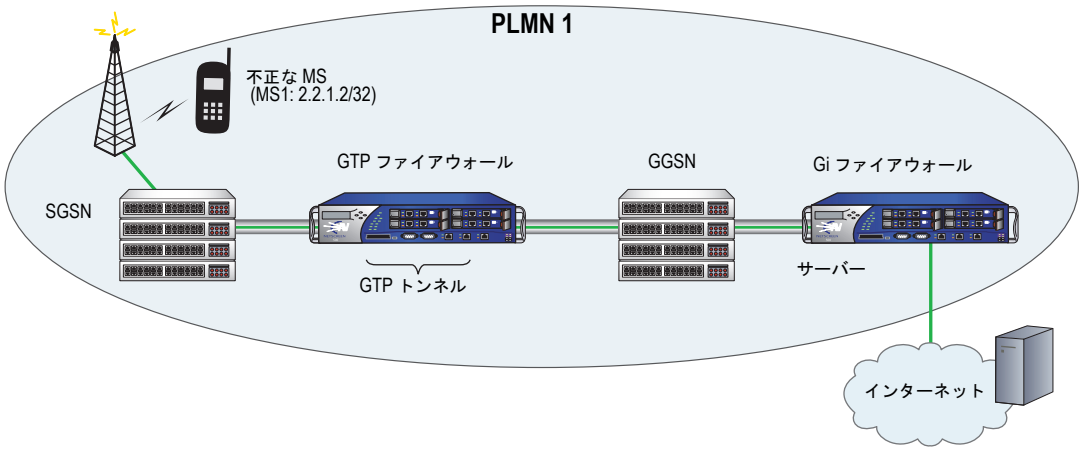


図 5 では、サーバーが MS1 宛のパケット送信を始めると、MS1 は同時に SGSN に対し GTP トンネルを削除するよう要求しますが、サーバーとのセッションがそのまま残っています。

サーバーは GGSN に対するパケット送信を続行します。Gi ファイアウォールは GTP トンネルが削除されたことを知らないので、パケットを GGSN に転送します。GGSN は、GTP トンネルがなくなったので、パケットを破棄します。

図 5: GTP トンネルの削除

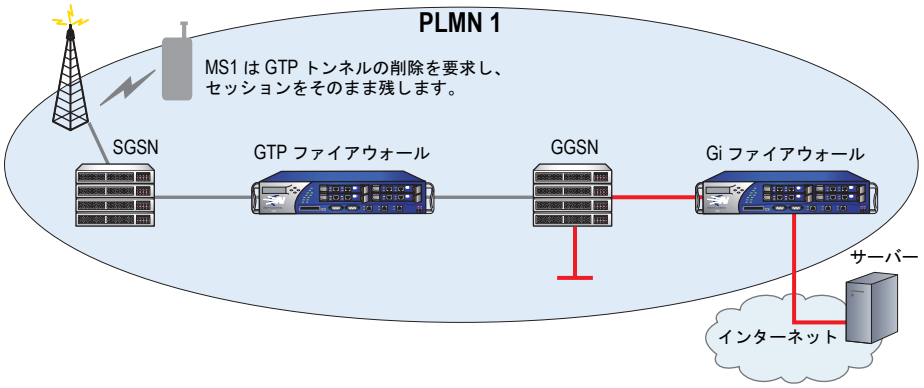
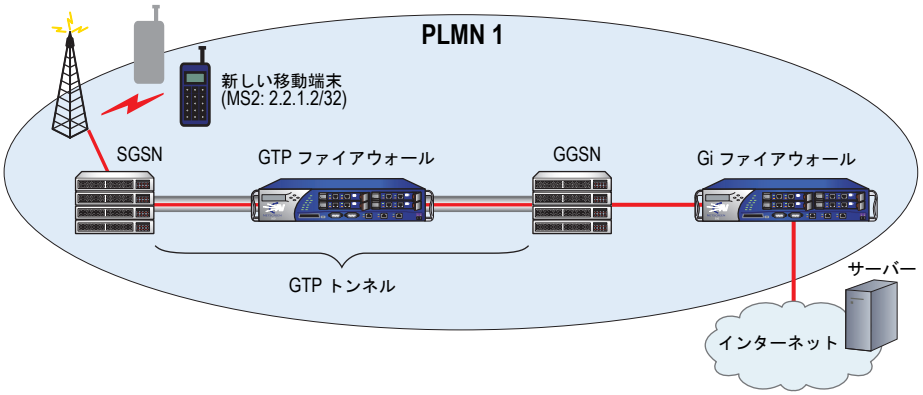


図 6 では、被害者の移動端末である MS2 は、SGSN に対して GGSN への GTP トンネルを作成するよう要求し、IP アドレス 2.2.1.2/32（MS1 が使っていたのと同じ）を得ます。SGSN は GGSN の新しい GTP トンネルを作成します。

GGSN は 2.2.1.2 宛の新しい GTP トンネルを検知しますが、同じ IP アドレスで異なる MS (MS1) 宛のセッションが残っているので、届いたパケットを MS2 に転送します。MS2 は、MS1 宛のトラフィックであるにも関わらず、その分を課金されてしまいます。

図 6: 意図しないデータの受信



過大請求攻撃の防御

PLMN 加入者を過大請求攻撃から守るためには、セキュリティデバイス 2 台を用意し、NetScreen ゲートキーパープロトコル (NSGP) および NSGP モジュールを組み込む必要があります。

NSGP モジュールには 2 つのコンポーネントがあります。それはクライアントとサーバーです。クライアントはサーバーに接続し、要求を送信し、それがサーバーにより処理されます。クライアントとサーバーの両者は互いに、そして他者にも同時に複数の接続をサポートします。

NSGP (NetScreen Gatekeeper Protocol) は TCP 上で動作するプロトコルで、所定の間隔で Hello メッセージを送ることにより、クライアントとサーバーの接続状態を監視します。現行の NSGP が対応している「セッション」タイプのコンテキスト (ユーザーセッション情報の管理領域) は、セキュリティゾーンに固定であり、一意的な番号 (コンテキスト ID) で識別するようになっています。

NSGP の設定に当たっては、クライアントとサーバーで同じコンテキスト ID を使わなければなりません。クライアントがサーバーに「クリアセッション」要求を送る場合、この要求にはコンテキスト ID とサーバーの IP アドレスを設定する必要があります。サーバーは「クリアセッション」要求を受け取ると、コンテキスト ID を照合した上で、自身の管理する表からセッション情報を削除します。

Gi ファイアウォール（サーバー）の役割を果たしているセキュリティデバイスは、ScreenOS 5.0.0 NSGP ファームウェアを実行し、GTP ファイアウォール（クライアント）の役割を果たしている他のデバイスは、ScreenOS 5.0.0 または ScreenOS 5.1.0 GPRS ファームウェアを実行しなければなりません。GTP ファイアウォール上の NSGP は、GTP トンネルが切断されれば Gi ファイアウォールに通知するよう設定します。また、Gi ファイアウォール上の NSGP は、GTP ファイアウォールから GTP トンネルが削除された旨の通知を受けると、セッションを自動的にクリアするよう設定します。これにより、意図しないトラフィックを解消することができるのです。

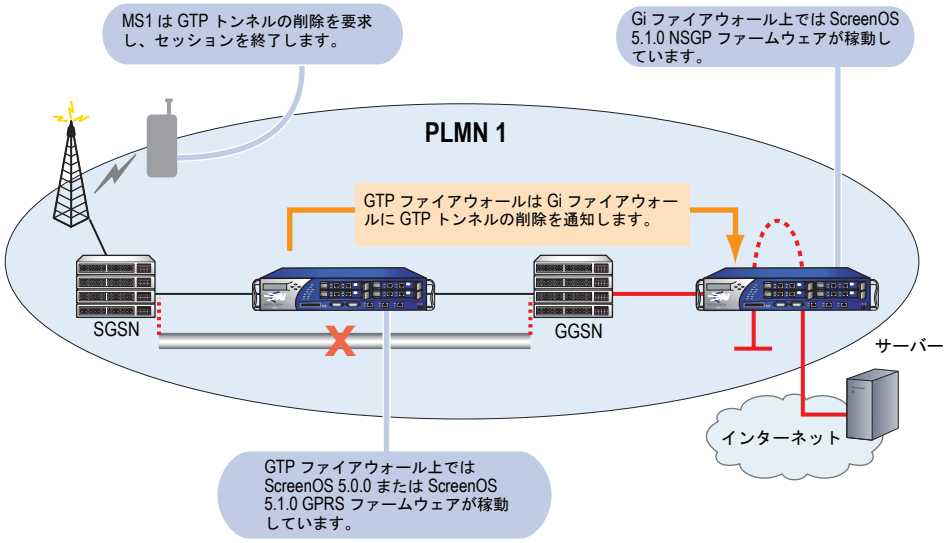
サーバーとのセッションを開始し、サーバーが MS1 にパケットを送信し始めると、MS1 は SGSN に対して GTP トンﾙを削除するよう要求し、セッションを終了します。

トンネルがなくなったので、GTP ファイアウォールは Gi ファイアウォールに対して、即座にその旨を通知します。Gi ファイアウォールは表からセッション情報を削除します。

その後、サーバーが GGSN にパケットを送ろうとしても、Gi ファイアウォールはこれを破棄します。

したがって新しい MS は、前の MS と同じ IP アドレスを使っていても、自分が意図しないトラフィックを受け取って課金されることはありません。

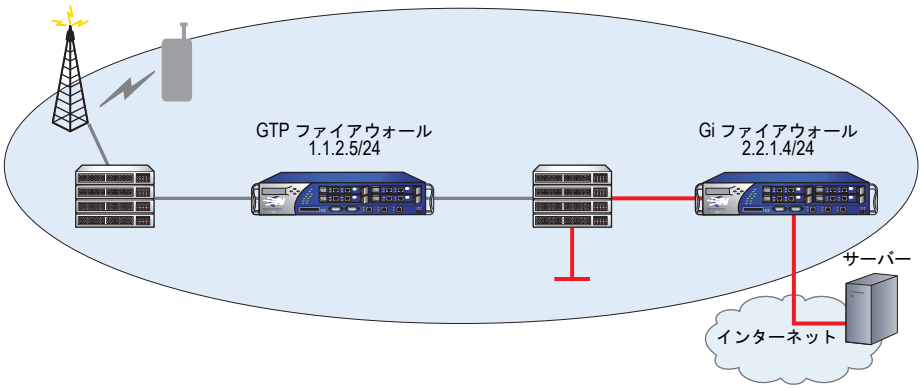
図 7: GTP トンネル削除通知



例：過大請求攻撃を回避するための設定

この例では GTP ファイアウォール（クライアント）と Gi ファイアウォール（サーバー）の両方に NSGP を設定します。「GPRS1」GTP 検査オブジェクトを GTP と Gi ファイアウォールの両方に設定したとします。

図 8: GTP と Gi ファイアウォールのセットアップ



GTP ファイアウォール（クライアント）

WebUI

Network > Interface > Edit (ethernet1/2): 以下を入力して **Apply** をクリックします。

Zone Name: Untrust(選択)
IP Address/Netmask: 1.1.2.5/24
Management Services: Telnet (選択)

Objects > GTP > Edit (GPRS1) > Overbilling: 以下を入力して **Apply** をクリックします。

Overbilling Notify: (選択)
Destination IP: 2.2.1.4
Source Interface: ethernet1/2
Destination Context: 2

Policies > (From: Untrust, To: Trust) New: 次のように入力してから **OK** をクリックします。

Source Address:
Address Book Entry: (選択), Any
Destination Address:
Address Book Entry: (選択), Any
Service: Any
GTP Inspection Object: GPRS1
Action: Permit

CLI

```
set interface ethernet1/2 zone Untrust
set interface ethernet1/2 ip 1.1.2.5/24
set interface ethernet1/2 manage telnet
set gtp config gprs1
(gtp:gprs1)-> set notify 2.2.1.4 src-interface ethernet1/2 context 2
(gtp:gprs1)-> exit
save
set policy from untrust to trust any any any permit
```

システムはポリシー ID を返します、例えば : policy id = 2

```
set policy id 2 gtp gprs1
save
```

Gi ファイアウォール（サーバー）

WebUI

Network > Interface > Edit (ethernet1/2): 以下を入力して **Apply** をクリックします。

Zone Name: Untrust (選択)
IP Address/Netmask: 2.2.1.4/24
Management Services: Telnet (選択)
Other Services: Overbilling (選択)

NSGP: 次のように入力して **Add** 、次いで **OK** をクリックします。

Context ID: 2
Zone: Untrust

CLI

```
set interface ethernet1/2 zone Untrust
set interface ethernet1/2 ip 2.2.1.4/24
set interface ethernet1/2 manage telnet
set interface ethernet1/2 nsgp
set nsgp context 2 type session zone untrust
save
```

GTP トラフィック監視

Juniper Networks セキュリティデバイスはリアルタイムでトラフィックを監視するための包括的なツールを提供しています。GTP トラフィックには、GTP トラフィックロギングおよび GTP トラフィックカウンティンク機能を使って、トラフィックを監視できます。

トラフィックロギング

GTP トラフィックロギング機能では、セキュリティデバイスを設定して、GTP パケットの状態に基づいてログに残します。それぞれのパケットについて、どれだけの情報（基本または拡張）を必要としているか指定できます。コンソール、syslog および WebUI を使って、トラフィックログを表示できます。

GTP パケットの状態は次のいずれかです。

- 転送 - GTP ポリシーが許可するのでセキュリティデバイスが転送するパケット。
- 拒否 - GTP ポリシーが拒否するのでセキュリティデバイスがドロップするパケット。
- レート制限 - 宛先 GSN の最大レート制限を越えるのでセキュリティデバイスがドロップするパケット。
- 状態無効 - パケット状態監視に合格しなかったので、セキュリティデバイスがドロップしたパケット。
- トンネル制限 - 宛先 GSN の最大 GTP トンネル数に到達したので、セキュリティデバイスにドロップされたパケット。

注： デフォルトでは、Juniper Networks セキュリティデバイスではトラフィックロギングは使用不可能になっています。

基本形におけるそれぞれのログエントリには、次の情報が含まれています。

- タイムスタンプ
- ソース IP アドレス
- 宛先 IP アドレス
- トンネル識別子 (TID) あるいはトンネルエンドポイント識別子 (TEID)
- メッセージタイプ

- パケット状態 : 転送、禁止、状態無効、レート制限またはトンネル制限
- インターフェース、vsys または vrouter 名（該当する場合）
- 公衆移動端末網 (PLMN) またはゾーン名

拡張形式におけるそれぞれのログエントリは、「基本」情報の他に、次の情報が含まれています。

- IMSI
- MSISDN
- APN
- 選択モード
- シグナリング用 SGSN アドレス
- ユーザデータ用 SGSN アドレス
- シグナリング用 GGSN アドレス
- ユーザデータ用 GGSN アドレス

注 : 監視機能の詳細は、3-55 ページの「セキュリティ デバイスの監視」を参照してください。

パケットレート制限状態の GTP パケットのロギングを使用可能にすると、ロギング頻度を指定して、セキュリティデバイスがこれらのメッセージをログに残す間隔を制御できます。例えば頻度値を 10 にすると、セキュリティデバイスは指定したレート制限を越えた 10 個ごとのメッセージだけログに残します。

ロギング頻度を設定して、syslog サーバーとセキュリティデバイスのリソースを節約し、メッセージのロギングオーバーフローを回避することができます。

例 : GTP パケットロギングを使用可能にする

この例では「 GPRS1 」GTP オブジェクト検査に対して、セキュリティログを設定してログ禁止、レート制限そして状態無効 GTP パケットにします。禁止およびレート制限パケットという基本ロギングを選び、レート制限パケットの頻度値は 10、そして状態無効パケットには拡張ロギングを指定します。

WebUI

Objects > GTP > Edit (GPRS1) > Log: 以下を入力して **Apply** をクリックします。

Packet Prohibited: Basic (**選択**)
Packet State-invalid: Extended (**選択**)
Packet Rate-Limited: Basic (**選択**)
When Packet Rate Limit is exceeded, log every other messages: 10

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set prohibited basic
(gtp:gprs1)-> set state-invalid extended
(gtp:gprs1)-> set rate-limited basic 10
(gtp:gprs1)-> exit
save
```

トラフックカウンティング

GTP トラフィックカウンティング機能では、セキュリティデバイスを設定して、保護している GGSN と SGSN から受信され、そして転送されるユーザデータとコントロールメッセージ（またはデータのバイト）の数を計算するようにできます。セキュリティデバイスはそれぞれの GTP トンネルごとに別々にトラフィックを計算し、GTP-User と GTP-Control メッセージを識別します。トンネルを削除すると、GGSN または SGSN から受信され、そして転送されるメッセージ数の合計またはデータのバイト数の合計を計算し、ログに残します。

トンネル削除のログエントリには、次の情報が含まれています。

- タイムスタンプ
- インターフェース名（該当する場合）
- SGSN IP アドレス
- GGSN IP アドレス
- TID
- 秒単位でのトンネルの時間
- SGSN に送信したメッセージの数
- GGSN に送信したメッセージの数

注： デフォルトでは、Juniper Networks セキュリティデバイスではトラフィックロギングは使用不可能になっています。

例：GTP トラリフィックカウンティングを使用可能にする

この例では、「GPRS1」GTP 検査オブジェクトのメッセージによるトラフィックカウンティングを使用可能にします。

WebUI

Objects > GTP > Edit (GPRS1) > Log: 以下を入力して **Apply** をクリックします。

Traffic Counters: Count by Message（選択）

CLI

```
set gtp config gprs1
(gtp:gprs1)-> log traffic-counters
(gtp:gprs1)-> exit
save
```

法に順守した傍受

セキュリティデバイスを設定して、IMSI プレフィックスまたは移動端末統合サービスデータネットワーク (MS-ISDN) 識別に基づいて、GTP-U または GTP-C メッセージの内容を識別し、ログに残すことができます。加入者を IMSI または MS-ISDN で識別し、加入者を行き来しているユーザデータおよびコントロールメッセージの内容をログに残すことできます。

セキュリティデバイスが同時に、積極的にトレースできる加入者の数を設定することができます。同時に積極的にトレースできる数（デフォルト）は 3 です。ユーザーデータを含む GTP パケットに関しては、ログに残すデータのバイト数を指定することができます。パケットの一部または全部をログに残すことができます。デフォルト値はゼロで、このときセキュリティデバイスは GTP-U パケットからの内容をまったくログに残しません。

セキュリティデバイスはログされたパケットを法に順守した傍受専用の外部サーバー（ Syslog など）に送信します。

例 : 法に順守した傍受を使用可能にする

この例では、セキュリティデバイスが「 GPRS1 」GTP 検査オブジェクトの IMSI プレフィックス 345678 の加入者をトレースできるようにします。また、アクティブトレース数を 2 とし、ログに残すバイト数を 1064 とします。

WebUI

Objects > GTP > Edit (GPRS1) > Subscriber Trace: 以下を入力して **Apply** をクリックします。

Maximum Simultaneous Active Trace: 2
Trace Message: 1064
Subscribers Identified by: **IMSI** を選択し、**12 3456789012345** を入力してから **Add** をクリックします。

CLI

```
set gtp config gprs1
(gtp:gprs1)-> set trace imsi 123456789012345
(gtp:gprs1)-> set trace max-active 2 save-length 1064
(gtp:gprs1)-> exit
save
```

索引

A

APN
- 選択モード....16
- フィルタリング....15–16

G

Gi インターフェース....2
Gn インターフェース....2
Gp インターフェース....2
GPRS トンネリングプロトコル (GTP)
- GTP を参照

GTP
- GTP-in-GTP パケットフィルタリング....14
- IMSI プレフィックスフィルタリング....17
- IP フラグメント化....14
- アクセスポイント名 (APN) のフィルタリング....15
- 基準....9
- 検査オブジェクト....5–7
- トンネルタイムアウト....26
- パケットサニティチェック....9
- パケット状態監視....25
- プロトコル....2
- ポリシーベース....5

GTP トラフィック....34, 32
GTP トンネル
- 制限....24
- タイムアウト....26
- フェールオーバー....26

GTP メッセージ....10, 11, 12
- 種類....10–11
- 長さ、フィルタリング....9

H

HA (high availability、高可用性)....4, 26

I

IMSI プレフィックスフィルタリング....17

L

L2TP....3

N

NAT モード....4

あ

アクセスポイント名
- APN を参照

い

移動端末 (MS) モード....16
インターフェース
- Gi....2
- Gn....2
- Gp....2

か

仮想システムサポート....5
過大請求攻撃
- 説明....27
- 防御策....29
- 予防....27–32
- 予防、設定....30

け

検証済みモード....16

こ

攻撃、過大請求....27–29

し

シーケンス番号検証....13

せ

選択モード
- APN....16
- 移動端末 (MS)....16
- 検証済み....16
- ネットワーク....16

た

タイプ、フィルタリング....10
タイムアウト....26

と

透過モード....4

動作可能モード
NAT....4
ルート....4
透過....4
トラフィック
カウンティング....5
ロギング....5

ね
ネットワークモード....16

は
バージョン 0 および 1....11

ほ
放置された GTP トンネル....26
法に順守した傍受....35
ポリシー....5
ポリシー、構成....6

も
モード、選択
APN....16
移動端末 (MS)....16
検証済み....16
ネットワーク....16
モード、動作
NAT....4
ルート....4
透過....4

る
ルートモード....4

れ
レート制限、GTP-C メッセージ....12
レート、制限....12

ろ
ロギング、トラフィック....5

わ
ワイルドカード....16

概念と用例
ScreenOS リファレンス ガイド

第 14 部 :
IPv6 によるデュアルスタックアーキテクチャ

リリース 6.0.0、改訂 02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

品番 : 530-017780-01-JP, 改訂 02

Copyright Notice

Copyright © 2007 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

目次

本編について vii

ドキュメントの対象 viii
ドキュメントの規則 viii
Web ユーザーインターフェースの規則 viii
コマンドラインインターフェースの規則 ix
ネーミング規則および文字タイプ ix
説明図の規則 x
技術ドキュメンおよびテクニカルサポート xi

第 1 章 インターネットプロトコルバージョン 6 の紹介 1

概要 2
IPv6 アドレス指定 2
表記 2
プレフィックス 3
アドレスのタイプ 3
ユニキャストアドレス 3
エニーキャストアドレス 4
マルチキャストアドレス 4
IPv6 ヘッダー 4
基本ヘッダー 4
拡張ヘッダー 5
IPv6 パケットの処理 6
IPv6 ルーターおよびホストのモード 7
IPv6 トンネリングのガイドライン 8

第 2 章 IPv6 の構成 9

概要 10
アドレスの自動構成 11
EUI（Extended Unique Identifier） 11
ルーターの通知メッセージ 12
ルーター要請メッセージ 12
プレフィックス一覧 12
隣接ノード発見 13
隣接ノードキャッシュテーブル 13
隣接ノード到達不能検出 14
隣接ノードエントリのカテゴリ 14
隣接ノード到達可能性状態 14
到達可能性状態の移行 15
IPv6 環境の有効化 18
デバイスレベルでの IPv6 の有効化 18
デバイスレベルでの IPv6 の無効化 19

IPv6 ホストの構成 19
IPv6 インターフェースのゾーンへのバインディング 20
IPv6 ホストモードの有効化 20
インターフェース ID の設定 20
アドレス自動構成の構成 21
隣接ノード発見の構成 21
IPv6 ルーターの構成 22
IPv6 インターフェースのゾーンへのバインディング 22
IPv6 ルーターモードの有効化 22
インターフェース ID の設定 23
アドレス自動構成の設定 23
Outgoing Router Advertisements フラグ 23
Managed Configuration フラグ 24
Other Parameters Configuration フラグ 24
アドレス自動構成の無効化 24
アドバタイジング時間間隔の設定 25
通知された到着可能時間間隔 25
通知された再送信時間間隔 26
最大通知間隔 26
最小通知間隔 26
通知されたデフォルトのルーター寿命 27
アドバタイジングパケットの性質 27
リンク MTU 値 27
現在のホップ制限 28
通知ルーターの性質 28
リンクレイヤーアドレスの設定 28
通知されたルーターの優先度 28
隣接ノード発見パラメータの構成 29
隣接ノード到達不能検出 29
MAC セッション ー キャッシング 29
静的隣接ノードキャッシュエントリ 30
ベース到着可能時間 30
プローブ時間 31
再送信時間 31
重複アドレス検出再試行カウント 31
IPv6 インターフェースパラメータの表示 32
隣接ノード発見構成の表示 32
現在の RA 構成の表示 32
設定例 32
IPv6 ルーター 32
IPv6 ホスト 33

第 3 章 接続およびネットワークサービス 35

概要 36
動的ホスト構成プロトコルバージョン 6 36
デバイスユニーク ID 37
ID アソシエーションプレフィックス委譲 ID 37
プレフィックスの特徴 37
サーバーの優先度 38
DHCPv6 サーバーの構成 38
DHCPv6 クライアントの構成 40
DHCPv6 設定の表示 41

ドメイン名システムサーバーの構成 42
DNS および DNS 検索リスト情報の要求 43
プロキシ DNS アドレス分割の設定 44
PPPoE の構成 46
フラグメント化の設定 47

第 4 章 静的および動的ルーティング 49

概要 50
デュアルルーティングテーブル 50
静的および動的ルーティング 51
上流および下流プレフィックスの委譲 51
静的ルーティング 52
RIPng の構成 53
RIPng インスタンスの作成と削除 54
RIPng インスタンスの作成 54
RIPng インスタンスの削除 54
RIPng をインターフェースで使用可能・不可にする 55
インターフェース上の RIPng を有効にする 55
インターフェース上の RIPng を停止する 55
RIPng に関する大域パラメータ 55
デフォルトルートの通知 56
デフォルトルートを拒否する 57
Trusted 隣接ノードを構成する 57
ルートの再配布 58
更新しきい値を設定してフラッディングを防止 59
インターフェースごとの RIPng パラメータ 60
ルート、インターフェース、およびオフセットメトリック 60
アクセスリストおよびルートマップ 61
静的ルートの再配布 61
ポイズンリバース付きスプリットホライズンの構成 63
ルーティングおよび RIPng 情報の表示 64
ルーティングテーブルの表示 64
RIPng データベースの表示 64
仮想ルーター別 RIPng の詳細の表示 65
インターフェース別 RIPng の詳細の表示 66
RIPng 隣接情報の表示 66
設定例 67
トンネルインターフェース上で RIPng を稼動させる 67
ISP ルーターへのトラフィックループの回避 69
顧客構内装置の構成 69
ゲートウェイの構成 73
ISP ルーターの構成 75
OSPF への Null インターフェース再配布の設定 76
発見したルートの OSPF への再配布 77
OSPF サマリーのインポートのセットアップ 77

第 5 章 アドレス変換 79

概要 80
ソース IP アドレスの変換 81
IPv6 から IPv4 への DIP 81
IPv4 から IPv6 への DIP 81
宛先 IP アドレスの変換 82
IPv6 から IPv4 への MIP 82

IPv4 から IPv6 への MIP 83
設定例 83
IPv6 ホストから複数 IPv4 ホストへの送信 84
IPv6 ホストから単一 IPv4 ホストへの送信 86
IPv4 ホストから複数 IPv6 ホストへの送信 87
IPv4 ホストから単一 IPv6 ホストへの送信 89
ドメイン名システムサーバーアドレスの変換 91

第 6 章 IPv4 環境での IPv6 95

概要 95
手動トンネリングの構成 96
6to4 トンネリングの構成 99
6to4 ルーター 99
6to4 リレールーター 100
リモートネイティブホストへのトンネル 101
リモート 6to4 ホストへのトンネル 104

第 7 章 IPSec トンネリング 107

概要 107
IPSec 6in6 トンネリング 108
IPSec 4in6 トンネリング 111
IPSec 6in4 トンネリング 115
フラグメント化を有効にした手動トンネリング 119
IPv6 to IPv6 ルートベースの VPN トンネル 120
IPv4 to IPv6 ルートベースの VPN トンネル 122

第 8 章 IPv6 XAuth ユーザー認証 125

概要 126
RADIUSv6 126
単一クライアント、単一サーバー 126
複数クライアント、単一サーバー 126
単一クライアント、複数サーバー 127
複数ホスト、単一サーバー 127
IPSec アクセスセッション管理 128
IPSec アクセスセッション 128
IAS 機能を使用可能にまたは使用不可能にする 130
IAS セッションの解除 130
IAS 制限設定 130
デッドピア検出 131
設定例 132
XAuth と RADIUS 132
RADIUS と XAuth ルートベース VPN 133
RADIUS と XAuth、およびドメイン名ストリッピング 136
IP プール範囲の割り当て 140
RADIUS リトライ 146
Calling-Station-Id 146
IPSec アクセスセッション 147
デッドピア検出 155

付録 A スイッチング A-I

索引 ..... IX-I

本編について

*第 14 部 : IPv6 によるデュアルスタックアーキテクチャ*は、ScreenOS のインターネットプロトコルバージョン 6 （IPv6）のサポート、トンネリングと IPSec による IPv6 および IPv4/IPv6 移行ネットワークのセキュリティ保護の方法について説明します。

ネットワーク上に IPv4/IPv6 境界間でトラフィックを通過させる IPv4 と IPv6 デバイスの両方を含みながら、インターフェースの IPv4 と IPv6 モードでの同時作動が可能になり、ネットワーク管理を簡素化できます。

本編は、以下の章および付録で構成されています。

- 第 1 章「インターネットプロトコルバージョン 6 の紹介」は、IPv6 のヘッダー、概念、およびトンネリングのガイドラインを説明しています。
- 第 2 章「IPv6 の構成」は、IPv6 ルーターまたはホストとして動作するためのインターフェースの構成方法を説明しています。
- 第 3 章「接続およびネットワークサービス」は、動的ホスト構成プロトコルバージョン 6（DHCPv6）、ドメイン名サービス（DNS）、PPPoE（Point-to-Point Protocol over Ethernet）、およびフラグメント化を構成する方法を説明しています。
- 第 4 章 「静的および動的ルーティング」は、静的および動的ルーティングをセットアップする方法を説明しています。この章では、RIPng（Routing Information Protocol-Next Generation）の ScreenOS によるサポートについて説明します。
- 第 5 章「アドレス変換」は、IPv4/IPv6 境界を通過するため、ネットワークアドレス変換（NAT）を動的 IP（DIP）およびマップ IP（MIP）アドレスと使用する方法を説明しています。
- 第 6 章「IPv4 環境での IPv6」、では、手動による、または動的なトンネリング方法を説明します。
- 第 7 章「IPSec トンネリング」では、異種ホストを接続するため IPSec トンネリングを構成する方法を説明しています。
- 第 8 章「IPv6 XAuth ユーザー認証」、では、RADIUS（Remote Authentication Dial In User Service）および IPSec アクセスセッション（IAS）管理を構成する方法を説明しています。
- 付録 A「スイッチング」では、IPv6 トラフィックを通過させるためスイッチとしてセキュリティデバイスを使用するオプションを示します。

ドキュメントの対象

このマニュアルは、IPv6 または IPv4/IPv6 環境においてセキュリティソリューションを配備、管理する必要がある、経験豊かなネットワーク管理者を対象としています。

ドキュメントの規則

このドキュメントは、次のセクションで説明されている規則を使用しています。

- viii ページの「Web ユーザーインターフェースの規則」
- ix ページの「コマンドラインインターフェースの規則」
- ix ページの「ネーミング規則および文字タイプ」
- x ページの「説明図の規則」

Web ユーザーインターフェースの規則

WebUI（Web ユーザーインターフェース）では、各作業の操作指示は、操作手順と構成設定値に分かれています。構成設定を入力できる WebUI ページを開くには、画面の左側にあるナビゲーション ツリーのメニュー項目をクリックして、そのページに移動します。先へ進むと、ナビゲーション パスが画面の上部に表示されます。各ページは角括弧で分離されています。

WebUI のパスおよびアドレスを定義するためのパラメータは、以下のとおりです。

Policy > Policy Elements > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (**選択**), 10.2.2.5/32
Zone: Untrust

構成設定のオンラインヘルプを開くには、画面の左上にある疑問符（?）をクリックします。

ナビゲーションツリーにも、Help > Config Guide 構成ページがあり、セキュリティポリシーおよび IPSec （インターネットプロトコルセキュリティ）の構成に役立ちます。ドロップダウンメニューからオプションを選択して、そのページの指示に従います。構成設定のオンラインヘルプを開くには、左上にある **?** 文字をクリックします。

コマンドラインインターフェースの規則

次の規則は、例とテキストにおいて、コマンドラインインターフェース（CLI）コマンドの構文を示すために使用されます。

例においては、次のように使用されます。

- 角括弧 [ ] 内にあるものはすべてオプションです。
- 中括弧 { } 内にあるものはすべて必須です。
- 選択肢が複数ある場合、各選択肢はパイプ (|) で区切られています。例えば、次のように表示されます。

```
set interface { ethernet1 | ethernet2 | ethernet3 } manage
```

- 変数は*斜体*で表示されます。

```
set admin user name1 password xyz
```

テキストにおいては、コマンドは**太字**で、変数は*斜体*で表示されます。

注 : キーワード入力時には、単語を間違いなく識別できる数の文字を入力すれば十分です。**set admin user wheezer j12fmt54** というコマンドを入力する際には、**set adm u whee j12fmt54** と入力するだけで十分です。ただし、本編に記載されたコマンドはすべて本来の形式で記載されています。

ネーミング規則および文字タイプ

ScreenOS はオブジェクトの名前 (アドレス、管理ユーザー、認証サーバー、IKE ゲートウェイ、仮想システム、VPN トンネルおよびゾーンなど、ScreenOS 構成に定義されているもの) に関して、次の規則に従います。

- 名前文字列に 1 つまたは複数のスペースが含まれる場合、文字列全体を二重引用符で囲む必要があります。例 :

  set address trust “local LAN” 10.1.1.0/24

- 二重引用符で囲まれた文字列の先頭または末尾のスペースを取り除きます。たとえば、「 **local LAN** 」は「**local LAN**」となります。
- 連続した複数のスペースは、一つのスペースとして扱われます。
- CLI キーワードの多くはケースセンシティブではありませんが、名前文字列はケースセンシティブです。たとえば、「**local LAN**」は「**local lan**」とは異なります。

ScreenOS は、次の文字タイプをサポートします。

- 1 バイト文字セット (SBCS) およびマルチバイト文字セット (MBCS)。SBCS の例に、ASCII、欧州言語、およびヘブライ語があります。2 バイト文字セット (DBCS) とも呼ばれる MBCS の例に、中国語、韓国語、および日本語があります。

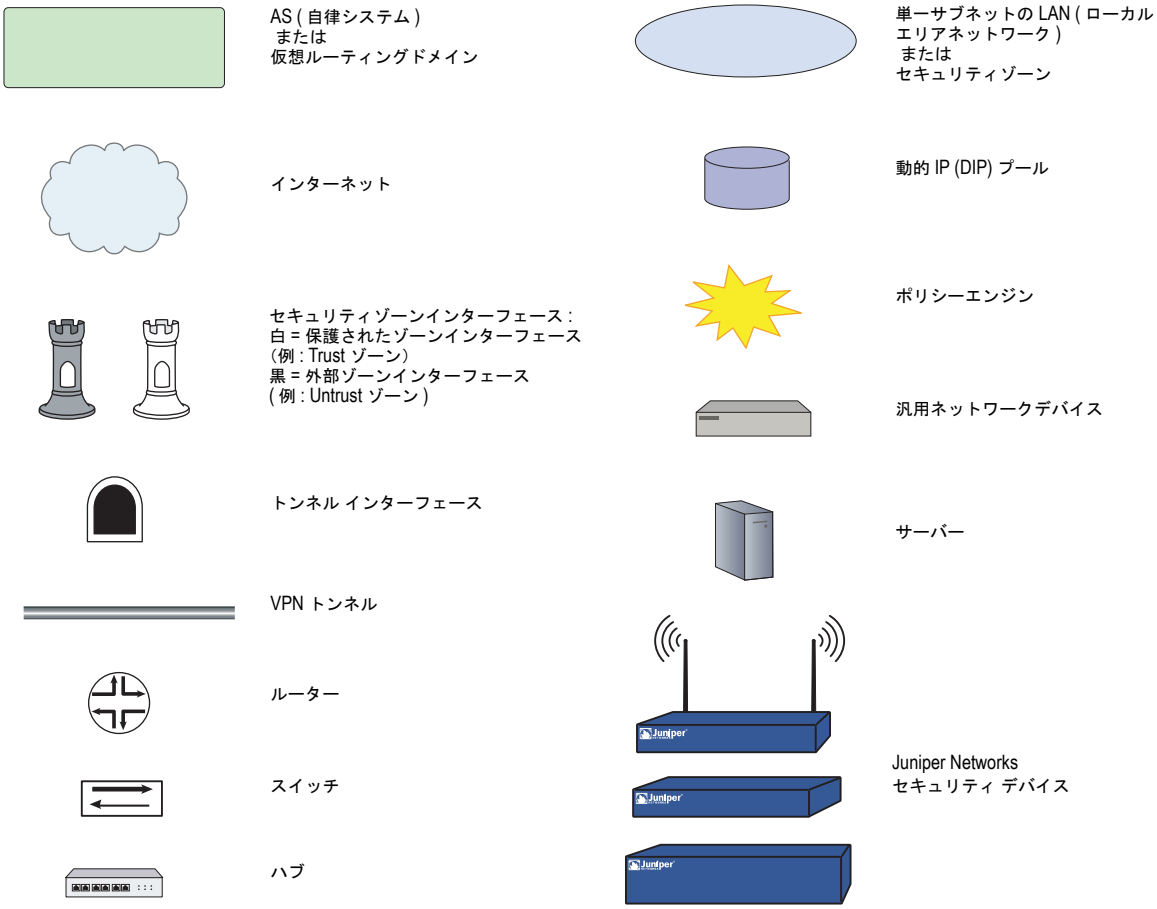
- ASCII 文字の 32（16 進数の 0x20）から 255（0xff)。ただし二重引用符 (“) は、スペースを含む名前文字列の先頭と末尾を示す特殊な意味をもつため、例外とします。

注： コンソール接続では、SBCS のみがサポートされます。ご利用のブラウザがサポートする文字セットに応じて、WebUI は SBCS および MBCS の両方をサポートします。

説明図の規則

次の図は、本編を通して説明図に使用されている画像の基本的なものです。

図 1: 説明図の画像



技術ドキュメンおよびテクニカルサポート

Juniper Networks 製品のいずれかの技術ドキュメントを入手するには、www.juniper.net/techpubs/ をご覧になってください。

テクニカルサポートについては、http://www.juniper.net/customers/support/ にある Case Manager を使って事例サポートを開くか、1-888-314-JTAC (米国内) か 1-408-745-9500 (その他の国) までお問い合わせください。

本書に間違いや欠落があった場合は、techpubs-comments@juniper.net までお知らせください。

第 1 章

インターネットプロトコルバージョン 6 の紹介

ScreenOS は、IETF（Internet Engineering Task force）が策定した、インターネットプロトコルバージョン 6（IPv6）をサポートします。

注： セキュリティデバイスには IPv6 をサポートするものがあります。ご使用のセキュリティプラットフォームのデータシートをチェックして、どの機能をサポートしているか判断してください。

本章のセクションは、以下のようになります。

- 2 ページの「概要」
- 2 ページの「IPv6 アドレス指定」
  - 2 ページの「表記」
  - 3 ページの「プレフィックス」
  - 3 ページの「アドレスのタイプ」
- 4 ページの「IPv6 ヘッダー」
  - 4 ページの「基本ヘッダー」
  - 5 ページの「拡張ヘッダー」
- 6 ページの「IPv6 パケットの処理」
- 7 ページの「IPv6 ルーターおよびホストのモード」
- 8 ページの「IPv6 トンネリングのガイドライン」

概要

IPv4 とは異なるアドレス指定およびスキーマを使用することにより、IPv6 では IPv4 より多くのホストに接続できます。さらに、IPv6 はパケット処理のオーバーヘッドを減らし、ネットワークのスケーラビリティを向上させます。これらの改善点により、データトラフィックの交換量を増やすことができます。

IPv6 は、IPv4 デバイスと IPv6 デバイスとの間の相互運用性を提供します。通常、IPv4 の機能を失わずにセキュリティデバイスに IPv6 をインストールできます。そのため、組織は、増分アップグレードが可能で、IPv4 から IPv6 への移行の間のサービスの中断を避けるこができます。

注： IPv6 の詳細については、RFC 2460 を参照してください。

ScreenOS の特徴はデュアルスタックアーキテクチャです。インターフェースは、IPv4 および IPv6 モードで同時に動作できます。デュアルスタックアーキテクチャでは、IPv4 および IPv6 デバイスを含むネットワークインフラストラクチャおよび IPv4/IPv6 境界を通過するトラフィックのセキュリティを確保できます。

IPv6 が有効な各セキュリティデバイスは、IPv6 ホストまたはルーターとして動作できます。

IPv6 アドレス指定

IPv6 のアドレスは、いくつかの点で IPv4 アドレスとは異なります。

- 表記
- プレフィックス
- アドレスのタイプ

これらの違いにより、IPv6 のアドレス指定は、IPv4 より簡潔さとスケーラビリティが向上しています。

表記

IPv6 アドレスは 128 ビット長（32 個の 16 進数として表現）で、コロンで区切った 8 つのセクションから構成されます。各セクションには 2 バイトが含まれ、各バイトは 0 から FF までの 16 進数として表現されます。

IPv6 アドレスは次のようになります。

2080:0000:0000:0000:0008:0800:200c:417a

各セクションの最初のゼロを省略するか、ゼロを含む連続したセクションを 2 つのコロンで置き換え、例のアドレスは次のように書くことができます。2080:0:0:0:8:800:200c:417a または 2080::8:800:200c:417a

たとえば、0000:0000:0000:0000:0000:0000:93fc:9303 は ::93fc:9303 と書くことができます。

1 つの IPv6 アドレス内で、二重コロンの区切りは 1 度しか使用できません。たとえば、IPv6 アドレス 32af:0:0:0:ea34:0:71ff:fe01 を 32af::ea34::71ff:fe01 とは表現できません。

プレフィックス

各 IPv6 アドレスには、ネットワークおよびノードまたはインターフェースを示すビットが含まれています。IPv6 プレフィックスは、IPv6 アドレスのネットワークを示す部分です。プレフィックス長は、最上位（左端の）ビットで始まる連続するビットの数を示す正の整数です。プレフィックス長は、前方スラッシュに続き、ほとんどの場合、組織が所有するアドレスの一部を示します。残りのビットはすべて（右端のビットまで）個々のノードまたはインターフェースを表します。

たとえば、32f1::250:af:34ff:fe26/64 のプレフィックス長は 64 です。

このアドレスの最初の 64 ビットはプレフィックス（32f1:0000:0000:0000）です。残りの部分（250:af:34ff:fe26）はインターフェースを示します。

アドレスのタイプ

RFC 2373 では、IPv6 アドレスの 3 つの主要カテゴリを説明しています。

- ユニキャスト
- エニーキャスト
- マルチキャスト

ユニキャストアドレス

ユニキャストアドレスは、1 つのインターフェースの ID です。ネットワークデバイスがパケットをユニキャストアドレスに送信すると、そのパケットは、そのアドレスで示される特定のインターフェースにしか届きません。

デバイスは、次のタイプのユニキャストアドレスを使用します。

- グローバルユニキャストアドレスは、ホストインターフェースに割り当てられる一意の IPv6 アドレスです。グローバルユニキャストアドレスは、IPv4 のパブリックアドレスと本質的に同じ役割を果たします。グローバルユニキャストアドレスは、集約可能であり、効率的な階層状のアドレス指定ができます。
- 6to4 アドレスは、IPv6 ホストインターフェースで 6to4 トンネリングを有効にします。6to4 インターフェースは、ホストと IPv4 ネットワーク空間との間の境界ルーターの役割を果たすことができます。ほとんどの場合、この方法は認証や暗号化パスワードなどの IPSec 動作には適していません。
- リンクローカル IPv6 アドレスでは、同じリンク上にある隣接ホスト間での通信が可能です。デバイスは、構成された各 IPv6 インターフェースについて、リンクローカルアドレスを自動的に生成します。
- IPv4 射影アドレスは、IPv4 と同等の特別な IPv6 アドレスです。デバイスは、IPv4 射影アドレスをアドレス変換に使用します。この時、デバイスはトラフィックを IPv6 ネットワークから IPv4 ネットワークへ送信する必要があります。

エニーキャストアドレス

エニーキャストアドレスは、通常は異なったノードに属する、インターフェースの集合の ID です。ネットワークデバイスがパケットをエニーキャストアドレスに送信すると、そのパケットは、そのアドレスで示されるインターフェースの 1 つに届きます。ネットワークで使用されるルーティングプロトコルは普通、どのインターフェースがエニーキャストアドレスの集合内で物理的に最も近いかを決定し、パケットを宛先への最短パスでルーティングします。

エニーキャストアドレスの詳細については、RFC 2526 を参照してください。

マルチキャストアドレス

マルチキャストアドレスは、通常は異なったノードに属する、インターフェースの集合の ID です。ネットワークデバイスがパケットをマルチキャストアドレスに送信すると、デバイスはそのパケットを、そのアドレスで示される全インターフェースにブロードキャストします。

デバイスは、次のタイプのマルチキャストアドレスを使用します。

- 隣接ノード要請（NS）メッセージのための要請ノードマルチキャストアドレス
- ルーター通知（RA）メッセージのための全ノードマルチキャストアドレス
- ルーター要請（RS）メッセージのための全ルーターマルチキャストアドレス

IPv6 ヘッダー

IETF では、低オーバーヘッドおよびスケーラビリティを考慮して IPv6 ヘッダーを設計しました。IPv6 ヘッダーは、オプションの拡張ヘッダーを使用でき、ネットワークデバイスが使用可能な追加情報を含みます。

基本ヘッダー

どの IPv6 パケットにも基本 IPv6 ヘッダーがあります。IPv6 ヘッダーは 40 バイト（320 ビット）を占有します。Figure 2 は、各フィールドを順に示します。

図 2: ヘッダー構造

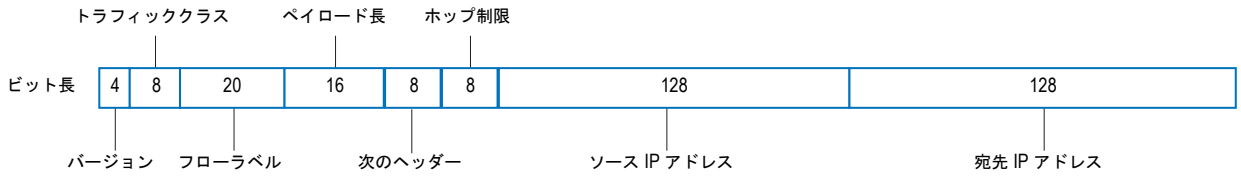


表 1 は、フィールドをビット長と目的とともに示しています。

表 1: IPv6 ヘッダーのフィールド、長さ、および目的

フィールド名	ビット長	目的
バージョン	4	ヘッダーおよびパケットが使用するインターネットプロトコルを指定します。この値は、宛先のインターネットデバイスに、パケットヘッダーおよびペイロードを処理するとき、どの IP スタック（IPv4 または IPv6）を使用するかを伝えます。IPv6 の「バージョン」フィールドは値が 6 になります。（IPv4 の「バージョン」フィールドは値が 4 になります。）
トラフィッククラス	8	ソースノードまたはルーターは、異なったクラス（または優先度）の IPv6 パケットを識別できます。（このフィールドは、パケット転送サービスのカテゴリを示す IPv4 の「サービスタイプ」フィールドに代わるものです。）
フローラベル	20	パケットが所属するフローを示します。フローの中のパケットは共通の目的を共有するか、または共通のカテゴリに属しています。ルーターや宛先ホストなどの外部デバイスにそのように解釈されます。通常、ソースホストは「フローラベル」値を発信パケットに挿入し、外部デバイスによる特別な処理を要求します。外部デバイスは、「フローラベル」値とソースアドレスを評価して、各フローを一意に識別できます。 ソースホストが送信したトラフィックには、1 つのフロー、複数のフロー内のパケットやフロー内にないパケット、あるいはいずれかを組み合わせたパケットが含まれています（フローに属さないパケットの「フローラベル」はゼロです。）
ペイロード長	16	オクタット単位で、IPv4 パケットペイロードの長さを指定します。
次のヘッダー	8	IPv6 ヘッダーの直後にあるヘッダーの IP プロトコルのタイプを示します。このプロトコルは、2 つのタイプのいずれかになります。 ■ IPv6 拡張ヘッダー。たとえば、デバイスが交換パケットに IPSec セキュリティを実行する場合、「次のヘッダー」値はおそらく 50（ESP 拡張ヘッダー）または 51（AH 拡張ヘッダー）になります。拡張ヘッダーはオプションです。 ■ 上位レイヤーのプロトコルデータユニット（PDU）。たとえば、「次のヘッダー」値が 6（TCP）、17（UDP）、または 56（ICMPv6）になります。 「次のヘッダー」フィールドは、IPv4 の「プロトコル」フィールドに代わるものです。このフィールドはオプションです。
ホップ制限	8	ホストデバイスからの送信後、パケットが移動できるホップの最大数を指定します。「ホップ制限」値がゼロの場合、デバイスはそのパケットをドロップし、エラーメッセージを生成します。（このフィールドは、Time to Live IPv4 フィールドに似ています。）
ソース IP アドレス	128	IPv6 パケットを生成したホストデバイスを示します。
宛先 IP アドレス	128	IPv6 パケットの宛先を示します。

拡張ヘッダー

拡張ヘッダーには、IPv6 パケットの転送または処理の方法を決めるため、ネットワークデバイス（ルーター、スイッチ、端点ホストなど）が使用する補足情報が含まれています。各拡張ヘッダーの長さは、8 オクテットの整数倍です。これにより、後続の拡張ヘッダーは 8 オクテット構造を使用できます。

拡張ヘッダーに続くヘッダーは、拡張ヘッダータイプを示す、「次のヘッダー」値を含んでいます。

拡張ヘッダーは必ず、次のように基本 IPv6 ヘッダーに続きます。

1. 「ホップバイホップオプション」ヘッダーは、宛先ホストへのパス上の各ホップでの配信パラメータを指定します。パケットがこのヘッダーを使用するとき、前のヘッダー（基本 IPv6 ヘッダー）の「次のヘッダー」値はゼロでなければなりません。

2. 「宛先オプション」ヘッダーは、中間宛先デバイスまたは最終宛先ホストのパケット配信パラメータを指定します。パケットがこのヘッダーを使用するとき、前のヘッダーの「次のヘッダー」値は 60 でなければなりません。

3. 「ルーティング」ヘッダーは、パケットの厳密なソースルーティングおよび緩やかなソースルーティングを定義します。（厳密なソースルーティングでは、各中間宛先デバイスは 1 ホップの距離になければなりません。緩やかなソースルーティングでは、中間宛先デバイスは 1 ホップ以上離れていてもかまいません。）パケットがこのヘッダーを使用するとき、前のヘッダーの「次のヘッダー」値は 43 でなければなりません。

4. 「フラグメント」ヘッダーは、IPv6 フラグメント化および再アセンブリサービスを実行する方法を指定します。パケットがこのヘッダーを使用するとき、前のヘッダーの「次のヘッダー」値は 44 でなければなりません。

5. 「認証」ヘッダーは、認証、データの保全性、および再生保護を提供します。パケットがこのヘッダーを使用するとき、前のヘッダーの「次のヘッダー」値は 51 でなければなりません。

6. 「セキュリティペイロードのカプセル化」ヘッダーは、セキュリティペイロードのカプセル化（ESP）パケットに対する、データの機密性、データの認証、および再生保護を提供します。パケットがこのヘッダーを使用するとき、前のヘッダーの「次のヘッダー」値は 50 でなければなりません。

IPv6 パケットの処理

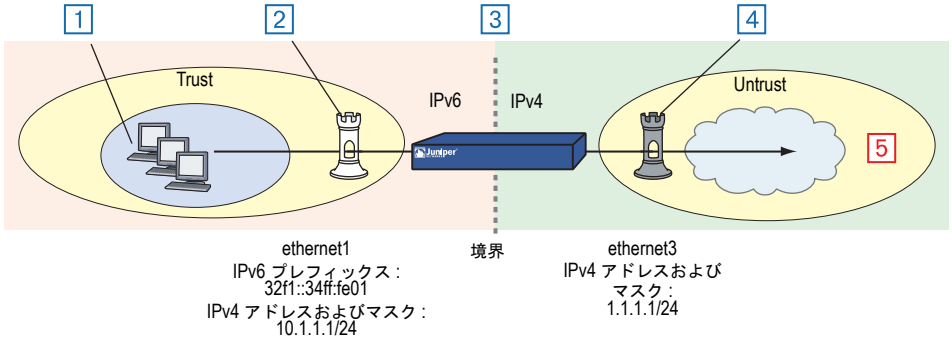
デュアルスタック動作用に構成されたインターフェースは、IPv4 および IPv6 の機能を両方とも提供します。このインターフェースは、1 つの IPv4 アドレス、少なくとも 1 つの IPv6 アドレス、あるいはその両方を持つことができます。

このインターフェースが、IPv4 ネットワークと IPv6 ネットワークとの間の境界に存在する場合、デバイスは、次のいずれかの方法で IP トラフィックに境界を通過させることができます。

- 境界を通過するパケットをカプセル化（して、隠してしまう）。
- パケットのソースおよび宛先アドレスにアドレス変換を行う。

図 1 は、IPv6 ホストが発信サービス要求パケットを IPv6/IPv4 境界を越えて IPv4 ネットワーク空間へ転送するときに行われるパケット処理フローを示します。

図 3: IPv6/IPv4 境界を越えたパケットの流れ



1. IPv6 ホストはサービス要求パケットを送信します。ソースおよび宛先アドレスは IPv6 形式を使用します。
2. IPv6 インターフェース ethernet1 がパケットを受信します。
3. セキュリティデバイスはポリシーをパケットに適用します。IPv4 パケット内に全パケットをカプセル化するか、アドレスを IPv4 形式に変換します。
4. IPv4 インターフェース ethernet3 は、（今度は IPv4 アドレス形式を使用して）パケットを送信します。
5. リモートゲートウェイノードがパケットを受信します。
   - カプセル化が行われた場合、このデバイスは、パケットを脱カプセル化するか、または IPv4 パケットとして処理を続ける場合があります。
   - IPv6/IPv4 アドレス変換が行われた場合、デバイスは、アドレスを IPv6 形式に変換するか、または IPv4 パケットとして処理を続ける場合があります。

IPv6 ルーターおよびホストのモード

セキュリティデバイスの各インターフェースを IPv6 ホストまたはルーターとして機能するよう構成できます。

- Host モードでは、インターフェースは IPv6 ホストとして機能し、他のデバイスからルーター通知（RA）メッセージを受け取り、自動構成を行います。
- Router モードではインターフェースは IPv6 ルーターとして機能します。IPv6 ルーターは、RA を送信して、IPv6 ホストからのルーター要請（RS）メッセージに応答します。さらに、インターフェースは、オンリンクのホストの更新を続けるため、定期的にまたは構成の変更に応じて RA をブロードキャストできます。

IPv6 トンネリングのガイドライン

どの種類のトンネリングを使用するか決める前に、上流サービスプロバイダに、どの IPv6 サービスをどのように提供しているかを確認します。次のガイドラインを推奨しています。

- ISP が、IPCP (Internet Protocol Control Protocol) と IPv6CP のデュアルスタック IPv6 しか提供していない場合、デュアルスタックのネイティブな IPv6 を構成します。6to4 アドレス指定はこの場合適していません。
- ISP が手動トンネル IPv6（IPv6-over-IPv4 トンネル）を提供している場合、手動トンネリングを使用します。
- ISP が IPv6 を提供していない場合、www.6bone.net を参照して、上流 IPv6 プロバイダを見つけ、その指示に従います。

IPv6 プロバイダが見つからない場合は、6to4 トンネリングを使用します。しかし、このオプションは、次ホップのルーターが 6to4 トンネリング用に構成されている場合だけ利用可能です。

第 2 章

IPv6 の構成

本章では、セキュリティデバイスで IPv6 機能を有効にする方法、および IPv6 ルーターまたは IPv6 ホストとしてセキュリティデバイスを構成する方法を説明しています。

本章のセクションは、以下のようになります。

- 10 ページの「概要」
  - 11 ページの「アドレスの自動構成」
  - 13 ページの「隣接ノード発見」
- 18 ページの「IPv6 環境の有効化」
  - 18 ページの「デバイスレベルでの IPv6 の有効化」
  - 19 ページの「デバイスレベルでの IPv6 の無効化」
- 19 ページの「IPv6 ホストの構成」
  - 20 ページの「IPv6 インターフェースのゾーンへのバインディング」
  - 20 ページの「IPv6 ホストモードの有効化」
  - 20 ページの「インターフェース ID の設定」
  - 21 ページの「アドレス自動構成の構成」

- 22 ページの「IPv6 ルーターの構成」
  - 22 ページの「IPv6 インターフェースのゾーンへのバインディング」
  - 22 ページの「IPv6 ルーターモードの有効化」
  - 23 ページの「インターフェース ID の設定」
  - 23 ページの「アドレス自動構成の設定」
  - 24 ページの「アドレス自動構成の無効化」
  - 25 ページの「アドバタイジング時間間隔の設定」
  - 27 ページの「アドバタイジングパケットの性質」
  - 28 ページの「通知ルーターの性質」
  - 29 ページの「隣接ノード到達不能検出」
  - 29 ページの「MAC セッション ー キャッシング」
  - 30 ページの「静的隣接ノードキャッシュエントリ」
  - 30 ページの「ベース到着可能時間」
  - 31 ページの「プローブ時間」
  - 31 ページの「再送信時間」
- 32 ページの「設定例」
  - 32 ページの「IPv6 ルーター」
  - 33 ページの「IPv6 ホスト」

概要

ScreenOS では、セキュリティデバイスを IPv6 ルーターまたは IPv6 ホストとして構成できます。

この概要では、以下のトピックについて説明しています。

- アドレスの自動構成
- 隣接ノード発見

概要に続くセクションでは、IPv6 ホストまたはルーターを構成する方法を説明します。

アドレスの自動構成

アドレスの自動構成では、ローカルホストは、EUI（extended unique identifier）値から IPv6 アドレスを自動構成できます。アドレス自動構成用に設定されたセキュリティデバイスは、IPv6 プレフィックスをローカル IPv6 ホストに通知します。ローカルホストは、このプレフィックスを使用して、EUI 値から IPv6 アドレスを自動構成します。

*アドレス自動構成*は、アドレスを各ホストに手動で割り当てる必要をなくします。IPv6 ホストで、アドレス自動構成が有効になっていることが理想です。IPv6 ルーターとして動作するよう構成されているインターフェースは、ローカルのオンリンク IPv6 ホストが自動構成をできるようにすることが可能です。自動構成は、DHCPv6（Dynamic Host Configuration Protocol version 6 - ダイナミック ホスト コンフィギュレーション プロトコル バージョン 6）のような、ステートフル構成プロトコルを必要としません。

EUI（Extended Unique Identifier）

EUI アドレスは、64 ビットの 16 進インターフェース ID です。EUI 値を明示的に指定しない場合、セキュリティデバイスは、値を IPv6 インターフェースの MAC アドレスから自動生成します。これは通常、はじめて IPv6 インターフェースを定義した場合すぐに行われます。

アドレス自動構成用に設定されたデバイスは、IPv6 プレフィックスをローカル IPv6 ホストに通知します。ローカルホストは、このプレフィックスを使用して、EUI 値から IPv6 アドレスを自動構成します。

注 : EUI の詳細については、http://standards.ieee.org/regauth/oui/tutorials/EUI64.html にある *Guidelines for 64-Bit Global Identifier (EUI-64) Registration Authority* を参照してください。

ルーターの通知メッセージ

ルーター通知（RA）は、ルーターがオンリンクのホストに定期的に、または他のルーターからのルーター要請（RS）要求への応答として、送信するメッセージです。RA の自動構成情報には、次のエントリが含まれます。

- IPv6 ルーターの IPv6 プレフィックス - これにより、オンリンクのホストがルーターにアクセスできます。
- 最大伝送単位（MTU） - オンリンクのホストに、交換パケットの最大サイズ（バイト数）を通知します。
- ルーターへの具体的なルート - これにより、オンリンクのホストは、ルーターへパケットを送信できます。
- IPv6 アドレス自動構成を行うかどうか、また適切な場合はプレフィックスの一覧
- 自動構成されたアドレスが有効であり優先される期間

ルーター要請メッセージ

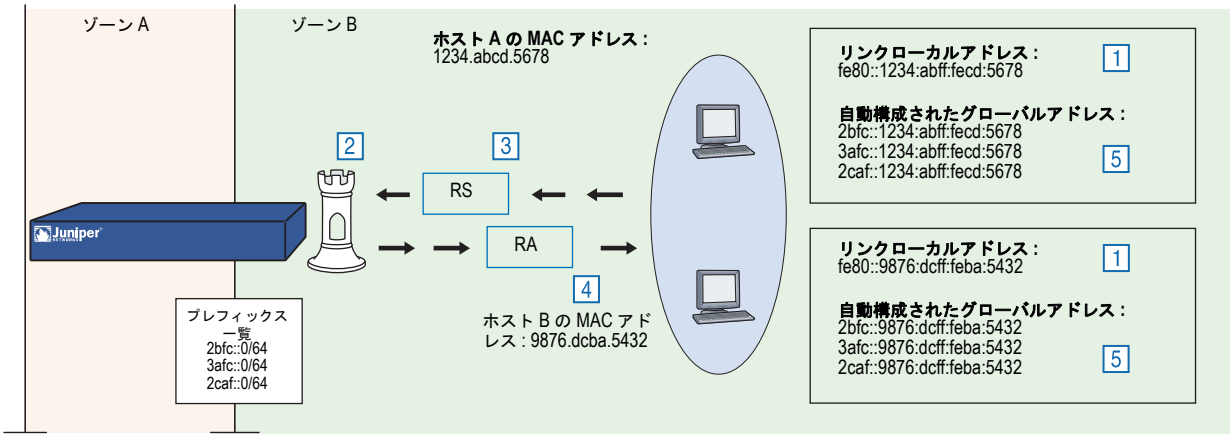
ルーター要請（RS）は、オンリンクのルーターの存在および属性を発見するため、ホストが送信するメッセージです。IPv6 ルーターがホストから RS 要求を受信すると、ホストに RA メッセージを送信することにより応答します。RA は、ルーターの存在を通知し、自動構成タスクを実行するのに必要とする情報をホストに提供します。

各 RS には、ソースホストのリンクローカルアドレスが含まれます。ホストは、リンクローカルアドレスを MAC アドレスから取得します。IPv6 ルーターが RS を受信すると、リンクローカルアドレスを使用して、RA をホストへ返信します。

プレフィックス一覧

*プレフィックス一覧*は、IPv6 プレフィックスを含む表です。エントリが一覧に存在する場合、ルーターは、オンリンクホストに送信する RA にそのエントリを含めます。ホストが RA を受信するごとに、プレフィックスを使用して、アドレス自動構成を行います。図 4 は、ホスト A およびホスト B が、これらのプレフィックスを使用して、ユニークなグローバル集約可能アドレスを生成している様子を示します。

図 4: アドレスの自動構成



1. IPv6 ホスト A および B は、起動時に MAC アドレスからリンクローカルアドレスを生成します。
2. 各ホストは RS メッセージをブロードキャストします。各メッセージは、ホストのリンクローカルアドレスを、RS パケットのソースアドレスとして使用します。
3. IPv6 ルーターが RS メッセージを受信します。
4. IPv6 ルーターは、ホストに確認 RA メッセージを送信します。これらのメッセージにはプレフィックス一覧が含まれています。
5. ホストは、プレフィックスを使用して自動構成を行います。

隣接ノード発見

隣接ノード発見（ND）は、ローカルリンクの隣接ノードの到達可能性状況をトラッキングするプロセスです。隣接ノードが IP トラフィックまたは隣接ノード要請（NS）要求を受信し処理したことの最近の確認をデバイスが受信すると、デバイスは隣接ノードが到達可能であると見なします。それ以外の場合は、隣接ノードは到達不可能であると見なします。明示的には要求されませんが、IPv6 ホストは ND が使用可能になっている場合があります。ND が使用可能な IPv6 ルーターは、ND 情報をダウンストリームへ送信できます。

隣接ノードキャッシュテーブル

隣接ノードキャッシュテーブルには、ホストが最近トラフィックを送信した隣接ノードに関する情報が含まれていますさらに、テーブルは、ローカルリンク上の隣接ノードの現在の到達可能性状況を追跡します。各エントリには次の情報が含まれています。

- 隣接ノードの IPv6 アドレス
- 隣接ノードの MAC アドレス
- 現在の隣接ノード到達可能性状態
- 隣接ノードエントリのエージ
- 宛先隣接ノードへの送信のため現在キューにはいっているパケットの数

テーブルエントリには IPv6 アドレスのキーが付いています。

隣接ノード到達不能検出

隣接ノード到達不能検出（NUD）は、隣接ノードキャッシュテーブルの構築と保守により機能します。テーブルには、ホストが最近トラフィックを送信した各隣接ノードのアドレスが含まれています。デバイスはこれらのエントリを使用して、隣接ノードの到達可能性状況の変化を記録します。NUD で、デバイスは各隣接ノードの到達可能性状態の変化を追跡し、トラフィック転送の決定を行うことができます。

隣接ノードエントリのカテゴリ

隣接ノードキャッシュテーブルのエントリは、4 つのカテゴリのいずれかに属することができます。エントリのカテゴリは、デバイスが最初にエントリを生成し、その後到達可能性状態を管理する方法を決定します。

- **端点ホストエントリ** - 端点ホストが隣接ノードにトラフィックを送信する最初の試行で、デバイスはそれに対応するエントリを隣接ノードキャッシュテーブルに自動的に生成します。デバイスはこのエントリを使用してその後の通信を行い、端点ホストの到達可能性状態を追跡します。

- **次ホップゲートウェイルーターエントリ** - ゲートウェイルーター用のデバイスで仮想ルーティングテーブルを作成するするとき、デバイスはそれに対応するエントリを隣接ノードキャッシュテーブルに自動的に生成します。デバイスは、このエントリを使用して、その後の通信を行い、ゲートウェイルーターの到達可能性状態を追跡します。

- **手動トンネルゲートウェイインターフェースエントリ** - 手動の IPv6 over IPv4 トンネルインターフェースをセットアップするとき、デバイスは、そのインターフェースのエントリを自動的に生成します。このエントリには IPv6 ローカルリンクアドレスが含まれています。デバイスはこのエントリを使用して、トンネルの到達可能性状態を監視します。

  - IPv6 over IPv4 トンネリングの詳細は、115 ページの「IPSec 6in4 トンネリング」を参照してください。

  - リンクローカルアドレスの詳細は、96 ページの「手動トンネリングの構成」を参照してください。

  - トンネルゲートウェイ移行の詳細は、17 ページの「トンネルゲートウェイ状態の移行」を参照してください。

- **静的エントリ** - 隣接ノードキャッシュエントリを静的に作成すると、デバイスはそれを使用して ND または NUD 操作を実行しません。代わりに、そのエントリには“Static”という特別な到達可能性状態が割り当てられます。これにより、すべての環境でこのエントリが有効になります。このエントリが存在する間は、デバイスは、示された隣接ノードへ送信されるトラフィックを転送します。

隣接ノード到達可能性状態

デバイスが隣接ノードに最初の NS 要求を送信するまで、隣接ノードについて隣接ノードキャッシュエントリは存在しません。それまでは、デバイスは隣接ノードの存在を認識しません。デバイスが最初の要求を送信すると、テーブルエントリを作成し“Incomplete”状態に設定します。

到達可能性状態は次のとおりです。

- **Incomplete:** ホストが、現在デバイスに未知の隣接ノードへトラフィックを送信しようと試みましたが、最初のアドレス解決がまだ進行中です。デバイスは、隣接ノードを発見するため（問い合わせ済みノードのマルチキャストアドレスを使用して）NS 要求をブロードキャストしますが、確認の隣接ノード通知（NA）をまだ受信していません。

  Incomplete 状態は、隣接ノードが次ホップのゲートウェイルーターであれば、異なった性質を持ちます。詳細については、16 ページの「次ホップゲートウェイルーター状態の移行」を参照してください。

- **Reachable:** デバイスは現在、隣接ノードから 確認 NA 応答を受信したので、隣接ノードが到着可能であると見なしています。エントリの状態が Reachable である間は、デバイスは、その隣接ノードへ送信されるトラフィックを転送します。エントリの状態は、到着可能期間（秒単位）が経過するまで、Reachable のままになります。その後、Stale へと変化します。

- **Stale:** 隣接ノードから直近の NA が来てから到着可能期間が経過したので、デバイスは、隣接ノードを到達不可能と見なします。しかし、ホストが隣接ノードへさらにトラフィックを送信しようと試みるまで、デバイスは到達可能性を確認しません。

- **Delay:** ホストは、状態が Stale である間に隣接ノードへトラフィックを送信しようと試みました。デバイスは、隣接ノードの到達可能性を積極的に確認しようとはしません。代わりに、上位レイヤーのプロトコルが到達可能性の確認を行ってくれるのを待ちます。デバイスは、5 秒間 Delay 状態にとどまります。デバイスが、この遅延時間に確認を受信すると、状態は Reachable に変化します。それ以外の場合は、状態が Probe に変化します。

- **Probe:** Delay の期間が経過し、デバイスは、上位レイヤーのアプリケーションから確認を受信しませんでした。デバイスは、2 件までのユニキャスト NS プローブを送信して、到達可能性を確認します。デバイスが、隣接ノードから NA メッセージを受信した場合、状態は Reachable へ変化します。それ以外の場合は、デバイスは、テーブルから到達可能性エントリを削除します。結果として、隣接ノードのエントリを削除することで、デバイスは隣接ノードを存在しないと見なします。

- **Probe Forever:** デバイスは、隣接ノードが到着可能とはもはや見なしていません。隣接ノードへトラフィックを転送しようと試み、到達可能性を確認するため、ユニキャスト NS プローブを送信しています。デバイスは、無制限に、または隣接ノードから到達可能性の確認を受信するまで、プローブを再送信し続けます。

  デバイスが Probe Forever 到達可能性状態を使用するのは、エントリが次ホップのゲートウェイルーターを表すとき *だけ*です。

注 : 隣接ノードキャッシュエントリは、Active および Inactive 状態でも存在する場合がありますが、隣接ノードが手動の IPv6in4 トンネルゲートウェイインターフェースであるときだけです。

到達可能性状態の移行

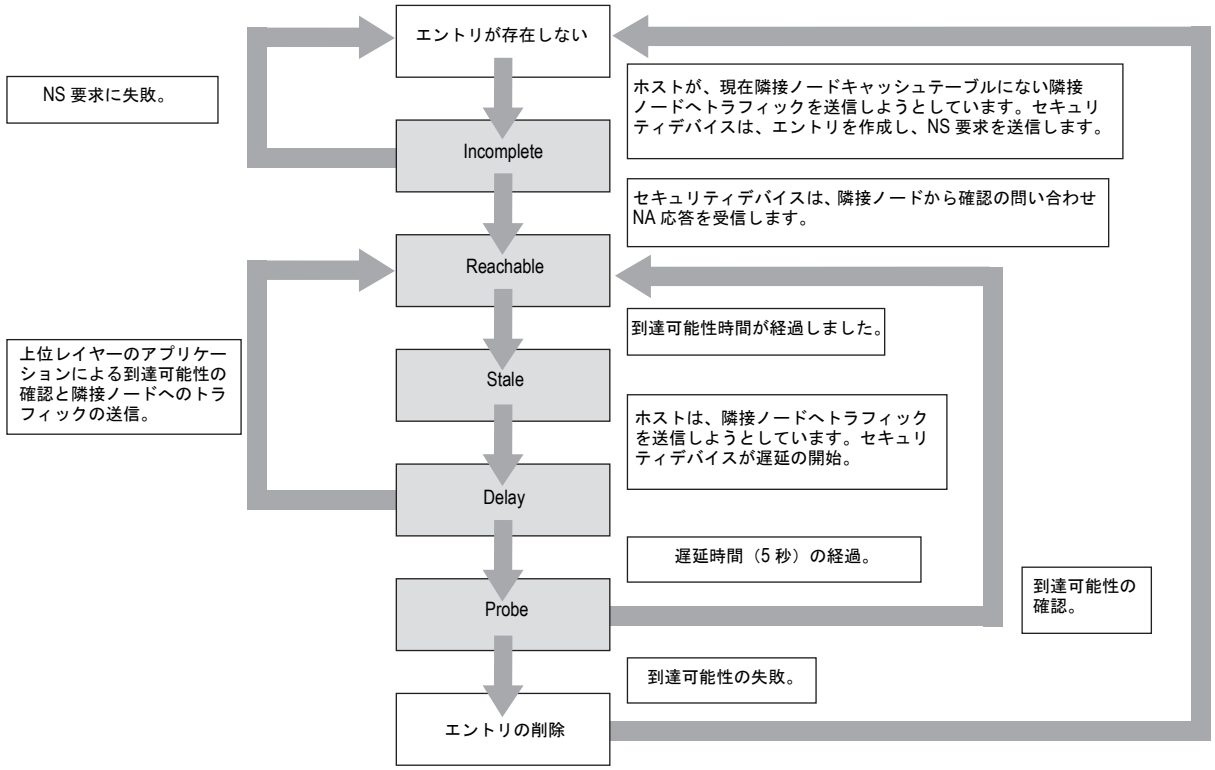
隣接ノードのカテゴリ、現在のエントリの状態、およびオンリンクホストが隣接ノードへトラフィックを送信しようとしているかどうかにより、デバイスは隣接ノードキャッシュエントリの到達可能性状態を変更します。

端点ホスト状態の移行

オンリンクのホストが隣接ノードへトラフィックを送信しようとすると、デバイスは、対応する隣接ノードキャッシュテーブルエントリを隣接ノードキャッシュテーブルで検索します。エントリが存在しない場合、デバイスは、隣接ノードに対する NS メッセージをブロードキャストします。次に、新しいテーブルエントリを作成し、それに Incomplete 状態を割り当てます。

図 5 は、隣接ノードキャッシュエントリを生成した後、デバイスが到達可能性状態の移行を処理する様子を示しています。

図 5: 端点ホスト到達可能性の移行

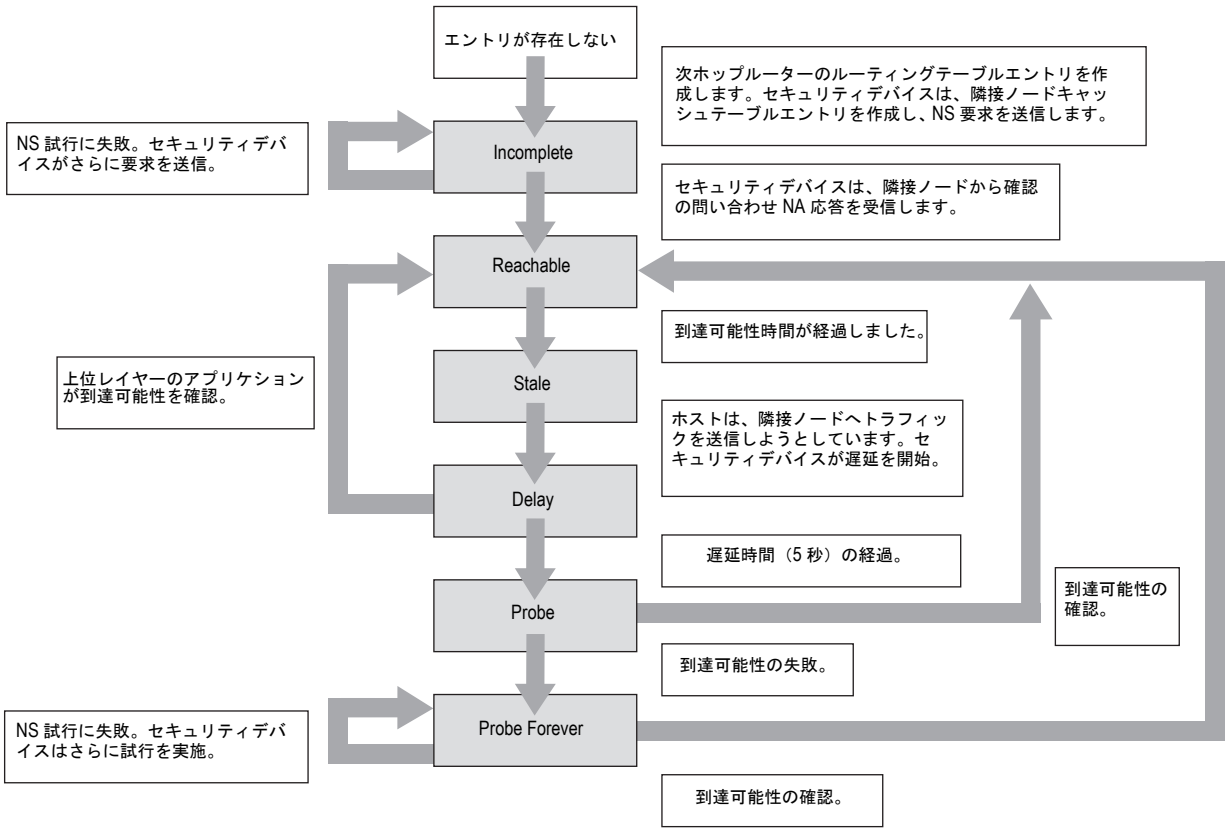


次ホップゲートウェイルーター状態の移行

IPv6 次ホップゲートウェイルーターへのルーティングテーブルエントリを作成するとき、デバイスは自動的に対応する隣接ノードキャッシュテーブルエントリを生成し、それに Incomplete 状態を割り当てます。

図 6 は、隣接ノードキャッシュエントリを初めて生成した後、デバイスが到達可能性状態の移行を処理する様子を示しています。

図 6: 次ホップゲートウェイルーター到達可能性の移行



デバイスが隣接ノードキャッシュテーブルエントリを作成したルーターを削除すると、デバイスは自動的にそのエントリを削除します。

トンネルゲートウェイ状態の移行

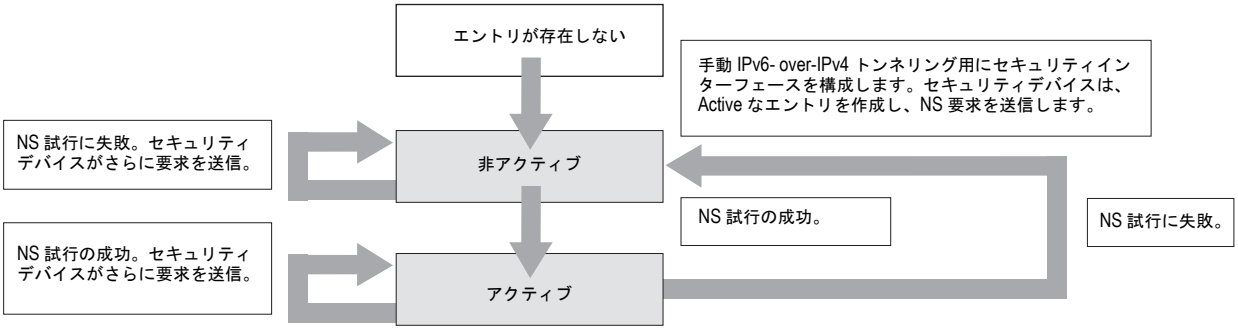
手動 IPv6-in-IPv4 トンネリングにインターフェースを構成するとき、デバイスは自動的に対応するエントリを隣接ノードキャッシュテーブルに生成します。

デバイスは、2 つのエントリ状態（ハートビート状態とも言う）を使用します。

- **Inactive:** デバイスは隣接ノードが到着可能であると見なしておらず、到達可能性をテストするため NS メッセージを送信しました。
- **Active:** デバイスは隣接ノードを到着可能であると見なしており、到達可能性を確認するため定期的に NS メッセージを送信します。

IPv6-over-IPv4 トンネルを作成するとき、デバイスは隣接ノードキャッシュエントリを生成し、それに Inactive 状態を割り当てます。図 7 は、最初のエントリを生成した後、デバイスが到達可能性状態の移行を処理する様子を示しています。

図 7: トンネルゲートウェイ状態の移行



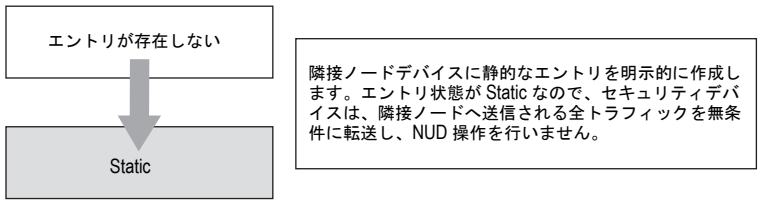
デバイスが隣接ノードキャッシュテーブルエントリを作成した手動トンネルを削除すると、デバイスは自動的にそのエントリを削除します。

IPv6 over IPv4 トンネリングの詳細は、107 ページの「IPSec トンネリング」を参照してください。

静的エントリの移行

静的なエントリを作成すとき、NUD 操作が適用されないので、デバイスは隣接ノードへ送信されるトラフィックを必ず転送します。

図 8: 静的エントリ状態の移行



IPv6 環境の有効化

セキュリティデバイスを IPv6 操作用にセットアップするには、最初にデバイスの IPv6 環境変数を有効にする必要があります。この手順を完了しないと、WebUI または CLI で IPv6 機能またはオプションを確認できません。

デバイスレベルでの IPv6 の有効化

デバイスで IPv6 を有効にするには、そのデバイスで CLI セッションを開始しなければなりません。Telnet や SSH（Secure Shell）のような、VT100 端末をエミュレートするソフトウェアを使用して、CLI セッションを確立できます。コンソールポートからの直接接続には、HyperTerminal が使用できます。CLI セッション確立の詳細は、セキュリティデバイスに付属する*ユーザーズガイド*を参照してください。

セキュリティデバイスの IPv6 状態を確認するには、次のコマンドを入力します。

```
get envar
```

デバイスで現在 IPv6 が有効な場合、次のようにコンソール出力に表示されます。

```
ipv6=yes
```

この出力が表示されない場合、デバイスで IPv6 は有効になっていません（デフォルト）。IPv6 を有効にするには、次のコマンドを入力します。

```
set envar ipv6=yes
save
reset save-config yes
```

確認プロンプトが表示されたら、**y** を入力します。

デバイスレベルでの IPv6 の無効化

HyperTerminal や他の端末エミュレーションソフトウェアでコンソール接続を確立し、デバイスとの CLI セッションを開始する必要があります。

IPv6 を無効にするには、次のコマンドを入力します。

```
unset envar ipv6
save
reset
```

確認プロンプトが表示されたら、**y** を入力します。

IPv6 ホストの構成

デバイスの IPv6 操作を有効にした後、次の手順を行って、そのデバイスを IPv6 ホストに構成できます。

1. インターフェースをゾーン（Trust、Untrust、またはユーザー定義ゾーン）にバインドします。
2. モードおよびインターフェースを有効にします。
3. アドレス自動設定を構成します。
4. 隣接ノード発見を構成します。

次のセクションでは、IPv6 ホスト構成に関連する ScreenOS 設定を説明します。

注 : オプションで、IPv6 アドレスに加えて、セキュリティデバイスは、同じインターフェースに関連付けられた IPv4 IP アドレスを持つこともできます。IPv4 インタフェースの構成方法については、*第 2 部: 基本*を参照してください。

IPv6 インターフェースのゾーンへのバインディング

WebUI または CLI で、インターフェースをカスタムのまたはあらかじめ設定したセキュリティゾーンへバインドできます。インターフェースの名前はプラットフォームにより異なります。ご使用のセキュリティデバイスのインターフェースを表示するには、**get interface** コマンドを使用します。

次の例では、ethernet1/2 という名前のインターフェースを Trust ゾーンにバインドします。

WebUI

Network > Interfaces: **Edit** を選択して、既存のインターフェースエントリのゾーンバインディングを変更するか、または **New** をクリックして、新しいインターフェースエントリを構成します。

CLI

```
set interface ethernet1/2 zone trust
save
```

IPv6 ホストモードの有効化

WebUI または CLI から IPv6 モードを有効にできます。モードオプションは、none (IPv6 を使用しない)、host または router です。

WebUI

Network > Interfaces: **Edit** を選択して、既存のインターフェースエントリの IPv6 モードを変更するか、または **New** をクリックして、新しいインターフェースエントリを構成します。**Host** モードを選択します。

Network > Interfaces > Edit (for ethernet1) > IPv6

CLI

```
set interface ethernet1/2 ipv6 mode host
set interface ethernet1/2 ipv6 enable
save
```

インターフェース ID の設定

インターフェースに EUI (Extended Unique Identifier) を構成できます。EUI は、MAC (Media Access Control) アドレスを 64 ビットの 16 進数で拡張したものです。デバイスは、この値を使用して、インターフェースの IPv6 リンクローカル IP アドレスを自動構成します。

WebUI

Network > Interfaces: **Edit** を選択して、既存のインターフェースエントリのゾーンバインディングを変更するか、または **New** をクリックして、新しいインターフェースエントリを構成します。**Interface ID** を入力します。

CLI

```
set interface ethernet1/2 ipv6 interface-id 0210dbfffe7ac108
save
```

アドレス自動構成の構成

アドレス自動構成のプレフィックスリストエントリを定義したら、IPv6 オンリンクホストは、そのプレフィックスを使用して、一意の IPv6 アドレスを生成できます。次の例では、プレフィックスリストエントリ 2bfc::0/64 を定義します。

WebUI

Network > Interfaces > Edit (for IPv6 interface) > Prefix lists 次のように入力してから **OK** をクリックします。

New IPV6 Prefix/Length: 2bfc::0/64
Prefix Flags
Autonomous: (**選択**)
Onlink (**選択**)

CLI

```
set interface ethernet3 ipv6 ra prefix 2bfc::0/64 autonomous onlink
```

この設定を行った後は、デバイスは、オンリンクホストへ送信する RA にこのプレフィックスを自動的に含めます。

隣接ノード発見の構成

インターフェースに指示して他のルーターの存在や素性を確認するには、IPv6 インターフェースの Accept Incoming RAs 設定を有効にできます。この設定が有効であれば、インターフェースは他の IPv6 ピアデバイスから RA メッセージを受け取ります。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Accept Incoming Router Advertisements: (**選択**)

CLI

```
set interface ethernet3 ipv6 ra accept
```

この設定を有効にした後、インターフェースは、リンク内にある他のホストから受信するルート通知を受け取ります。インターフェースがこの通知を受信すると、通知された IPv6 アドレスおよび MAC アドレスを隣接ノードキャッシュテーブルに保管します。

インターフェースが通知されたルートを受信、保管したか確認するには、次のコマンドを実行して NDP テーブルの内容を表示できます。

get ndp

IPv6 ルーターの構成

IPv6 ルーターを構成するには、次の手順を行います。

1. デバイスで IPv6 環境を有効にします。
2. インターフェースをゾーン（Trust、Untrust、またはユーザー定義ゾーン）にバインドします。
3. モードおよびインターフェースを有効にします。
4. アドレス自動設定を構成します。
5. ルーター通知（RA）パラメータを構成します。
6. 隣接ノード発見（ND）パラメータを構成します。

次のセクションでは、IPv6 ルーター構成に関連する ScreenOS 設定を説明します。

注： オプションで、IPv6 アドレスに加えて、セキュリティデバイスは、同じインターフェースに関連づけられた IPv4 IP アドレスを持つこともできます。IPv4 インターフェース構成の詳細は、*第 2 部: 基本* を参照してください。

IPv6 インターフェースのゾーンへのバインディング

WebUI または CLI で、インターフェースをカスタムのまたはあらかじめ設定したセキュリティゾーンへバインドできます。インターフェースの名前はプラットフォームにより異なります。

次の例では、ethernet1/2 という名前のインターフェースを Trust ゾーンにバインドします。

WebUI

Network > Interfaces: Edit を選択して、既存のインターフェースエントリのゾーンバインディングを変更するか、または **New** をクリックして、新しいインターフェースエントリを構成します。

CLI

```
interface ethernet1/2 zone trust
save
```

IPv6 ルーターモードの有効化

WebUI または CLI から IPv6 モードを有効にできます。モードオプションは、none（IPv6 を使用しない）、host、または router です。

WebUI

Network > Interfaces: Edit を選択して、既存のインターフェースエントリの IPv6 モードを変更するか、または **New** をクリックして、新しいインターフェースエントリを構成します。**Router** モードを選択します。

Network > Interfaces > Edit (for ethernet1) > IPv6

CLI

```
set interface ethernet1/2 ipv6 mode router
set interface ethernet1/2 ipv6 enable
save
```

インターフェース ID の設定

IPv6 インターフェース ID は、インターフェースの EUI（Extended Unique Identifier）を設定します。EUI は、MAC（Media Access Control ）アドレスを 64 ビットの 16 進数で拡張したものです。デバイスは、この値を使用して、インターフェースの IPv6 リンクローカル IP アドレスを自動構成します。

WebUI

Network > Interfaces: Edit を選択して、既存のインターフェースエントリのゾーンバインディングを変更するか、または **New** をクリックして、新しいインターフェースエントリを構成します。**Interface ID** を入力します。

CLI

```
set interface ethernet1/2 ipv6 interface-id 0210dbfffe7ac108
save
```

アドレス自動構成の設定

IPv6 ルーターにホスト自動構成を設定するには、次の手順をすべて行う必要があります。

- Outgoing Router Advertisements 設定を有効にします。
- Managed Configuration Flag を無効にします。
- Other Parameters Configuration Flag を無効にします。

Outgoing Router Advertisements フラグ

Outgoing Router Advertisements フラグを有効にすると、インターフェースはオンリンクホストへルーター通知（RA）メッセージを送信できます。この設定を有効にした後、インターフェースは直ちにリンク内のホストへルート通知をブロードキャストします。また、ホストからルーター要請（RS）を受信するか、またはインターフェースの RA 設定をユーザーが変更すると、RA を自動的にブロードキャストします。

次の例では、Allow RA Transmission 設定を有効にします。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Allow RA Transmission: (選択)

CLI

```
set interface ethernet3 ipv6 ra transmit
```

Managed Configuration フラグ

Managed Configuration フラグを有効にすると、ローカルホストは、DHCPv6 のようなステートフルアドレス自動構成プロトコルを使用して、ホストアドレスを生成します。

ローカルホストは、この設定が有効な間、ステートレスアドレス自動構成はできません。

次の例では、Managed Configuration フラグを無効にして、自動構成を許可します。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Managed Configuration Flag: (選択解除)

CLI

```
set interface ethernet3 ipv6 ra managed
```

Other Parameters Configuration フラグ

Other Parameters Configuration フラグを有効にすると、ローカルホストは、ステートフルアドレス自動構成プロトコル（DHCPv6）を使用して、ホストアドレス以外のパラメータを構成します。

ローカルホストは、この設定が有効な間、ステートレスアドレス自動構成はできません。

次の例では、Other Parameters Configuration フラグを無効にして、自動構成を許可します。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Other Parameters Configuration Flag: (選択解除)

CLI

```
set interface ethernet3 ipv6 ra other
```

アドレス自動構成の無効化

IPv6 ルーターのホスト自動構成を無効にするには、次の手順を行います。

- オンリンクホストがルーター通知を送信できないように、Outgoing Router Advertisements 設定を無効にします。
- Managed Configuration フラグを有効にして、強制的にホストに DHCPv6 のようなステートフルアドレス指定プロトコルを使用させます。
- Other Parameters Configuration Flag を有効にします。

次の例では、IPv6 ルーターでアドレス自動構成を無効にします。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Allow RA Transmission: (選択解除)
Managed Configuration Flag: (選択)
Other Parameters Configuration Flag: (選択)

CLI

```
unset interface ethernet3 ipv6 ra transmit
unset interface ethernet3 ipv6 ra managed
unset interface ethernet3 ipv6 ra other
```

アドバタイジング時間間隔の設定

アドレス自動構成は、IPv6 ルーター用の通知された時間間隔を使用します。これらの間隔は、イベントの頻度や識別されたオブジェクトの寿命を決定します。

通知された到着可能時間間隔

Reachable Time 設定を有効にすると、インターフェースは、発信 RA メッセージに到着可能時間間隔を含めます。この間隔は、インターフェースから RA を受信してから、何秒間 IPv6 インターフェースが到着可能であると見なせるかをオンリンクのホストに伝えます。

インターフェースは、現在の Base Reachable Time 設定に基づいて到着可能時間を決めます。Base Reachable Time の詳細は、30 ページの「ベース到着可能時間」を参照してください。

インターフェースは、この値を使用して、隣接ノード到達不可能性検出（NUD）を行います。セキュリティデバイスは、隣接ノードキャッシュテーブルの構築と保守を行い、テーブルには、ホストが最近トラフィックを送信した各隣接ノードのアドレスが含まれています。デバイスはこれらのエントリを使用して、隣接ノードの到達可能性状況の変化を記録します。NUD で、デバイスは各隣接ノードの到達可能性状態の変化を追跡し、それに従ってトラフィック転送の決定を行うことができます。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Reachable Time: (選択)

CLI

```
set interface ethernet3 ipv6 ra reachable-time
```

通知された再送信時間間隔

Retransmission Time を有効にすると、インターフェースは、発信 RA メッセージに再送信時間間隔を含めます。この間隔（秒単位）は、NS メッセージの再送信の間に経過する時間のことです。

再送信時間間隔の詳細は、31 ページの「再送信時間」を参照してください。

インターフェースは、NUD を実行する間、この値を使用します。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Retransmission Time: (選択)

CLI

set interface ethernet3 ipv6 ra retransmit-time

最大通知間隔

最大通知間隔は、IPv6 インターフェースからの自発的マルチキャスト RA の送信の間に許される最大秒数を指定します。

次の例では、間隔を 500 秒に設定します。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Maximum Advertisement Interval: 500

CLI

set interface ethernet3 ipv6 ra max-adv-int 500

最小通知間隔

最小通知間隔は、IPv6 インターフェースからの自発的マルチキャスト RA の送信のに許される最小秒数を指定します。

次の例では、間隔を 100 秒に設定します。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Minimum Advertisement Interval: 100

CLI

set interface ethernet3 ipv6 ra min-adv-int 100

通知されたデフォルトのルーター寿命

Default Router Lifetime 設定は、ホストが最後の RA をインターフェースから受信した後、ホストがインターフェースをデフォルトのルーターであると確認できる秒数を指定します。

次の例では、寿命を 1500 秒に設定します。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Minimum Advertisement Interval: 1500

CLI

set interface ethernet3 ipv6 ra default-life-time 1500

アドバタイジングパケットの性質

RA はオンリンクホストデバイスに、リンク MTU やホップ制限など、IPv6 インターフェースを通じて交換されるパケットに関する情報を提供できます。

リンク MTU 値

Link MTU フラグを有効にすると、IPv6 インターフェースは RA メッセージに Link MTU フィールドを含めます。Link MTU は、リンク上のホストが送信する IPv6 パケットの最大サイズ（バイト）です。

注 : Ethernet について、デフォルトの Link MTU 値は 1500 バイトです。PPPoE のデフォルトは 1490 バイトです。この値は、1280 ～ 1500 でなければなりません。プラットフォームによっては MTU 値を変更できます。MTU 値を設定できるかを確認するには、ご使用のセキュリティデバイスに付属する文書を参照してください。

次の例では、リンク MTU の通知を有効にします。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Link MTU: (選択)

CLI

set interface ethernet3 ipv6 ra link-mtu

現在のホップ制限

Current Hop Limit 設定は、アドレス自動構成にこのインターフェースからの RA を使用する、ローカルの IPv6 ホストが送信するパケットに対する、ホップ制限を指定します。Current Hop Limit 値をゼロに設定すると、ホップ数を指定しないことになります。

次の例では、Current Hop Limit 値を 50 ホップに設定します。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Current Hop Limit: 50

CLI

```
set interface ethernet3 ipv6 ra hop-limit 50
```

通知ルーターの性質

IPv6 インターフェースは、RA を使用して、インターフェースのリンクレイヤー（MAC）アドレスやルーターの優先レベルなど、ルーターの属性をオンリンクのホストに通知します。

リンクレイヤーアドレスの設定

Link Layer Address フラグを有効にすると、IPv6 インターフェースは、送信 RA メッセージにインターフェースのリンクレイヤー（MAC）アドレスを含めます。

次の例では、Link Layer Address フラグを有効にします。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Link Layer Address: (選択)

CLI

```
set interface ethernet3 ipv6 ra link-address
```

通知されたルーターの優先度

Advertised Router Preference 設定は、ルーターの優先レベルを指定します。

ホストが IPv6 インターフェースから RA を受信し、他の IPv6 ルーターが存在する場合、ホストがインターフェースを 1 次ルーターと見なすか 2 次ルーターと見なすかは、優先レベルが決定します。

次の例では、優先度を High に設定し、インターフェースが 1 次ルーターであることを示しています。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Advertised Router Preference: High (選択)

CLI

set interface ethernet3 ipv6 ra preference high

隣接ノード発見パラメータの構成

IPv6 操作にインターフェースを構成するとき、インターフェースは、同じリンク上の隣接ノードの存在をインターフェースとして確認する必要があります。隣接ノード発見（ND）で、デバイスは、ローカルリンクの隣接ノードの到達可能性状況を追跡できます。

隣接ノード到達不能検出

隣接ノード到達不能検出（NUD）を有効にすると、インターフェースは NUD を実行します。テーブルの各エントリは、隣接ノードを表し、隣接ノードの現在の到達可能性状態を含んでいます。

次の例では、IPv6 インターフェース ethernet3 について NUD を有効にします。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

NUD (Neighbor Unreachability Detection): (選択)

CLI

set interface ethernet3 ipv6 nd nud

MAC セッション ー キャッシング

デフォルトでは、インターフェースは MAC アドレスセッションキャッシングを使用して、アドレス解決の速度と効率を向上させます。always-on-dest 設定を有効にすると、インターフェースはこのプロセスをバイパスします。隣接ノードへトラフィックを送信する前に、セッションで MAC アドレスをキャッシングする代わりに、必ず隣接ノードキャッシュテーブルを参照します。

MAC セッションキャッシングをバイパスするには、次の CLI コマンドを入力します。

set ndp always-on-dest

静的隣接ノードキャッシュエントリ

隣接ノードキャッシュテーブルで静的なエントリを作成するには、CLI コマンド **set ndp** を使用して、隣接ノード発見パラメータ（NDP）を設定します。

set ndp *ip_addr mac_addr interface*

場所 :

- *ip_addr* は隣接ノードの IPv6 アドレスです。
- *mac_addr* は隣接ノードの MAC アドレスです。
- *interface* はデバイスのインターフェースです。

次の例では、隣接ノードキャッシュテーブルの新しいエントリを開始します。

- 隣接 IP アドレス 32f1::250:af:34ff:fe27
- MAC アドレス 1234abcd1234
- デバイス インターフェース ethernet3

set ndp 32f1::250:af:34ff:fe27 1234abcd1234 ethernet3

このエントリを削除するには、**unset ndp** *ip_addr interface* コマンドを入力します。

ベース到着可能時間

IPv6 インターフェースが隣接ノード要請（NS）メッセージを隣接ノードに送信し、応答として隣接ノード通知（NA）メッセージを受信すると、デバイスは隣接ノード到達可能性状態を Reachable に設定します。Base Reachable Time 設定は、インターフェースが Reachable 状態を維持するおおよその時間（秒）を指定します。

この時間が経過すると、状態は Stale モードへと変わります。

注 : Base Reachable Time 設定は、状態が Reachable である実際の時間のおおよそを指定するだけです。実際の時間は到着可能時間と呼ばれます。インターフェースは、Base Reachable Time をベースとして、到着可能時間をランダムに決定します。その結果、到達可能時間は通常、Base Reachable Time 設定の 50 ～ 150 パーセント以内になります。

次の例では、（IPv6 インターフェース ethernet3 の）Base Reachable Time を 45 秒に設定します。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Base Reachable Time: 45

CLI

set interface ethernet3 ipv6 nd base-reachable-time 45

プローブ時間

（隣接ノードが次ホップゲートウェイの場合のように）エントリ状態が Incomplete または Probe Forever である間、インターフェースは、隣接ノードの到達可能性を確認しようとします。各試行は*プローブ*と呼ばれます。プローブの間、インターフェースは隣接ノードへ NS 要求を送信します。端点ホスト状態モードの Probe Time 設定は、プローブ間の間隔（秒）を指定します。

次の例では、（IPv6 インターフェース ethernet3 の）Probe Time を 3 秒に設定します。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Retransmission Time: 3

CLI

set interface ethernet3 ipv6 nd probe-time 3

再送信時間

IPv6 インターフェースがプローブを開始すると、NS 要求を隣接ノードへ送信します。Retransmission Time 設定は、NS 要求間の経過時間（秒）を指定します。

次の例では、（IPv6 インターフェース ethernet3 の）Retransmission Time を 2 秒に設定します。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

Retransmission Time: 2

CLI

set interface ethernet3 ipv6 nd retransmit-time 2

重複アドレス検出再試行カウント

重複アドレス検出（DAD）は、2 つ以上のオンリンクデバイスが同じユニキャストアドレスを持っていないか確認します。DAD Retry Count 設定は、IPv6 インターフェース の DAD を行いながら送信する、連続した NS メッセージの数を指定します。

次の例では、（IPv6 インターフェース ethernet3 の）DAD Retry Count を 2 回に設定します。

WebUI

Network > Interfaces > Edit (for IPv6 interface): 次のように入力してから **OK** をクリックします。

DAD (Duplicate Address Detection) Retry Count: 2

CLI

set interface ethernet3 ipv6 nd dad-count 2

IPv6 インターフェースパラメータの表示

WebUI または CLI で IPv6 構成情報を表示できます。

WebUI

Network > Interfaces > IPv6

CLI

get interface

隣接ノード発見構成の表示

WebUI または CLI を使用して、現在の隣接ノード発見（ND）設定を表示できます。次の例では、IPv6 インターフェース (ethernet3) の現在の ND 設定を表示します。

WebUI

Network > Interfaces > Edit (for IPv6 interface)

CLI

get interface ethernet3 ipv6 config

現在の RA 構成の表示

IPv6 インターフェースが IPv6 ルーターとして機能するよう構成する前に、現在の RA 構成をチェックすることを推奨します。

次の例では、IPv6 インターフェース ethernet3 の RA 構成設定を表示します。

WebUI

Network > Interfaces > Edit (for IPv6 interface ethernet3): 現在の設定を表示します。

CLI

get interface ethernet3 ipv6 ra

設定例

このセクションでは、IPv6 ルーターおよびホストの構成の例を示します。CLI コマンドだけを示します。

IPv6 ルーター

この例は、IPv6 ルーターモードで動作する 2 つのインターフェースを持つセキュリティデバイスを示します。

CLI

```
set interface ethernet2 zone trust
set interface ethernet2 ipv6 mode router
set interface ethernet2 ipv6 enable
set interface ethernet2 ipv6 interface-id 1111111111111111
```

```
set interface ethernet2 ipv6 ip 2eee::1/64
set interface ethernet2 ipv6 ra transmit

set interface ethernet3 zone trust
set interface ethernet3 ipv6 mode router
set interface ethernet3 ipv6 enable
set interface ethernet3 ipv6 interface-id 2222222222222222
set interface ethernet3 ipv6 ip 3eee::1/64
set interface ethernet3 ipv6 ra transmit
```

IPv6 ホスト

次のコマンドは IPv6 ホストを構成します。

CLI (デバイス B)

```
set interface ethernet2 zone trust
set interface ethernet2 ip 20.1.1.2/24
set interface ethernet2 ipv6 mode host
set interface ethernet2 ipv6 enable
set interface ethernet2 ipv6 interface-id 3333333333333333
set interface ethernet2 ipv6 ra accept
```

第 3 章

接続およびネットワークサービス

IPv6 が有効なインターフェースは、動的ホスト構成プロトコルバージョン 6（DHCPv6）および PPPoE（Point-to-Point Protocol over Ethernet）をサポートしています。

本章のセクションは、以下のようになります。

- 36 ページの「概要」
- 36 ページの「動的ホスト構成プロトコルバージョン 6」
  - 37 ページの「デバイスユニーク ID」
  - 37 ページの「ID アソシエーションプレフィックス委譲 ID」
  - 37 ページの「プレフィックスの特徴」
  - 38 ページの「サーバーの優先度」
  - 38 ページの「DHCPv6 サーバーの構成」
  - 40 ページの「DHCPv6 クライアントの構成」
  - 41 ページの「DHCPv6 設定の表示」
- 42 ページの「ドメイン名システムサーバーの構成」
  - 43 ページの「DNS および DNS 検索リスト情報の要求」
  - 44 ページの「プロキシ DNS アドレス分割の設定」
- 46 ページの「PPPoE の構成」
- 47 ページの「フラグメント化の設定」

概要

本章では、次のネットワークおよび接続サービスについて説明します。

- 動的ホスト構成プロトコルバージョン 6（DHCPv6）
- ドメイン名システム (DNS)
- PPPoE (Point-to-Point over Ethernet)
- フラグメント化

次のセクションで、各ネットワークまたは接続サービスを概観します。

動的ホスト構成プロトコルバージョン 6

IPv6 ルーターは DHCPv6 サーバーにしかなることができません。IPv6 ホストは DHCPv6 クライアントにしかなることができません。

DHCPv6 クライアントとして、インターフェースは（DHCPv6 サーバーから）次の項目を要求できます。

- 管理境界を横断した long-lived プレフィックスの委譲。サーバーは、対象となるローカルネットワークのトポロジを知っている必要はありません。たとえば、ISP は、DHCPv6 を使用して、ダウンストリームの DHCP クライアントを通じてダウンストリームのネットワークへプレフィックスを割り当てることができます。クライアントとサーバーの対話を加速するには、クライアントは（有効な場合）高速コミットを要求できます。高速コミットは、メッセージ数を 4 から 2 へ削減します。

注： 高速コミットオプションを使用する影響の詳細は、RFC 3315 および 3633 を参照してください。

- 利用可能な DNS サーバーの IP アドレス。インターフェースは、DNS 検索リスト情報も要求できます。このリストには、ドメイン名の一部が含まれ、入力されたユーザー名をドメイン名に連結することにより、DNS 検索を支援します。

DHCPv6 サーバーとして、インターフェースはこれらのサービスを両方とも DHCPv6 クライアントへ提供できます。プレフィックス委譲を高速化するため、DHCPv6 サーバーとして構成されている IPv6 ルーターは、高速コミットオプションをサポートできます。サーバー優先度オプションも設定できます。

注： DHCPv6 はアドレス自動構成と補完関係にあります。これらのサービスは互換性がありません。

デバイスユニーク ID

デバイスユニーク ID（DUID）は、ホストやルーターのようなネットワークデバイスを識別します。DUID（または DUID に関連付けられた名前）を使用して、特定の DUID を持つ特定のルーターまたはホストに対するプレフィックス委譲をデバイスが行う方法を決めることができます。

ID アソシエーションプレフィックス委譲 ID

ID アソシエーションプレフィックス委譲 ID（IAPD-ID）は、サーバーのあるプレフィックスを表す正の整数です。クライアントは、この値を使用して、サーバーから特定のプレフィックスを要求できます。ゼロではない IAPD-ID 値を指定すると、その値は、サーバー上で同じ IAPD-ID を持つ 1 つのプレフィックスへ自動的にマッピングされます。ゼロの IAPD-ID 値を指定するか、値を省略する（デフォルトではゼロの値を割り当てます）と、IAPD-ID は、サーバー上のプレフィックスのプールへ、その値を動的にマッピングします。デバイスは、ゼロの IAPD-ID を持つプレフィックスをすべてこのプールに所属するとして扱います。

DHCPv6 サーバーは、クライアント DUID あたり 16 個のプレフィックスを含めることができます。

プレフィックスの特徴

DHCPv6 サーバーが委譲するプレフィックスには、次の要素が含まれています。

- トップレベルアグリゲータ（TLA）は、ルーティング階層で最上位（IPv6 アドレスの左端の部分）を示します。TLA は通常、ISP のような組織について所有されているアドレス空間を指定します。プレフィックス長を使用して、TLA の長さを指定します。
- サイトローカルアグリゲータ（SLA）は、その組織が使用するネットワークまたはサブネットを表します。

たとえば、サーバーは次のプレフィックスを委譲する場合があります。

2001:908e:1::/48

場所 :

- TLA は 2001:908e
- SLA は 1

同じサーバーが、次のプレフィックスも委譲する場合があります。

2001:908e:2::/48

場所 :

- TLA は 2001:908e
- SLA は 2

SLA は各例で異なりますが、これは、各プレフィックスが、異なったネットワークにマッピングを行うが、同じ所有アドレス空間に属しているからです。

サーバーの優先度

オプションで、デバイスが DHCPv6 クライアントへ送信する DHCP 通知メッセージで、サーバーの優先値を送信できます。DHCPv6 クライアントはこの値を使用して、サーバーの選択を行います。

デフォルト値は -1 で、クライアントに送信された通知メッセージに優先度が示されていないことを表します。0（優先度最低）から 255（優先度最高）までの値を設定できます。

次の例では、インターフェース ethernet1/2 のサーバー優先度を優先度最高の 255 に設定します。

WebUI

Network > DHCPV6 > Edit (Server): Server Preference Number フィールドに 255 を入力し、**Apply** をクリックします。

CLI

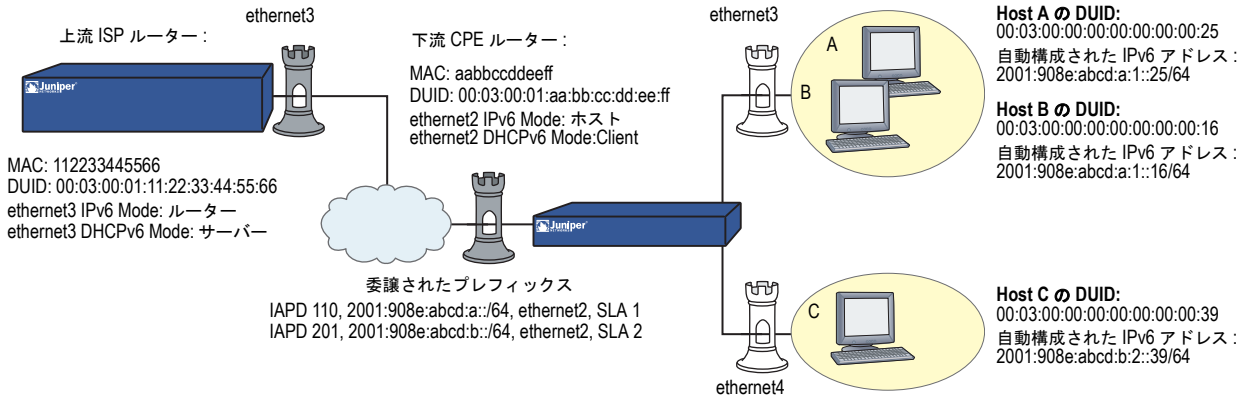
set interface ethernet1/2 dhcp6 server preference 255

DHCPv6 サーバーの構成

エンドユーザーが外部のネットワークにアクセスできる ISP のような環境では、セキュリティデバイスが、異なった SLA を持つ異なったプレフィックスを委譲するように設定できます。図 9 は、上流ルーターが、下流ルーターへの DHCPv6 プレフィックスを委譲するように設定している様子を示します。

IPv6 ルーターは、それぞれ異なった SLA を持つ 2 つのプレフィックスを委譲します。下流の CPE ルーターは、この 2 つの異なった SLA を使用して、プレフィックスを 2 つの異なったネットワークへ割り当てできます。

図 9: DHCPv6 プレフィックスの委譲



この例では、インターフェース ethernet3 を DHCPv6 サーバーとして構成し、上流 ISP ルーターに 2 つのプレフィックスを指定します。プレフィックスは、下流の顧客構内装置（CPE）ルーターへの委譲に利用可能になります。

- 下流のクライアント DUID 00:03:00:01:aa:bb:cc:dd:ee:ff を指定します。これにより、クライアントは、サーバーからプレフィックス委譲を要求できます。
- 次のプレフィックスを委譲します。
  - 2001:908e:abcd:a::/64, SLA 1, IAPD 110, 優先寿命 259200 秒、有効寿命 345600 秒
  - 2001:908e:abcd:b::/64, SLA 2, IAPD 201, 優先寿命 172800 秒、有効寿命 345600 秒
- 非ゼロの IAPD 数のため、サーバーは（動的ではなく）静的に両方のプレフィックスを委譲します。

注 : WebUI セクションでは、デバイス構成ページへの到るナビゲーションパスのみを一覧表示します。具体的な値については、それに続く CLI セクションを参照してください。

WebUI

1. **サーバーインターフェース**
   Network > Interfaces > Edit (for ethernet3) > IPv6

   Network > DHCPV6 > Edit (for ethernet3)

2. **下流クライアントの識別**
   Network > DHCPv6 > DUID/Prefix Delegation List (for ethernet3) > New DUID

3. **委譲されたプレフィックス**
   Network > DHCPv6 > DUID/Prefix Delegation List (for ethernet3) > Add Prefix Entry

CLI

1. **サーバーインターフェース**
   set interface ethernet3 ipv6 mode router
   set interface ethernet3 ipv6 enable
   set interface ethernet3 dhcp6 server

2. **下流クライアントの識別**
   set interface ethernet3 dhcp6 server options client-duid
   00:03:00:01:aa:bb:cc:dd:ee:ff

3. **委譲されたプレフィックス**
   set interface ethernet3 dhcp6 server options pd duid
   00:03:00:01:aa:bb:cc:dd:ee:ff iapd-id 110 prefix 2001:908e:abcd:a::/64
   259200 345600
   set interface ethernet3 dhcp6 server options pd duid
   00:03:00:01:aa:bb:cc:dd:ee:ff iapd-id 201 prefix 2001:908e:abcd:b::/64
   172800 345600
   save

DHCPv6 クライアントの構成

次の例では、下流の CPE ルーターを DHCPv6 クライアントとして構成します。ルーターは、上流ルーターからプレフィックスを要求し、そのプレフィックスから得た IPv6 アドレスをローカルホストへ自動的にプッシュできます。図 9 を参照してください。

- 優先されるサーバーを DUID 00:03:00:01:11:22:33:44:55:66 で指定します。
- サーバーから次の優先プレフィックスを要求します。
  - 2001:908e:abcd:a::/64, SLA 1, IAPD 110, 優先寿命 259200 秒（3 日間）、有効寿命 345600 秒（4 日間）
  - 2001:908e:abcd:b::/64, SLA 2, IAPD 201, 優先寿命 172800 秒（2 日間）、有効寿命 345600 秒（4 日間）
- Ethernet3 および ethernet4 を下流インターフェースとして指定します。
  - SLA が 1 のプレフィックスは ethernet3 へ
  - SLA が 2 のプレフィックスは ethernet4 へ

注： WebUI セクションでは、デバイス構成ページへの到るナビゲーションパスのみを一覧表示します。具体的な値については、それに続く CLI セクションを参照してください。

WebUI

1. **下流 CPE インターフェース**
   Network > Interfaces > Edit (for ethernet4)

   Network > Interfaces > Edit (for ethernet4) > IPv6

   Network > Interfaces > Edit (for ethernet3)

   Network > Interfaces > Edit (for ethernet3) > IPv6

2. **クライアントインターフェース（上流ルーターへ）**
   Network > Interfaces > Edit (for ethernet2)

   Network > Interfaces > Edit (for ethernet2) > IPv6

   Network > DHCPv6 > Edit (for ethernet2)

3. **優先プレフィックス（上流ルーターから）**
   Network > DHCPv6 > Prefix Assignment List (for ethernet2) > Learned (Suggested) Prefix add

4. **下流インターフェース**
   Network > DHCPv6 > Prefix Assignment List (for ethernet2) > Prefix Distribution add

CLI

1. **下流 CPE インターフェース**
   set interface ethernet4 zone trust
   set interface ethernet4 ipv6 mode router
   set interface ethernet4 ipv6 enable
   set interface ethernet3 zone trust
   set interface ethernet3 ipv6 mode router
   set interface ethernet3 ipv6 enable

2. **クライアントインターフェース（上流ルーターへ）**
   set interface ethernet2 ipv6 mode host
   set interface ethernet2 ipv6 enable
   set interface ethernet2 dhcp6 client
   set interface ethernet2 dhcp6 client options request pd
   set interface ethernet2 dhcp6 client prefer-server
   00:03:00:01:11:22:33:44:55:66

3. **優先プレフィックス（上流ルーターから）**
   set interface ethernet2 dhcp6 client pd iapd-id 110 prefix 2001:908e:abcd:a::/64
   259200 345600
   set interface ethernet2 dhcp6 client pd iapd-id 201 prefix 2001:908e:abcd:b::/64
   172800 345600

4. **下流インターフェース**
   set interface ethernet2 dhcp6 client pd iapd-id 110 ra-interface ethernet3 sla-id 1
   sla-len 2
   set interface ethernet2 dhcp6 client pd iapd-id 201 ra-interface ethernet4 sla-id 2
   sla-len 2
   set interface ethernet2 dhcp6 client enable
   save

DHCPv6 設定の表示

DHCPv6 サーバーおよびクライアントの設定はコマンドラインインターフェースから表示できます。

DHCPv6 設定を表示するには、次のコマンドを入力します。

get interface *interface_name* dhcp6

出力例 :

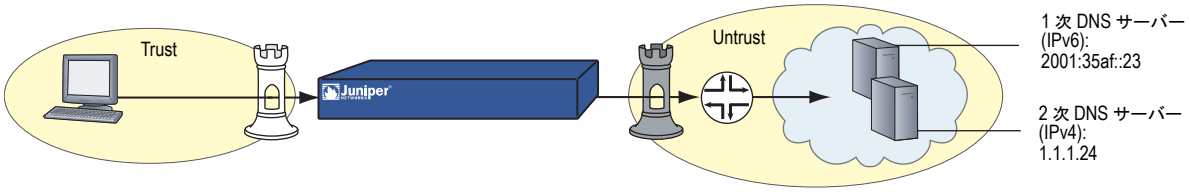
```
device-> get interface ethernet1/2 dhcp6
DHCPv6 Configuration, enabled.
------------------------------------------------------------------------
        Mode            : server
        DUID            : 00:03:00:01:00:10:db:7a:c1:08
        Interface: ethernet1/2
        Allow rapid-commit: yes
        Preference      : 255
------------------------------------------------------------------------
```

ドメイン名システムサーバーの構成

ドメイン名システム（DNS）をドメイン名のアドレス解決に使用するには、1 次および 2 次 DNS サーバーの IP アドレスを入力して、デバイスを構成する必要があります。構成するのに選択する DNS サーバーは、IPv4 または IPv4 アドレスを使用できます。

図 10 は、ルーターの背後の Untrust ゾーンにある 1 次および 2 次 DNS サーバーを示します。

図 10: ドメイン名システムサーバー



次の例では、IPv6 サーバーを 1 次サーバーに、IPv4 サーバーを 2 次サーバーに指定します。

- IPv6 アドレス 2001:35af::23 にある 1 次サーバー
- IPv4 アドレス 1.1.1.24 にある 2 次サーバー
- DNS 更新は毎日午後 11:00

WebUI

Network > DNS > Host

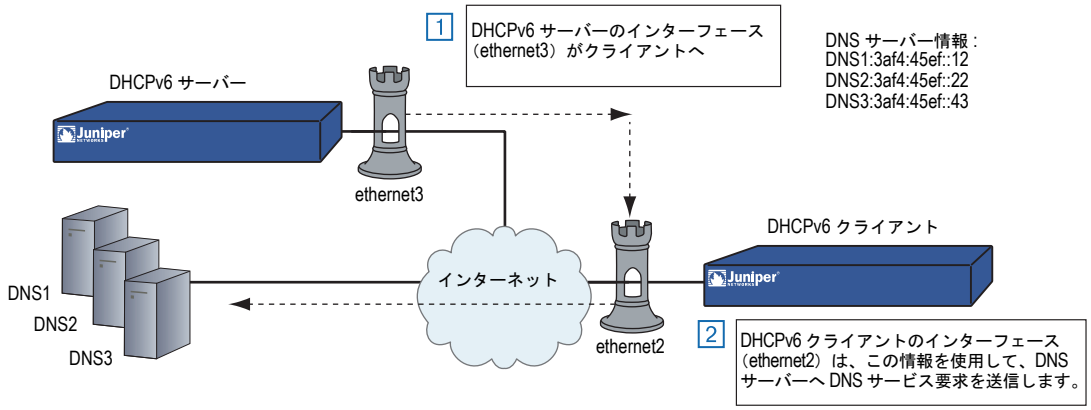
CLI

```
set dns host dns1 2001:35af::23
set dns host dns2 1.1.1.24
set dns host schedule 23:00
save
```

DNS および DNS 検索リスト情報の要求

図 11 は、DHCPv6 サーバーおよび DHCPv6 クライアントを示しています。DHCPv6 クライアントは、DHCPv6 サーバーのインターフェース ethernet3 から DNS デバイスに関する情報を受信します。このインターフェースは、1 次、2 次、3 次 DNS に関する情報を自動的に送信します。すると、DHCPv6 クライアントは、DNS サーバーのいずれかに DNS サービス要求を送信できます。

図 11: DNS サーバーおよび DHCPv6 クライアント



WebUI（サーバー）

Network > Interfaces > Edit (for ethernet3) > IPv6

Network > DHCPv6 > Edit (for ethernet3)

WebUI（クライアント）

Network > Interfaces > Edit (for ethernet3) > IPv6

Network > DHCPv6 > Edit (for ethernet3)

CLI（サーバー）

```
set interface ethernet3 ipv6 mode router
set interface ethernet3 ipv6 enable
set interface ethernet3 dhcp6 server
set interface ethernet3 dhcp6 server enable
set interface ethernet3 dhcp6 server options dns dns1 3af4:45ef::12
set interface ethernet3 dhcp6 server options dns dns2 3af4:45ef::22
set interface ethernet3 dhcp6 server options dns dns3 3af4:45ef::43
save
```

CLI（クライアント）

```
set interface ethernet2 ipv6 mode host
set interface ethernet2 ipv6 enable
set interface ethernet2 dhcp6 client
set interface ethernet2 dhcp6 client enable
set interface ethernet2 dhcp6 client options request dns
set interface ethernet2 dhcp6 client options request search-list
save
```

プロキシ DNS アドレス分割の設定

ScreenOS は、プロキシ DNS アドレス分割をサポートしています。これにより、選択したドメイン名クエリーを特定の DNS サーバーへ転送できます。アドレス分割には 2 つの利点があります。

- オーバーヘッドを低減します。関連のないサービス要求の処理から DNS サーバーを解放できます。
- トラフィックを保護します。DNS サーバーへ送信されたクエリーで IPSec トンネリングを実行できます。

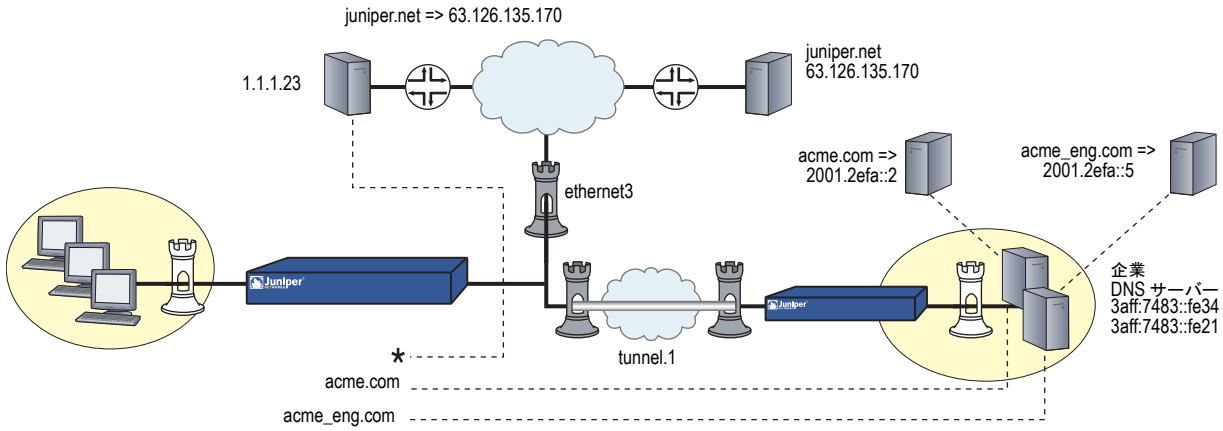
DNS プロキシは、ドメイン名の一部またはすべてに従って、DNS クエリーを特定の DNS サーバーに選択的に転送します。この機能は、VPN トンネルや PPPoE 仮想リンクが複数のネットワーク接続を提供し、複数の DNS クエリーをある特定のネットワークに、あるいは他のクエリーを別のネットワークに転送する必要がある場合に有効です。

DNS プロキシの利点は次の通りです。

- 通常のドメインルックアップが効率的になります。たとえば、（marketing.acme.com などの）企業ドメインに関連する DNS クエリーを企業の DNS サーバーに排他的に転送して、他のクエリーはすべて ISP DNS サーバーに転送します。これによって、企業サーバーへの負荷が軽減されます。さらに、企業ドメイン情報のインターネットへの漏洩を防ぐことができます。
- DNS プロキシを使用すると、選択した DNS クエリーをトンネルインターフェース経由で転送でき、悪意のあるユーザーに内部のネットワーク構成を知られないようにできます。たとえば、企業サーバーにバウンドされた DNS クエリーは、トンネルインターフェース経由で通過でき、認証や暗号化、応答防止などのセキュリティ機能を使用できます。

以下の例では、DNS クエリーをさまざまなサーバーに選択的に転送するプロキシ DNS エントリが 2 つ作成されます。図 12 を参照してください。

図 12: 分割サーバーを使用するプロキシ DNS



- ドメイン名 acme.com が含まれている FQDN に関連付けられた任意の DNS クエリーは、トンネルインターフェース tunnel.1 を経由して、IPv6 アドレス 3aff:7483::fe34 にある企業 DNS サーバーに転送されます。

  たとえば、ホスト側で www.acme.com に関連する DNS クエリーを送信すると、デバイス側でその クエリーをこのサーバーに自動的に転送します。（この例では、サーバーがクエリーを IPv6 アドレス 2001.2efa::2 へ解決すると仮定しています。）

- ドメイン名 acme_engineering.com が含まれている FQDN に関連付けられた任意の DNS クエリーは、トンネルインターフェース tunnel.1 を経由して、IPv6 アドレス 3aff:7483::fe21 にある DNS サーバーに転送されます。

  たとえば、ホスト側で intranet.acme_eng.com に関連する DNS クエリーを送信すると、デバイス側でそのクエリーをこのサーバーに転送します。（この例では、サーバーがクエリーを IPv6 アドレス 2001.2efa::5 へ解決すると仮定しています。）

- その他の DNS クエリー（* で表記）はすべて、企業サーバーに転送されません。ethernet3 インターフェースを経由して、IPv4 アドレス 1.1.1.23 にある DNS サーバーに転送されます。

  たとえば、ホスト名とドメイン名が www.juniper.net である場合、デバイス側で企業サーバーを自動的に回避して、そのクエリーをこの DNS サーバーに自動的に転送します。この DNS サーバーは、IPv4 アドレス 63.126.135.170 にその DNS クエリーを解決しています。

WebUI

Network > DNS > Proxy

Network > DNS > Proxy > New

CLI

```
set dns proxy
set dns proxy enable
set dns server-select domain .acme.com outgoing-interface tunnel.1
    primary-server 3aff:7483::fe34
set dns server-select domain .acme_eng.com outgoing-interface tunnel.1
    primary-server 3aff:7483::fe21
set dns server-select domain * outgoing-interface ethernet3 primary-server
    1.1.1.23
```

PPPoE の構成

IPv6 が有効なインターフェースは、PPPoE（Point-to-Point Protocol over Ethernet）クライアントになることができます。これにより、IPv6 Ethernet LAN のメンバーは、ISP との個別の PPP 接続が可能になります IPv4 実装の場合と同様に、デバイスは、各発信 IPv4 パケットを PPP ペイロード内でカプセル化し、次にその PPP ペイロードを PPPoE 内部でカプセル化します。PPPoE では、デバイスは、クライアントのインターネットアクセスのため、PPPoE を使用する ISP が運営しているデジタル加入者線（DSL）や Ethernet Direct、ケーブルネットワークでの互換動作が可能になっています。

インターフェースレベルで PPPoE を設定し、インターフェースを有効にします。インターフェースは、IPCP（Internet Protocol Control Protocol）プレフィックスについて、次に IPv6CP（IPv6 Control Protocol）プレフィックスについて、アクセスコンセントレータとネゴシエートします。

注： デュアルスタック IPv6 環境での PPPoE に関する詳細は、RFC 4241 を参照してください。

インターフェースを PPPoE（デュアルスタックモード）に設定するには、次の手順を行います。

1. ユーザー名とパスワードを持つ PPPoE インスタンスを作成します。
2. その PPPoE インスタンスが、PPPoE アクセスコンセントレータ（AC）から IPv4 および IPv6 プレフィックスを取得するように指定します。
3. デバイスを IPv6 Host モードに構成します。

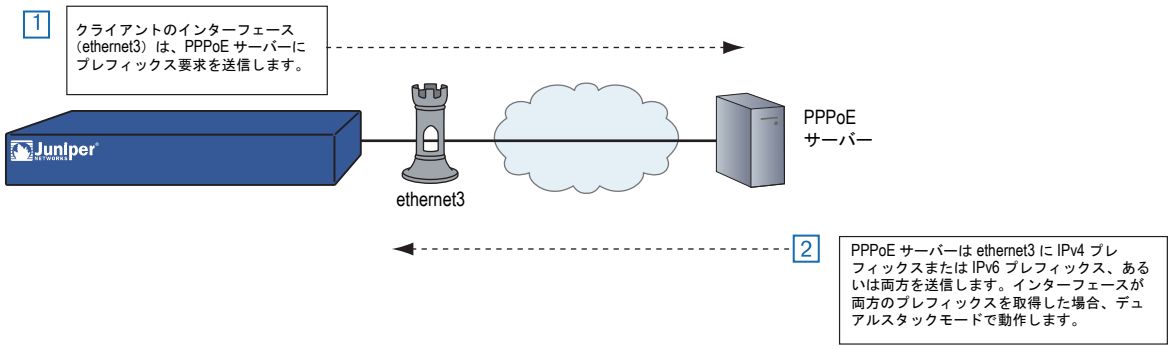
インターフェースの PPPoE を有効にした後、インターフェースは、IPCP プレフィックス、そして次に IPv6CP プレフィックスについて AC とネゴシエートします。これらの試行のいずれか一方または両方が成功する可能性があります。両方が成功した場合、インターフェースはデュアルスタックモードで動作します。その他の場合は、シングルスタックモードで動作します。

次の例では、インターフェース ethernet3 を PPPoE に構成します。

- NY_Office という名前の PPPoE を ethernet3 にバインド
- PPPoE ユーザー名 Richard_B、パスワード er5cmdj
- PPPoE インスタンスは、最初に IPv4 アドレスを次に IPv6 アドレスを取得します。

図 13 は、PPPoE クライアントとサーバーのやりとりを示します。

図 13: PPPoE クライアントおよびサーバー



注 : WebUI セクションでは、デバイス構成ページへの到るナビゲーションパスのみを一覧表示します。具体的な値については、それに続く CLI セクションを参照してください。

WebUI

1. **PPPoE インスタンス**
   Network > PPPoE > New

2. **クライアントインターフェース**
   Network > Interfaces > Edit (for ethernet3)

   Network > Interfaces > Edit (for ethernet3) > IPv6

CLI

1. **PPPoE インスタンス**
   set pppoe name NY_Office username richard_b password er5cmdj
   set pppoe name NY_Office ppp ipcp ipv6cp
   set pppoe name NY_Office interface ethernet3

2. **クライアントインターフェース**
   set interface ethernet3 zone untrust
   set interface ethernet3 ipv6 mode host
   set interface ethernet3 ipv6 enable

フラグメント化の設定

ScreenOS を実行する IPv6 ルーターは、MTU とともにパス MTU を使用して、フラグメント化を決定します。

注 : IPv6 のパス MTU に関する詳細は、RFC 1981 を参照してください。

IPv6 インターフェースは、パスの最初のホップの MTU と等しくなるように、はじめに パス MTU を決定します。そのパスに送信されたパケットが大きすぎて、パス上のルーターが転送できない場合、そのルーターはパケットを廃棄して、発信元ルーターに ICMPv6（Internet Control Message Protocol version 6）PTB（Packet Too Big）メッセージを返します。PTB メッセージを受信すると、送信元

ルーターは、PTB メッセージで報告された MTU と一致するように、そのパス MTU を小さくします。このプロセスが複数回行われてから、パス MTU 発見プロセスが終了する場合もあります。パケットは、パス上の MTU が小さい他のルーターを通過しなければならない場合もあるからです。

デバイスは、そのデバイスを通過するトラフィックおよびそのデバイスが発信元のトラフィックにパス MTU を適用します。通過トラフィックについては、フローレベルのインターフェースからパケットを転送する前にフラグメント化が必要な場合、インターフェースは、MTU を発信インターフェースの MTU に設定した ICMPv6 PTB メッセージを返信します。

注： パス MTU の構成ができないデバイスでは、この値は 1500 です。

フラグメント化が実行されるには、インターフェースの パス MTU を有効にしなければなりません。構成した値を受け入れるデバイスでは、値を 1280 から 1500 までに設定できます。

WebUI

Network > Interfaces > Edit

Maximum Transfer Unit (MTU) Admin MTU: で MTU 値を入力し、**OK** をクリックします。

CLI

```
set interface trust trust-vr mtu 1280
save
```

注： フラグメント化を有効にした手動トンネリングの進んだ構成例は、119 ページの「フラグメント化を有効にした手動トンネリング」を参照してください。

第 4 章
静的および動的ルーティング

ScreenOS は、RIPng（Routing Information Protocol next-generation）による静的ルーティングおよび動的ルーティングをサポートします。

本章のセクションは、以下のようになります。

- 50 ページの「概要」
  - 50 ページの「デュアルルーティングテーブル」
  - 51 ページの「静的および動的ルーティング」
  - 51 ページの「上流および下流プレフィックスの委譲」
- 52 ページの「静的ルーティング」
- 53 ページの「RIPng の構成」
  - 54 ページの「RIPng インスタンスの作成と削除」
  - 55 ページの「RIPng をインターフェースで使用可能・不可にする」
- 55 ページの「RIPng に関する大域パラメータ」
  - 56 ページの「デフォルトルートの通知」
  - 57 ページの「デフォルトルートを拒否する」
  - 57 ページの「Trusted 隣接ノードを構成する」
  - 58 ページの「ルートの再配布」
  - 59 ページの「更新しきい値を設定してフラッディングを防止」
- 60 ページの「インターフェースごとの RIPng パラメータ」
  - 60 ページの「ルート、インターフェース、およびオフセットメトリック」
  - 63 ページの「ポイズンリバース付きスプリットホライズンの構成」

- 64 ページの「ルーティングおよび RIPng 情報の表示」
  - 64 ページの「ルーティングテーブルの表示」
  - 64 ページの「RIPng データベースの表示」
  - 65 ページの「仮想ルーター別 RIPng の詳細の表示」
  - 66 ページの「インターフェース別 RIPng の詳細の表示」
  - 66 ページの「RIPng 隣接情報の表示」
- 67 ページの「設定例」
  - 67 ページの「トンネルインターフェース上で RIPng を稼動させる」
  - 69 ページの「ISP ルーターへのトラフィックループの回避」
  - 76 ページの「OSPF への Null インターフェース再配布の設定」
  - 77 ページの「発見したルートの OSPF への再配布」
  - 77 ページの「OSPF サマリーのインポートのセットアップ」

概要

デュアルスタックアーキテクチャでは、セキュリティデバイスは、IPv6 トラフィックの受信、処理、および転送が可能であり、IPv4 アドレス、少なくとも 1 つの IPv6 プレフィックス、あるいはその両方の割り当てをサポートします。このため、デバイスは異質のネットワーク間でパケットを交換でき、異質の WAN バックボーンでのリモートネットワーク間のセキュリティポリシーをサポートします。

次のセクションでは、IPv4/IPv6 ルーティングテーブル、および静的ルーティングと動的ルーティングの概念を説明します。

デュアルルーティングテーブル

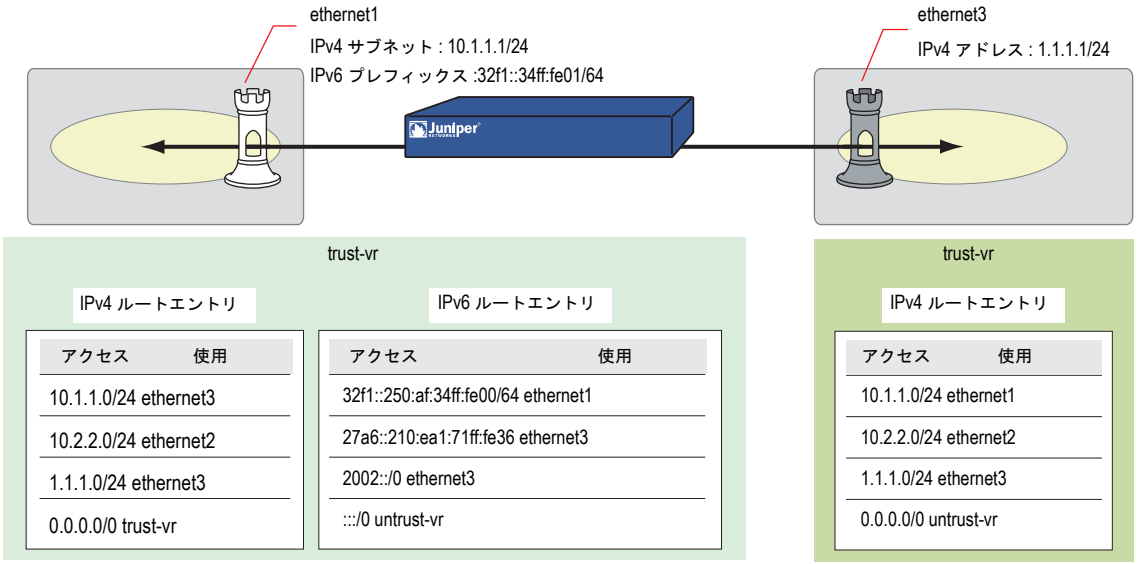
インターフェースを IPv4 アドレスと IPv6 アドレスの両方を持つように構成する場合、インターフェースがバインドされる仮想ルーターには、2 つの別々のルーティングテーブルが含まれます。1 つは IPv4 エントリ用であり、もう 1 つは IPv6 エントリ用です。両方のテーブルが同じ仮想ルーターにあります。

たとえば、インターフェースを trust-vr 仮想ルーターにバインドされたゾーンへバインドし、そのインターフェースをデュアルスタックモード用に構成する場合、trust-vr 仮想ルーターは、IPv4 ルーティングテーブルと IPv6 ルーティングテーブルを構築し維持します。

図 14 は、2 つの Ethernet インターフェースを持つセキュリティデバイスを示します。

- Ethernet1 はデュアルスタックモードで動作し、2 つのルーティングテーブルを維持してします。
- Ethernet3 は IPv4 モードでのみ動作します。ethernet3 の trust-vr は、ルーティングテーブルを 1 つだけ維持しています。

図 14: デュアルスタックルーターの動作



静的および動的ルーティング

ScreenOS は、RIPng（Routing Information Protocol-Next Generation）およびホップ数をメトリックとして使用し宛先までの最善のルートを決定するのに距離ベクトルアルゴリズムを使用する IGP（Interior Gateway Protocol）による静的ルーティングおよび動的ルーティングをサポートしています。RIPng は、ルートの再配布をサポートし、異なるプロトコルを実行しているルーターから現行の RIPng ルーティングインスタンスに、既知のルートをインポートします。たとえば、仮想ルーターからの静的ルートを RIPng インスタンスにインポートできます。RIPng は、IPv6 ネットワークでしか使用できません。

注 : RIPng の詳細は、RFC 2080 および 2081 を参照してください。

上流および下流プレフィックスの委譲

ネットワークトポロジによっては、デバイスがプレフィックスを下流デバイスに委譲する場合があります。デバイスはプレフィックスを使用して、他のデバイスを自動構成できます。たとえば、企業 WAN は、次のように使用される複数のセキュリティデバイスを使用する場合があります。

- IP アドレスをローカルホストへ委譲するための顧客構内装置（CPE）ルーター
- サブネットワークプレフィックスを CPE ルーティングへ委譲するためのゲートウェイルーター
- ネットワークプレフィックスをゲートウェイルーターへ委譲するための、さらに上流の ISP（Internet Service Provider）ルーター

静的ルーティング

IPv6 インターフェースの静的ルーティングを構成するプロセスは、IPv4 インターフェースと同じです。異なるのはアドレス表記です。IPv4 の静的ルーティングの詳細については、1 ページの「静的ルーティング」を参照してください。

次の例では 2 つのインターフェースを構成します。

- Ethernet2 IPv4 アドレス 1.1.2.1/24（オプション）
- Ethernet2 を IPv6 アドレス 32f1:250a::02/48 を使って Router モードで構成
- Ethernet2 を trust ゾーンへバインドし、ローカルホストへのルート通知を有効化
- Ethernet3 を IPv6 アドレス 32f1:250a::03/48 を使って Router モードで構成
- 2 つの静的ルーティングエントリ :
  - 32f1:250a::01/48 ethernet2 用、ローカルホストへ通知
  - ::/0 ethernet3 用、外部ゲートウェイ 27a6::210:ea1:71ff:fe36

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (ethernet2)

   Network > Interfaces > Edit (ethernet2) Static IP（選択)

   Network > Interfaces > Edit (ethernet2) > IPv6

   Network > Interfaces > Edit (ethernet2) > IPv6 > ND/RA Settings

   Network > Interfaces > Edit (ethernet3)

2. **ルート**
   Network > Routing > Routing Entries New (trust-vr)

   Network > Routing > Routing Entries New (trust-vr) > Gateway: (選択)

CLI

1. **インターフェース**
   set interface ethernet2 zone trust
   set interface ethernet2 ip 1.1.2.1/24
   set interface ethernet2 ipv6 mode router
   set interface ethernet2 ipv6 enable
   set interface ethernet2 ipv6 ip 32f1:250a::02/48
   set interface ethernet2 ipv6 ra transmit
   set interface ethernet2 ipv6 ra link-mtu
   set interface ethernet2 ipv6 ra link-address

   set interface ethernet3 zone untrust
   set interface ethernet2 ipv6 mode router
   set interface ethernet2 ipv6 enable
   set interface ethernet3 ipv6 32f1:250a::03/48

2. **ルート**
   set vrouter trust-vr route 32f1:250a::01/48 interface ethernet2
   set vrouter trust-vr route::/0 interface ethernet3 gateway 27a6::210:ea1:71ff:fe36

RIPng の構成

セキュリティデバイス上に仮想ルーターベースで RIPng を作成します。システム内に仮想ルーターが複数ある場合は、複数の RIPng インスタンスを有効にできます。

注 : 動的ルーティングプロトコルをセキュリティデバイス上で構成する前に、VR ID を割り当てる必要があります。詳細については、*第 2 部 : 基本*を参照してください。

ここではセキュリティデバイスで RIPng を設定する基本的な手順を説明します。

1. 仮想ルーターに RIPng ルーティングインスタンスを作成します。
2. RIPng インスタンスを有効にします。
3. 他の RIPng ルーターに接続するインターフェースについて、RIPng を有効にします。
4. 他のルーティングプロトコル（OSPF、BGP、静的ルートなど）で収集したルート情報を、RIPng インスタンスに再配布します。

以下、この手順にそって、具体的な操作方法を説明します。CLI を使う方法と、WebUI 画面から操作する方法があります。

さらに、以下のような RIPng パラメータも設定できます。

- RIPng の仮想ルーターごとに設定する大域パラメータ。タイマー、信頼できる RIPng 隣接ノードなど（55 ページの「RIPng に関する大域パラメータ」を参照）
- RIPng についてインターフェースごとに設定するインターフェースパラメータ（60 ページの「インターフェースごとの RIPng パラメータ」を参照）

RIPng インスタンスの作成と削除

セキュリティデバイス上の特定の仮想ルーター（VR）に RIPng ルーティングインスタンスを作成して使用可能にします。この作業が終わると、RIPng が有効になっている VR 上の各インターフェースと、パケットをやり取りできるようになります。

VR から RIPng ルーティングインスタンスを削除すると、VR に属するインターフェースすべてについて、RIPng 設定情報が削除されます。

仮想ルーターやその設定方法については*第 7 部: ルーティング*を参照。

RIPng インスタンスの作成

Trust-vr に RIPng ルーティングインスタンスを作成してから、RIPng を有効にします。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit: Virtual Router ID を入力して **Create RIP Instance** を選びます。

Enable RIPng を選択して **OK** をクリックします。

CLI

1. **ルーター ID**
   set vrouter trust-vr router-id 10
2. **RIPng ルーティングインスタンス**
   set vrouter trust-vr protocol ripng
   set vrouter trust-vr protocol ripng enable
   save

RIPng インスタンスの削除

ここでは trust-vr 上に作成した RIPng ルーティングインスタンスを無効にします。trust-vr の RIPng が有効になっている全インターフェースに対し、RIPng パケットの送信・処理を停止します。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIPng Instance: Enable RIPng をオフにして **OK** をクリックします。

Network > Routing > Virtual Router (trust-vr) > Edit > Delete RIPng Instance を実行。確認プロンプトが現れるので **OK** をクリックします。

CLI

unset vrouter trust-vr protocol ripng enable
unset vrouter trust-vr protocol ripng
save

RIPng をインターフェースで使用可能・不可にする

デフォルトでは、VR のどのインターフェースでも RIPng は無効になっているため、稼動させようとするインターフェースごとに、明示的に有効にする必要があります。あるインターフェースについて RIPng を無効にすると、そこでは RIPng パケットの送受信を行わないようになります。ただし設定パラメータはそのまま保存されます。

注 : VR 上で RIPng ルーティングインターフェースを無効にする（54 ページの「RIPng インスタンスの削除」を参照）と、RIPng が有効になっている他のインターフェースに対し、RIPng パケットを送信・処理することはなくなります。

インターフェース上の RIPng を有効にする

ここでは Trust インターフェース上で RIPng を有効にします。

WebUI

Network > Interface > Edit (for Trust) > RIPng: **Protocol RIPng Enable** を選択し、**Apply** をクリックします。

CLI

```
set interface trust protocol ripng enable
save
```

インターフェース上の RIPng を停止する

ここでは Trust インターフェース上の RIPng を停止します。**unset interface** *interface_name* **protocol ripng** コマンドが、既存の RIPng インスタンスをインターフェースからアンバインドします。インターフェースの RIP を使用不可にするには、保存する前に、**unset interface** *interface_name* **protocol ripng enable** コマンドを入力します。

WebUI

Network > Interface (for Trust) > RIPng: **Protocol RIPng Enable** をクリアし、**Apply** をクリックします。

CLI

```
unset interface trust protocol ripng
unset interface trust protocol ripng enable
save
```

RIPng に関する大域パラメータ

この節では、仮想ルーター（VR）ごとに設定できる RIPng の大域パラメータについて解説します。VR に対して RIPng パラメータを設定すると、RIPng を有効にしたすべてのインターフェースの動作に反映されます。大域パラメータの設定は、CLI の RIPng ルーティングプロトコルコンテキストから実行するほか、WebUI 画面からも変更できます。

表 2 は、RIPng 大域パラメータとそのデフォルト値を説明します。

表 2: RIPng 大域パラメータおよびデフォルト値

RIPng に関する大域パラメータ	説明	デフォルト値
Advertise default route	デフォルトルート（::/0）を通知するかどうかを指定。	無効
Default metric	OSPF や BGP など、他のプロトコルから RIPng にインポートしたルートの、デフォルトメトリック値。	10
Flush timer	ルート情報が無効になってから、実際に削除するまでの時間 (秒単位)。	120 秒
Invalid timer	隣接ノードからの通知がなくなってから、ルート情報を無効と看做すまでの時間 (秒単位)。	180 秒
Maximum neighbors	RIPng 隣接ノードの最大数。特定のインターフェースについて隣接ノードを表示するには、**get interface** *interface_name* **protocol ripng** コマンドを入力します。	256
Redistribute routes	OSPF（Open Shortest Path First）などの他の動的ルーティングプロトコル、または静的ルートに由来するトラフィックをルーティングする方法を提供。	無効
Reject default routes	他のプロトコルで収集したデフォルトルート情報を拒否する旨の指定。57 ページの「デフォルトルートを拒否する」を参照してください。	無効
Incoming route map	RIPng で収集したルート情報を分別するためのフィルタを指定。	なし
Outgoing route map	RIPng で通知するルートのフィルタを指定。	なし
Update threshold	更新タイマーが期限切れとなる前に、デバイスが処理する更新の数を指定。しきい値が 5 に設定されており、更新タイマーが期限切れとなる前に 10 件の更新（ルートの数ではない）を受信した場合、デバイスは後の 5 件の更新をドロップします。更新タイマーがリセットされると、その 5 件の更新が受け入れられます。	ゼロ秒
Trusted neighbors	RIPng 隣接ノードを定義したアクセスリストを指定。この指定がない場合は、マルチキャストまたはブロードキャストにより、当該インターフェース上の隣接ノードを検出します。57 ページの「Trusted 隣接ノードを構成する」を参照してください。	隣接ノードはすべて信頼できると看做す。
Update timer	近隣ノードに RIPng ルート情報の更新通知を送る間隔（秒単位）。	30 秒

デフォルトルートの通知

RIPng 設定を変更して、デフォルトルート（非 RIPng ルート）の通知を含むようにし、特定の VR ルーティングテーブルにあるデフォルトルートに関連しているメトリックを変更することができます。

デフォルトでは、デフォルトルート（::/0）は RIPng 近隣ノードに通知しないようになっています。次のコマンドは、仮想ルーター trust-vr 上の RIPng 近隣ノードに対し、デフォルトルートのメトリック値が 5 であると通知します（メトリック値を指定してください）。このデフォルトルートは、ルーティングテーブルに登録されているものと想定します。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIPng Instance: 次のように入力してから **OK** をクリックします。

Advertising Default Route: (**選択**)
Metric: 5

CLI

```
set vrouter trust-vr protocol ripng adv-default-route metric number 5
save
```

デフォルトルートを拒否する

Route Detour Attack では、あるルーターがデフォルトルート（::/0）をルーティングドメインに挿入してパケットをそのルーターに迂回させます。このルーターは、パケットを破棄することでサービスの中断を招いたり、パケットを転送する前に内部の機密情報を得ることができます。Juniper Networks セキュリティデバイスのデフォルトでは、RIPng により収集したデフォルトルート情報をすべて受け入れ、ルーティングテーブルに登録するようになっています。

次の例では、仮想ルーター trust-vr 上で稼動する RIPng ルーティングインスタンスに対し、デフォルトルートの情報を RIPng で収集しないよう設定します。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIPng Instance: 次のように入力してから **OK** をクリックします。

Reject Default Route Learnt by RIPng: (**選択**)

CLI

```
set vrouter trust-vr protocol ripng reject-default-route
save
```

Trusted 隣接ノードを構成する

マルチアクセス環境にすると、ルーターなどのデバイスが、比較的容易にネットワークに接続できてしまします。そのため、接続されたデバイスが信頼性に欠ける場合、安定性や性能に問題が生じる可能性があります。これを回避するため、所定のノードだけが RIPng 近隣ノードになれるよう、アクセスリストを定義して制限することができます。デフォルトでは、仮想ルーターと同一のサブネットに属するデバイスだけが、RIPng 隣接ノードになれるよう制限しています。

ここでは、仮想ルーター trust-vr で稼動する RIPng ルーティングインスタンスに対して、次のような大域パラメータを設定します。

- RIPng 近隣ノードの最大数を 1 とします。
- 信頼できる近隣ノード IP アドレス 2eee::5/64 をアクセスリストで指定します。

WebUI

Network > Routing > Virtual Router (trust-vr) > Access List > New: 次のように入力してから **OK** をクリックします。

Access List ID: 10
Sequence No.: 1
IP/Netmask: 2eee::5/64
Action: Permit (**選択**)

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIPng Instance: 次のように入力してから **OK** をクリックします。

Trusted Neighbors: (**選択**), 10
Maximum Neighbors: 1

CLI

```
set vrouter trust-vr
device(trust-vr)-> set access-list 10 permit ip 2eee::5/64 1
device(trust-vr)-> set protocol ripng
device(trust-vr/ripng)-> set max-neighbor-count 1
device(trust-vr/ripng)-> set trusted-neighbors 10
device(trust-vr/ripng)-> exit
device(trust-vr)-> exit
save
```

ルートの再配布

ルート再配布とは、ルーティングプロトコル間のルート情報の交換のことです。たとえば以下のようなルート情報を、同一の仮想ルーターにある RIPng ルーティングインスタンスに再配布することができます。

- BGP により学習したルート情報
- OSPF により学習したルート情報
- 直接接続されたルート
- インポートされたルート
- 静的に構成されたルート

ルート情報再配布の設定に当たっては、再配布するルートを分別するためのルートマップを指定する必要があります。ルート再配布のためのルートマップ作成の詳細は、*第 7 部: ルーティング*を参照してください。

他のプロトコルから RIPng にインポートしたルートの、デフォルトのメトリック値は 10 です。これは変更できます（55 ページの「RIPng に関する大域パラメータ」を参照）。

この例では、サブネットワーク 2eee::/64 内の静的ルートを、仮想ルーター trust-vr に属する RIPng 隣接ノードに再配布します。そのために、サブネット 2eee::/64 に属するアドレスを許可するアクセスリストを作成します。次に、このアクセスリストに一致するアドレスを許可するよう、ルートマップを設定します。最後に、このルートマップを使って、静的ルートを RIPng ルーティングインスタンスに再配布するよう指定します。

WebUI

Network > Routing > Virtual Router (trust-vr) > Access List > New: 次のように入力してから **OK** をクリックします。

Access List ID: 20
Sequence No.: 1
IP/Netmask: 2eee::/64
Action: Permit (**選択**)

Network > Routing > Virtual Router (trust-vr) > Route Map > New: 次のように入力してから **OK** をクリックします。

Map Name: rtmap1
Sequence No.: 1
Action: Permit (選択)
Match Properties:
Access List: (選択), 20 (選択)

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIPng Instance > Redistributable Rules: 次のように入力してから **Add** をクリックします。

Route Map: rtmap1 (選択)
Protocol: Static (選択)

CLI

```
set vrouter trust-vr access-list 20 permit ip 2eee::/64 1
set vrouter trust-vr route-map name rtmap1 permit 1
set vrouter trust-vr route-map rtmap1 1 match ip 20
set vrouter trust-vr protocol ripng redistribute route-map rtmap1 protocol static
save
```

更新しきい値を設定してフラッディングを防止

ルーターが正しく設定されていなかったり、攻撃を受けたりした場合、RIPng 更新パケットを近隣ノードに大量に送りつけて、フラッディング（洪水）してしまうことがあります。仮想ルーターに対して、更新間隔内に RIPng インターフェース上で受け取る更新パケットの最大数を制限することにより、これを回避できます。この数以上のパケットは破棄されます。このしきい値を設定していない場合は、更新パケットをすべて受理します。

隣接ノードが大きなルーティングテーブルを持っているネットワークでは、更新しきい値を指定することにより、セキュリティデバイスが有効なルーターを知る機能を損なう場合があります。大きなルーティングテーブルは、ある期間内にフラッシュアップデートを含む、多数のルーティングの更新を受け取り生成します。変更したしきい値を超える、セキュリティデバイスへの更新パケットは、ドロップされ、重要なルートが学習されない場合があります。

ここではあるインターフェースで RIPng が受け取る更新パケットの最大数を 4 と設定します。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIPng Instance: 次のように入力してから **OK** をクリックします。

Maximum Number Packets per Update Time: (選択), 4

CLI

```
set vrouter trust-vr protocol ripng threshold-update 4
save
```

インターフェースごとの RIPng パラメータ

この節では、インターフェースごとに設定できる RIPng パラメータについて説明します。これは当該インターフェース上の動作にのみ影響を及ぼします。パラメータの設定は、**interface** という CLI コマンドを使うか、または WebUI 画面から行います。

表 3 は、RIPng インターフェースパラメータとそのデフォルト値を説明します。

表 3: RIPng インターフェースパラメータおよびデフォルト値

RIPng インターフェースパラメータ	説明	デフォルト値
RIPng metric	インターフェースの RIPng メトリックを指定。	1
Passive mode	インターフェースが RIPng パケットの受信のみを行い、送信はしないよう設定。	なし
Incoming route map	RIPng で収集したルート情報を分別するためのフィルタを指定。	なし
Outgoing route map	RIPng で通知するルートのフィルタを指定。	なし
Split-horizon	スプリットホライズン (split-horizon) コントロールをするか否かを指定（あるインターフェースから受信したルート情報を、同一のインターフェースに対しては通知しないよう制限する機能です）。さらにポイズンリバース (poison-reverse) 機能を有効にすることもできます。この場合、インターフェースから収集したルートを、メトリック値が 16 の状態にして、同一のインターフェースに送信するようになります。	スプリットホライズンは有効 ポイズンリバースは無効

ルート、インターフェース、およびオフセットメトリック

RIPng は、ルーターへ到達するのに必要なホップ数を示すのに、正の整数を使用します。デバイスは、3 つの値を使用して、この数を計算します。

- *ルート*メトリックは、特定のルートプレフィックスと関連付けられた整数です。
- *インターフェースコスト*メトリックは、RIPng 動作用に構成された特定のインターフェースと関連付けられた整数です。
- *オフセット*メトリックは、合計に追加される値です。

デバイスがメトリックの合計を得る方法は、トラフィックが流れるインターフェースによります。

- インターフェースが受信トラフィックを受信する場合、合計メトリックは次のようになります。

  ルートメトリック + インターフェースコストメトリック + オフセットメトリック

- インターフェースが発信トラフィックを送信する場合、インターフェースのコストメトリックは適用されず、合計メトリックは次のようになります。

  ルートメトリック + オフセットメトリック

アクセスリストおよびルートマップ

この例では、trust-vr の IPv6 アクセスリストをセットアップします。アクセス制御リスト（ACL）の ID は 10 で、プレフィックスが ::/0 のルートマップを作成します。

注 : IPv4 アクセスリストおよびルートマップの作成は、40 ページの「ルートマップの設定」を参照してください。

WebUI

Network > Routing > Virtual Routers > Access Lists > New (trust-vr)

Network > Routing > Virtual Routers > Route Maps (trust-vr) > New

CLI

```
set vrouter trust-vr
set access-list ipv6 10
set access-list 10 permit ip ::/0 10
set route-map ipv6 name rm_six permit 10
set match ip 10
end
```

静的ルートの再配布

次の例では、2 つのデバイス、デバイス A とデバイス B を RIPng 用に構成します。デバイス B では、ルートマップが受信するメトリック値に 2 を加えます（デフォルトは 1）。

デバイスを次のように構成します。

- デバイス A は、次のメトリックでデバイス B へ発信トラフィックを送信します。
  - ルートメトリック（5）+
  - オフセットメトリック（デフォルトは 1）

  発信パケットの 合計 RIPng メトリックは 6 です。
- デバイス B は、デバイス A からのトラフィックを次のメトリックで受信します。
  - ルートメトリック（4）+
  - インターフェースコストメトリック（7）+
  - オフセットメトリック（2）

  受信パケットの合計 RIPng メトリックは 13 です。

WebUI（デバイス A）

1. **IPv6 インターフェース**
   Network > Interfaces > Edit (for ethernet3)

   Network > Interfaces > Edit (for ethernet2) > IPv6

   Network > Interfaces > Edit (for ethernet2) > IPv6 > ND/RA Settings

   Network > Interfaces > Edit (for ethernet2) > RIPng

2. **RIPng 仮想ルーティング**
   Network > Routing > Virtual Routers > Edit (for trust-vr) > Create RIPng Instance

3. **RIPng インターフェースメトリック**
   Network > Interfaces > Edit (for ethernet2) > IPv6

CLI（デバイス A）

1. **IPv6 インターフェース**
   set interface ethernet3 zone trust
   set interface ethernet3 ipv6 mode router
   set interface ethernet3 ipv6 enable
   set interface ethernet3 ipv6 ip 2eee::1/64
   set interface ethernet3 ipv6 interface-id 1111111111111111
   set interface ethernet3 ipv6 ra transmit
   set interface ethernet3 protocol ripng enable

2. **RIPng 仮想ルーティング**
   set vrouter trust-vr protocol ripng
   set vrouter trust-vr protocol ripng enable
   set vrouter trust-vr protocol ripng advertise-def-route always metric 5

3. **RIPng インターフェースメトリック**
   set interface ethernet3 protocol ripng metric 1

WebUI（デバイス B）

1. **IPv6 インターフェース**
   Network > Interfaces > Edit (for Trust)

   Network > Interfaces > Edit (for Trust) > IPv6

   Network > Interfaces > Edit (for Trust) > IPv6 > ND/RA Settings

2. **静的ルート**
   Network > Routing > Routing Entries

3. **RIPng 仮想ルーター**
   Network > Routing > Virtual Routers > Edit (for trust-vr) > Create RIPng Instance

   Network > Interfaces > Edit (for Trust) > RIPng:

   Network > Routing > Virtual Routers > Access List: > New (for trust-vr)

4. **IPv6 ルートマップ**
   Network > Routing > Virtual Routers > Route Map > New (for trust-vr)

   Network > Routing > Virtual Router > Edit (for trust-vr) > Create RIPng Instance

5. **静的ルートの再配布**
   Network > Routing > Virtual Router > Edit (for trust-vr) > Edit RIPng Instance > Redistributable Rules

CLI（デバイス B）

1. **IPv6 インターフェース**
   set interface trust zone trust
   set interface trust ipv6 mode host
   set interface trust ipv6 enable
   set interface trust ipv6 interface-id 2222222222222222
   set interface trust ipv6 ra accept

2. **静的ルート**
   set route 3a51:94ef::1/48 interface trust metric 2 tag 23
   set route 3a51:ee45::1/48 interface trust metric 3 tag 37

3. **RIPng 仮想ルーター**
   set vrouter trust-vr protocol ripng
   set vrouter trust-vr protocol ripng enable
   set interface trust protocol ripng enable
   set interface trust protocol ripng metric 7
   set vrouter trust-vr access-list ipv6 10
   set vrouter trust-vr access-list ipv6 10 permit ip 3a51::1/16 10

4. **IPv6 ルートマップ**
   set vrouter trust-vr route-map ipv6 name abc permit 25
   set vrouter trust-vr route-map abc 25 match ip 10
   set vrouter trust-vr route-map abc 25 metric 4
   set vrouter trust-vr route-map abc 25 offset-metric 2
   set vrouter trust-vr protocol ripng route-map abc out
   set interface trust protocol ripng route-map abc out

5. **静的ルートの再配布**
   set vrouter trust-vr protocol ripng redistribute route-map abc protocol static
   save

ポイズンリバース付きスプリットホライズンの構成

次の例では、インターフェースにポイズンリバース付きスプリットホライズンを構成します。

WebUI

Network > Interfaces > Edit (for Trust) > RIPng 次のように入力してから **OK** をクリックします。

Split Horizon: Enabled with poison reverse (選択)

CLI

set interface trust protocol ripng split-horizon poison-reverse
save

ルーティングおよび RIPng 情報の表示

RIPng パラメータを変更すると、RIPng の詳細について以下の項目を参照できます。

- データベース。ルーティング情報を表示します。
- プロトコル。仮想ルーターの RIPng とインターフェースの詳細を表示します。
- 隣接ノード

ルーティングテーブルの表示

ルート情報は、CLI から確認できます。

WebUI

注 : ルーティングテーブル全体を表示するには、CLI を使用してください。

CLI

get route v6

出力例 :

```
untrust-vr (0 entries)
--------------------------------------------------------------------------------
C - Connected, S - Static, A - Auto-Exported, I - Imported, R - RIP
iB - IBGP, eB - EBGP, O - OSPF, E1 - OSPF external type 1
E2 - OSPF external type 2
trust-vr (6 entries)
--------------------------------------------------------------------------------------------------
   ID           IP-Prefix    Interface       Gateway           P   Pref  Mtr     Vsys
--------------------------------------------------------------------------------------------------
*  5               : :/0    trust   fe80::210:dbff:fe22:3017  U    251    2      none
*  2           3abc::1/64    trust   fe80::210:dbff:fe22:3017  R    100   11      Root
*  3           2abc::1/64    trust   fe80::210:dbff:fe22:3017  R    100   11      Root
*  6  2eee::210:dbff:fe20    trust              ::             C     1     0      Root
   1           2eee::1/64    trust   fe80::210:dbff:fe22:3017  R    100    2      Root
```

RIPng データベースの表示

RIPng ルーティング情報は、CLI から確認できます。RIPng データベースの全エントリの一覧を表示するか、1 エントリを表示するかを選択できます。

この例では、RIPng データベースの詳細情報を表示します。参照する仮想ルーターの IP アドレスとマスクを追加することにより、データベースの全エントリを参照するか、または 1 つのデータベースエントリのみを参照するかを選択することができます。

この例では、trust-vr を指定して、プレフィックスと IP アドレス 10.10.10.0/24 を追加することにより、1 つのテーブルエントリのみを参照します。

WebUI

注 : RIPng データベースを表示するには、CLI を使用してください。

CLI

get vrouter trust-vr protocol ripng database prefix 10.10.10.0/24

次の CLI コマンドを入力すると、RIPng データベースエントリが表示されます。

device-> **get vrouter trust-vr protocol ripng database 10.10.10.0/24**

RIPng データベースには以下のフィールドがあります。

- **DBID**: エントリのデータベース識別子
- **Prefix**: IP アドレスおよびプレフィックス
- **Nexthop**: 次ホップ (ルーター）のアドレス
- **If**: 接続の種類（ethernet または tunnel）
- ソースからの距離を示すために割り当てたコストメトリック値

Flag には、以下のいずれか 1 つ以上が当てはまります。multipath（M）、RIPng（R）、Redistributed（I）、Advertised default（D）、Permanent（P）、Summary（S）、Unreachable（U）、または Hold（H）。

この例では、データベース識別子は 7、IP アドレスおよびプレフィックスは 2eee::/64、次ホップは 2eee::100/64 となっています。また、コスト 2 のイーサネット接続です。Flag は M と R で、このルートがマルチパスで RIPng が稼働していることを示しています。

仮想ルーター別 RIPng の詳細の表示

仮想ルーターの RIPng の全情報を表示して、構成をチェックしたり保存されている変更内容がアクティブかどうかを確認できます。表示出力をインターフェースの要約テーブルのみに制限するには、CLI コマンドに *interface* を追加します。

WebUI

注 : RIPng の詳細を表示するには、CLI を使用してください。

CLI

get vrouter trust-vr protocol ripng

出力例 :

```
device-> get vrouter trust-vr protocol ripng
VR: trust-vr
---------------------------------
State: enabled
Version: 1
Default metric for routes redistributed into RIPng: 10
Maximum neighbors per interface: 256
Next RIPng update scheduled after: 7 sec
Advertising default route: disabled
Default routes learnt by RIPng will  be accepted
Incoming routes filter and offset-metric: not configured
Outgoing routes filter and offset-metric: not configured
Update packet threshold is not configured
Total number of RIPng interfaces created on vr(trust-vr): 1

Update Invalid Flush (Timers in seconds)
-----------------------------------------------------------
    30     180   120
```

```
Flags: Split Horizon - S, Split Horizon with Poison Reverse - P, Passive - I

Interface   IP-Prefix        Admin      State    Flags   NbrCnt Metric Ver-Rx/Tx
-------------------------------------------------------------------------------
ethernet3/4 fe80::210:dbff:fe8d enabled    enabled  S           1      1   1/1
```

RIPng の設定、パケットの詳細、RIPng のタイマー情報、インターフェース表の概要を表示することができます。

インターフェース別 RIPng の詳細の表示

特定のインターフェースの RIPng の全情報を表示して、構成をチェックしたり保存されている変更内容がアクティブかどうかを確認できます。

WebUI

注： RIPng の詳細を表示するには、CLI を使用してください。

CLI

get interface ethernet3/4 protocol ripng

出力例 :

```
VR: trust-vr
---------------------------------
Interface: ethernet3/4, IP: fe80::210:dbff:fe8d:3ea0/64, RIPng: enabled, Router:
enabled
Receive version 1, Send Version 1
State: Up, Passive: No
Metric: 1, Split Horizon: enabled, Poison Reverse: disabled
Incoming routes filter and offset-metric: not configured
Outgoing routes filter and offset-metric: not configured
Current neighbor count: 1
Next update after: 16 sec
Transmit Updates: 30 (3 triggered), Receive Updates: 68
Update packets dropped because flooding: 0
Bad packets: 0, Bad routes: 0
Neighbors on interface ethernet3/4
-------------------------------------------------------------------------------
IpAddress       Version  Age          Expires      BadPackets BadRoutes
-------------------------------------------------------------------------------
fe80::210:dbf.. 1        00:12:13     00:02:39             0         0
```

RIPng 隣接情報の表示

仮想ルーターの RIPng 隣接情報の詳細を表示することができます。表示する隣接情報の IP アドレスを追加することにより、全隣接情報の一覧または特定の隣接情報のエントリのみを取得できます。これらの統計から、ルートのステータスをチェックしたり、隣接ルーターとセキュリティデバイス間の接続を確認することができます。

次の例では、trust-vr の RIPng 隣接情報を表示します。

WebUI

注 : RIPng 隣接情報を表示するには、CLI を使用してください。

CLI

get vrouter trust-vr protocol ripng neighbors

このコマンドは、次に似た出力を生成します。

```
n2-> get vr trust protocol ripng neighbors
VR: trust-vr
----------------------------------
Neighbors on interface trust
------------------------------------------------------------------------------
IpAddress       Version  Age          Expires      BadPackets BadRoutes
------------------------------------------------------------------------------
fe80::210:dbf.. 1        00:06:52     00:02:29              0         0
```

IP アドレスだけでなく、以下の RIPng 近隣情報も参照できます。

- エントリのエージ
- 有効期限
- 不良パケット数
- 不良ルート数
- Flags: static (S)、demand circuit (T)、NHTB (N)、down (D)、up (U)、poll (P)、あるいは demand circuit init (I)。

設定例

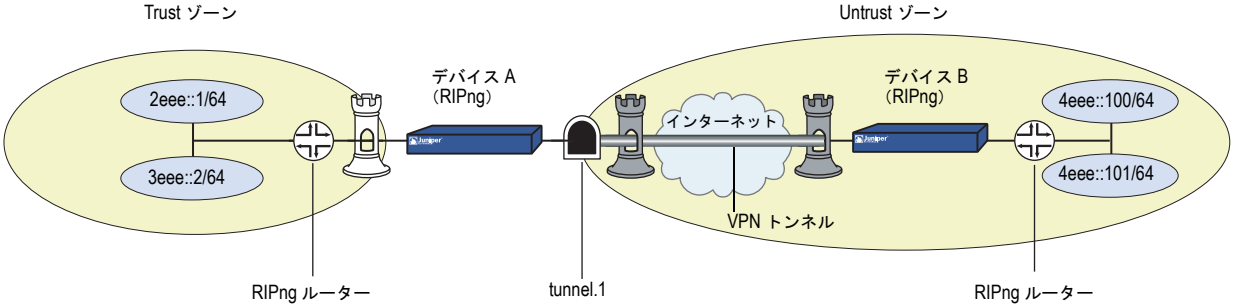
このセクションには、他のデバイスの上流または下流に位置する、IPv6 ホストまたは IPv6 ルーターとして動作するセキュリティデバイスが複数あるトンネルと、RIPng および静的ルーティングを使用する例が含まれます。

トンネルインターフェース上で RIPng を稼動させる

この例では、デバイス A の仮想ルーター trust-vr に、RIPng ルーティングインスタンスを作成し、稼動させます。VPN トンネルインターフェースと Trust ゾーンインターフェースの両方について、RIPng を有効にします。サブネット 2eee::/64 内のルートだけを、デバイス B 上の RIPng 隣接ノードに通知します。そのためにまず、サブネット 2eee::/64 に属するアドレスのみを許可するアクセスリストを作ります。次に、このアクセスリストに合致するルートのみを許可するルートマップ *abcd* を指定します。最後に、このルートマップを使って、RIPng 隣接ノードに通知するルートを分別します。

図 15 は説明したネットワークシナリオを示します。

図 15: RIPng を使ったトンネルインターフェースの例



WebUI (デバイス A)

Network > Routing > Virtual Router > Edit (for trust-vr) > Create RIPng Instance: **Enable RIPng** を選択して **OK** をクリックします。

Network > Routing > Virtual Router > Access List (for trust-vr) > New: 次のように入力してから **OK** をクリックします。

Access List ID: 10
Sequence No.: 10
IP/Netmask: 2eee::/64
Action: Permit

Network > Routing > Virtual Router > Route Map (for trust-vr) > New: 次のように入力してから **OK** をクリックします。

Map Name: abcd
Sequence No.: 10
Action: Permit
Match Properties:
Access List: (選択), 10

Network > Routing > Virtual Router > Edit (for trust-vr) > Edit RIPng Instance: 次のように選択してから **OK** をクリックします

Outgoing Route Map Filter: abcd

Network > Interfaces > Edit (for tunnel.1) > RIPng: 以下を入力して **Apply** をクリックします。

Enable RIPng: (選択)

Network > Interfaces > Edit (for Trust) > RIPng: 以下を入力して **Apply** をクリックします。

Enable RIPng: (選択)

CLI (デバイス A)

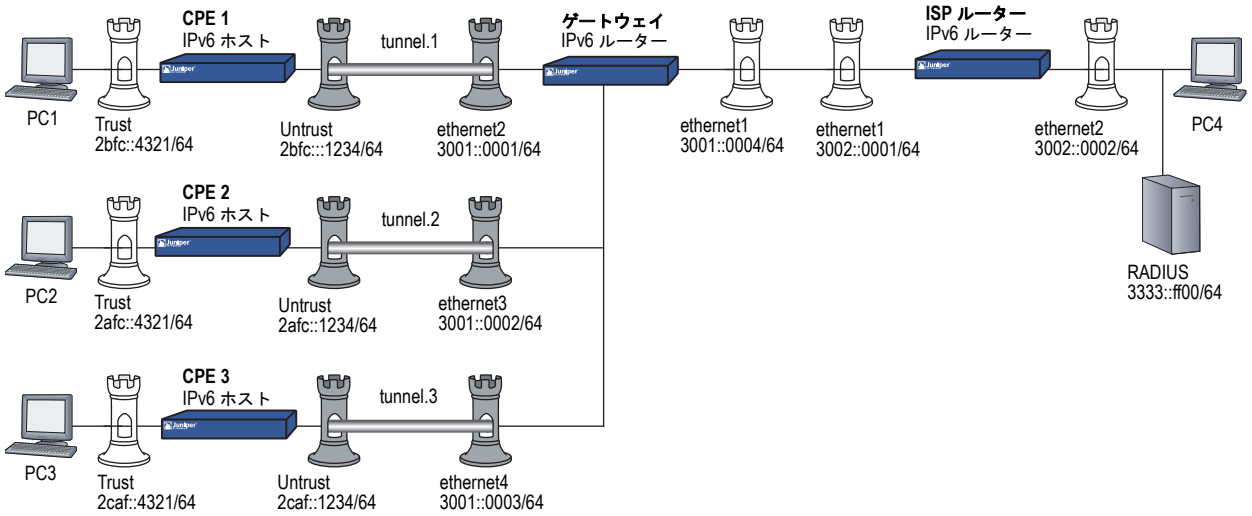
```
set vrouter trust-vr protocol ripng
set vrouter trust-vr protocol ripng enable
set interface tunnel.1 protocol ripng enable
set interface trust protocol ripng enable
set vrouter trust-vr access-list 10 permit ipv6 2eee::/64 10
set vrouter trust-vr route-map ipv6 name abcd permit 10
set vrouter trust-vr route-map ipv6 abcd 10 match ip 10
set vrouter trust-vr protocol ripng route-map abcd out
save
```

ISP ルーターへのトラフィックループの回避

図 16 は、上流 ISP ルーターへのトラフィックループを回避するよう構成された複数のデバイスを示します。ISP およびゲートウェイルーターは、IPv6 Router モードです。3 つの顧客構内装置（CPE）デバイスは、IPv6 ホストであり、ゲートウェイルーターを通じて ISP ルーターから 委譲された IPv6 プレフィックスを受信します。RADIUS サーバーは、ゲートウェイデバイスの Trust ゾーンにあります。

この例では、ISP ルーターに接続されたゲートウェイのインターフェースで、**route-deny** 機能を有効にします。この機能は、ゲートウェイ上のデフォルトのルートが、ISP ルーターへのトラフィックループを作成するのを防ぎます。

図 16: RADIUSv6 IKE の例



顧客構内装置の構成

このセクションでは、CPE 1、CPE 2、および CPE 3 をセットアップする構成手順を説明します。CPE デバスは IPv6 ホストです。IPv6 アドレスは、各デバイスが自動構成可能な値のプレースホルダーです。

1. すべての CPE デバイスについて IPv6 インターフェースを構成します。CPE デバイスのインターフェースを IPv6 Host モードで構成するとき、IPv6 プレフィックスを明示的に割り当てる必要はありません。デバイスは、ゲートウェイルーターからプレフィックスを受け取ります。各 CPE デバイスの構成について、各 IPv6 インターフェースにインターフェース ID を割り当てることを推奨します。

2. 次のトンネルを構成します。

   a. インターフェース tunnel.1 を持つ CPE 1

   b. インターフェース tunnel.2 を持つ CPE 2

   c. インターフェース tunnel.3 を持つ CPE 3

3. 各 CPE に VPN を定義します。

4. XAuth クライアントのユーザーをユーザー名およびホストへのパスワードとともに定義します。

5. ゲートウェイルーターを構成します。

注： お使いのネットワークで、1 つ以上の CPE デバイスが IPv6 プレフィックスを指定せず、1 つ以上の IPv4 アドレスを使用する場合、ゲートウェイルーターインターフェースに IPv4 アドレスを割り当てる必要があります。

6. IPv4 ルーターを構成します。

注： WebUI セクションには、CPE 1、CPE 2、および CPE 3 のデバイス構成ページへのナビゲーションパスのみを示します。具体的な値については、それに続く個別の CPE CLI セクションを参照してください。

WebUI（CPE 1、CPE 2、CPE 3）

1. インターフェース

Network > Interfaces > Edit (for Trust)

Network > Interfaces > Edit (for Trust) > IPv6

Network > Interfaces > Edit (for untrust)

Network > Interfaces > Edit (for untrust) > IPv6

2. Tunnel

Network > Interfaces > New (Tunnel IF)

Network > Interfaces > Edit (for tunnel.*n*) > IPv6

3. Route

Network > Routing > Routing Table > New (trust-vr)

4. IKE

VPNs > AutoKey Advanced > Gateway > New

VPNs > AutoKey Advanced > Gateway > Edit

5. VPN

VPNs > AutoKey IKE > New

VPNs > AutoKey IKE > Edit

6. ポリシー

Policies > (From: Untrust, To: Trust) > New

Policies > (From: Trust, To: Untrust) > New

CLI（CPE 1）

1. インターフェース

```
set interface trust zone trust
set interface trust ipv6 mode host
set interface trust ipv6 enable
set interface trust ipv6 interface-id 3333333333333333
set interface trust ipv6 ra accept

set interface trust manage
set interface trust route

set interface untrust zone trust
set interface untrust ipv6 mode host
set interface untrust ipv6 enable
set interface untrust ipv6 interface-id 4444444444444444
set interface untrust ipv6 ra accept

set interface untrust manage
set interface untrust route
```

2. トンネル

```
set interface tunnel.1 zone untrust
```

3. 静的ルート

```
set vrouter trust-vr route 3002::0001/64 interface tunnel.1
set vrouter trust-vr route::/0 interface untrust gateway 3001::0001/64
```

4. IKE

```
set ike gateway CPE1_G add 3001::0001/64 main outgoing-interface untrust
    preshare abc123 sec-level standard
set ike gateway CPE1_G xauth client any username PC1 password PC1
```

5. VPN

```
set vpn CPE1toG gateway CPE1_G sec-level standard
set vpn CPE1toG bind interface tunnel.1
```

6. ポリシー

```
set policy from trust to untrust any any any permit
set policy from untrust to trust any any any permit
```

CLI（CPE 2）

1. インターフェース

```
set interface trust zone trust
set interface trust ipv6 mode host
set interface trust ipv6 enable
set interface trust ipv6 interface-id 3333333333333333
set interface trust ipv6 ra accept

set interface trust manage
set interface trust route

set interface untrust zone trust
set interface untrust ipv6 mode host
set interface untrust ipv6 enable
set interface untrust ipv6 interface-id 4444444444444444
set interface untrust ipv6 ra accept

set interface untrust manage
set interface untrust route
```

2. **トンネル**
   set interface tunnel.2 zone untrust

3. **静的ルート**
   set vrouter trust-vr route 3002::0001/64 interface tunnel.2
   set vrouter trust-vr route::/0 interface untrust gateway 3001::0001/64

4. **IKE**
   set ike gateway CPE2_G add 3001::0001/64 main outgoing-interface untrust
   preshare abc123 sec-level standard
   set ike gateway CPE2_G xauth client any username PC1 password PC1

5. **VPN**
   set vpn CPE2toG gateway CPE2_G sec-level standard
   set vpn CPE2toG bind interface tunnel.2

6. **ポリシー**
   set policy from trust to untrust any any any permit
   set policy from untrust to trust any any any permit

CLI（CPE 3）

1. **インターフェース**
   set interface trust zone trust
   set interface trust ipv6 mode host
   set interface trust ipv6 enable
   set interface trust ipv6 interface-id 5555555555555555
   set interface trust ipv6 ra accept

   set interface trust manage
   set interface trust route

   set interface untrust zone trust
   set interface untrust ipv6 mode host
   set interface untrust ipv6 enable
   set interface untrust ipv6 interface-id 6666666666666666
   set interface untrust ipv6 ra accept

   set interface untrust manage
   set interface untrust route

2. **トンネル**
   set interface tunnel.3 zone untrust

3. **静的ルート**
   set vrouter trust-vr route 3002::0001/64 interface tunnel.3
   set vrouter trust-vr route::/0 interface untrust gateway 3001::0001/64

4. **IKE**
   set ike gateway CPE3_G add 3001::0001/64 main outgoing-interface untrust
   preshare abc123 sec-level standard
   set ike gateway CPE3_G xauth client any username PC3 password PC3

5. **VPN**
   set vpn CPE3toG gateway CPE3_G sec-level standard
   set vpn CPE3toG bind interface tunnel.3

6. **ポリシー**
   set policy from trust to untrust any any any permit
   set policy from untrust to trust any any any permit

ゲートウェイの構成

このセクションでは、IPv6 ルーターであるゲートウェイルーターをセットアップする構成手順を示します。

1. ゲートウェイの ethernet1 インターフェースを route-deny 機能で構成します。
2. ゲートウェイを 3 つのトンネル（tunnel.1、tunnel.2、および tunnel.3）で構成します。
3. （CPE 1、CPE 2、および CPE 3 から）3 つの IKE ゲートウェイのユーザーで XAuth サーバーを構成します。RADIUS 共有秘密値（juniper）およびポート番号（1812）を指定します。
4. RADIUS サーバーとゲートウェイとの間の静的ルートを定義し、ゲートウェイから ISP ルーターへのデフォルトのルートを定義します。
5. ゲートウェイ（デバイス 2）で、2fba::5555 から 2fba::8888 までの IP の範囲で、IP プール（P1）を定義します。

WebUI（ゲートウェイ）

1. インターフェース

Network > Interfaces > Edit (for Trust):

Network > Interfaces > Edit (for Trust) > IPv6

Network > Interfaces > Edit (for untrust)

Network > Interfaces > Edit (for untrust) > IPv6

2. トンネル

Network > Interfaces > New (Tunnel IF)

Network > Interfaces > Edit (for tunnel.6) > IPv6

3. ルート

Network > Routing > Routing Table > New (trust-vr)

4. IKE

VPNs > AutoKey Advanced > Gateway > New

VPNs > AutoKey Advanced > Gateway > Edit

5. VPN

VPNs > AutoKey IKE > New

VPNs > AutoKey IKE > Edit

6. ポリシー

Policies > (From: Untrust, To: Trust) > New

Policies > (From: Trust, To: Untrust) > New

CLI（ゲートウェイ）

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ipv6 mode router
set interface ethernet1 ipv6 enable
set interface ethernet1 ipv6 interface-id 1111111111111111
set interface ethernet1 ipv6 ip 2eee::1/64
set interface ethernet1 ipv6 ra transmit
set interface ethernet1 manage
set interface ethernet1 route
set interface ethernet1 route-deny

set interface ethernet2 zone untrust
set interface ethernet2 ipv6 mode router
set interface ethernet2 ipv6 enable
set interface ethernet2 ipv6 interface-id 1111111111111111
set interface ethernet2 ipv6 ip 2eee::1/64
set interface ethernet2 ipv6 ra transmit
set interface ethernet2 manage
set interface ethernet2 route

set interface ethernet3 zone untrust
set interface ethernet3 ipv6 mode router
set interface ethernet3 ipv6 enable
set interface ethernet3 ipv6 interface-id 1111111111111111
set interface ethernet3 ipv6 ip 2eee::1/64
set interface ethernet3 ipv6 ra transmit
set interface ethernet3 zone untrust
set interface ethernet3 manage
set interface ethernet3 route

set interface ethernet4 zone untrust
set interface ethernet4 ipv6 mode router
set interface ethernet4 ipv6 enable
set interface ethernet4 ipv6 interface-id 1111111111111111
set interface ethernet4 ipv6 ip 2eee::1/64
set interface ethernet4 ipv6 ra transmit
set interface ethernet4 manage
set interface ethernet2 route
```

2. トンネル

```
set interface tunnel.1 zone untrust
set interface tunnel.2 zone untrust
set interface tunnel.3 zone untrust
```

3. ルート

```
set vrouter trust-vr route 2fbc::4321/64 interface tunnel.1
set vrouter trust-vr route 2afc::4321/64 interface tunnel.2
set vrouter trust-vr route 2caf::4321/64 interface tunnel.3
set vrouter trust-vr route::/0 interface ethernet1 gateway 3002::0001
```

4. RADIUS

```
set ippool P1 2fba::5555 2fba::8888
set auth-server RAD1 id 1
set auth-server RAD1 server-name 3333::ff00
set auth-server RAD1 account-type xauth
set auth-server RAD1 radius secret juniper
set auth-server RAD1 radius port 1812
set xauth default ippool P1
```

5. IKE

```
set ike gateway G_CPE1 add 20.1.1.1 main outgoing-interface ethernet2 preshare
    abc123 sec-level standard
set ike gateway G_CPE1 xauth server RAD1 query-config user PC4
set ike gateway G_CPE1 modecfg server action add-route

set ike gateway G_CPE2 add 60.1.1.1 main outgoing-interface ethernet3 preshare
    abc123 sec-level standard
set ike gateway G_CPE2 xauth server RAD1 query-config user PC4
set ike gateway G_CPE2 modecfg server action add-route

set ike gateway G_CPE3 add 80.1.1.1 main outgoing-interface ethernet4 preshare
    abc123 sec-level standard
set ike gateway G_CPE3 xauth server RAD1 user PC4
set ike gateway G_CPE3 modecfg server action add-route
```

6. VPN

```
set vpn GtoCPE1 gateway NS2_NS1 sec-level standard
set vpn G2toCPE1 bind interface tunnel.1

set vpn GtoCPE2 gateway NS2_NS3 sec-level standard
set vpn GtoCPE2 bind interface tunnel.2

set vpn GtoCPE3 gateway NS2_NS4 sec-level standard
set vpn GtoCPE3 bind interface tunnel.3
```

7. Policies

```
set policy from trust to untrust any any any permit
set policy from untrust to trust any any any permit
```

ISP ルーターの構成

このセクションでは、IPv6 ルーターである ISP ルーターをセットアップする構成手順を示します。

1. ゲートウェイルーターおよび RADIUS サーバーへ到達するように ISP ルーターを構成します。

2. RADIUS サーバー用のアカウントを構成します。

3. 100.100.100.0/24 ネットワークに到達できるように、ISP ルーターで静的ルートを定義します。次ホップをゲートウェイの ethernet1 インターフェースの IP アドレスにします。

WebUI（ISP ルーター）

1. インターフェース

Network > Interfaces > Edit (for Trust):

Network > Interfaces > Edit (for Trust) > IPv6

Network > Interfaces > Edit (for untrust)

Network > Interfaces > Edit (for untrust) > IPv6

2. ルート

Network > Routing > Routing Table > New (trust-vr)

CLI（ISP ルーター）

1. インターフェース

```
set interface ethernet1 zone trust
set interface ethernet1 ipv6 mode router
set interface ethernet1 ipv6 enable
set interface ethernet1 ipv6 interface-id 1111111111111111
set interface ethernet1 ipv6 ip 3002::0001/64
set interface ethernet1 ipv6 ra transmit
set interface ethernet1 manage
set interface ethernet1 route

set interface ethernet2 zone trust
set interface ethernet2 ipv6 mode router
set interface ethernet2 ipv6 enable
set interface ethernet2 ipv6 interface-id 2222222222222222
set interface ethernet2 ipv6 ip 3002::0002/64
set interface ethernet2 ipv6 ra transmit
set interface ethernet2 manage
set interface ethernet2 route
```

2. ルート

```
set vrouter trust-vr route 2fba::5555/64 interface ethernet1 gateway
    3001::0004/64
```

OSPF への Null インターフェース再配布の設定

この例では、Null インターフェースへの静的ルートを設定し、OSPF（Open Shortest Path First）ルーティングプロトコルを使用して、ISP ルーターへのルートを再配布します。このルートへ送信されたトラフィックは、OSPF への再配布の対象となり、外部の OSPF デバイスが利用できます。

1. 69 ページで示すように CPE 1、CPE 2、および CPE 3 を構成します。
2. 73 ページで示すように、ゲートウェイルーターを構成します。
3. 75 ページで示すように、ISP ルーターを構成します。

WebUI（ゲートウェイルーター用 OSPF）

Network > Routing > Virtual Router > Edit

CLI（ゲートウェイ）

```
set vrouter trust-vr route 2fba::5555/64 interface null

set vrouter trust-vr
set protocol ospf
set area 0
set enable
set interface ethernet1 protocol ospf area 0
set interface ethernet1 protocol ospf enable
set vrouter trust-vr
set route-map name abc permit 10
set match ip 10
set access-list 10 permit ip 2fba::5555/64 10
set vrouter trust-vr protocol ospf redistribute route-map abc protocol static
```

WebUI（ISP）

Network > Routing > Virtual Router > Edit

CLI（ISP）

```
set vrouter trust-vr
set protocol ospf
set area 0
set enable
set interface ethernet1 protocol ospf area 0
set interface ethernet1 protocol ospf enable
```

発見したルートの OSPF への再配布

発見したルートを OSPF（Open Shortest Path First）ルーティングプロトコルへ再配布するよう、ゲートウェイルーターを構成できます。これには、69 ページで示す構成に次のコマンド情報を追加します。

WebUI（ゲートウェイ）

Network > Routing > Virtual Router > Edit

CLI（ゲートウェイ）

```
set vrouter trust-vr protocol ospf redistribute route-map abc protocol discovered
```

OSPF サマリーのインポートのセットアップ

この例では、発見したルートを OSPF ルーティングプロトコルへ再配布するよう、ゲートウェイおよび ISP ルーターをセットアップします。完全な構成およびイラストは 69 ページを参照してください。

1. 69 ページで説明したように CPE 1、CPE 2、および CPE 3 を構成し、75 ページで説明したように ISP ルーターを構成します。
2. 73 ページで説明したようにゲートウェイを構成し、静的ルートを ISP ルーターへ再配布します。下の構成を追加します。
3. OSPF のインポートサマリー機能を構成します。

WebUI（ゲートウェイ）

Network > Routing > Routing Table > New (trust-vr)

Network > Routing > Virtual Router > Edit

CLI（ゲートウェイ）

3. OSPF

```
set vrouter trust-vr
set protocol ospf
set area 0
set enable
set interface ethernet1 protocol ospf area 0
set interface ethernet1 protocol ospf enable
set vrouter trust-vr
set route-map name abc permit 10
set match ip 10
exit
set access-list 10 permit ip 2fba::5555/64 10
set vrouter trust-vr protocol ospf redistribute route-map abc protocol discovered
set vrouter trust protocol ospf summary-import 2fba::5555/64
```

第 5 章

アドレス変換

別々の IP スタックを使用する 2 つのホストがセキュリティデバイスを介してサービス要求を交換する場合、デバイスが IPv4/IPv6 の境界を越えて要求を送信するためにはすべてのパケットについてアドレス変換を実行しなければなりません。この章では、変換プロセスについて説明します。本章のセクションは、以下のようになります。

- 80 ページの「概要」
  - 81 ページの「ソース IP アドレスの変換」
  - 82 ページの「宛先 IP アドレスの変換」
- 83 ページの「設定例」
  - 81 ページの「ソース IP アドレスの変換」
  - 82 ページの「宛先 IP アドレスの変換」
  - 84 ページの「IPv6 ホストから複数 IPv4 ホストへの送信」
  - 87 ページの「IPv4 ホストから複数 IPv6 ホストへの送信」
  - 89 ページの「IPv4 ホストから単一 IPv6 ホストへの送信」
  - 91 ページの「ドメイン名システムサーバーアドレスの変換」

概要

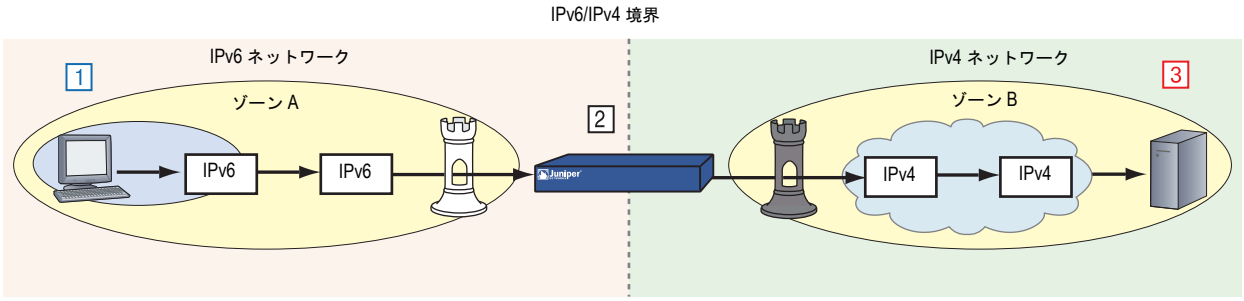
ネットワークアドレス変換 - ポート変換（NAT-PT）は、互換性のない別々の IP スタックを使用しているホスト間で送信されるパケットのアドレス変換を実行するメカニズムです。たとえば、IPv6 ホストによって生成されたパケットが IPv4 のみのバックボーンを通して IPv4 ホストに送信されるためには、パケットが IPv4 ソースアドレスと宛先アドレスを持っていなければなりません。NAT-PT は、そのようなアドレスを元の IPv6 ソースおよび宛先アドレスを IPv4 に変換することにより提供します。

デバイスは次のメカニズムを使用して、アドレス変換を実行します。

- 動的 IP（DIP）。これは、定義されたアドレスプールから新しいソースアドレスを生成します。
- マップ IP（MIP）。これは、あるアドレスと別のアドレスの間でダイレクトマッピングを実行することにより宛先アドレスを変換します。MIP は、指定されたサブネットにアドレスをマッピングすることもできます。

図 17 は、IPv4 ホストに IPv6 サービス要求パケットを送信するために、デバイスがどのように NAT-PT を使用するかを示しています。

図 17: IPv4/IPv6 境界間のネットワークアドレス変換（NAT）



1. IPv6 ホストがセキュリティデバイスのローカル IPv6 インターフェースに IPv6 サービス要求パケットを送信します。
2. セキュリティデバイスがパケットアドレスを IPv4 に変換します。ソースアドレスの変換には DIP を使用し、宛先アドレスの変換には MIP を使用します。
3. 宛先ホストが IPv4 パケットを受け取り処理します。

NAT-PT が IPv6 パケットを IPv4 パケットに、IPv6 パケットを IPv4 パケットに変換しますので、IPv6/IPv4 間のルーティングが可能になります。

IPv4 ホストが IPv4 と IPv6 の間でアドレスを変換する場合、MIP を使用して *IPv4 にマッピングされた*宛先アドレスを生成します。IPv4 にマッピングされたアドレスは、埋込み型の IPv4 アドレスを含んでいるグローバルユニキャスト IPv6 アドレスです。IPv4 にマッピングされるアドレスのフォーマットは、*IPv6*::*a.b.c.d* となり、この場合、

- *IPv6* は、宛先アドレスの IPv6 サブネットの部分。
- *a.b.c.d* は、組み込み IPv4 アドレス（十進表記法で表示）を表します。

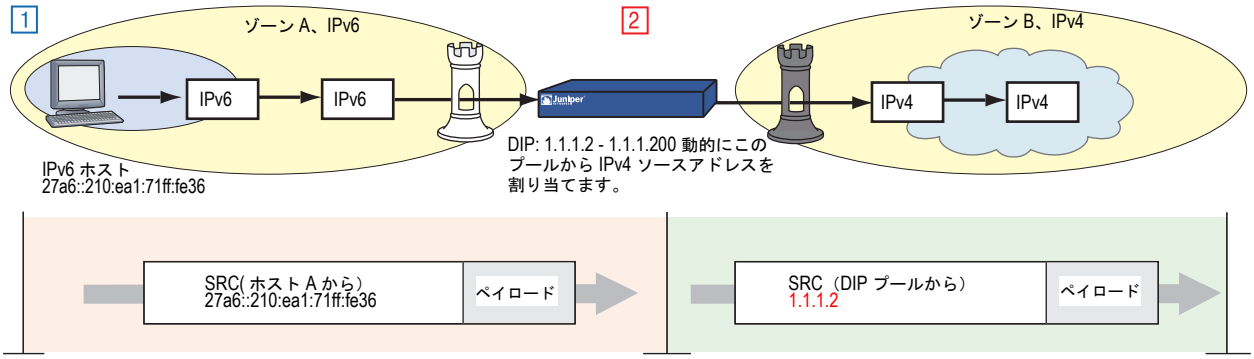
ソース IP アドレスの変換

異なる IP スタックを使用する 2 つのホストがデバイスを介してパケットを交換する場合、デバイスは各パケットのソースアドレスを宛先ホストと互換性のあるアドレスに変換しなければなりません。たとえば、IPv4 ネットワークに IPv6 パケットを送信するためには、IPv4 ソースアドレスが必要です。IPv4 ソースアドレスがなければ、パケットは、IPv4 と IPv6 の境界を越えることができません。デバイスは、ソースアドレスを変換するために動的 IP（DIP）を使用することができます。これは定義されたアドレスプールからソース IP アドレスを自動的に生成するメカニズムです。

IPv6 から IPv4 への DIP

図 18 は、IPv4 バックボーン上で、IPv4 サーバーへ要求パケットを送る IPv6 ホストを示しています。IPv6 ルーターであるセキュリティデバイスは、パケットヘッダー内の IPv6 ソースアドレスを IPv4 アドレスに置換します。

図 18: IPv6 から IPv4 への DIP

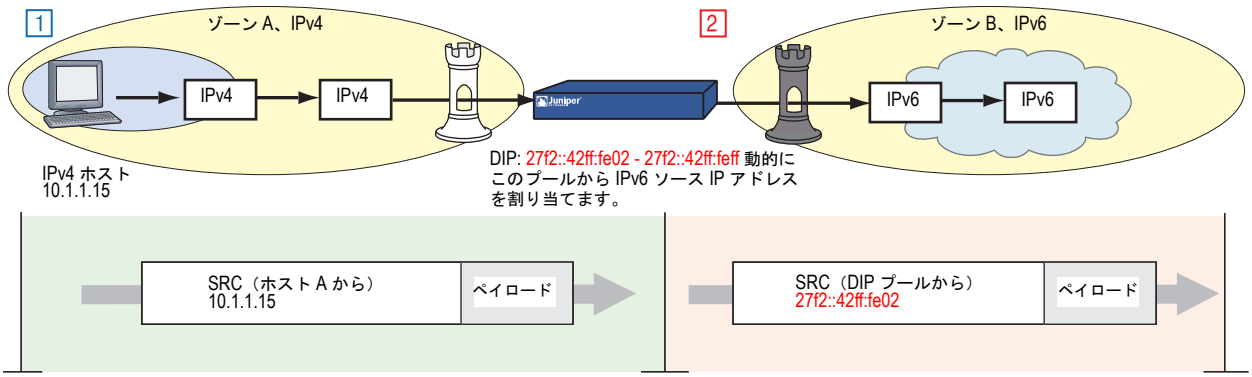


この例では、デバイスは DIP プールから IPv4 ソースアドレス 1.1.1.2 を取得し、元の IPv6 ソースアドレスをこのアドレスに置換します（27a6::210:ea1:71ff:fe36）。それからパケットを IPv6 と IPv4 の境界を越えて送信します。

IPv4 から IPv6 への DIP

図 19 は、IPv6 バックボーン上で、ゾーン B 内の IPv6 サーバーへ要求パケットを送る IPv4 ホストを示しています。セキュリティデバイスは、パケットヘッダー内の IPv4 ソースアドレスを IPv6 アドレスに置換します。

図 19: IPv4 から IPv6 への DIP



この例では、デバイスは DIP プールから IPv6 ソースアドレス 27f2::42ff:fe02 を生成し、元の IPv4 ソースアドレス（10.1.1.15）をこのアドレスに置換します。それからパケットを IPv4 と IPv6 の境界を越えて送信します。

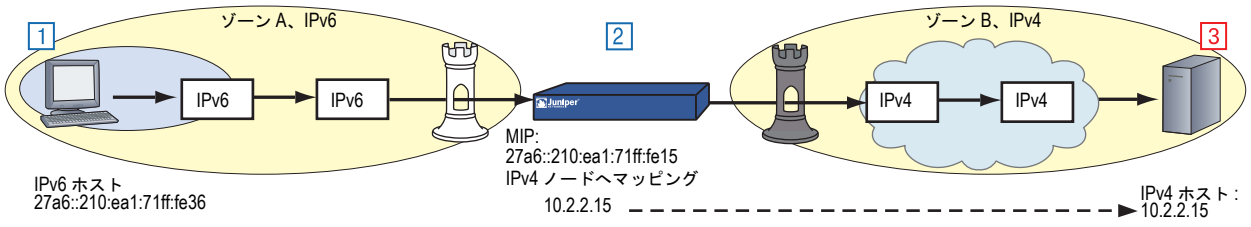
宛先 IP アドレスの変換

異なる IP スタックを使用する 2 つのホストがデバイスを介してパケットを交換する場合、デバイスは各パケットの宛先アドレスを宛先ホストと互換性のあるアドレスに変換しなければなりません。たとえば、IPv4 ネットワークに IPv6 パケットを送信するためには、IPv4 宛先アドレスが必要です。IPv4 ソースアドレスがなければ、パケットは IPv4 と IPv6 の境界を越えることができません。この変換には、デバイスはマップ IP（MIP）を使用します。

IPv6 から IPv4 への MIP

図 20 は、IPv4 バックボーン上で IPv4 サーバーに要求パケットを送る IPv6 ホストを示しています。デバイスは、宛先ホストの IP アドレスフォーマットと一致する宛先アドレスを使用しなければなりません。

図 20: IPv6 から IPv4 への MIP



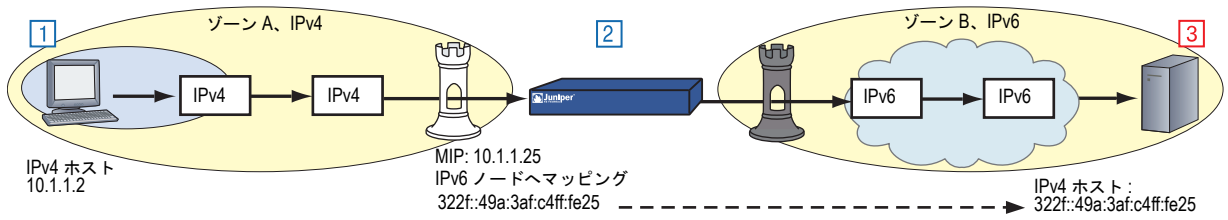
1. IPv6 ホストが IPv6 サービス要求パケットを生成し、セキュリティデバイスに送ります。パケットはゾーン A に入ります。
2. デバイスが宛先アドレスを MIP アドレスに置換し、パケットをゾーン B に送ります。
3. 宛先デバイスは、パケットをゾーン B 内で受け取ります。このデバイスにとってはこのパケットは IPv4 パケットです。

この例では、IPv6 ホストはパケットを MIP アドレス（27a6::210:ea1:71ff:fe15）に宛てています。デバイスはこの MIP をリモート IPv4 ホストのアドレス（10.2.2.15）に変換します。

IPv4 から IPv6 への MIP

図 21 は、IPv6 バックボーン上で、IPv6 サーバーへ要求パケットを送る IPv4 ホストを示しています。セキュリティデバイスは、宛先ホストの IP アドレスフォーマットと一致する宛先アドレスを使用します。

図 21: IPv4 から IPv6 への MIP



1. IPv4 ホストが IPv4 サービス要求パケットを生成し、セキュリティデバイスに送ります。パケットはゾーン A に入ります。

2. セキュリティデバイスが宛先アドレスを MIP アドレスに置換し、パケットをゾーン B に送ります。

3. 宛先デバイスは、パケットをゾーン B 内で受け取ります。このデバイスにとっては、このパケットは IPv6 パケットです。

この例では、IPv4 ホストは、パケットを MIP アドレス（10.1.1.25）に宛てています。デバイスはこの MIP をリモート IPv6 ホストのアドレス（322f::49a:3af:c4ff:fe25）に変換します。

MIP は、IPv6 ネットワークおよびサブネットにマッピングすることもできます。

設定例

次のセクションは、各種 NAT-PT シナリオとドメイン名サービスによる変換の例を示しています。

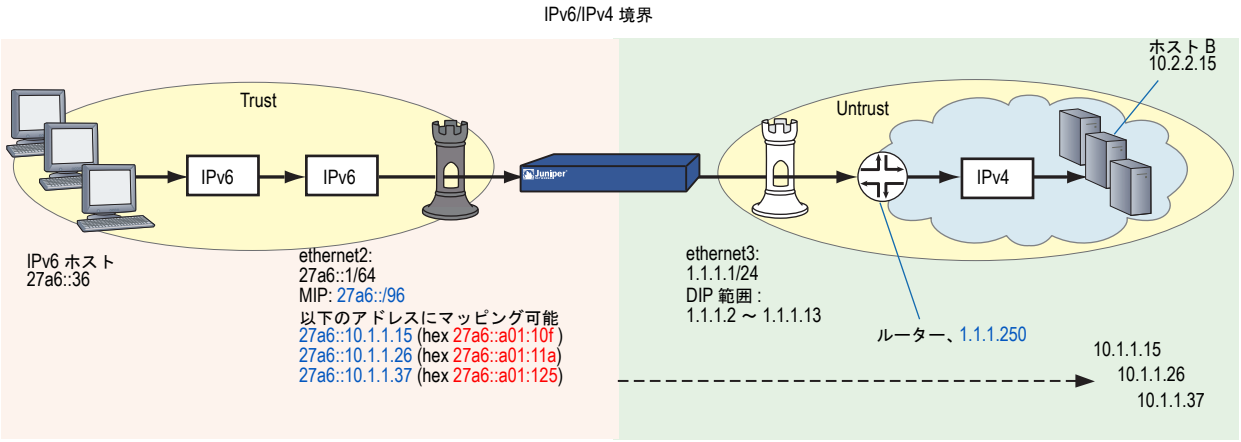
デバイスがホストからサービス要求パケットを送信し、異なる IP スタックを使用する別のホストへそれを転送する場合、デバイスは NAT-PT ポリシーを使用して送信パケットの IPv6 ソースアドレスおよび宛先アドレスを変換することができます。たとえば、IPv6 ネットワークと IPv4 WAN 間の境界に設置されているデバイスは、ソースアドレスと宛先アドレスを IPv4 に変換する NAT-PT ポリシーを使用して、IPv6 ホストから送られる IPv6 サービス要求を送信することができます。

IPv6 ホストから複数 IPv4 ホストへの送信

IPv6 ホストから複数の IPv4 宛先ホストにサービス要求を送信する必要がある場合、宛先アドレスの変換に *IPv6-to-IPv4 ネットワークマッピング*を使用するポリシーを定義します。

図 22 は、ローカル IPv6 アドレスをリモート IPv4 ネットワーク内の IPv4 アドレスへマッピングする NAT-PT メカニズムを示しています。ローカル IPv6 ホストがデバイスを介してサービス要求パケットを送信する場合、デバイスは MIP を使用して、IPv4 にマッピングされたフォーマットを使用する IPv6 宛先アドレスを生成します。IPv4/IPv6 境界を越えてパケットを送信するときに、デバイスはこれらの宛先アドレスを IPv4 アドレスに変換します。

図 22: IPv4 にマッピングされたアドレス



IPv6 ホストは、デバイスを介して IPv6/IPv4 境界を越えて HTTP 要求を送信することができます。この要求を送信するには、ユーザーはブラウザの URL フィールドに IPv4 にマッピングされたアドレス (27a6::10.1.1.15 等) を入力します。この入力は http://[27ab::10.1.1.15] のように表示されます。デバイスは、自動的にこのアドレスを 16 進法アドレスに変換します。IPv6 ホスト側では、宛先が IPv6 互換のデバイスであるように見えます。しかし、境界を越えて HTTP 要求を送信する前にデバイスがアドレスを IPv4 形式アドレスに変換するので、パケットは IPv4 WAN を通過することができます。宛先 IPv4 サーバー側にとってパケットは IPv4 と完全に互換性があります。

次の例では、アイランド IPv6 ネットワーク内のホストからリモート IPv4 ネットワーク内のホストへの HTTP サービス要求送信を可能にするよう、デバイスを設定します。宛先アドレスが単一ホストではなくネットワークであるので、デバイスは個々のリモートノードを表示するため、*IPv4 にマッピングされたアドレス*を使用します。

ホスト A は IPv6 サービス要求パケットを生成し、ホスト B に宛てます。MIP テーブル内の表の IPv6 宛先アドレスを指定します。次にパケットはゾーン A からゾーン B に移動します。

デバイス A は DIP プールからソースアドレスを取得し、MIP アドレスを宛先ホストの IPv4 アドレスに変換します。それからパケットをデバイス B のインターフェースに送信します。

デバイスは IPv4 にマッピングされたアドレスを IPv4 形式アドレスに変換し、送信パケットの宛先アドレスに割り当てます。

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (for ethernet2)

   Network > Interfaces > Edit (for ethernet2) > IPv6

   Network > Interfaces > Edit (for ethernet3)

2. **MIP**
   Network > Interfaces > Edit (for ethernet2) > IPv6 > MIP > New

3. **DIP**
   Network > Interfaces > Edit (for ethernet3) > DIP > New

4. **ルーター**
   Network > Routing > Routing Entries New (for trust-vr)

5. **ポリシー**
   Policies > New (for Trust to Untrust)

   Policies > Edit (for policy) > Advanced

CLI

1. **インターフェース**
   set interface ethernet2 zone trust
   set interface ethernet2 ipv6 mode host
   set interface ethernet2 ipv6 enable
   set interface ethernet2 ipv6 ip 27a6::1/64
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **MIP**
   set interface ethernet2 mip 27a6::/96 ipv6 ipv4

3. **DIP**
   set interface ethernet3 dip 7 1.1.1.2 1.1.1.13

4. **ルーター**
   set vrouter trust-vr route 0.0.0.0/0 gateway 1.1.1.250

5. **ポリシー**
   set policy from trust to untrust any-ipv6 mip(27a6::/96) http nat src dip-id 7 permit
   save

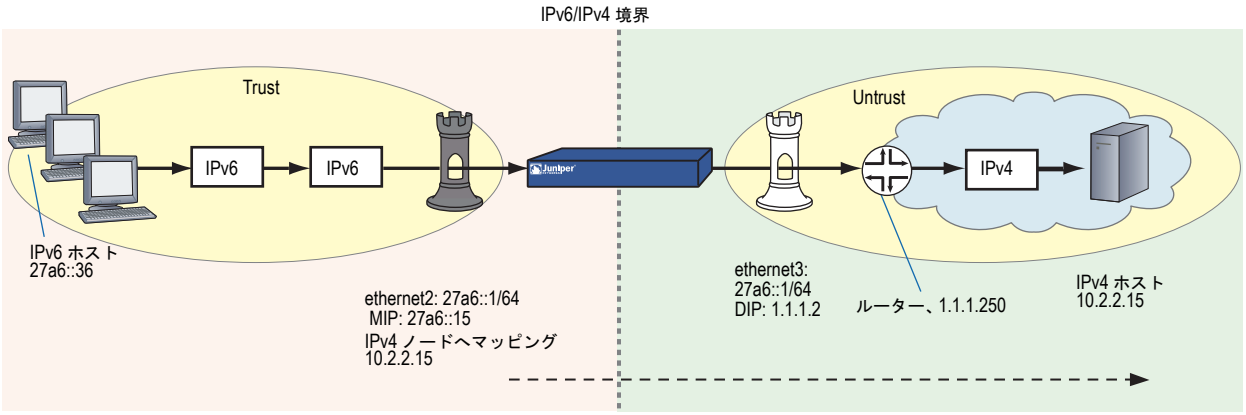
IPv6 ホストから単一 IPv4 ホストへの送信

IPv6 ホストから単一の IPv4 ホストにサービス要求を送信する必要がある場合、宛先アドレスの変換に *IPv6-to-IPv4 ホストマッピング*を使用するポリシーを定義することができます。

この NAT-PT メカニズムは、IPv6 アドレスを単一のリモート IPv4 ホストの IPv4 アドレスにマッピングします。ローカル IPv6 ホストがデバイスを介してサービス要求パケットを送信する場合、デバイスはパケットヘッダー内の IPv4 宛先アドレスにマッピングされたアドレスを使用します。この変換により送信パケットは IPv6 と IPv4 の境界を越えることができ、リモートホストとのコミュニケーションを確立することができます。

図 23 は、デバイスを介して、IPv6/IPv4 境界を越えて、単一 IPv4 サーバーに HTTP 要求を送信する IPv6 ホストを示しています。

図 23: IPv6-to-IPv4 ホストマッピング



要求を送信するには、ユーザーはブラウザの URL フィールドに IPv6 アドレス (27a6::15 等) を入力します。IPv6 ホスト側では、宛先が IPv6 互換のデバイスであるように見えます。しかし、Pv6/IPv4 境界を越えて HTTP 要求を送信する前にデバイスがアドレスをマッピングされた IPv4 アドレスに変換するので、パケットは IPv4 WAN を通過することができます。宛先 IPv4 サーバー側にとってパケットは IPv4 と完全に互換性があります。

次の例では、アイランド IPv6 ネットワーク内のホストから単一リモート IPv4 ホスト（10.2.2.15）への HTTP サービス要求送信を可能にするようにデバイスを設定します。

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (for ethernet2)

   Network > Interfaces > Edit (for ethernet2) > IPv6

   Network > Interfaces > Edit (for ethernet3)

2. **MIP**
   Network > Interfaces > Edit (for ethernet2) > IPv6 > MIP > New

3. **DIP**
   Network > Interfaces > Edit (for ethernet3) > DIP > New

4. **ルーター**
   Network > Routing > Routing Entries New (for trust-vr)

5. **ポリシー**
   Policies > New (for Trust to Untrust)

   Policies > Edit (for policy) > Advanced

CLI

1. **インターフェース**
   set interface ethernet2 zone trust
   set interface ethernet2 ipv6 mode host
   set interface ethernet2 ipv6 enable
   set interface ethernet2 ipv6 ip 27a6::1/64
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **MIP**
   set interface ethernet2 mip 27a6::15 ipv6 host 10.2.2.15

3. **DIP**
   set interface ethernet3 dip 7 1.1.1.2 1.1.1.13

4. **ルーター**
   set vrouter trust-vr route 0.0.0.0/0 gateway 1.1.1.250

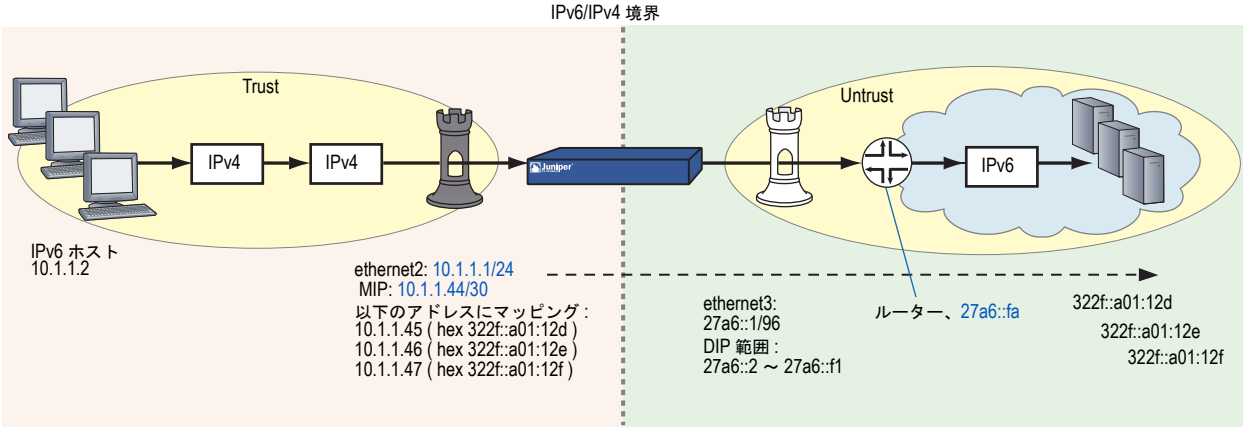
5. **ポリシー**
   set policy from trust to untrust any-ipv6 mip(27a6::15) http nat src dip-id 7 permit

IPv4 ホストから複数 IPv6 ホストへの送信

ローカル IPv4 ホストから複数の IPv6 ホストにサービス要求を送信する必要がある場合、*IPv4-to-IPv6 ネットワークマッピング*を使用するポリシーを定義することができます。

図 24 は、ローカル IPv4 アドレスを IPv6 ネットワーク（またはサブネット）にマッピングする NAT-PT を示しています。ローカル IPv4 ホストがデバイスを介して IPv4 サービス要求パケットを送信する場合、デバイスはマッピングされたアドレスを IPv6 アドレスに変換し、これをパケットヘッダーの宛先アドレスに割り当てます。この変換により送信パケットは IPv4 と IPv6 の境界を越えることができ、リモート IPv6 ホストとのコミュニケーションを確立することができます。

図 24: IPv4-to-IPv6 ネットワークマッピング



マッピングされた IPv4 アドレスは間接的にリモート IPv6 ホストを表示しています。実際、ローカル IPv4 ホストにはリモートホストはローカル IPv4 ネットワークの一部として見えます。

MIP がローカル IPv4 ホストと同じサブネットに属するのでホストはローカル IPv4 ネットワークの一部としてリモートホストを見ることができるのです。

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (for ethernet2)

   Network > Interfaces > Edit (for ethernet3)

   Network > Interfaces > Edit (for ethernet3) > IPv6

2. **MIP**
   Network > Interfaces > Edit (for ethernet2) > IPv6 > MIP > New

3. **DIP**
   Network > Interfaces > Edit (for ethernet3) > DIP > New

4. **ルーター**
   Network > Routing > Routing Entries New (for trust-vr)

5. **ポリシー**
   Policies > New (for Trust to Untrust)

   Policies > Edit (for policy) > Advanced

CLI

1. **インターフェース**
   set interface ethernet2 zone trust
   set interface ethernet2 ip 10.1.1.1/24
   set interface ethernet3 zone untrust
   set interface ethernet3 ipv6 mode host
   set interface ethernet3 ipv6 enable
   set interface ethernet3 ipv6 ip 27a6::1/64

2. **MIP**
   set interface ethernet2 mip 10.1.1.44 ipv6 prefix 322f::44/96 netmask 255.255.255.252

3. **DIP**
   set interface ethernet3 dip 7 27a6::2 27a6::f1

4. **ルーター**
   set vrouter trust-vr route::/0 interface ethernet3 gateway 27a6::fa

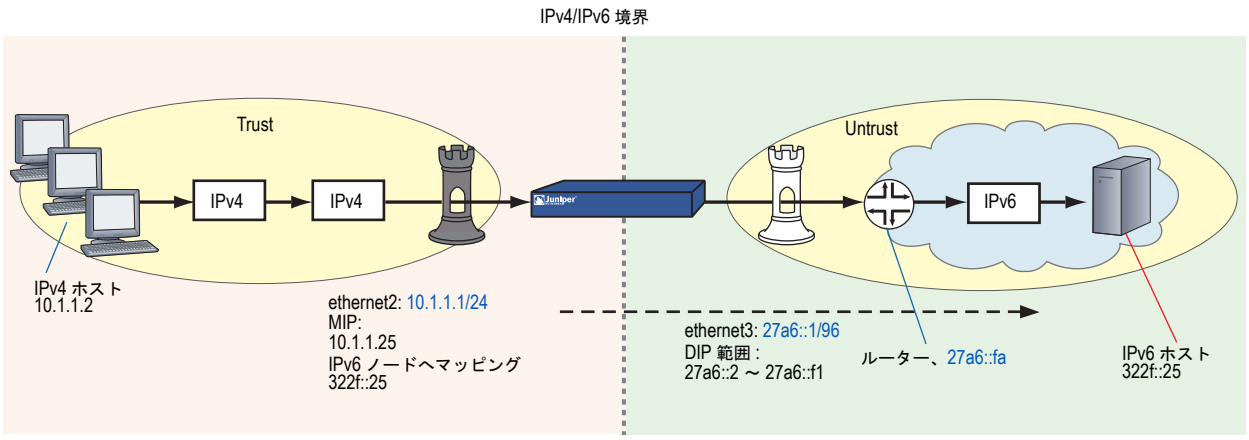
5. **ポリシー**
   set policy from trust to untrust any-ipv4 mip(10.1.1.44/30) http nat src dip-id 7 permit

IPv4 ホストから単一 IPv6 ホストへの送信

ローカル IPv4 ホストから単一のリモート IPv6 ホストへとサービス要求を送信する必要がある場合、*IPv4-to-IPv6 ホストマッピング*を使用するポリシーを定義します。

図 25 は、デバイスを介して IPv4 サービス要求パケットを送信する IPv4 ホストを示しています。デバイスは マッピングされたアドレスを IPv6 アドレスに変換し、パケットヘッダーの宛先アドレスに割り当てます。この変換により送信パケットは IPv4 と IPv6 の境界を越えることができ、リモート IPv6 ホストとのコミュニケーションを確立することができます。

図 25: IPv4-to-IPv6 ホストマッピング



MIP がローカル IPv4 ホストと同じサブネットに属するので、ホストはローカル IPv4 ネットワークの一部としてリモートホストを見ることができます。

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (for ethernet2)

   Network > Interfaces > Edit (for ethernet3)

   Network > Interfaces > Edit (for ethernet3) > IPv6

2. **MIP**
   Network > Interfaces > Edit (for ethernet2) > IPv6 > MIP > New

3. **DIP**
   Network > Interfaces > Edit (for ethernet3) > DIP > New

4. **ルーター**
   Network > Routing > Routing Entries New (for trust-vr)

5. **ポリシー**
   Policies > New (for Trust to Untrust)

   Policies > Edit (for policy) > Advanced

CLI

1. **インターフェース**
   set interface ethernet2 zone trust
   set interface ethernet2 ip 10.1.1.1/24
   set interface ethernet3 zone untrust
   set interface ethernet3 ipv6 mode host
   set interface ethernet3 ipv6 enable
   set interface ethernet3 ipv6 ip 27a6::1/96

2. **MIP**
   set interface ethernet2 mip 10.1.1.25 ipv6 host 322f::25

3. **DIP**
   set interface ethernet3 dip 7 27a6::2 27a6::f1

4. **ルーター**
   set vrouter trust-vr route::/0 interface ethernet3 gateway 27a6::fa

5. **ポリシー**
   set policy from trust to untrust any-ipv4 mip(10.1.1.25) http nat src dip-id 7 permit

ドメイン名システムサーバーアドレスの変換

ドメイン名システム（DNS）はネットワークデバイスが互いを識別するのに、IP アドレスの代わりにドメイン名を使用します。外部 DNS サーバーは、ドメイン名テーブルを維持し、各ドメイン名には少なくとも 1 つの関連する IP アドレスがあります。これらのドメイン名（および IP アドレス）をポリシー定義の際のエンドポイントの識別に使用できます。

いくつかのドメイン名は IPv4 および IPv6 アドレスの両方を持つことができます。たとえば、acme.com および juniper.net というドメイン名があった場合、以下のアドレスを持つことができます。

ドメイン名	IPv4 アドレス	IPv6 アドレス
www.acme.com	1.2.2.15	27a6::e02:20f
	1.2.2.62	27a6::23ee:51a
	2.3.5.89	27a6::5542:225
www.juniper.net	3.1.1.21	3090::e02:20f
	3.20.7.96	3090::23ee:51a
	4.6.5.89	2e66::3354:722
	4.200.7.88	2e66::3354:722

エンドポイントとしてドメイン名を使用するポリシーを定義し、両方のドメイン名が IPv4 と IPv6 のアドレスを持っている場合、デバイスはどちらのプロトコルを使ってもエンドポイント間のセキュアなコミュニケーションを確立することができます。たとえば、以下のコマンドはドメイン名 juniper.net と acme.com の間のポリシーを定義します。

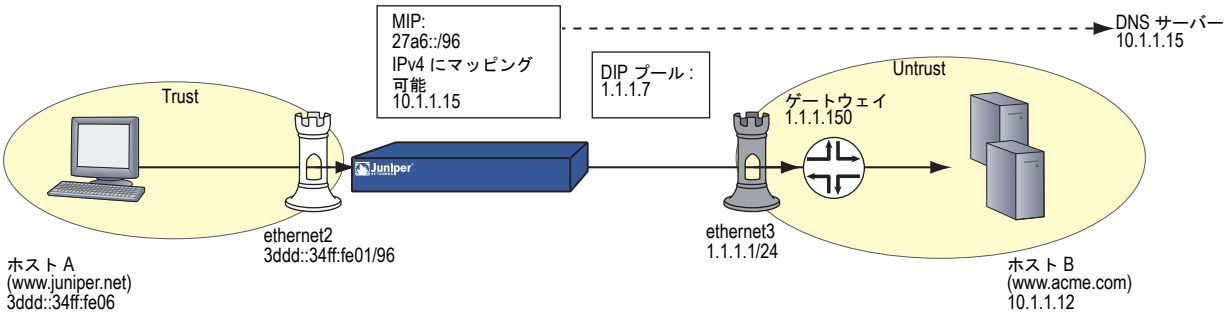
```
set address trust juniper www.juniper.net
set address untrust acme www.acme.com
set policy from trust to untrust juniper acme any permit
```

ドメイン名がどちらも IPv4 と IPv6 のアドレスを持っているので、2 つのエンドポイントはどちらのタイプのトラフィックもやり取りすることができます。

一方のドメイン名がもう一方のドメイン名が使用していない IP スタックを使用している場合には、NAT-PT を使用して送信 DNS 要求のソースアドレスおよび宛先アドレスを変換しなければなりません。たとえば、juniper.net が IPv6 アドレスだけを持っており、acme.com が IPv4 アドレスだけを持っている場合、一方らもう一方に送信されるサービス要求は NAT-PT アドレス変換を通さなければなりません。

次の例では、IPv6 ホスト（www.juniper.net）が IPv4 ホスト（www.acme.com）へサービス要求を送信しています。IPv4 DNS サーバーから宛先ホストの IPv4 アドレスを取得します。

図 26: NAT-PT DNS の例



デバイスには 次の 2 つのポリシーが必要です。

- サービス要求の送信を許可し、ソースアドレスと宛先アドレスに対して NAT-PT を実施するポリシー。
- www.juniper.net から www.acme.com へのサービス要求送信を許可するポリシー。

次の例では、ホスト A（www.juniper.net）からホスト B（www.acme.com）へのサービス要求の送信を許可するようにデバイスを設定します。ホストのドメイン名がコミュニケーションエンドポイントの役目を果たします。

WebUI

1. **インターフェース**
   Network > Interfaces > Edit (for ethernet2)

   Network > Interfaces > Edit (for ethernet2) > IPv6

   Network > Interfaces > Edit (for ethernet3)

2. **MIP**
   Network > Interfaces > Edit (for ethernet2) > IPv6 > MIP > New

3. **DIP**
   Network > Interfaces > Edit (for ethernet3) > DIP > New

4. **ルーター**
   Network > Routing > Routing Entries New (for trust-vr)

5. **アドレス**
   Policy > Policy Elements > Addresses > List > New (for Trust)

   Policy > Policy Elements > Addresses > List > New (for untrust)

6. **ポリシー**
   Policies > New (for Trust to Untrust)

   Policies > Edit (for policy) > Advanced > Advanced

CLI

1. **インターフェース**
   set interface ethernet2 zone trust
   set interface ethernet2 ipv6 mode host
   set interface ethernet2 ipv6 enable
   set interface ethernet2 ipv6 ip 3ddd::34ff:fe01/96
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **MIP**
   set interface ethernet2 mip 3ddd::/96 ipv6 ipv4 vrouter trust-vr

3. **DIP**
   set interface ethernet3 dip 7 1.1.1.7

4. **アドレス**
   set address trust juniper.net 3ddd::34ff:fe06/96
   set address untrust acme www.acme.com

5. **ルーター**
   set vrouter trust-vr route 0.0.0.0/0 gateway 1.1.1.250

6. **ポリシー**
   set policy from trust to untrust any-ipv6 mip(3ddd::/96) any nat dip-id 7 permit
   set policy from trust to untrust any-ipv4 acme any permit
   save

第 6 章

IPv4 環境での IPv6

6over4 トンネリングとは、IPv6 パケットが IPv4 WAN（ワイドエリアネットワーク）を行き来できるように、IPv6 パケットを IPv4 パケットヘッダー内にカプセル化するプロセスです。

本章のセクションは、以下のようになります。

- 95 ページの「概要」
- 96 ページの「手動トンネリングの構成」
- 99 ページの「6to4 トンネリングの構成」
  - 99 ページの「6to4 ルーター」
  - 100 ページの「6to4 リレールーター」
  - 101 ページの「リモートネイティブホストへのトンネル」
  - 104 ページの「リモート 6to4 ホストへのトンネル」

概要

6over4 トンネリングは、交換するトラフィックの認証および暗号化が必要ないときに、IPv4 WAN（ワイドエリアネットワーク）上で IPv6 トラフィックを送信する方法です。たとえば、ユーザーの組織で、IPv4 WAN 上のアイランド IPv6 ネットワーク間でトラフィックを交換する必要があるとします。この場合、セキュリティデバイスは、ファイアウォールサービスしか提供しません。

6over4 トンネルには次の 2 種類があります。

- *手動トンネリング*は、手動で構成した静的なリモートエンドのトンネル終端ポイントを使用します。
- *6to4 トンネリング*は、リモートエンド終端ポイントを動的に取得します。

注： 6to4 トンネリングの詳細については、RFC 3056 を参照してください。

ほとんどの場合、使用するトンネリングの種類は、WAN インフラストラクチャに存在するルーターなどのデバイスの種類によります。たとえば、ISP（インターネットサービスプロバイダ）は、追加サービスとして顧客に手動トンネルを提供し、6to4 トンネリングの必要がない場合もあります。さらに、WAN 上でユーザーの組織の 6to4 トンネリングをサポートするには、Ipv6 バックボーンに不十分な 6to4 構成のリレーしかない場合もあります。

6to4 トンネリングは、ユーザーの組織が 1 対多構成を確立する必要がある場合に、適切なことがあります。そこでは、1 つの IPv6 ネットワークが、複数の 6to4 リレールーターにより、複数の指定していないアイランド IPv6 ネットワークにアクセスできます。この場合、6to4 トンネリングが、最前のソリューションとなります。

手動トンネリングの構成

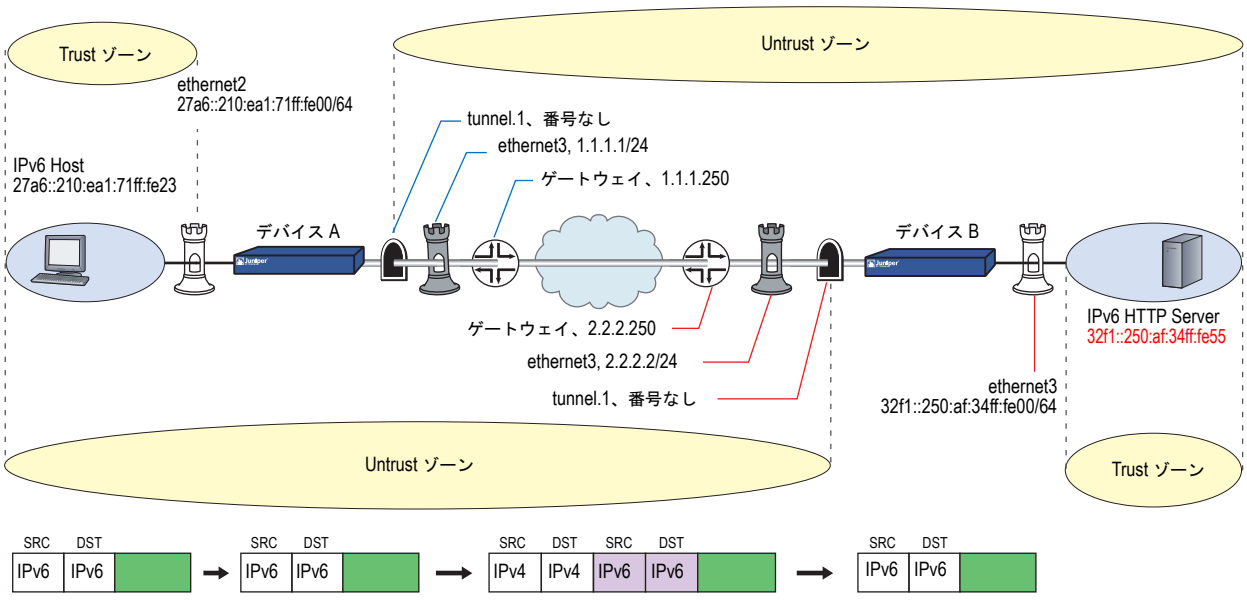
手動トンネリングは、厳格な制御が必要な用途に最適であり、通常は 6to4 トンネリングよりも高いセキュリティを提供します。手動トンネリングは、宛先ゲートウェイの Ipv4 アドレスを明示的に指定するので、アドレス変換を必要としません。

IPv4 ホストは、IPv4 WAN バックボーン上で IPv6 サーバーと通信するのに、トンネルを使用します。トンネルの端点は、デバイス A と B のインターフェースです。

デバイスを手動トンネリング向けに構成するとき、デバイスは、各送信 Ipv6 パケットを Ipv4 ネットワーク空間へ送信する前に Ipv4 パケット内部にカプセル化します。

図 27 は、2 つの静的な定義済み端点の間の手動トンネルを示します。

図 27: Ipv4 カプセル化を使用した Ipv6 トンネリングの例



次の例では、手動 6to4 トンネルの端点として 2 つのデバイス（A および B）を設定しています。

WebUI（デバイス A）

インターフェース

Network > Interfaces > Edit (for ethernet2)

Network > Interfaces > Edit (for ethernet2) > IPv6

Network > Interfaces > Edit (for ethernet3)

トンネルインターフェース

Network > Interfaces > New (Tunnel IF)

Network > Interfaces > Edit (for tunnel.1) > IPv6

Network > Interfaces > Edit (for tunnel.1) > Encapsulation

ルーター

Network > Routing > Routing Table > New (trust-vr)

Network > Routing > Route Table > New (trust-vr)

アドレス帳入力

Policy > Policy Elements > Addresses > List (Trust) > New

ポリシー

Policies > (From: Untrust, To: Trust) > New

WebUI（デバイス B）

インターフェース

Network > Interfaces > Edit (for ethernet2)

Network > Interfaces > Edit (for ethernet2) > IPv6

Network > Interfaces > Edit (for ethernet3)

トンネルインターフェース

Network > Interfaces > New (Tunnel IF)

Network > Interfaces > Edit (for tunnel.1) > IPv6

Network > Interfaces > Edit (for tunnel.1) > Encapsulation

ルーター

Network > Routing > Routing Table > New (trust-vr)

Network > Routing > Route Table > New (trust-vr)

アドレス帳入力

Policy > Policy Elements > Addresses > List (Trust) > New

ポリシー

Policies > (From: Untrust, To: Trust) > New

CLI（デバイス A）

1. インターフェース

```
set interface ethernet2 zone trust
set interface ethernet2 ip 10.1.1.1/24
set interface ethernet2 ipv6 mode router
set interface ethernet2 ipv6 enable
set interface ethernet2 ipv6 ip 2abc::1/64
set interface ethernet2 ipv6 ra link-mtu
set interface ethernet2 ipv6 ra link-address
set interface ethernet2 ipv6 ra transmit
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. トンネル インターフェース

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
set interface tunnel.1 ipv6 mode host
set interface tunnel.1 ipv6 enable
set interface tunnel.1 tunnel encap ip6in4 manual
set interface tunnel.1 tunnel local-if ethernet3 dst-ip 2.2.2.2
```

3. ルーター

```
set vrouter trust-vr route 3abc::/64 interface tunnel.1
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

4. アドレス

```
set address trust L_Hosts 2abc::/64
set address untrust R_Server 3abc::100/128
```

5. ポリシー

```
set policy from trust to untrust L_Hosts R_Server http permit
```

CLI（デバイス B）

1. インターフェース

```
set interface ethernet2 zone trust
set interface ethernet2 ip 1.100.2.1/24
set interface ethernet2 ipv6 mode host
set interface ethernet2 ipv6 enable
set interface ethernet2 ipv6 ip 3abc::1/64
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
```

2. トンネル インターフェース

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
set interface tunnel.1 ipv6 mode host
set interface tunnel.1 ipv6 enable
set interface tunnel.1 tunnel encap ip6in4 manual
set interface tunnel.1 tunnel local-if ethernet3 dst-ip 1.1.1.1
```

3. ルーター

```
set vrouter trust-vr route 2abc::/64 interface tunnel.1
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
```

4. **アドレス**
   set address trust L_Server 3abc::100/128
   set address untrust R_Clients 2abc::/64

5. **ポリシー**
   set policy from untrust to trust R_Clients L_Server http permit

6to4 トンネリングの構成

デバイスが *6to4 トンネリング*を使用しているとき、デバイスは、リモートエンドのトンネル終端ポイント（ゲートウェイ）をルーティングテーブルエントリから動的に決定します。VPN トンネルの 1 つの終端ポイントを明示的に指定する手動トンネリングと異なり、6to4 トンネリングでは、任意の数のデバイスがトンネルのリモートゲートウェイとして機能できます。これにより、保護されたアイランド Ipv6 ネットワークと複数の外部 Ipv6 ネットワーク間の 1 対多の通信が可能になります。

ネットワークデバイスは、6to4 ホストとして機能するには、6to4 アドレスで構成されたインターフェースを持っている必要あります。そのアドレスがない IPv6 ホストは、*ネイティブ*または非 6to4 と呼ばれます。たとえばホストに、グローバルな統合 IPv6 アドレスを持つインターフェースはあるが、6to4 アドレスを持つインターフェースがない場合、そのホストはネイティブホストです。一方、ホストに（他の種類の IPv6 アドレスがあってもなくても）6to4 アドレスで構成されたインターフェースがある場合、そのホストは 6to4 ホストとして機能します。

2 つのデバイス間で 6to4 トンネルをセットアップするには、各通信インターフェースを 6to4 アドレスで構成する必要があります。そうすると、インターフェースは、仮想境界ルーターとして機能し、IPv4 空間と IPv6 空間との間の移行を処理します。

6to4 仮想ルーターには 2 種類あります。

- **6to4** ルーターは、IPv4 WAN と 6to4 ネットワーク間の境界ルーターとして機能します。
- **6to4 リレー** ルーターは、IPv4 WAN とネイティブネットワーク間の境界ルーターとして機能します。

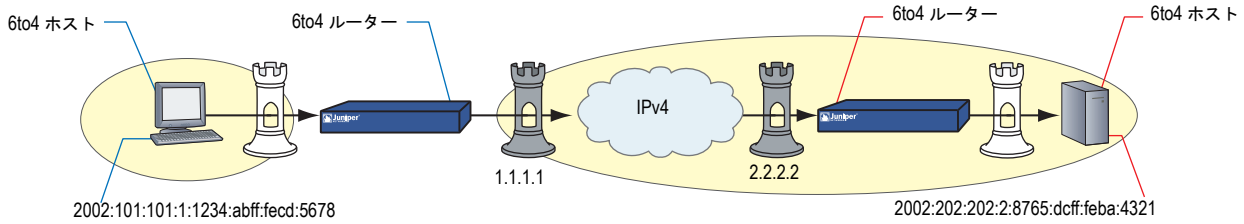
6to4 ルーター

*6to4 ルーター*は、IPv4 WAN 上の 6to4 ホストと他の 6to4 ホストの間でのパケット交換をサポートするよう構成されたルーターです。IPv4 インターフェースを 6to4 用に構成することにより、デバイスは 6to4 ルーターとして使用できます。

6to4 ホストからのパケットがデバイスを通過すると、6to4 ルーターは、パケットを IPv4 パケット内にカプセル化し、IPv4 ネットワーク空間へ送信します。6to4 ルーターは、そのカプセル化されたパケットを受信し、脱カプセル化して、6to4 デバイスへ転送することもできます。

図 28 は、6to4 ホストが、IPv4 WAN 上でサービス要求を他の 6to4 ホストへ送信している様子を示します。デバイス A の 6to4 ルーターは、送信パケットをカプセル化し、デバイス B の 6to4 ルーターがそのパケットを脱カプセル化します。

図 28: 6to4 ルーター

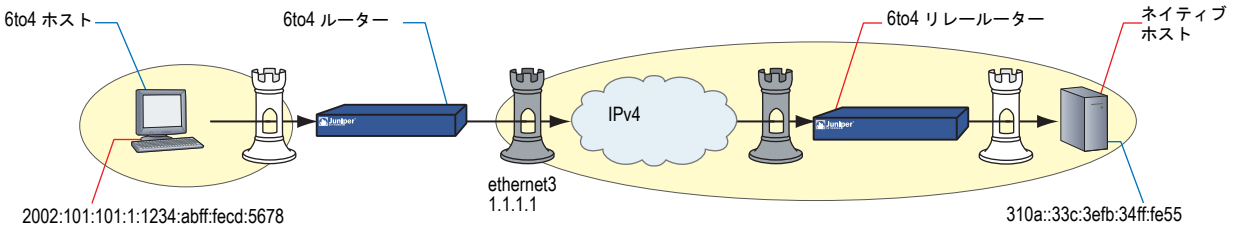


6to4 リレールーター

*6to4 リレールーター*は、IPv4 WAN 上の 6to4 ホストとネイティブ（非 6to4）ホストの間でのパケット交換をサポートするよう構成されたルーターです。6to4 ルーターと同様、6to4 トンネリングを処理するため IPv4 インターフェースを構成することにより、6to4 ルーターとして機能できるようになります。6to4 リレールーターは、受信カプセル化 6to4 パケットを受信すると、パケットを脱カプセル化して、ネイティブの宛先ホストへ転送します。ネイティブホストが送信パケットを送信すると、6to4 リレールーターは、そのパケットを IPv4 パケット内にカプセル化し、IPv4 ネットワーク空間へ送信します。

図 29 は、6to4 ホストが、IPv4 WAN 上でサービス要求をネイティブ（非 6to4）ホストへ送信している様子を示します。デバイス B は、ネイティブ IPv6 アドレスを宛先アドレスとして使用して、受信パケットを脱カプセル化します。

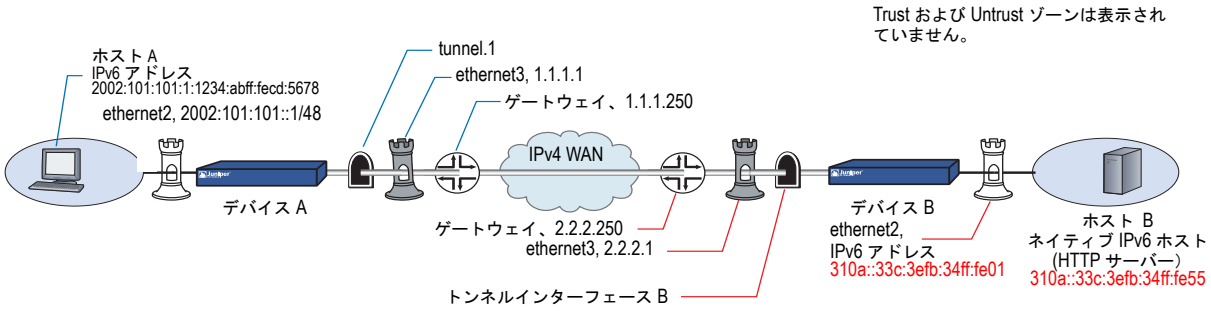
図 29: ネイティブアドレスを持つ 6to4 ルーター



リモートネイティブホストへのトンネル

6to4 ホストがリモート ネイティブホストへサービス要求を送信すると、デバイスは、ルーティングテーブルエントリからリモート終端ポイント（ゲートウェイ IP アドレス）を取得します。図 30 は、デバイス A が、デバイス B によって保護されているネイティブサーバーへ HTTP サービス要求を送信している様子を示します。

図 30: 6over6 手動トンネリング



デバイス A の 6to4 ルーターは、リモートゲートウェイ IPv4 アドレス（2.2.2.1）を構成済みルーティングテーブルエントリ 2002:0202:201:2:9876:abff:fecd:5432 から取得します。（この例では、リモートゲートウェイインターフェースの MAC アドレスは 9876abcd5432 です。）

デバイスは、IPv4 WAN 上の 6to4 ホストとネイティブホストとの間を通過するパケットを次のようにアドレス指定します。

1. IPv6 ホスト（ホスト A）は、IPv6 パケットを生成し、デバイス A へ送信します。
2. デバイス A は、6to4 ルーターであり、送信 IPv6 パケットを IPv4 パケット内にカプセル化し、IPv4 WAN 上をトンネルインターフェースからデバイス B へ送信します。
3. デバイス B は、パケットを脱カプセル化して、ホスト B へ転送します。
4. ホスト B はリレーパケットを生成します。デバイス B はそのパケットをカプセル化して、デバイス A へ転送します。
5. デバイス A は、トンネルインターフェースを通じてカプセル化されたリレーパケットを受信します。デバイス A は、パケットを脱カプセル化して、ホスト A へ転送します。

この例では、IPv6 ホストからネイティブホスト（HTTP サーバー）へ IPv4 WAN インフラストラクチャ上で HTTP 要求を送信するようにデバイスを構成しています。

WebUI（デバイス A）

インターフェース

Network > Interfaces > Edit (for ethernet2)

Network > Interfaces > Edit (for ethernet2) > IPv6

Network > Interfaces > Edit (for ethernet3)

トンネルインターフェース

Network > Interfaces > New (Tunnel IF)

Network > Interfaces > Edit (for tunnel.1) > IPv6

Network > Interfaces > Edit (for tunnel.1) > Encapsulation

ルーター

Network > Routing > Routing Table > New (trust-vr)

アドレス帳入力

Policy > Policy Elements > Addresses > List (Trust) > New

ポリシー

Policies > (From: Untrust, To: Trust) > New

WebUI（デバイス B）

インターフェース

Network > Interfaces > Edit (for ethernet2)

Network > Interfaces > Edit (for ethernet2) > IPv6

Network > Interfaces > Edit (for ethernet3)

トンネルインターフェース

Network > Interfaces > New (Tunnel IF)

Network > Interfaces > Edit (for tunnel.1) > IPv6

Network > Interfaces > Edit (for tunnel.1) > Encapsulation

ルーター

Network > Routing > Routing Table > New (trust-vr)

Network > Routing > Routing Table > trust-vr New: 次のように入力してから **OK** をクリックします。

Network > Routing > Routing Table > trust-vr Edit > Gateway: (選択)

アドレス帳入力

Policy > Policy Elements > Addresses > List (Trust) > New

Policy > Policy Elements > Addresses > List (Untrust) > New

ポリシー

Policies > (From: Untrust, To: Trust) > New: 次のように入力してから **OK** をクリックします。

Policies > (From: Untrust, To: Trust) > Edit > Advanced:

CLI（デバイス A）

1. **インターフェース**
   set interface ethernet2 zone trust
   set interface ethernet2 ip 10.1.1.1/24
   set interface ethernet2 ipv6 mode host
   set interface ethernet2 ipv6 enable
   set interface ethernet2 ipv6 ip 2002:101:101::1/48
   set interface ethernet2 ipv6 ra link-mtu
   set interface ethernet2 ipv6 ra link-address
   set interface ethernet2 ipv6 ra transmit
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **トンネル インターフェース**
   set interface tunnel.1 zone untrust
   set interface tunnel.1 ip unnumbered interface ethernet3
   set interface tunnel.1 ipv6 mode router
   set interface tunnel.1 ipv6 enable
   set interface tunnel.1 tunnel encap ip6in4 6to4
   set interface tunnel.1 tunnel local-if ethernet3

3. **ルーター**
   set vrouter trust-vr route 0.0.0.0/0 gateway 1.1.1.250
   set vrouter trust-vr route 3abc::/16 interface tunnel.1 gateway 2002:0202:201::1

4. **アドレス帳入力**
   set address trust L_Hosts 2002:101:101::/48
   set address untrust R_Server 3abc::100/128

5. **ポリシー**
   set policy from trust to untrust L_Hosts R_Server http permit

CLI（デバイス B）

1. **インターフェース**
   set interface ethernet2 zone trust
   set interface ethernet2 ip 10.2.2.1/24
   set interface ethernet2 ipv6 mode host
   set interface ethernet2 ipv6 enable
   set interface ethernet2 ipv6 ip 310a::33c:3efb:34ff:fe01/64
   set interface ethernet2 ipv6 ra link-mtu
   set interface ethernet2 ipv6 ra link-address
   set interface ethernet2 ipv6 ra transmit
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 2.2.2.1/24

2. **トンネル インターフェース**
   set interface tunnel.1 zone untrust
   set interface tunnel.1 ip unnumbered interface ethernet3
   set interface tunnel.1 ipv6 mode router
   set interface tunnel.1 ipv6 enable

```
set interface tunnel.1 tunnel encap ip6in4 6to4
set interface tunnel.1 tunnel local-if ethernet3
```

3. **ルーター**
```
set vrouter trust-vr route 0.0.0.0/0 gateway 2.2.2.250
set vrouter trust-vr route 2002::/16 interface tunnel.1
```

4. **アドレス帳入力**
```
set address trust L_Server 310a::33c:3efb:34ff:fe55/128
set address untrust R_Clients 2002:101:101::/48
```

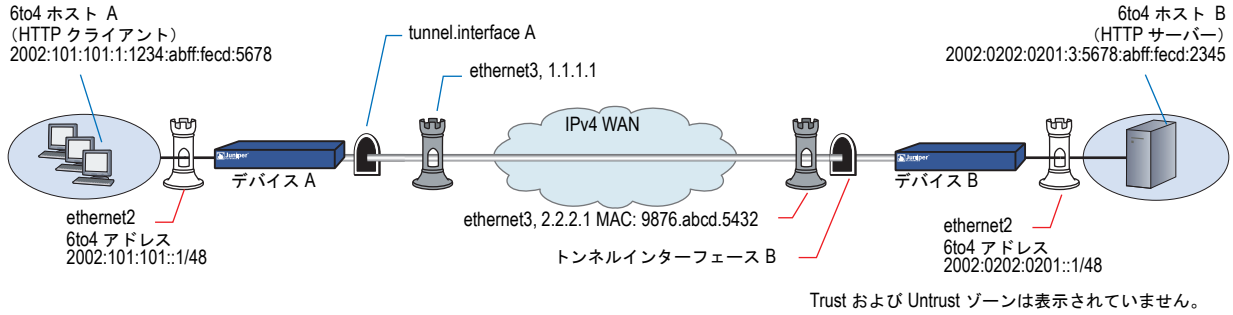
5. **ポリシー**
```
set policy from untrust to trust R_Clients L_Server http permit
```

リモート 6to4 ホストへのトンネル

6to4 ホストがリモート 6to4 ホストへサービス要求を送信すると、デバイスは、送信要求パケットの宛先 IP アドレスからリモート終端ポイント（ゲートウェイ IPv4 アドレス）を取得します。

図 31 は、ホスト A が、デバイス B によって保護されているサーバーへ HTTP サービス要求を送信している様子を示します。

図 31: 6to4 トンネル



この例では、送信パケットの 6to4 宛先アドレスは 2002:0202:0201:3:5678:abff:fecd:2345 です。これは、6to4 ホスト B のアドレスです。（デバイス A 上の）6to4 ルーターは、この宛先アドレスからリモートゲートウェイ IPv4 アドレス（2.2.2.1）を取得します。

デバイスは、IPv4 WAN 上の 6to4 ホストと他の 6to4 ホストとの間を通過するパケットを次のようにアドレス指定します。

1. IPv6 ホスト A は、IPv6 パケットを生成し、デバイス A へ送信します。
2. デバイス A は、リモートゲートウェイの IPv4 宛先アドレス（2.2.2.1）を送信パケットの宛先アドレスから取得します。
3. デバイス A は、送信 6to4 パケットを IPv4 パケット内にカプセル化し、トンネルインターフェースからゾーン B へ送信します。
4. デバイス B は、パケットを脱カプセル化して、ホスト B へ転送します。
5. ホスト B はリレーパケットを生成します。
6. デバイス B はそのパケットをカプセル化して、デバイス A へ転送します。

この例では、IPv6 ホストから IPv6 サーバーへ IPv4 WAN インフラストラクチャ上で HTTP 要求を送信するようにデバイスを構成しています。

WebUI（デバイス A）

インターフェース

Network > Interfaces > Edit (for ethernet2)

Network > Interfaces > Edit (for ethernet2) > IPv6

Network > Interfaces > Edit (for ethernet3)

トンネルインターフェース

Network > Interfaces > New (Tunnel IF)

Network > Interfaces > Edit (for tunnel.1) > IPv6

Network > Interfaces > Edit (for tunnel.1) > Encapsulation

ルーター

Network > Routing > Routing Table > New (trust-vr)

Network > Routing > Routing Table > New (untrust-vr)

アドレス帳入力

Policy > Policy Elements > Addresses > List (Trust) > New

ポリシー

Policies > (From: Untrust, To: Trust) > New

WebUI（デバイス B）

インターフェース

Network > Interfaces > Edit (for ethernet2)

Network > Interfaces > Edit (for ethernet2) > IPv6

Network > Interfaces > Edit (for ethernet3)

トンネルインターフェース

Network > Interfaces > New (Tunnel IF)

Network > Interfaces > Edit (for tunnel.1) > IPv6

Network > Interfaces > Edit (for tunnel.1) > Encapsulation

ルーター

Network > Routing > Routing Table > untrust-vr New

アドレス帳入力

Policy > Policy Elements > Addresses > List (Trust) > New

Policy > Policy Elements > Addresses > List (Untrust) > New

ポリシー

Policies > (From: Untrust, To: Trust) > New

CLI（デバイス A）

1. インターフェース

```
set interface ethernet2 zone trust
set interface ethernet2 ip 10.1.1.1/24
set interface ethernet2 ipv6 mode router
set interface ethernet2 ipv6 enable
set interface ethernet2 ipv6 ip 2002:101:101::1/48
set interface ethernet2 ipv6 ra link-mtu
set interface ethernet2 ipv6 ra link-address
set interface ethernet2 ipv6 ra transmit
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. トンネル インターフェース

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
set interface tunnel.1 ipv6 mode router
set interface tunnel.1 ipv6 enable
set interface tunnel.1 tunnel encap ip6in4 6to4
set interface tunnel.1 tunnel local-if ethernet3
```

3. ルーター

```
set vrouter trust-vr route 2002:0202:0201::/48 interface tunnel.1
```

4. アドレス帳入力

```
set address trust L_Hosts 2002:101:101::/48
set address untrust R_Server 2002:202:201:0:5678:abff:fecd:2345/128
```

5. ポリシー

```
set policy from trust to untrust L_Hosts R_Server any permit
```

CLI（デバイス B）

1. インターフェース

```
set interface ethernet2 zone trust
set interface ethernet2 ip 10.2.2.1/24
set interface ethernet2 ipv6 mode host
set interface ethernet2 ipv6 enable
set interface ethernet2 ipv6 ip 2002:202:0201::1/48
set interface ethernet2 ipv6 ra link-mtu
set interface ethernet2 ipv6 ra link-address
set interface ethernet2 ipv6 ra transmit
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.1/24
```

2. トンネル インターフェース

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
set interface tunnel.1 ipv6 mode router
set interface tunnel.1 ipv6 enable
set interface tunnel.1 tunnel encap ip6in4 6to4
set interface tunnel.1 tunnel local-if ethernet3
```

3. ルーター

```
set vrouter trust-vr route 2002::/16 interface tunnel.1
```

4. アドレス帳入力

```
set address untrust R_Clients 2002:101:101::/48
set address trust L_Server 2002:202:0201:3:5678:abff:fecd:2345/128
```

5. ポリシー

```
set policy from untrust to trust R_Clients L_Server http permit
```

第 7 章

IPSec トンネリング

6in6、4in6、および 6in4 トンネリングでは、仮想プライベートネットワークを作成できます。これらのメカニズムは、パケットのカプセル化を自動的に行い、WAN 上での安全なパケット交換を確実にします。

本章のセクションは、以下のようになります。

- 107 ページの「概要」
- 108 ページの「IPSec 6in6 トンネリング」
- 111 ページの「IPSec 4in6 トンネリング」
- 115 ページの「IPSec 6in4 トンネリング」
- 119 ページの「フラグメント化を有効にした手動トンネリング」
  - 120 ページの「IPv6 to IPv6 ルートベースの VPN トンネル」
  - 122 ページの「IPv4 to IPv6 ルートベースの VPN トンネル」

概要

ScreenOS では、仮想プライベートネットワーク（VPN）を作成できます。VPN 接続は、2 つの LAN（ローカルエリアネットワーク）、あるいはリモートダイヤルアップユーザーと LAN を接続できます。この 2 つのポイントを流れるトラフィックは、ルーター、スイッチ、および他のネットワーク設備などの共有リソースを通過します。これらの設備によって公開 WAN が構成されます。VPN 通信を安全に行うために、2 つの参加者は IPSec（IP セキュリティ）トンネルを作成します。

認証や暗号化などの IPSec セキュリティサービスを提供するため、ポリシーを作成するか、またはプライベートアドレス空間を定義するために NAT（ネットワークアドレス変換）を使用します。NAT の詳細については、*第 8 部: アドレス変換* を参照してください。セキュリティの概念および VPN に関する詳細は、*第 2 部: 基本*および*第 5 部: 仮想プライベート ネットワーク*を参照してください。

本章には、VPN トンネルを純粋な IPv6 環境で使用している構成例や IPv4 または IPv6 アイランドネットワークまたはホストのための他のシナリオが含まれています。

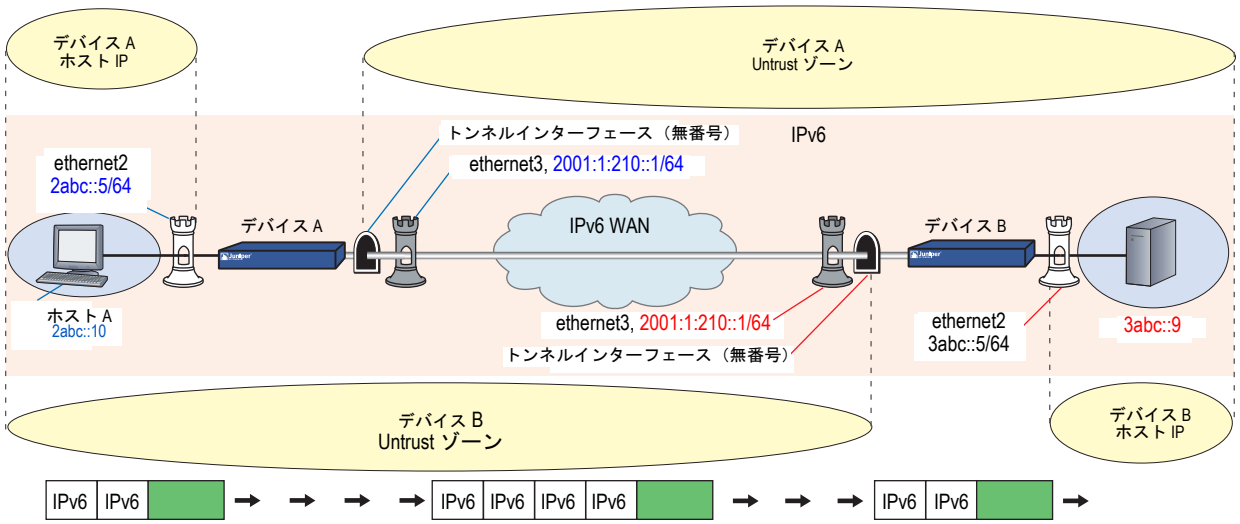
IPSec 6in6 トンネリング

6in6 トンネリングは、IPv6 パケットを IPv6 パケット内部でカプセル化する方法です。これは、交換される情報が、IPv6 ドメイン内を移動しなければならない場合に使用され、データの機密性および保全性を確保する保護が必要です。

IPv6 インフラストラクチャ上で IPv6 ホストと他の IPv6 ホストとの間でのセキュアな通信を確立する必要があるときに、IPSec を 6in6 トンネリングと組み合わせて使用します。たとえば、IPv6 WAN 上の IPv6 ネットワークと IPv6 サーバーとの間で保護されたトラフィックを交換する必要がある場合が、これにあたります。

図 32 は、IPv6 WAN インフラストラクチャ上で、IPv6 ホストが IPv6 Web サーバーに HTTP サービス要求を送信している様子を示します。両方のデバイスが、IPSec セキュリティを使用するポリシーを持っています。

図 32: IPSec と 6in6 トンネルの例



次に、IPv4-to-IPv6 ホストマッピング用に構成されたデバイスが、発信サービス要求パケットのソースおよび宛先アドレスを変換する手順を示します。

1. ホスト A は、サービス要求パケットを生成し、そのパケットを IPv6 宛先アドレス（3abc::9）へ割り当てます。

2. デバイス A は、別の IPv6 パケットの内部に IPv6 パケット全体をカプセル化します。次に、トンネルインターフェースからデバイス B にパケットを送信します。

3. リモートの IPv6 ホストデバイスは応答パケットを送信します。

4. デバイス A は、応答パケットを脱カプセル化して、IPv6 ホストへ送信します。

次の例では、IPv6 ネットワークと リモートの IPv6 ネットワークまたはサブネットとの間の HTTP 通信を許可する、IPSec ポリシーをセットアップします。トラフィックは IPv6 WAN 環境を移動します。

WebUI（デバイス A）

1. インターフェース

Network > Interfaces > Edit (for ethernet2)

Network > Interfaces > Edit (for ethernet2) > IPv6

Network > Interfaces > Edit (for ethernet3)

Network > Interfaces > Edit (for ethernet3) > IPv6

2. トンネル

Network > Interfaces > New (Tunnel IF)

Network > Interfaces > Edit (for tunnel.1) > IPv6

3. IKE

VPNs > AutoKey Advanced > Gateway > New

VPNs > AutoKey Advanced > Gateway > Edit (for gw-test) > Advanced

4. VPN

VPNs > AutoKey IKE > New

VPNs > AutoKey IKE > Edit (for vpn-test) > Advanced

5. ルート

Network > Routing > Routing Entries > New

6. ポリシー

Policies > New (Trust to Untrust)

Policies > New (Untrust to Trust)

CLI（デバイス A）

1. インターフェース

```
set interface ethernet2 zone trust
set interface ethernet2 ipv6 mode router
set interface ethernet2 ipv6 enable
set interface ethernet2 ipv6 ip 2abc::5/64
set interface ethernet3 ipv6 mode host
set interface ethernet3 ipv6 enable
set interface ethernet3 ipv6 ip 2001:1:210::1/64
```

2. トンネル インターフェース

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ipv6 mode host
set interface tunnel.1 ipv6 enable
```

3. IKE

```
set ike gateway gw-test address 2001:1:210::2 main outgoing-interface ethernet3
    local-address 2001:1:210::1 preshare abcd1234 proposal pre-g2-des-md5
```

4. VPN

```
set vpn vpn-test gateway gw-test proposal g2-esp-des-md5
set vpn vpn-test bind interface tunnel.1
set vpn vpn-test proxy-id local-ip ::/0 remote-ip ::/0 any
```

5. ルート

```
set route 3abc::/16 interface tunnel.1
```

6. **ポリシー**
   set policy from trust to untrust any-ipv6 any-ipv6 any permit
   set policy from untrust to trust any-ipv6 any-ipv6 any permit

WebUI（デバイス B）

1. **インターフェース**
   Network > Interfaces > Edit (for ethernet2)

   Network > Interfaces > Edit (for ethernet2) > IPv6

   Network > Interfaces > Edit (for ethernet3)

   Network > Interfaces > Edit (for ethernet3) > IPv6

2. **トンネル インターフェース**
   Network > Interfaces > New (Tunnel IF)

   Network > Interfaces > Edit (for tunnel.1) > IPv6

3. **IKE**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > AutoKey Advanced > Gateway > Edit (for gw-test) > Advanced

4. **VPN**
   VPNs > AutoKey IKE > New

   VPNs > AutoKey IKE > Edit (for vpn-test) > Advanced

5. **ルート**
   Network > Routing > Routing Entries > New

6. **ポリシー**
   Policies > New (Trust to Untrust)

   Policies > New (Untrust to Trust)

CLI（デバイス B）

1. **インターフェース**
   set interface ethernet2 zone trust
   set interface ethernet2 ipv6 mode router
   set interface ethernet2 ipv6 enable
   set interface ethernet2 ipv6 ip 3abc::5/64
   set interface ethernet3 ipv6 mode host
   set interface ethernet3 ipv6 enable
   set interface ethernet3 ipv6 ip 2001:1:210::1/64

2. **トンネル インターフェース**
   set interface tunnel.1 zone untrust
   set interface tunnel.1 ipv6 mode host
   set interface tunnel.1 ipv6 enable

3. **IKE**
   set ike gateway gw-test address 2001:1:210::1 main outgoing-interface ethernet3
   local-address 2001:1:210::2 preshare abcd1234 proposal pre-g2-des-md5

4. **VPN**
   set vpn vpn-test gateway gw-test proposal g2-esp-des-md5
   set vpn vpn-test bind interface tunnel.1
   set vpn vpn-test proxy-id local-ip ::/0 remote-ip ::/0 ANY

5. **ルート**
   set route 2abc::/16 interface tunnel.1

6. **ポリシー**
   set policy from trust to untrust any-ipv6 any-ipv6 any permit
   set policy from untrust to trust any-ipv6 any-ipv6 any permit

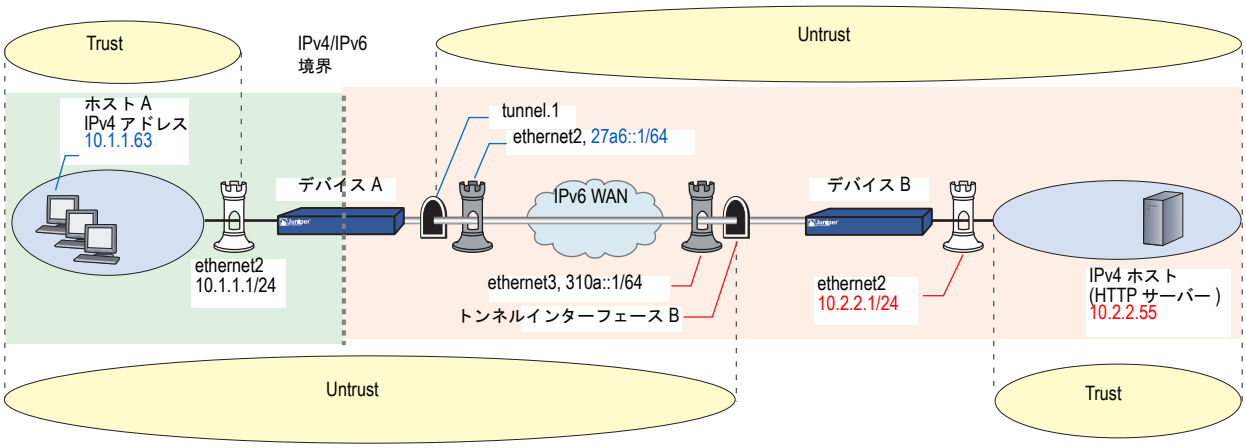
IPSec 4in6 トンネリング

4in6 トンネリングでは、IPv6 バックボーン上の IPv4 ネットワーク間の通信を設定できます。この移行メカニズムは、IPSec を使用して、IPv6 バックボーン上の IPv4 ネットワーク間で交換されるパケットをカプセル化します。カプセル化により、交換されるパケットは IPv6 ネットワーク空間を横断したルーティングが可能になります。

パケットのカプセル化の他に、IPSec は、認証および暗号化を行うことができます。

図 33 は、リモートの IPv4 ネットワーク間の IPSec トンネルを示します。この例では、各ゲートウェイデバイス上のトンネルインターフェースを定義し、トンネルを IPv6 ネットワーク空間の境界となるゾーンにバインドします。

図 33: IPSec 4in6 トンネルの例



デバイスは、次の方法で、IPv4 アイランドネットワーク内の IPv4 ホストと IPv6 WAN バックボーン上の別の IPv4 ホストとの間を移動するパケットをアドレス指定します。

1. ホスト A は、IPv6 サービス要求パケットを生成し、ホスト B にそれを宛てます。そのパケットはゾーン A からゾーン B へ移動します。

2. デバイス A は IPv6 パケット内部で発信 IPv4 パケットをカプセル化し、トンネルインターフェースから送信します。

3. デバイス B は、パケットを脱カプセル化して、ホスト B へ転送します。

4. デバイス B は応答パケットを生成し、カプセル化して、デバイス A へ転送します。

5. デバイス A は、トンネルインターフェースを通じてカプセル化されたリレーパケットを受信します。デバイス A は、パケットを脱カプセル化して、ホスト A へ転送します。

4in6 トンネリングのセットアップ手順は次の通りです。

1. 保護された IPv4 ネットワークとの通信用にインターフェースを構成します。
   - インターフェースをゾーン（通常は Trust ゾーン）にバインドします。
   - インターフェースに IPv4 アドレスおよびサブネットマスクを割り当てます。
2. IPv6 WAN 上での通信用にインターフェースを構成します。
   - インターフェースをゾーン（通常は Untrust ゾーン）にバインドします。
   - インターフェースを IPv6 Host モードに構成します。
   - インターフェースに IPv6 アドレスおよびサブネットマスクを割り当てます。
   - ゾーンでトンネルインターフェース（無番号）を作成し、IPv6 インターフェースへバインドします。
   - トンネルインターフェースを IPv6 Host モードに構成します。
3. 同様にして、ピアデバイスのインターフェースをセットアップします。
4. ピアデバイス間の IPSec をセットアップします。IPSec の他の例は、*第 5 部: 仮想プライベート ネットワーク* を参照してください。
5. 各デバイスで、IPv6 ホスト、サブネット、またはネットワークを示すアドレス帳エントリを作成します。
6. ホストが互いにアクセスできるルーティングエントリをセットアップします。
7. セキュリティポリシーをセットアップします。

次の例では、IPv6 端点間で IPSec トンネルを作成します。デバイス A の背後の IPv4 デバイスは、デバイス B の背後のホストへサービス要求を送信します。デバイス A は、IPSec を使用して、IPv6 パケット内部にサービス要求パケットをカプセル化します。デバイス B は、そのパケットを受信して脱カプセル化します。

WebUI（デバイス A）

インターフェース

Network > Interfaces > Edit (for ethernet2)

Network > Interfaces > Edit (for ethernet3)

Network > Interfaces > Edit (for ethernet3) > IPv6

トンネル

Network > Interfaces > New (Tunnel IF)

Network > Interfaces > Edit (for tunnel.1) > IPv6

IKE

VPNs > AutoKey Advanced > Gateway > New

VPN

VPNs > AutoKey IKE > New

ルーター

Network > Routing > Routing Table > New (trust-vr)

Network > Routing > Routing Table > New (untrust-vr)

ポリシー

Policies > (From: Trust, To: Untrust) > New

CLI（デバイス A）

1. **インターフェース**

```
set interface ethernet2 zone trust
set interface ethernet2 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 ipv6 mode host
set interface ethernet3 ipv6 enable
set interface ethernet3 ipv6 ip 27a6::1/64
```

2. **トンネル**

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
set interface tunnel.1 ipv6 mode host
set interface tunnel.1 ipv6 enable
```

3. **IKE**

```
set ike gateway IPSec_Servers ip 310a::1 main outgoing-interface ethernet3
    local-address 27a6::1 proposal rsa-g2-aes128-sha
```

4. **VPN**

```
set vpn Tunnel_Servers gateway IPSec_Servers no-replay tunnel sec-level standard
set vpn Tunnel_Servers bind interface tunnel.1
```

5. **ルート**

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3
set vrouter trust-vr route 310a::0/64 interface tunnel.1 gateway 310a::1
```

6. **ポリシー**

```
set policy from trust to untrust any any any permit
```

WebUI（デバイス B）

インターフェース

Network > Interfaces > Edit (for ethernet2)

Network > Interfaces > Edit (for ethernet3)

Network > Interfaces > Edit (for ethernet3) > IPv6

トンネル

Network > Interfaces > New (Tunnel IF)

Network > Interfaces > Edit (for tunnel.1) > IPv6

IKE

VPNs > AutoKey Advanced > Gateway > New

VPN

VPNs > AutoKey IKE > New

ルーター

Network > Routing > Routing Table > New (trust-vr)

アドレス

Policy > Policy Elements > Addresses > List (Trust) > New

Policy > Policy Elements > Addresses > List (Untrust) > New

ポリシー

Policies > (From: Trust, To: Untrust) > New

CLI（デバイス B）

1. **インターフェース**

```
set interface ethernet2 zone trust
set interface ethernet2 ip 10.2.2.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.1/24
set interface ethernet3 ipv6 mode host
set interface ethernet3 ipv6 enable
set interface ethernet3 ipv6 ip 310a::1/96
```

2. **トンネル**

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
set interface tunnel.1 ipv6 mode host
set interface tunnel.1 ipv6 enable
```

3. **IKE**

```
set ike gateway IPSec_Clients ip 27a6::1 main outgoing-interface ethernet3
    local-address 310a::1 proposal rsa-g2-aes128-sha
```

4. **VPN**

```
set vpn Tunnel_Clients id 1 gateway IPSec_Clients no-replay tunnel sec-level
    standard
set vpn Tunnel_Clients id 2 bind interface tunnel.1
```

5. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
   set vrouter untrust-vr route 27a6::0/64 interface tunnel.1 gateway 27a6::1

6. **アドレス**
   set address trust L_Server 10.2.2.55/32
   set address untrust R_Clients 10.1.1.1/24

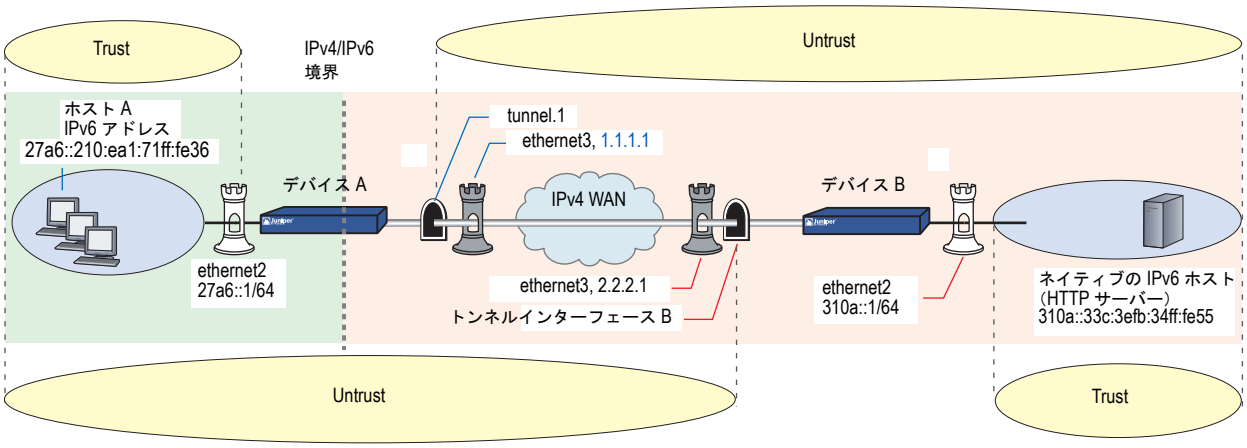
7. **ポリシー**
   set policy from untrust to trust R_Clients L_Server any permit

IPSec 6in4 トンネリング

セキュリティデバイスが、IPv4 WAN の上のリモートの IPv6 アイランドネットワーク間でパケットを送信するとき、認証と暗号化をサポートする IPSec トンネリングを使用してパケットをカプセル化できます。

図 34 は、リモートの IPv6 アイランドネットワーク間の IPSec トンネルを示します。この例では、最初に各ゲートウェイデバイス上のトンネルインターフェースを定義し、次にトンネルを IPv6 ネットワーク空間の境界となるゾーンにバインドします。

図 34: トンネルインターフェースおよびゾーンの例



デバイスは、次の方法で、IPv6 アイランドネットワーク内のホストと IPv4 WAN バックボーン上の別の IPv6 ホストとの間を移動するパケットをアドレス指定します。

1. ホスト A は、IPv6 サービス要求パケットを生成し、ホスト B にそれを宛てます。そのパケットはゾーン A からゾーン B へ移動します。

2. デバイス A は IPv4 パケット内部で発信 IPv6 パケットをカプセル化し、トンネルインターフェースからゾーン B へ送信します。

3. デバイス B は、パケットを脱カプセル化して、ホスト B へ転送します。

4. デバイス B は応答パケットを生成し、カプセル化して、デバイス A へ転送します。

5. デバイス A は、トンネルインターフェースを通じてカプセル化されたリレーパケットを受信します。デバイス A は、パケットを脱カプセル化して、ホスト A へ転送します。

ほとんどの場合、必要なセットアップ作業は次の通りです。

1. 保護されたアイランド IPv6 ネットワークとの通信用にインターフェースを構成します。
   - インターフェースをゾーン（通常は Trust ゾーン）にバインドします。
   - インターフェースを IPv6 Host モードに構成します。
   - インターフェースにグローバルユニキャストプレフィックスを割り当てます。(グローバルユニキャストアドレスについては 3 ページの「アドレスのタイプ」を参照)。
2. IPv4 WAN 上での通信用にインターフェースを構成します。
   - インターフェースをゾーン（通常は Untrust ゾーン）にバインドします。
   - インターフェースに IPv4 アドレスおよびサブネットマスクを割り当てます。
   - ゾーンでトンネルインターフェース（無番号）を作成し、IPv4 インターフェースへバインドします。
3. 手順 1 と 2 に従って、ピアデバイスのインターフェースをセットアップします。
4. ピアデバイス間の IPSec をセットアップします。IPSec に関する詳細は、*第 5 部: 仮想プライベートネットワーク* を参照してください。
5. 各デバイスで、IPv6 ホスト、サブネット、またはネットワークを示すアドレス帳エントリを作成します。
6. ホストが互いにアクセスできるルーティングエントリをセットアップします。
7. セキュリティポリシーをセットアップします。

次の例では、IPv4 端点間で IPSec トンネルを作成します。デバイス A の背後の IPv6 デバイスは、デバイス B の背後のホストへサービス要求を送信します。デバイス A は、IPSec を使用して、IPv4 パケット内部にサービス要求パケットをカプセル化します。デバイス B は、そのパケットを受信して脱カプセル化します。Figure 34 on page 115 を参照してください。

デバイスは、AutoKey IKE トンネルネゴシエーションのフェーズ 1 を次のように行います。

- RSA 認証
- Diffie-Hellman グループ 2
- AES128 暗号化アルゴリズム
- SHA ハッシングアルゴリズム

デバイスは、標準のプロポーザルを使用して、トンネルネゴシエーションのフェーズ 2 を実行します。

- Diffie-Hellman グループ 2
- ESP（セキュリティペイロードのカプセル化）トンネリング
- 3DES 暗号化アルゴリズム
- SHA ハッシングアルゴリズム

WebUI（デバイス A）

インターフェース

Network > Interfaces > Edit (for ethernet2)

Network > Interfaces > Edit (for ethernet2) > IPv6

Network > Interfaces > Edit (for ethernet3)

トンネル

Network > Interfaces > New (Tunnel IF)

IKE

VPNs > AutoKey Advanced > Gateway > New

VPN

VPNs > AutoKey IKE > New

ルーター

Network > Routing > Routing Table > New (trust-vr)

アドレス

Policy > Policy Elements > Addresses > List (Trust) > New

Policy > Policy Elements > Addresses > List (Untrust) > New

ポリシー

Policies > (From: Trust, To: Untrust) > New

CLI（デバイス A）

1. **インターフェース**

```
set interface ethernet2 zone trust
set interface ethernet2 ip 10.1.1.1/24
set interface ethernet2 ipv6 mode host
set interface ethernet2 ipv6 enable
set interface ethernet2 ipv6 ip 27a6::1/64
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. **トンネル**

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
set interface tunnel.1 ipv6 mode host
set interface tunnel.1 ipv6 enable
```

3. **IKE**
   set ike gateway IPSec_Servers ip 2.2.2.1 main outgoing-interface ethernet3
   proposal rsa-g2-aes128-sha

4. **VPN**
   set vpn Tunnel_Servers gateway IPSec_Servers no-replay tunnel sec-level standard
   set vpn Tunnel_Servers bind interface tunnel.1

5. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3
   set vrouter trust-vr route::/0 interface tunnel.1

6. **アドレス**
   set address trust L_Clients 27a6::210:ea1:71ff:fe36/64
   set address untrust R_Servers 32f1::250:af:34ff:fe34/64

7. **ポリシー**
   set policy from trust to untrust L_Clients R_Servers any permit

WebUI（デバイス B）

インターフェース

Network > Interfaces > Edit (for ethernet2)

Network > Interfaces > Edit (for ethernet2) > IPv6

Network > Interfaces > Edit (for ethernet3)

トンネル

Network > Interfaces > New (Tunnel IF)

IKE

VPNs > AutoKey Advanced > Gateway > New

VPN

VPNs > AutoKey IKE > New

ルーター

Network > Routing > Routing Table > New (trust-vr)

Network > Routing > Routing Table > New (untrust-vr)

アドレス

Policy > Policy Elements > Addresses > List (Trust) > New

Policy > Policy Elements > Addresses > List (Untrust) > New

ポリシー

Policies > (From: Untrust, To: Trust) > New

CLI（デバイス B）

1. **インターフェース**
   set interface ethernet2 zone trust
   set interface ethernet2 ip 10.2.2.1/24
   set interface ethernet2 ipv6 mode host
   set interface ethernet2 ipv6 enable
   set interface ethernet2 ipv6 ip 310a::1/64
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 2.2.2.1/24

2. **トンネル**
   set interface tunnel.1 zone untrust
   set interface tunnel.1 ip unnumbered interface ethernet3
   set interface tunnel.1 ipv6 mode host
   set interface tunnel.1 ipv6 enable

3. **IKE**
   set ike gateway IPSec_Clients ip 1.1.1.1 main outgoing-interface ethernet3
   proposal rsa-g2-aes128-sha

4. **VPN**
   set vpn Tunnel_Clients id 1 gateway IPSec_Clients no-replay tunnel sec-level
   standard
   set vpn Tunnel_Clients id 2 bind interface tunnel.1

5. **ルート**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3
   set vrouter trust-vr route::/0 interface tunnel.1

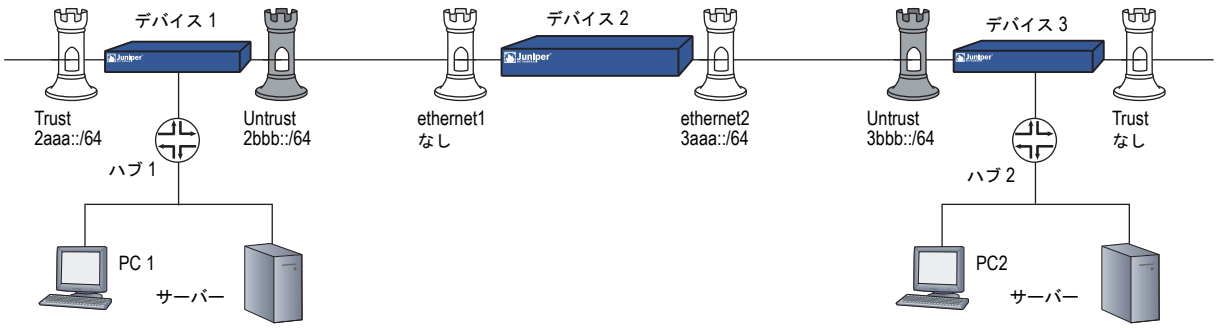
6. **アドレス**
   set address trust L_Server 310a::33c:3efb:34ff:fe55/128
   set address untrust R_Clients 27a6::210:ea1:71ff:fe36/64

7. **ポリシー**
   set policy from untrust to trust R_Clients L_Server any tunnel vpn Tunnel_Clients

フラグメント化を有効にした手動トンネリング

図 35 は、次のトンネリング例で使用されるネットワークの構成を示します。

図 35: 手動トンネリング例



IPv6 to IPv6 ルートベースの VPN トンネル

次の例では、3DES 暗号化を使用するルートベースの VPN により、IPv6 トンネルを介して IPv6 パケットを送信します。また、フラグメント化を有効にします。

CLI（デバイス 1）

1. **汎用**
   ```
   set console time 0
   unset zone untrust block
   ```

2. **インターフェース**
   ```
   set interface ethernet1/1 zone trust
   set interface ethernet1/1 ipv6 mode router
   set interface ethernet1/1 ipv6 ip 2aaa::/64
   set interface ethernet1/1 ipv6 enable
   set interface ethernet1/1 ipv6 interface-id 0000000000000001
   set interface ethernet1/1 ipv6 ra transmit
   set interface ethernet1/1 route
   set interface ethernet1/1 manage

   set interface ethernet1/2 zone untrust
   set interface ethernet1/2 ipv6 mode host
   set interface ethernet1/2 ipv6 ip 2bbb::/64
   set interface ethernet1/2 ipv6 enable
   set interface ethernet1/2 ipv6 interface-id 0000000000000002
   set interface ethernet1/2 route
   set interface ethernet1/2 manage
   ```

3. **IKE**
   ```
   set ike gateway ton6 address 3aaa::5 outgoing-interface ethernet1/2
       local-address 2bbb::2 preshare abc sec-level standard
   set vpn vpn4 gateway ton6 sec-level standard
   ```

4. **トンネル**
   ```
   set interface tunnel.6 zone untrust
   set interface tunnel.6 ipv6 mode host
   set interface tunnel.6 ipv6 enable
   set interface tunnel.6 ip unnumbered interface ethernet1/2
   set vpn vpn4 bind interface tunnel.6
   ```

5. **ポリシー**
   ```
   set policy from trust to untrust any-ipv6 any-ipv6 any permit
   set policy from untrust to trust any-ipv6 any-ipv6 any permit
   ```

6. **ルート**
   ```
   set vrouter trust-vr route::/0 interface ethernet1/2 gateway 2bbb::3
   set vrouter trust-vr route 3bbb::/64 interface tunnel.6
   ```

CLI（デバイス 2）

1. **汎用**
   set console time 0
   unset zone untrust block

2. **インターフェース**
   set interface untrust zone untrust
   set interface untrust ipv6 mode host
   set interface untrust ipv6 enable
   set interface untrust ipv6 ip 2bbb::/64
   set interface untrust ipv6 interface-id 0000000000000003
   set interface untrust manage
   set interface untrust route

   set interface trust zone trust
   set interface trust ipv6 mode host
   set interface ethernet2 ipv6 ip 3abc::1/64
   set interface trust ipv6 enable
   set interface trust ipv6 interface-id 0000000000000004
   set interface trust route
   set interface trust manage

3. **ルート**
   set vrouter trust-vr route 3bbb::/64 interface trust gateway 3aaa::5
   set vrouter trust-vr route 2aaa::/64 interface untrust gateway 2bbb::2

4. **ポリシー**
   set policy from trust to untrust any-ipv6 any-ipv6 any permit
   set policy from untrust to trust any-ipv6 any-ipv6 any permit

CLI（デバイス 3）

1. **汎用**
   set console time 0
   unset zone untrust block

2. **インターフェース**
   set interface untrust zone untrust
   set interface untrust ipv6 mode host
   set interface untrust ipv6 ip 3aaa::/64
   set interface untrust ipv6 interface-id 0000000000000005
   set interface untrust ipv6 enable
   set interface untrust route
   set interface untrust manage

   set interface trust zone trust
   set interface trust ipv6 mode router
   set interface trust ipv6 ip 3bbb::/64
   set interface trust ipv6 interface-id 0000000000000006
   set interface trust ipv6 enable
   set interface trust ipv6 ra transmit
   set interface trust route
   set interface trust manage

3. **トンネル**
   set interface tunnel.6 zone untrust
   set interface tunnel.6 ipv6 mode host
   set interface tunnel.6 ipv6 enable
   set interface tunnel.6 ip unnumbered interface untrust

4. **IKE**
   set ike gateway ton4 address 2bbb::2 outgoing-interface untrust local-address 3aaa::5 preshare abc sec-level standard

5. **VPN**
   set vpn vpn6 gateway ton4 sec-level standard
   set vpn vpn6 bind interface tunnel.6

6. **ポリシー**
   set policy from trust to untrust any-ipv6 any-ipv6 any permit
   set policy from untrust to trust any-ipv6 any-ipv6 any permit

7. **ルート**
   set vrouter trust-vr route::/0 interface untrust gateway 3aaa::4
   set vrouter trust-vr route 2aaa::/64 interface tunnel.6

IPv4 to IPv6 ルートベースの VPN トンネル

次の例にでは、3DES 暗号化を使用するルートベースの VPN により、IPv4 トンネルを通って IPv4 パケットを送信します。また、フラグメント化を有効にします。

CLI（デバイス 1）

1. **汎用**
   set console time 0
   unset zone untrust block

2. **インターフェース**
   set interface ethernet1/1 zone trust
   set interface ethernet1/1 ipv6 mode router
   set interface ethernet1/1 ipv6 ip 2aaa::/64
   set interface ethernet1/1 ipv6 enable
   set interface ethernet1/1 ipv6 interface-id 0000000000000001
   set interface ethernet1/1 ipv6 ra transmit
   set interface ethernet1/1 route
   set interface ethernet1/1 manage

   set interface ethernet1/2 zone untrust
   set interface ethernet1/2 ipv6 mode router
   set interface ethernet1/2 ipv6 ip 2bbb::/64
   set interface ethernet1/2 ipv6 enable
   set interface ethernet1/2 ipv6 interface-id 0000000000000002
   set interface ethernet1/2 ipv6 ra transmit
   set interface ethernet1/2 route
   set interface ethernet1/2 manage

3. **IKE**
   set ike gateway ton6 address 3aaa::5 outgoing-interface ethernet1/2 local-address 2bbb::2 preshare abc sec-level standard
   set vpn vpn4 gateway ton6 sec-level standard

4. **トンネル**
   set interface tunnel.6 zone untrust
   set interface tunnel.6 ipv6 mode router
   set interface tunnel.6 ipv6 enable
   set interface tunnel.6 ip unnumbered interface ethernet1/2
   set interface tunnel.6 ipv6 ra transmit

5. **VPN**
   set vpn vpn4 bind interface tunnel.6

6. **ポリシー**
   set policy from trust to untrust any-ipv6 any-ipv6 any permit
   set policy from untrust to trust any-ipv6 any-ipv6 any permit

7. **ルート**
   set vrouter trust-vr route::/0 interface ethernet1/2 gateway 2bbb::3
   set vrouter trust-vr route 3bbb::/64 interface tunnel.6
   set interface ethernet1/1 ip 1.1.1.1/24
   set route 4.1.1.0/24 interface tunnel.6

8. **ポリシー**
   set policy from trust to untrust any any any permit
   set policy from untrust to trust any any any permit

CLI（デバイス 2）

1. **汎用**
   set console time 0
   unset zone untrust block

2. **インターフェース**
   set interface untrust zone untrust
   set interface untrust ipv6 mode host
   set interface untrust ipv6 enable
   set interface untrust ipv6 interface-id 0000000000000003
   set interface untrust ipv6 ra accept
   set interface untrust manage
   set interface untrust route

   set interface trust zone trust
   set interface trust ipv6 mode router
   set interface ethernet2 ipv6 ip 3abc::1/64
   set interface trust ipv6 enable
   set interface trust ipv6 interface-id 0000000000000004
   set interface trust ipv6 ra transmit
   set interface trust route
   set interface trust manage

3. **ルート**
   set vrouter trust-vr route 3bbb::/64 interface trust gateway 3aaa::5
   set vrouter trust-vr route 2aaa::/64 interface untrust gateway 2bbb::2

4. **ポリシー**
   set policy from trust to untrust any-ipv6 any-ipv6 any permit
   set policy from untrust to trust any-ipv6 any-ipv6 any permit

CLI（デバイス 3）

1. 汎用

```
set console time 0
unset zone untrust block
```

2. インターフェース

```
set interface untrust zone untrust
set interface untrust ipv6 mode host
set interface untrust ipv6 interface-id 0000000000000005
set interface untrust ipv6 enable
set interface untrust ipv6 ra accept
set interface untrust route
set interface untrust manage

set interface trust zone trust
set interface trust ipv6 mode router
set interface trust ipv6 ip 3bbb::/64
set interface trust ipv6 interface-id 0000000000000006
set interface trust ipv6 enable
set interface trust ipv6 ra transmit
set interface trust route
set interface trust manage
```

3. トンネル

```
set interface tunnel.6 zone untrust
set interface tunnel.6 ipv6 mode host
set interface tunnel.6 ipv6 enable
set interface tunnel.6 ip unnumbered interface untrust
set interface tunnel.6 ipv6 ra accept
```

4. IKE

```
set ike gateway ton4 address 2bbb::2 outgoing-interface untrust local-address
    3aaa::5 preshare abc sec-level standard
set vpn vpn6 gateway ton4 sec-level standard
set vpn vpn6 bind interface tunnel.6
```

5. ポリシー

```
set policy from trust to untrust any-ipv6 any-ipv6 any permit
set policy from untrust to trust any-ipv6 any-ipv6 any permit

set policy from trust to untrust any any any permit
set policy from untrust to trust any any any permit
```

6. ルート

```
set vrouter trust-vr route::/0 interface untrust gateway 3aaa::4
set vrouter trust-vr route 2aaa::/64 interface tunnel.6
set interface trust ip 4.1.1.1/24
set route 1.1.1.0/24 interface tunnel.6
```

第 8 章

IPv6 XAuth ユーザー認証

本章では IPv6 ユーザー認証とデッドピア検出（DPD）について説明し、設定例を示します。

本章のセクションは、以下のようになります。

- 126 ページの「概要」
  - 126 ページの「RADIUSv6」
  - 128 ページの「IPSec アクセスセッション管理」
  - 131 ページの「デッドピア検出」
- 132 ページの「設定例」
  - 132 ページの「XAuth と RADIUS」
  - 133 ページの「RADIUS と XAuth ルートベース VPN」
  - 136 ページの「RADIUS と XAuth、およびドメイン名ストリッピング」
  - 140 ページの「IP プール範囲の割り当て」
  - 146 ページの「RADIUS リトライ」
  - 146 ページの「Calling-Station-Id」
  - 147 ページの「IPSec アクセスセッション」
  - 155 ページの「デッドピア検出」

概要

ScreenOS XAuth for IPv6 は、フェーズ 1 IKE ネゴシエーション後の、個々のユーザーおよびユーザーグループの認証を可能にします。

XAuth を使用すると、VPN ゲートウェイやデバイスだけを認証するのではなく、リモート仮想プライベートネットワーク（VPN）ユーザー（またはユーザーグループ）を個別に認証することができ、また IP アドレスや、ネットマスク、DNS サーバーおよび WINS サーバー割り当て等の TCP/IP 設定情報を割り当てることができます。

RADIUSv6

ScreenOS は、RADIUS の次世代バージョンである RADIUSv6 をサポートしています。デバイスが XAuth サーバーの役割を果たす場合、デバイスは IPv4、IPv6 または両方について有効化されている RADIUS サーバーにユーザー名とパスワードを送信します。

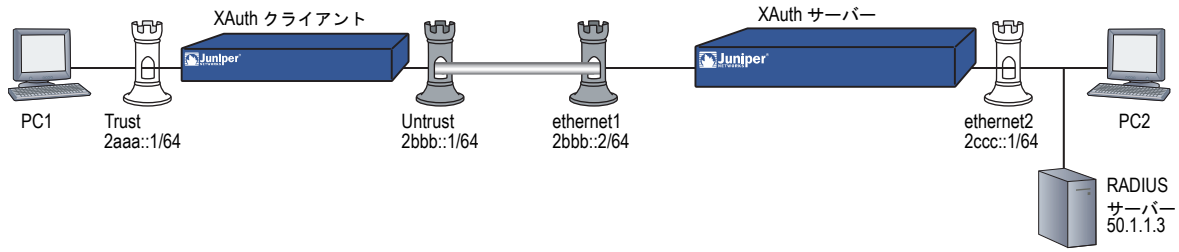
注： RADIUS および IPv6 の詳細については、RFC 3162 および RFC 2882 を参照してください。

以下のセクションでさまざまシナリオについて説明します。構成例は、以下のシナリオに基づいています。

単一クライアント、単一サーバー

図 36 は、単一クライアントデバイスと、XAuth 認証を実行する RADIUS サーバーと情報をやりとりする単一サーバーを示しています。

図 36: RADIUS と単一クライアント、単一サーバーの組み合わせ

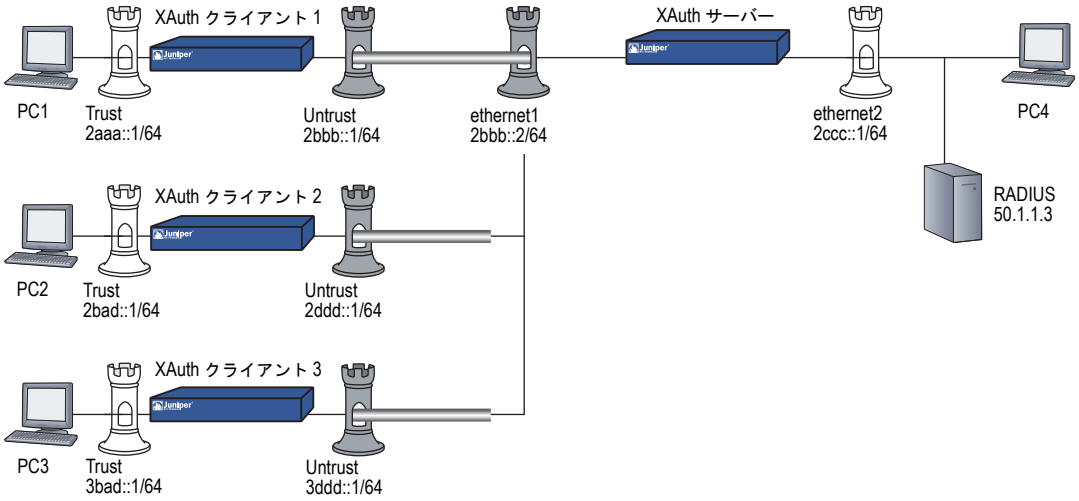


RADIUS サーバーは XAuth サーバーの Trust ゾーン内に置かれています。保護されるサブネットは各々、1 つ以上の保護されたホストを含むことができます。この図では 1 つだけが示されています。

複数クライアント、単一サーバー

図 37 は、複数のクライアントデバイスと、XAuth 認証を実行する RADIUS サーバーと情報をやりとりする単一サーバーを示しています。

図 37: RADIUS と複数クライアント、単一サーバーの組み合わせ

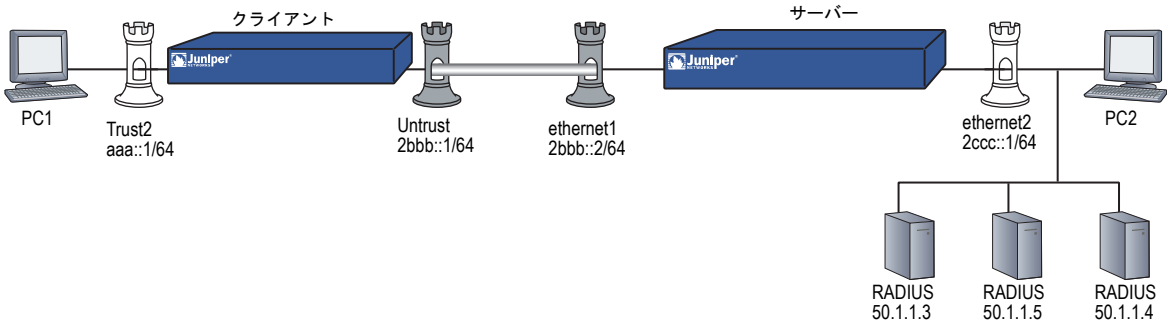


RADIUS サーバーはサーバーの Trust ゾーン内に置かれています。各クライアントデバイスはそれぞれ別個のサブネットを保護しています。保護されるサブネットは各々、1 つ以上の保護されたホストを含むことができます。この図では 1 つだけが示されています。

単一クライアント、複数サーバー

図 38 は、単一クライアントデバイスと、複数 RADIUS サーバーと情報をやりとりする単一サーバーを示しています。

図 38: RADIUS と単一クライアント、複数サーバーの組み合わせ

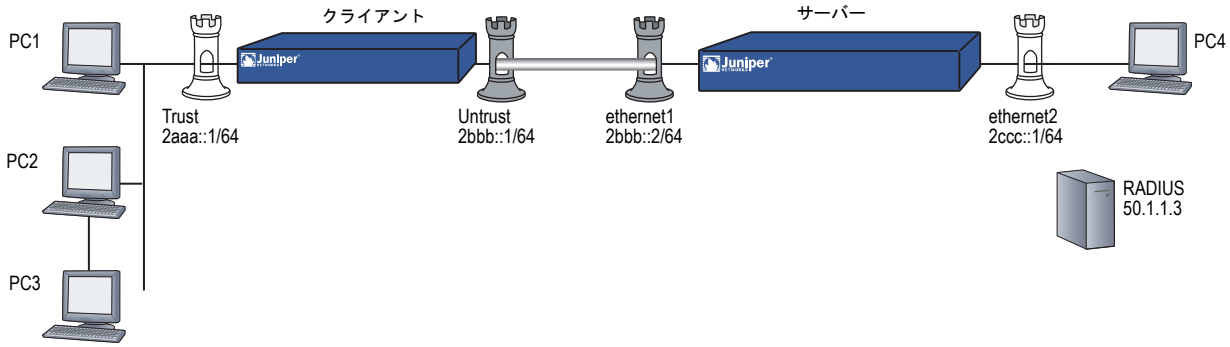


RADIUS サーバーはデバイス 2 の Trust ゾーン内に置かれています。保護されるサブネットは各々、1 つ以上の保護されたホストを含むことができます。この図では 1 つだけが示されています。

複数ホスト、単一サーバー

図 39 は、複数ホストを保護する単一クライアントデバイス（デバイス 1）と、RADIUS サーバーと情報をやりとりする単一サーバー（デバイス 2）を示しています。

図 39: RADIUS と複数ホスト、単一サーバーの組み合わせ



RADIUS サーバーはセキュリティサーバーの Trust ゾーン内に置かれています。

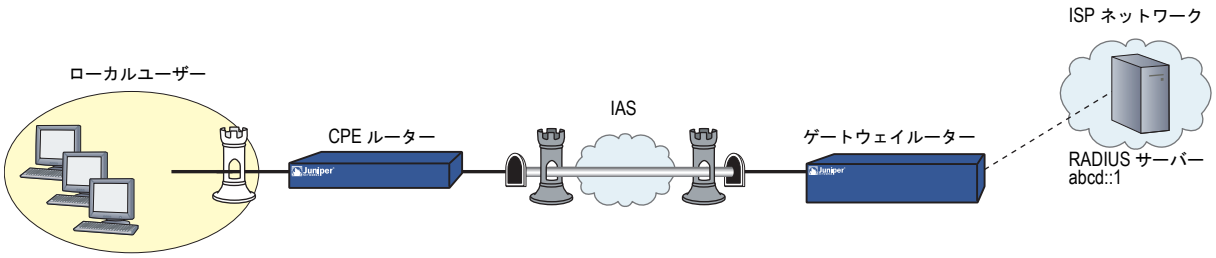
IPSec アクセスセッション管理

ユーザーネットワークが外部ネットワークにアクセスできるようにするには、複数のセキュリティデバイスを使用し、1 つ以上のローカル顧客構内装置（CPE）ルーターと、1 つ以上のゲートウェイルーターを設置します。アクセスネットワーク上で送信されるパケットを保護するため、CPE とゲートウェイデバイスで IPSec トンネルを確立することができます。ゲートウェイは、RADIUS サーバーと共に、ネットワークアクセスセッションを管理し、アカウンティングを記録します。

IPSec アクセスセッション

ネットワークアクセスセッションが存在している時間間隔を IPSec アクセスセッション（IAS）と呼びます。IAS 時間間隔は、最初のエンドユーザーがアクセスネットワークに接続した時点で開始し、最後のユーザーがネットワークから切断した時点で終了します。図 40 は、ISP がどのようにセキュリティデバイスを CPE やゲートウェイルーターとして使用するかを示しています。

図 40: RADIUS サーバーでの IPSec アクセスセッション



IAS を開始するため、CPE デバイスは 1 回のフェーズ 1 インターネットキーエクスチェンジ（IKE) と、少なくとも 1 回のフェーズ 2 IKE を実行します。

注： ScreenOS のセキュリティコンセプトおよび IKE の詳細については、5-1 ページの「インターネットプロトコルセキュリティ」を参照してください。

各 IAS には、以下の特性があります。

- CEP デバイスは、各 IP アドレスについて 1 つの IAS フェーズ 1 セキュリティアソシエーション（SA) しか持てません。例えば、CPE デバイスに 3 つの IPv6 アドレスがある場合、デバイスは 3 つのフェーズ 1 SA をホストすることができます。しかしながら、各フェーズ 1 SA には複数のフェーズ 2 SA がある可能性があります。

- IAS の寿命中、CPE とゲートウェイデバイスは IKE フェーズ 1 およびフェーズ 2 リキー等の複数の IPSec 作業を行うことができます。

- IAS の寿命中、CPE はフェーズ 1 セッションが終了した場合はいつでも、フェーズ 1 SA リキーを開始します。

- IAS の寿命中、CPE は SA を常にオンの状態に維持するため、フェーズ 2 セッションが*終了する前に*、新しいフェーズ 2 SA を開始しなければなりません。

各 IAS は、それが存在している間は以下のコンポーネントを含んでおりこれらを使用します。

情報フィールド	説明
CPE IPv6 Address	CPE デバイスのアドレス。アドレスは一意的であり、同じ CPE IP アドレスを持つ IAS が 2 つ以上存在することはありません。
IKE Phase I ID	IAS のフェーズ 1 ゲートウェイを識別する ID。この ID には、以下のいずれかを含むことができます。 ■ ゲートウェイデバイスを識別する文字数字の列 ■ ゲートウェイデバイスの ASN1 ドメイン名 ■ ゲートウェイデバイスの完全修飾ドメイン名（FQDN） ■ ゲートウェイデバイスの IP アドレス（IPv4 または IPv6） ■ ゲートウェイデバイスのユーザー完全修飾ドメイン名（u_FQDN）
XAuth User Name	XAuth ユーザーの名前。
IKE Phase 1 Cookie Pair	IKE フェーズ 1 SA クッキー。IAS に関連するフェーズ 1 SA を示しています。
Number of Phase 2 SAs	IAS に現在存在するフェーズ 2 SA の数。IAS が存在するためには、1 つ以上のフェーズ 2 SA がなければなりません。
Assigned IP address	IKE モード設定フェーズ中に、ゲートウェイから CPE に割り当てられた IP4 アドレス。
Phase 2 SA SPIs	セキュリティパラメーターインデックス (SPI)。新旧両方の SPI を含む。
IAS Start Time	IAS が開始する時間。

CPE ゲートウェイデバイスが IAS の開始に成功すると、その IAS に関する RADIUS アカウンティングを開始します。フェーズ 2 SA が終了した場合、または失敗した場合、CPE デバイスはゲートウェイデバイスとの間のセキュアなコミュニケーションを継続するため、別の SA を確立しなければなりません。RADIUS サーバーがどのようにフェーズ 2 リキーを扱うかは、現在 IAS 機能が有効化されているか無効化されているかにより異なります。

IAS 機能が無効になっている場合、CPE が新しい SA を確立した後に、RADIUS アカウンティングセッションが開始します。フェーズ 2 セッションが失敗またはタイムアウトしたときは必ず新しいアカウンティングセッションが必要です。また、RADIUS サーバーは複数の請求機能（また、場合により他のアカウントに関連する機能）を生成しなければなりません。

しかし、IAS 機能が有効になっている場合は、各フェーズ 2 SA リキーが行われた後に元の RADIUS アカウンティングセッションが再開されます。これにより、RADIUS サーバーは、単一の連続的なアカウンティングセッションを継続することができるので、請求機能や他のアカウント関連機能を単純化することができます。

IAS 機能を使用可能にまたは使用不可能にする

CPE ゲートウェイの IAS 機能を使用可能にするには、以下のコマンドを入力します。

set ipsec-access-session enable

CPE ゲートウェイの IAS 機能を使用不可能にするには、以下のコマンドを入力します。

unset ipsec-access-session enable

IAS セッションの解除

IPSec アクセスセッションは、**clear ike all** で解除することができます。

IAS 制限設定

以下の設定により、同時にアクティブな IAS の数を制限できます。

- *maximum* で、デバイスが許可する同時 IAS の最大数を指定します。デフォルトでは 5000 セッションに設定されており、可能な設定範囲は 0 セッションから 5000 セッションまでです。

  この制限数を設定するには、以下のコマンドを入力します。

  set ipsec access-session maximum *maximum_number*

- *lower IAS threshold* で、SNMP トラップをトリガーする前に、デバイスが許可する同時 IAS の最小数を指定します。デフォルトでは 1000 セッションに設定されており、可能な設定範囲は 1 セッションから 5000 セッションまでです。この値は、最大値よりも小さい値でなければなりません。

  この制限数を設定するには、以下のコマンドを入力します。

  set ipsec access-session lower-threshold *minimum_number*

- *upper IAS threshold* で、SNMP トラップをトリガーする前に、デバイスが許可する同時 IAS の最大値を指定します。デフォルトでは 1000 セッションに設定されており、可能な設定範囲は 1 セッションから 5000 セッションまでです。この値は、最小値よりも小さい値でなければなりません。

  この制限数を設定するには、以下のコマンドを入力します。

  set ipsec access-session upper-threshold *maximum_number*

デッドピア検出

デッドピア検出（DPD）は、指定された時間間隔内にピアからの IPSec トラフィックが受信されなかった場合に、他の IPSec ピアデバイスの存在および活動状態を確認するプロトコルです。

デバイスは、暗号化された IKE フェーズ 1 通知ペイロード（R-U-THERE）をピアに送信し、ピアからの DPD 確認応答（R-U-THERE-ACK）を待つことで DPD 検証を行います。デバイスは、指定した DPD 間隔以内にピアからトラフィックを受信しなかった場合に限り、R-U-THERE 要求を送信します。DPD 機能を有効にしているデバイスがトンネル上のトラフィックを受信した場合、デバイスはそのトンネルに対する R-U-THERE カウンタをリセットし、これによって新しい間隔が開始されます。デバイスは、この間隔以内にピアから R-U-THERE-ACK を受信した場合は、ピアがアライブであると見なします。デバイスは、この間隔以内に R-U-THERE-ACK 応答を受信しなかった場合は、ピアがデッドであると判断します。

デバイスはデッドピアのフェーズ 1 SA とすべてのフェーズ 2 SA を削除します。

CLI または WebUI のどちらかから、以下の DPD パラメータを構成することができます。

- interval パラメータは、DPD 間隔を指定します。この間隔は、ピアがデッドであるとデバイスが見なすまでの許容経過時間です（秒単位）。ゼロに設定すると、DPD は無効になります。
- always-send パラメータは、ピアとの IPSec トラフィックの有無に関わらず、DPD 要求を送信するようデバイスに指示します。
- retry パラメータは、ピアがデッドであるとデバイスが見なすまでの間に、R-U-THERE 要求を送信できる最大回数を指定します。IKE ハートビート設定と同様に、デフォルトの送信回数は 5 回で、指定可能な範囲は 128 ～ 128 回です。

注 : DPD と IKE ハートビートはどちらか一方を使用可能にすることができますが、両方を同時に使用可能にすることはできません。IKE ハートビートを有効化した後に、DPD 設定をしようとすると、セキュリティデバイスは以下のようなエラーメッセージを生成します。

IKE: DPD cannot co-exist with IKE heartbeat.

DPD を有効にした後に IKE ハートビートを設定しようとした場合も、同様のエラーが生成されます。

設定例

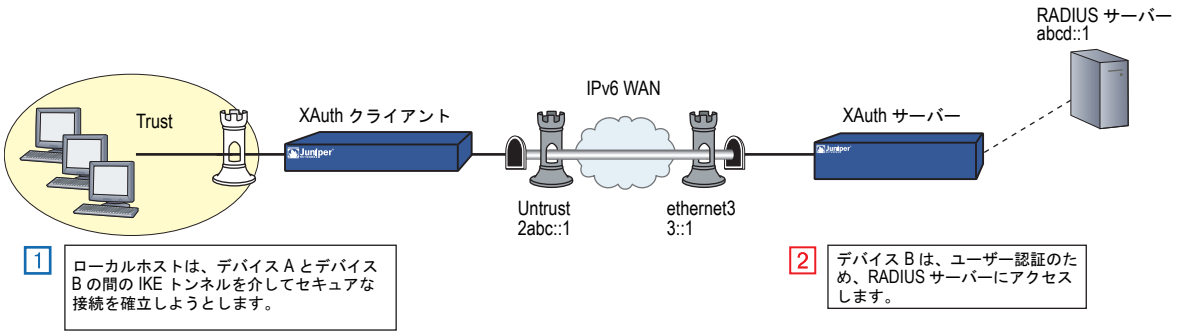
このセクションには RADIUS、IAS、および DPD に関する例が含まれています。

注： 各例の WebUI セクションに示されているのは、デバイス設定ページまでのナビゲーションパスだけです。具体的な値については、それに続く CLI セクションを参照してください。

XAuth と RADIUS

図 41 は、ローカルネットワーク内のユーザーに対して XAuth 認証を実行するデバイス A、および RADIUS サーバーを使用して、IKE トンネルを介する認証に応答して XAuth を実行するデバイス B を示しています。

図 41: XAuth 例



WebUI（XAuth クライアント）

VPNs > AutoKey IKE > New

VPNs > AutoKey IKE > Edit

VPNs > AutoKey IKE > Advanced

CLI （XAuth クライアント）

```
set ike gateway client_gw6 address 3::1 main outgoing-interface untrust
    local-address 2abc::1 preshare 1234 proposal pre-g2-des-md5
set ike gateway client_gw6 cert peer-cert-type x509-sig
set ike gateway client_gw6 xauth client any username chris password swordfish
```

WebUI（XAuth サーバー）

1. **RADIUS**

   Configuration > Auth > Auth Servers > Edit

2. **IKE**

   VPNs > AutoKey IKE > New

   VPNs > AutoKey IKE > Edit

   VPNs > AutoKey IKE > Advanced

CLI（XAuth サーバー）

1. RADIUS

```
set auth-server xauth-rad id 1
set auth-server xauth-rad server-name 1.1.1.1
set auth-server xauth-rad account-type xauth
set auth-server xauth-rad radius secret "juniper"
set xauth default auth server xauth-rad query-config
```

2. IKE

```
set ike gateway server_gw6 address 2abc::1 aggressive outgoing-interface
    ethernet3 local-address 3::1 preshare 1234 proposal pre-g2-des-md5
set ike gateway server_gw6 cert peer-cert-type x509-sig
set ike gateway server_gw6 xauth server xauth-rad query-config
```

RADIUS と XAuth ルートベース VPN

この例では、XAuth クライアントは、XAuth と RADIUS を使用し、prefix delegation と mode config により、ルートベース VPN 上で、認証と承認を実行します。これは、RADIUS サーバーから取得した IP アドレスを（クライアントが別のインターフェースを指定しないかぎり）XAuth クライアント上のトンネルインターフェースに委譲します。

注 : この例の VPN はルートベースです。ポリシーベースの VPN の場合、または「/32」以外のフレーム化ネットマスクがある場合、デバイスはトンネルインターフェースに IP アドレスをインストールします。

---

126 ページの図 36、「RADIUS と単一クライアント、単一サーバーの組み合わせ」を参照してください。

この例の設定手順は次のとおりです。

1. （VPN の）IPv6 CPE オペレーションを実行するには、XAuth クライアントを設定します。
2. サーバー設定を実行するには、（VPN の）XAuth IPv6 ゲートウェイを設定します。
3. IP アドレス 50.1.1.3 で XAuth サーバー（RAD1）を使用可能にします。RADIUS に共有秘密と、ポート番号 1812 を割り当てます。
4. XAuth クライアントから、ユーザーの有効なユーザー名（PC1）および有効なパスワード（PC1）を指定します。

WebUI（XAuth クライアント）

1. インターフェース

Network > Interfaces > Edit (for Trust)

Network > Interfaces > Edit (for Trust) > IPv6

Network > Interfaces > Edit (for untrust)

Network > Interfaces > Edit (for untrust) > IPv6

2. **トンネル**
   Network > Interfaces > New (Tunnel IF)

   Network > Interfaces > Edit (for tunnel.6) > IPv6

3. **ルート**
   Network > Routing > Routing Table > New (trust-vr)

4. **IKE**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > AutoKey Advanced > Gateway > Edit

5. **VPN**
   VPNs > AutoKey IKE > New

   VPNs > AutoKey IKE > Edit

6. **ポリシー**
   Policies > (From: Untrust, To: Trust) > New

   Policies > (From: Trust, To: Untrust) > New

CLI（XAuth クライアント）

1. **インターフェース**

```
set interface trust ipv6 mode router
set interface trust manage
set interface trust ipv6 enable
set interface trust ipv6 interface-id 1111111111111111
set interface trust ipv6 ip 2aaa::1/64
set interface trust ipv6 ra transmit
set interface trust route

set interface untrust ipv6 mode router
set interface untrust manage
set interface untrust ipv6 enable
set interface untrust ipv6 interface-id 1222222222222222
set interface untrust ipv6 ip 2bbb::1/64
set interface untrust route
```

2. **トンネル**

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ipv6 mode router
set interface tunnel.1 ipv6 enable
set interface tunnel.1 ipv6 unnumbered
```

3. **ルート**

```
set vrouter trust route ::/0 interface untrust gateway 2bbb::2
set vrouter trust route 2ccc::0/64 interface tunnel.1
```

4. **IKE**

```
set ike gateway NS1_NS2 add 2bbb::2 outgoing-interface untrust local-address
    2bbb::1 preshare abc123 sec-level standard
set ike gateway NS1_NS2 xauth client any username PC1 password PC1
```

5. **VPN**
   set vpn NS1toNS2 gateway NS1_NS2 sec-level standard
   set vpn NS1toNS2 bind interface tunnel.1

6. **ポリシー**
   set policy from untrust to trust any-ipv6 any-ipv6 any permit
   set policy from trust to untrust any-ipv6 any-ipv6 any permit

WebUI（XAuth サーバー）

1. **インターフェース**
   Network > Interfaces > Edit (for Trust):

   Network > Interfaces > Edit (for Trust) > IPv6

   Network > Interfaces > Edit (for untrust)

   Network > Interfaces > Edit (for untrust) > IPv6

2. **トンネル**
   Network > Interfaces > New (Tunnel IF)

   Network > Interfaces > Edit (for tunnel.6) > IPv6

3. **ルート**
   Network > Routing > Routing Table > New (trust-vr)

4. **RADIUS**
   Configuration > Auth > Auth Servers > New

   Configuration > Auth > Auth Servers > Edit

5. **IKE**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > AutoKey Advanced > Gateway > Edit

6. **VPN**
   VPNs > AutoKey IKE > New

   VPNs > AutoKey IKE > Edit

7. **ポリシー**
   Policies > (From: Untrust, To: Trust) > New

   Policies > (From: Trust, To: Untrust) > New

CLI（XAuth サーバー）

1. **インターフェース**
   set interface ethernet1 zone untrust
   set interface ethernet1 ipv6 mode router
   set interface ethernet1 manage
   set interface ethernet1 ipv6 enable
   set interface ethernet1 ipv6 interface-id 2111111111111111

```
set interface ethernet1 ipv6 ip 2bbb::2/64
set interface ethernet1 route

set interface ethernet2 zone trust
set interface ethernet2 ipv6 mode router
set interface ethernet2 manage
set interface ethernet2 ipv6 enable
set interface ethernet2 ipv6 interface-id 2222222222222222
set interface ethernet2 ipv6 ip 2ccc::1/64
set interface ethernet2 ip 50.1.1.1/24
set interface ethernet2 route
set interface ethernet2 ipv6 ra transmit
```

2. **トンネル**

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ipv6 mode router
set interface tunnel.1 ipv6 enable
```

3. **ルート**

```
set vrouter trust route ::/0 interface ethernet1 gateway 2bbb::1
set vrouter trust route 2aaa::0/64 interface tunnel.1
```

4. **RADIUS**

```
set auth-server RAD1 id 1
set auth-server RAD1 server-name 50.1.1.3
set auth-server RAD1 account-type xauth
set auth-server RAD1 radius secret juniper
set auth-server RAD1 radius port 1812
```

5. **IKE**

```
set ike gateway NS2_NS1 add 2bbb::1 outgoing-interface ethernet1 local-address
    2bbb::2 preshare abc123 sec-level standard
set ike gateway NS2_NS1 xauth server RAD1 query-config user PC1
```

6. **VPN**

```
set vpn NS2toNS1 gateway NS2_NS1 sec-level standard
set vpn NS2toNS1 bind interface tunnel.1
```

7. **ポリシー**

```
set policy from untrust to trust any-ipv6 any-ipv6 any permit
set policy from trust to untrust any-ipv6 any-ipv6 any permit
```

RADIUS と XAuth、およびドメイン名ストリッピング

以下の例では、ドメイン名をチェックする（一番右端の文字から、セパレータ文字の後ろの最も左の文字まで）ドメイン名チェック機能を使用しますこの機能を使うことにより、デバイスは、特定のドメインからのユーザーのみを許可することができます。

126 ページの図 36、「RADIUS と単一クライアント、単一サーバーの組み合わせ」を参照してください。

この例の設定手順は次のとおりです。

1. （VPN の）IPv6 CPE 設定を有効にし、XAuth クライアント上の XAuth を設定します。

2. XAuth サーバー上の（VPN の）IPv6 ゲートウェイ設定を使用可能にします。

3. IP アドレス 50.1.1.3 で、XAuth サーバーを RADIUS RAD1 として使用可能にします。RADIUS 共有秘密（juniper）とポート番号（1812）を割り当てます。

4. コマンドを入力して、以下を実行します。

   - XAuth クライアント上で、そのユーザーのユーザー名（PC1@juniper.net）とパスワード（PC1）を指定します。
   - XAuth サーバー上で、
     - XAuth クライアントから来るユーザー名を PC1@juniper.net に設定します。
     - ドメイン“juniper.net”からのユーザーのみを許可します。
     - ユーザー名のセパレータ文字（@）までの文字を、右側から左に向かって除去します。

WebUI（XAuth クライアント）

1. インターフェース

Network > Interfaces > Edit (for Trust):

Network > Interfaces > Edit (for Trust) > IPv6

Network > Interfaces > Edit (for untrust)

Network > Interfaces > Edit (for untrust) > IPv6

2. トンネル

Network > Interfaces > New (Tunnel IF)

Network > Interfaces > Edit (for tunnel.6) > IPv6

3. ルート

Network > Routing > Routing Table > New (trust-vr)

4. IKE

VPNs > AutoKey Advanced > Gateway > New

VPNs > AutoKey Advanced > Gateway > Edit

5. VPN

VPNs > AutoKey IKE > New

VPNs > AutoKey IKE > Edit

6. ポリシー

Policies > (From: Untrust, To: Trust) > New

Policies > (From: Trust, To: Untrust) > New

CLI（XAuth クライアント）

1. インターフェース

```
set interface trust ipv6 mode router
set interface trust manage
set interface trust ipv6 enable
set interface trust ipv6 interface-id 1111111111111111
set interface trust ipv6 ip 2aaa::1/64
set interface trust ipv6 ra transmit
set interface trust route

set interface untrust ipv6 mode router
set interface untrust manage
set interface untrust ipv6 enable
set interface untrust ipv6 interface-id 1222222222222222
set interface untrust ipv6 ip 2bbb::1/64
set interface untrust route
```

2. トンネル

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ipv6 mode router
set interface tunnel.1 ipv6 enable
```

3. IKE

```
set ike gateway NS1_NS2 add 2bbb::2 outgoing-interface untrust local-address
    2bbb::1 preshare abc123 sec-level standard
set ike gateway NS1_NS2 xauth client any username PC1@juniper.net password
    PC1
```

4. VPN

```
set vpn NS1toNS2 gateway NS1_NS2 sec-level standard
set vpn NS1toNS2 bind interface tunnel.1
```

5. ルーター

```
set vrouter trust route ::/0 interface untrust gateway 2bbb::2
set vrouter trust route 2ccc::0/64 interface tunnel.1
```

6. ポリシー

```
set policy from untrust to trust any-ipv6 any-ipv6 any permit
set policy from trust to untrust any-ipv6 any-ipv6 any permit
```

WebUI（XAuth サーバー）

1. インターフェース

Network > Interfaces > Edit (for Trust):

Network > Interfaces > Edit (for Trust) > IPv6

Network > Interfaces > Edit (for untrust)

Network > Interfaces > Edit (for untrust) > IPv6

2. トンネル

Network > Interfaces > New (Tunnel IF)

Network > Interfaces > Edit (for tunnel.6) > IPv6

3. **ルート**
   Network > Routing > Routing Table > New (for trust-vr)

4. **RADIUS**
   Configuration > Auth > Auth Servers > New

   Configuration > Auth > Auth Servers > Edit

5. **IKE**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > AutoKey Advanced > Gateway > Edit

6. **VPN**
   VPNs > AutoKey IKE > New

   VPNs > AutoKey IKE > Edit

7. **ポリシー**
   Policies > (From: Untrust, To: Trust) > New

   Policies > (From: Trust, To: Untrust) > New

CLI（XAuth サーバー）

1. **インターフェース**

```
set interface ethernet1 zone untrust
set interface ethernet1 ipv6 mode router
set interface ethernet1 manage
set interface ethernet1 ipv6 enable
set interface ethernet1 ipv6 interface-id 2111111111111111
set interface ethernet1 ipv6 ip 2bbb::2/64
set interface ethernet1 route

set interface ethernet2 zone trust
set interface ethernet2 ipv6 mode router
set interface ethernet2 manage
set interface ethernet2 ipv6 enable
set interface ethernet2 ipv6 interface-id 2222222222222222
set interface ethernet2 ipv6 ip 2ccc::1/64
set interface ethernet2 ip 50.1.1.1/24
set interface ethernet2 route
set interface ethernet2 ipv6 ra transmit
```

2. **トンネル**

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ipv6 mode router
set interface tunnel.1 ipv6 enable
```

3. **ルート**

```
set vrouter trust route ::/0 interface ethernet1 gateway 2bbb::1
set vrouter trust route 2aaa::0/64 interface tunnel.1
```

4. **RADIUS**

```
set auth-server RAD1 id 1
set auth-server RAD1 server-name 50.1.1.3
set auth-server RAD1 account-type xauth
```

```
set auth-server RAD1 radius secret juniper
set auth-server RAD1 radius port 1812
set auth-server RAD1 username domain juniper.net
set auth-server RAD1 username separator @ number 1
```

5. **IKE**

```
set ike gateway NS2_NS1 add 2bbb::1 outgoing-interface ethernet1 local-address
    2bbb::2 preshare abc123 sec-level standard
set ike gateway NS2_NS1 xauth server RAD1 query-config user PC1@juniper.net
```

6. **VPN**

```
set vpn NS2toNS1 gateway NS2_NS1 sec-level standard
set vpn NS2toNS1 bind interface tunnel.1
```

7. **ポリシー**

```
set policy from untrust to trust any-ipv6 any-ipv6 any permit
set policy from trust to untrust any-ipv6 any-ipv6 any permit
```

IP プール範囲の割り当て

RADIUS サーバーが 255.255.255.254 のフレーム化 IP アドレスを返した場合、デバイスはユーザーにローカル IP プールから IP アドレスを割り当てます。デフォルトの IP プール内に含まれる範囲内の IP アドレスがすべて使用尽くされた場合、デバイスは次の IP 範囲からの IP アドレスを使用します。

127 ページの図 37、「RADIUS と複数クライアント、単一サーバーの組み合わせ」を参照してください。

この例の設定手順は次のとおりです。

1. （VPN の）IPv6 CPE 設定と、クライアント 1、クライアント 2 およびクライアント 3 上の XAuth クライアント設定を有効にします。

2. XAuth サーバー上で、

   - （VPN の）IPv6 ゲートウェイ設定を有効にします。
   - クライアント 1、クライアント 2 およびクライアント 3 用のトンネルを設定します。
   - IP アドレス 50.1.1.3 で XAuth サーバー（RAD1）を使用可能にします。RADIUS 共有秘密（juniper）と、ポート番号（1812）を指定します。
   - 2 つの IP 範囲を持つローカル IP プール（P1）を定義します。
     - 80.1.1.1 ～ 80.1.1.2
     - 80.1.1.3 ～ 80.1.1.4.
   - デフォルトの XAuth IP プール（P1）を使用可能にします。
   - XAuth クライアント（デバイス 1、デバイス 2 およびデバイス 3）から、これらのユーザーの有効なユーザー名（PC4）および有効なパスワード（PC4）を指定します。

3. RADIUS サーバー上で、ユーザー PC4 についてサブネットマスク 255.255.255.254 のフレーム化 IP アドレスを挿入します。

WebUI(XAuth クライアント 1、XAuth クライアント 2、および XAuth クライアント 3)

注 : WebUI パスはどの XAuth クライアントも同じです。フィールドに入力する値はクライアントにより異なります。適切な値については CLI コマンドを参照してください。

1. **インターフェース**
   Network > Interfaces > Edit (for Trust)

   Network > Interfaces > Edit (for Trust) > IPv6

   Network > Interfaces > Edit (for untrust)

   Network > Interfaces > Edit (for untrust) > IPv6

2. **トンネル**
   Network > Interfaces > New (Tunnel IF)

   Network > Interfaces > Edit (for tunnel.6) > IPv6

3. **ルート**
   Network > Routing > Routing Table > New (trust-vr)

4. **IKE**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > AutoKey Advanced > Gateway > Edit

5. **VPN**
   VPNs > AutoKey IKE > New

   VPNs > AutoKey IKE > Edit

6. **ポリシー**
   Policies > (From: Untrust, To: Trust) > New

   Policies > (From: Trust, To: Untrust) > New

CLI（XAuth クライアント 1）

1. **インターフェース**

```
set interface trust ipv6 mode router
set interface trust manage
set interface trust ipv6 enable
set interface trust ipv6 interface-id 1111111111111111
set interface trust ipv6 ip 2aaa::1/64
set interface trust ipv6 ra transmit
set interface trust route

set interface untrust ipv6 mode router
set interface untrust manage
set interface untrust ipv6 enable
set interface untrust ipv6 interface-id 1222222222222222
set interface untrust ipv6 ip 2bbb::1/64
set interface untrust route
```

2. **トンネル**
   set interface tunnel.1 zone untrust
   set interface tunnel.1 ipv6 mode router
   set interface tunnel.1 ipv6 enable

3. **ルート**
   set vrouter trust route ::/0 interface untrust gateway 2bbb::2
   set vrouter trust route 2ccc::0/64 interface tunnel.1

4. **IKE**
   set ike gat NS1_NS2 add 2bbb::2 outgoing-interface untrust local-add 2bbb::1
   preshare abc123 sec-level standard
   set ike gateway NS1_NS2 xauth client any username PC4 password PC4

5. **VPN**
   set vpn NS1toNS2 gateway NS1_NS2 sec-level standard
   set vpn NS1toNS2 bind interface tunnel.1

6. **ポリシー**
   set policy id 1 from untrust to trust any-ipv6 any-ipv6 any permit
   set policy id 2 from trust to untrust any-ipv6 any-ipv6 any permit

CLI（XAuth クライアント 2）

1. **インターフェース**
   set interface trust ipv6 mode router
   set interface trust manage
   set interface trust ipv6 enable
   set interface trust ipv6 interface-id 3111111111111111
   set interface trust ipv6 ip 2bad::1/64
   set interface trust ipv6 ra transmit
   set interface trust route

   set interface untrust ipv6 mode router
   set interface untrust manage
   set interface untrust ipv6 enable
   set interface untrust ipv6 interface-id 3222222222222222
   set interface untrust ipv6 ip 2ddd::1/64
   set interface untrust route

2. **トンネル**
   set interface tunnel.2 zone untrust
   set interface tunnel.2 ipv6 mode router
   set interface tunnel.2 ipv6 enable

3. **ルート**
   set vrouter trust route ::/0 interface untrust gateway 2ddd::2
   set vrouter trust route 2ccc::0/64 interface tunnel.2

4. **IKE**
   set ike gateway NS3_NS2 add 2ddd::2 outgoing-interface untrust local-add 2ddd::1
   preshare abc123 sec-level standard
   set ike gateway NS3_NS2 xauth client any username PC4 password PC4

5. **VPN**
   set vpn NS3toNS2 gateway NS3_NS2 sec-level standard
   set vpn NS3toNS2 bind interface tunnel.2

6. ポリシー

set policy id 1 from untrust to trust any-ipv6 any-ipv6 any permit
set policy id 2 from trust to untrust any-ipv6 any-ipv6 any permit

CLI（XAuth クライアント 3）

1. インターフェース

set interface trust ipv6 mode router
set interface trust manage
set interface trust ipv6 enable
set interface trust ipv6 interface-id 4111111111111111
set interface trust ipv6 ip 3bad::1/64
set interface trust ipv6 ra transmit
set interface trust route

set interface untrust ipv6 mode router
set interface untrust manage
set interface untrust ipv6 enable
set interface untrust ipv6 interface-id 4222222222222222
set interface untrust ipv6 ip 3ddd::1/64
set interface untrust route

2. トンネル

set interface tunnel.3 zone untrust
set interface tunnel.3 ipv6 mode router
set interface tunnel.3 ipv6 enable

3. ルート

set vrouter trust route ::/0 interface untrust gateway 3ddd::2
set vrouter trust route 2ccc::0/64 interface tunnel.3

4. IKE

set ike gateway NS4_NS2 add 3ddd::2 outgoing-interface untrust local-add 3ddd::1
preshare abc123 sec-level standard
set ike gateway NS4_NS2 xauth client any username PC4 password PC4

5. VPN

set vpn NS4toNS2 gateway NS4_NS2 sec-level standard
set vpn NS4toNS2 bind interface tunnel.3

6. ポリシー

set policy id 1 from untrust to trust any-ipv6 any-ipv6 any permit
set policy id 2 from trust to untrust any-ipv6 any-ipv6 any permit

WebUI（XAuth サーバー）

1. インターフェース

Network > Interfaces > Edit (for Trust)

Network > Interfaces > Edit (for Trust) > IPv6

Network > Interfaces > Edit (for untrust)

Network > Interfaces > Edit (for untrust) > IPv6

2. トンネル

Network > Interfaces > New (Tunnel IF)

Network > Interfaces > Edit (for tunnel.6) > IPv6

3. **ルート**
   Network > Routing > Routing Table > New (trust-vr)

4. **RADIUS**
   Configuration > Auth > Auth Servers > New

   Configuration > Auth > Auth Servers > Edit

5. **XAuth**
   Objects > IP Pools > New

   Objects > IP Pools > Edit

   VPNs > L2TP > Default Settings

6. **IKE**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > AutoKey Advanced > Gateway > Edit

7. **VPN**
   VPNs > AutoKey IKE > New

   VPNs > AutoKey IKE > Edit

8. **ポリシー**
   Policies > (From: Untrust, To: Trust) > New

   Policies > (From: Trust, To: Untrust) > New

CLI（XAuth サーバー）

1. **インターフェース**

```
set interface ethernet1 zone untrust
set interface ethernet1 ipv6 mode router
set interface ethernet1 manage
set interface ethernet1 ipv6 enable
set interface ethernet1 ipv6 interface-id 2111111111111111
set interface ethernet1 ipv6 ip 2bbb::2/64
set interface ethernet1 route

set interface ethernet2 zone trust
set interface ethernet2 manage
set interface ethernet2 ipv6 mode router
set interface ethernet2 ipv6 enable
set interface ethernet2 ipv6 interface-id 2222222222222222
set interface ethernet2 ipv6 ip 2ccc::1/64
set interface ethernet2 ipv6 ra transmit
set interface ethernet2 ip 50.1.1.1/24
set interface ethernet2 route

set interface ethernet3 zone untrust
set interface ethernet3 manage
set interface ethernet3 ipv6 mode router
set interface ethernet3 ipv6 enable
set interface ethernet3 ipv6 interface-id 2333333333333333
```

```
set interface ethernet3 ipv6 ip 2ddd::2/64
set interface ethernet3 route

set interface ethernet4 zone untrust
set interface ethernet4 manage
set interface ethernet4 ipv6 mode router
set interface ethernet4 ipv6 enable
set interface ethernet4 ipv6 interface-id 2444444444444444
set interface ethernet4 ipv6 ip 3ddd::2/64
set interface ethernet2 route
```

2. トンネル

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ipv6 mode router
set interface tunnel.1 ipv6 enable
set interface tunnel.2 zone untrust
set interface tunnel.2 ipv6 mode router
set interface tunnel.2 ipv6 enable
set interface tunnel.3 zone untrust
set interface tunnel.3 ipv6 mode router
set interface tunnel.3 ipv6 enable
```

3. ルート

```
set vrouter trust route 2aaa::0/64 interface ethernet1 gateway 2bbb::1 metric 2
set vrouter trust route 2aaa::0/16 interface tunnel.1
set vrouter trust route 2bad::0/64 interface ethernet3 gateway 2ddd::1 metric 2
set vrouter trust route 2bad::0/16 interface tunnel.2
set vrouter trust route 3bad::0/64 interface ethernet4 gateway 2ddd::1 metric 2
set vrouter trust route 3bad::0/16 interface tunnel.3
```

4. RADIUS

```
set auth-server RAD1 id 1
set auth-server RAD1 server-name 50.1.1.3
set auth-server RAD1 account-type xauth
set auth-server RAD1 radius secret juniper
set auth-server RAD1 radius port 1812
```

5. XAuth

```
set ippool P1 80.1.1.1 80.1.1.2
set ippool P1 80.1.1.3 80.1.1.4
set xauth default ippool P1
```

6. IKE

```
set ike gateway NS2_NS1 add 2bbb::1 outgoing-interface ethernet1 local-add
    2bbb::2 preshare abc123 sec-level standard
set ike gateway NS2_NS3 add 2ddd::1 outgoing-interface ethernet3 local-add
    2ddd::2 preshare abc123 sec-level standard
set ike gateway NS2_NS4 add 3ddd::1 outgoing-interface ethernet4 local-add
    3ddd::2 preshare abc123 sec-level standard
set ike gateway NS2_NS1 xauth server RAD1 query-config user PC4
set ike gateway NS2_NS3 xauth server RAD1 query-config user PC4
set ike gateway NS2_NS4 xauth server RAD1 query-config user PC4
```

7. VPN

```
set vpn NS2toNS1 gateway NS2_NS1 sec-level standard
set vpn NS2toNS1 bind interface tunnel.1
set vpn NS2toNS3 gateway NS2_NS3 sec-level standard
set vpn NS2toNS3 bind interface tunnel.2
```

```
set vpn NS2toNS4 gateway NS2_NS4 sec-level standard
set vpn NS2toNS4 bind interface tunnel.3
```

8. ポリシー

```
set policy id 1 from untrust to trust any-ipv6 any-ipv6 any permit
set policy id 2 from trust to untrust any-ipv6 any-ipv6 any permit
```

RADIUS リトライ

単一 XAuth クライアントと複数 RADIUS サーバーを有する XAuth サーバーという環境において、XAuth サーバーがバックアップサーバーをトライする前に RADIUS サーバーがリトライを行う回数を設定できます。リトライのデフォルト値は 3 回（つまり合計 4 回）です。たとえば、デバイスのリトライを 20 回に設定した場合、デバイスはバックアップサーバーをトライする前に、合計で 21 回の要求を一次 RADIUS サーバーに送信します。

この例では、127 ページの図 38 で示されているトポロジに基づき、XAuth サーバーの RADIUS の設定のみを示しています。

WebUI（XAuth サーバー、RADIUS 設定）

Configuration > Auth > Auth Servers > New

Configuration > Auth > Auth Servers > Edit

CLI （XAuth サーバー、RADIUS 設定）

```
set auth-server RAD1 id 1
set auth-server RAD1 server-name 50.1.1.3
set auth-server RAD1 backup1 50.1.1.5
set auth-server RAD1 account-type xauth
set auth-server RAD1 radius secret juniper
set auth-server RAD1 radius port 1812
set auth-server RAD1 radius retries 20
```

Calling-Station-Id

デフォルトでは、Calling-Station-Id 属性は、アクセス要求パケットおよびアカウンティング要求パケットでは見えないように設定されています。この属性は、パケット内に表示するよう設定することができます。ike-ip address がアクセス要求パケット内で送信されます。

126 ページの図 36 に基づく次の例では、パケットに Calling-Station-Id 属性を含むように XAuth サーバーを設定します。この例は、XAuth サーバーの RADIUS 設定のみを示しています。

WebUI（デバイス 2）

Configuration > Auth > Auth Servers > New

Configuration > Auth > Auth Servers > Edit

CLI（デバイス 2）

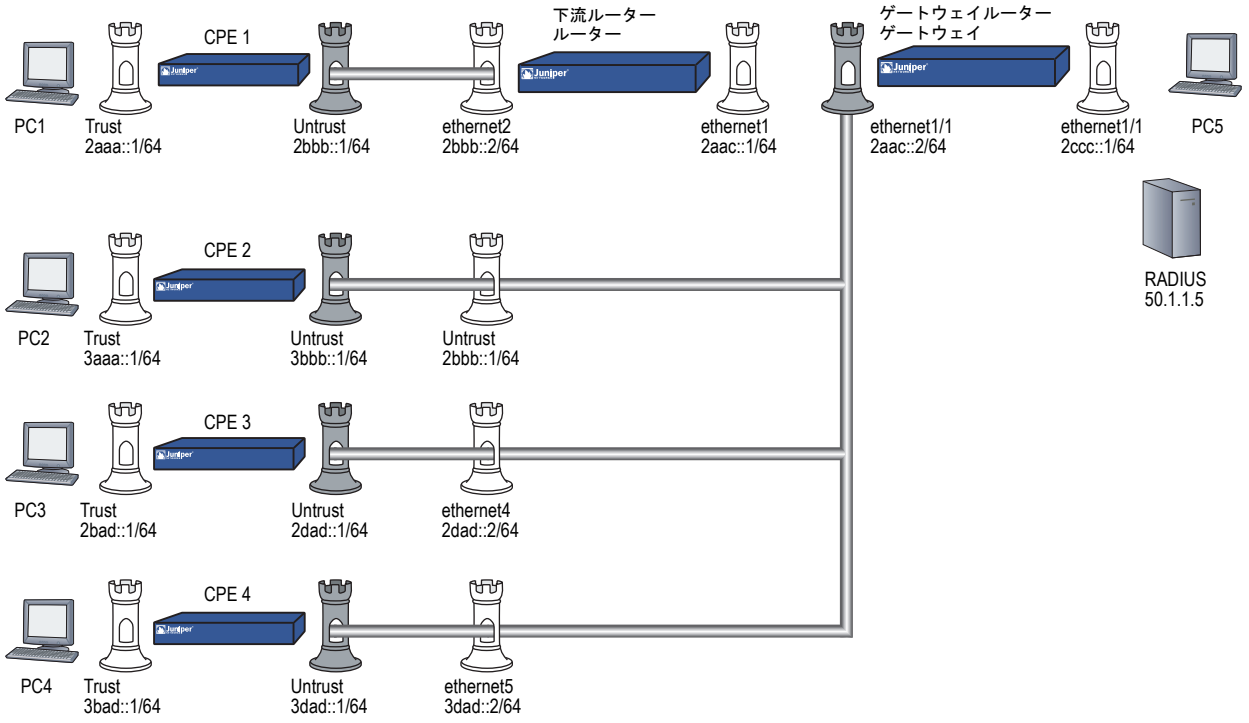
```
set auth-server RAD1 id 1
set auth-server RAD1 server-name 50.1.1.3
set auth-server RAD1 backup1 50.1.1.5
set auth-server RAD1 account-type xauth
```

```
set auth-server RAD1 radius secret juniper
set auth-server RAD1 radius port 1812
set auth-server RAD1 radius attribute calling-station-id
```

IPSec アクセスセッション

図 42 は、下流のルーター（デバイス 2）を介して上流のゲートウェイルーター（デバイス 5）とやり取りを行う CPE ルーターとして設定されている 4 つのデバイスを示しています。すべての場合において、IPSec アクセスセッション機能が有効化されているので RADIUS サーバーは単一の連続的な RADIUS アカウンティングセッションを維持することができます。

図 42: IPSec アクセスセッションの例



次の例では、4 つの CPE がゲートウェイルーター (ethernet1、IP アドレス 2aac::2) 上の同じインターフェースへのトンネルを設立しています。ゲートウェイ上で IAS セッションを開始すると、別々のユーザー名およびパスワードを使用する 4 人の別々の XAuth ユーザー（CPE ルーター 1 基につき 1 人）が許可されます。

注 : WebUI セクションでは、デバイス構成ページへの到るナビゲーションパスのみを一覧表示します。具体的な値については、それに続く CLI セクションを参照してください。

この例の基本実行手順は次のとおりです。

1. 4 基の CPE デバイス、ルーターおよびゲートウェイを下記の CLI のように設定します。

2. 4 基の CPE の各基から XAuth ユーザー情報（PC1、PC2、PC3 および PC11。パスワードは PC1、PC2、PC3、PC11 のそれぞれのパスワード）を送信します。さらに、すべての CPE を XAuth クライアントとして設定します。

3. すべての CPE からドメイン名 「juniper.net」を送信し、VPN をアグレッシブモードネゴシエーションに設定します。

4. ゲートウェイ上で以下を行います。

   a. XAuth サーバー設定を行います。

   b. RADIUS 共有秘密（juniper）と、ポート番号（1812）を指定します。

   c. ユーザーグループ（group1）を追加し、ドメイン名“juniper.net”、share limit 10 のユーザー（n1）を追加します。

   RADIUS 上で以下を行います。

   a. ユーザー PC1、PC2、PC3 および PC4 を追加し、それぞれについて、パスワード PC1、PC2、PC3 および PC4 を指定します。

   b. すべてのユーザーについて必要な属性（フレーム化 IP アドレス等）をすべて指定します。

WebUI（CPE 1、CPE 2、CPE 3 および CPE 4）

1. インターフェース

Network > Interfaces > Edit (for trust)

Network > Interfaces > Edit (for trust) > IPv6

Network > Interfaces > Edit (for untrust)

Network > Interfaces > Edit (for untrust) > IPv6

2. トンネル

Network > Interfaces > New (Tunnel IF)

Network > Interfaces > Edit (for tunnel.6) > IPv6

3. ルート

Network > Routing > Routing Table > New (trust-vr)

4. IKE

VPNs > AutoKey Advanced > Gateway > New

VPNs > AutoKey Advanced > Gateway > Edit

5. **VPN**
   VPNs > AutoKey IKE > New

   VPNs > AutoKey IKE > Edit

6. **ポリシー**
   Policies > (From: Untrust, To: Trust) > New

   Policies > (From: Trust, To: Untrust) > New

CLI（CPE 1）

1. **インターフェース**
```
set interface ethernet1 zone trust
set interface ethernet1 manage
set interface ethernet1 ipv6 mode router
set interface ethernet1 ipv6 enable
set interface ethernet1 ipv6 interface-id 6111111111111111
set interface ethernet1 ipv6 ip 2aaa::1/64
set interface ethernet1 ipv6 ra transmit
set interface ethernet1 route

set interface ethernet2 zone untrust
set interface ethernet2 manage
set interface ethernet2 ipv6 mode host
set interface ethernet2 ipv6 enable
set interface ethernet2 ipv6 interface-id 6222222222222222
set interface ethernet2 ipv6 ip 2bbb::1/64
set interface ethernet2 route
```

2. **トンネル**
```
set interface tunnel.1 zone untrust
set interface tunnel.1 ipv6 mode host
set interface tunnel.1 ipv6 enable
```

3. **ルート**
```
set vrouter trust-vr route::/0 interface ethernet2 gateway 2bbb::2
set vrouter trust-vr route 2ccc::/64 interface tunnel.1
```

4. **IKE**
```
set ike gateway touniversal add 2aac::2 aggressive local-id juniper.net
    outgoing-interface ethernet2 local-address 2bbb::1 preshare abc123 sec-level
    standard
set ike gateway touniversal xauth client any username PC1 password PC1
```

5. **VPN**
```
set vpn vpn1 gateway touniversal sec-level standard
set vpn vpn1 bind interface tunnel.1
```

6. **ポリシー**
```
set policy from trust to untrust any-ipv6 any-ipv6 any permit
set policy from untrust to trust any-ipv6 any-ipv6 any permit
```

CLI（CPE 2）

1. **インターフェース**

```
set interface trust zone trust
set interface trust manage
set interface trust ipv6 mode router
set interface trust ipv6 enable
set interface trust ipv6 interface-id 3111111111111111
set interface trust ipv6 ip 3aaa::1/64
set interface trust ipv6 ra transmit
set interface trust route

set interface untrust zone untrust
set interface untrust manage
set interface untrust ipv6 mode host
set interface untrust ipv6 enable
set interface untrust ipv6 interface-id 3222222222222222
set interface untrust ipv6 ip 3bbb::1/64
set interface untrust route
```

2. **トンネル**

```
set interface tunnel.2 zone untrust
set interface tunnel.2 ipv6 mode host
set interface tunnel.2 ipv6 enable
```

3. **ルート**

```
set vrouter trust-vr route::/0 interface untrust gateway 3bbb::2
set vrouter trust-vr route 2ccc::/64 interface tunnel.2
```

4. **IKE**

```
set ike gateway touniversal add 2aac::2 aggressive local-id juniper.net
    outgoing-interface untrust local-address 3bbb::1 preshare abc123 sec-level
    standard
set ike gateway touniversal xauth client any username PC2 password PC2
```

5. **VPN**

```
set vpn vpn2 gateway touniversal sec-level standard
set vpn vpn2 bind interface tunnel.2
```

6. **ポリシー**

```
set policy from trust to untrust any-ipv6 any-ipv6 any permit
set policy from untrust to trust any-ipv6 any-ipv6 any permit
```

CLI（CPE 3）

1. **インターフェース**

```
set interface trust zone trust
set interface trust manage
set interface trust ipv6 mode router
set interface trust ipv6 enable
set interface trust ipv6 interface-id 4111111111111111
set interface trust ipv6 ip 2bad::1/64
set interface trust ipv6 ra transmit
set interface trust route

set interface untrust zone untrust
set interface untrust manage
set interface untrust ipv6 mode host
set interface untrust ipv6 enable
```

set interface untrust ipv6 interface-id 4222222222222222
set interface untrust ipv6 ip 2dad::1/64
set interface untrust route

2. トンネル

set interface tunnel.3 zone untrust
set interface tunnel.3 ipv6 mode host
set interface tunnel.3 ipv6 enable

3. ルート

set vrouter trust-vr route::/0 interface untrust gateway 2dad::2
set vrouter trust-vr route 2ccc::/64 interface tunnel.3

4. IKE

set ike gateway touniversal add 2aac::2 aggressive local-id juniper.net
outgoing-interface untrust local-address 2dad::1 preshare abc123 sec-level
standard
set ike gateway touniversal xauth client any username PC3 password PC3

5. VPN

set vpn vpn3 gateway touniversal sec-level standard
set vpn vpn3 bind interface tunnel.3

6. ポリシー

set policy from trust to untrust any-ipv6 any-ipv6 any permit
set policy from untrust to trust any-ipv6 any-ipv6 any permit

CLI（CPE 4）

1. インターフェース

set interface trust zone trust
set interface trust manage
set interface trust ipv6 mode router
set interface trust ipv6 enable
set interface trust ipv6 interface-id 5111111111111111
set interface trust ipv6 ip 3bad::1/64
set interface trust ipv6 ra transmit
set interface trust route

set interface untrust zone untrust
set interface untrust manage
set interface untrust ipv6 mode host
set interface untrust ipv6 enable
set interface untrust ipv6 interface-id 5222222222222222
set interface untrust ipv6 ip 3dad::1/64
set interface untrust route

2. トンネル

set interface tunnel.4 zone untrust
set interface tunnel.4 ipv6 mode host
set interface tunnel.4 ipv6 enable

3. ルート

set vrouter trust-vr route::/0 interface untrust gateway 3dad::2
set vrouter trust-vr route 2ccc::/64 interface tunnel.4

4. **IKE**

```
set ike gateway touniversal add 2aac::2 aggressive local-id juniper.net
    outgoing-interface untrust local-address 3dad::1 preshare abc123 sec-level
    standard
set ike gateway touniversal xauth client any username PC11 password PC11
```

5. **VPN**

```
set vpn vpn4 gateway touniversal sec-level standard
set vpn vpn4 bind interface tunnel.4
```

6. **ポリシー**

```
set policy from trust to untrust any-ipv6 any-ipv6 any permit
set policy from untrust to trust any-ipv6 any-ipv6 any permit
```

WebUI（デバイス 2、ルーター）

1. **インターフェース**

Network > Interfaces > Edit (for trust):

Network > Interfaces > Edit (for trust) > IPv6

Network > Interfaces > Edit (for untrust)

Network > Interfaces > Edit (for untrust) > IPv6

2. **ルート**

Network > Routing > Routing Table > New (trust-vr)

CLI（デバイス 2、ルーター）

1. **インターネット**

```
set interface ethernet1 zone trust
set interface ethernet1 manage
set interface ethernet1 ipv6 mode host
set interface ethernet1 ipv6 enable
set interface ethernet1 ipv6 interface-id 1111111111111111
set interface ethernet1 ipv6 ip 2aac::1/64
set interface ethernet1 route

set interface ethernet2 zone trust
set interface ethernet2 manage
set interface ethernet2 ipv6 mode host
set interface ethernet2 ipv6 enable
set interface ethernet2 ipv6 interface-id 1222222222222222
set interface ethernet2 ipv6 ip 2bbb::2/64
set interface ethernet2 route

set interface ethernet3 zone trust
set interface ethernet3 manage
set interface ethernet3 ipv6 mode host
set interface ethernet3 ipv6 enable
set interface ethernet3 ipv6 interface-id 1333333333333333
set interface ethernet3 ipv6 ip 3bbb::2/64
set interface ethernet3 route

set interface ethernet4 zone trust
set interface ethernet4 manage
set interface ethernet4 ipv6 mode host
```

```
set interface ethernet4 ipv6 enable
set interface ethernet4 ipv6 interface-id 1444444444444444
set interface ethernet4 ipv6 ip 2dad::2/64
set interface ethernet2 route

set interface ethernet5 zone trust
set interface ethernet5 manage
set interface ethernet5 ipv6 mode host
set interface ethernet5 ipv6 enable
set interface ethernet5 ipv6 interface-id 1555555555555555
set interface ethernet5 ipv6 ip 3dad::2/64
set interface ethernet5 route
unset zone trust block
```

2. ルート

```
set vrouter trust-vr route 2ccc::/64 interface ethernet1 gateway 2aac::2
set vrouter trust-vr route 2aaa::/64 interface ethernet2 gateway 2bbb::1
set vrouter trust-vr route 3aaa::/64 interface ethernet3 gateway 3bbb::1
set vrouter trust-vr route 2bad::/64 interface ethernet4 gateway 2dad::1
set vrouter trust-vr route 3bad::/64 interface ethernet5 gateway 3dad::1
```

WebUI（ゲートウェイルーター）

1. インターフェース

Network > Interfaces > Edit (for trust):

Network > Interfaces > Edit (for trust) > IPv6

Network > Interfaces > Edit (for untrust)

Network > Interfaces > Edit (for untrust) > IPv6

2. トンネル

Network > Interfaces > New (Tunnel IF)

Network > Interfaces > Edit (for tunnel.6) > IPv6

3. ルート

Network > Routing > Routing Table > New (trust-vr)

4. ユーザー

Objects > Users > Local > New

Objects > Users > Local > Edit

Objects > User > Local Groups > New

Objects > User > Local Groups > Edit

5. RADIUS

Configuration > Auth > Auth Servers > New

Configuration > Auth > Auth Servers > Edit

6. **IKE**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > AutoKey Advanced > Gateway > Edit

7. **VPN**
   VPNs > AutoKey IKE > New

   VPNs > AutoKey IKE > Edit

8. **ポリシー**
   Policies > (From: Untrust, To: Trust) > New

   Policies > (From: Trust, To: Untrust) > New

CLI（ゲートウェイルーター）

1. **インターフェース**
   set interface ethernet1/1 zone untrust
   set interface ethernet1/1 manage
   set interface ethernet1/1 ipv6 mode host
   set interface ethernet1/1 ipv6 en
   set interface ethernet1/1 ipv6 interface-id 2111111111111111

   set interface ethernet1/1 ipv6 ip 2aac::2/64
   set interface ethernet1/1 route
   set interface ethernet1/2 zone trust
   set interface ethernet1/2 manage
   set interface ethernet1/2 ipv6 mode router
   set interface ethernet1/2 ipv6 enable

   set interface ethernet1/2 ipv6 interface-id 2222222222222222
   set interface ethernet1/2 ipv6 ip 2ccc::1/64
   set interface ethernet1/2 route
   set interface ethernet1/2 ipv6 ra transmit
   set interface ethernet1/2 ip 50.1.1.1/24

2. **トンネル**
   set interface tunnel.1 zone untrust
   set interface tunnel.1 ipv6 mode host
   set interface tunnel.1 ipv6 enable

3. **ルート**
   set vrouter trust-vr route::/0 interface ethernet1/1 gateway 2aac::1
   set vrouter trust-vr route 2aaa::/64 interface tunnel.1
   set vrouter trust-vr route 3aaa::/64 interface tunnel.1
   set vrouter trust-vr route 2bad::/64 interface tunnel.1
   set vrouter trust-vr route 3bad::/64 interface tunnel.1
   set ipsec access-session enable

4. **ユーザー**
   set user n1 uid 1
   set user n1 ike-id fqdn juniper.net share-limit 10
   set user n1 type ike
   set user n1 enable
   set user-group group1 id 1
   set user-group group1 user n1

5. **RADIUS**
   set auth-server RAD1 id 1
   set auth-server RAD1 server-name 50.1.1.5
   set auth-server RAD1 account-type xauth
   set auth-server RAD1 radius port 1812
   set auth-server RAD1 radius secret juniper

6. **IKE**
   set ike gateway universal dialup group1 aggressive outgoing-interface ethernet1/1 local-address 2aac::2 preshare abc123 sec-level standard
   set ike gateway universal xauth server RAD1 query-config
   set ike gateway universal dpd interval 15
   set ike gateway universal dpd retry 2

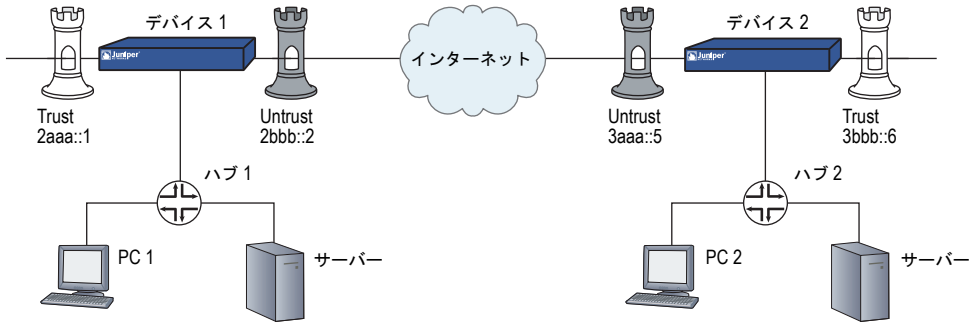
7. **VPN**
   set vpn VPN1 gateway universal sec-level standard
   set vpn VPN1 bind interface tunnel.1

8. **ポリシー**
   set policy id 1 from Untrust to Trust "Dial-up VPN ipv6" any-ipv6 any permit
   set policy id 2 from trust to unTrust any-ipv6 "Dial-up VPN ipv6" any permit
   set policy id 3 from untrust to Trust any-ipv6 any-ipv6 any permit

デッドピア検出

図 43 は、デッドピア検出（DPD) 用に設定しているデバイス 2 基を示しています。

図 43: デッドピア検出例



注 : WebUI セクションでは、デバイス構成ページへの到るナビゲーションパスのみを一覧表示します。具体的な値については、それに続く CLI セクションを参照してください。

デバイス 1 上で、

- デバイス 1 を IPv6 ルーターとして Trust インターフェースおよび Untrust インターフェースを設定します。
  - Trust インターフェースを、プレフィックス 2aaa:: をアドバタイズするよう設定します。
  - Untrust インターフェースを、プレフィックス 2bbb:: をアドバタイズするよう設定します。

- IKE ゲートウェイを設定します。
- VPN を設定します。
- DPD 時間間隔を 15 秒に設定し、リトライを 10 回に設定します。

デバイス 2 上で、

- RA を受け入れられるように、Untrust インターフェースを IPv6 ホストとして設定します。
- Trust インターフェースを、プレフィックス 3bbb:: をアドバタイズする IPv6 ルーターとして設定します。
- IKE ゲートウェイを設定します。
- VPN を設定します。

注： オプションとして、**set ike gateway ton4 dpd always-send** コマンドの入力により DPD Always Send を設定することができます。

WebUI（デバイス 1）

1. **インターフェース**
   Network > Interfaces > Edit (for trust)

   Network > Interfaces > Edit (for trust) > IPv6

   Network > Interfaces > Edit (for untrust)

   Network > Interfaces > Edit (for untrust) > IPv6

2. **トンネル**
   Network > Interfaces > New (Tunnel IF)

   Network > Interfaces > Edit (for tunnel.6) > IPv6

3. **ルート**
   Network > Routing > Routing Table > New (trust-vr)

4. **IKE**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > AutoKey Advanced > Gateway > Edit

5. **VPN**
   VPNs > AutoKey IKE > New

   VPNs > AutoKey IKE > Edit

6. **ポリシー**
   Policies > (From: Untrust, To: Trust) > New

   Policies > (From: Trust, To: Untrust) > New

CLI（デバイス 1）

1. インターフェース

```
unset zone untrust block
set interface trust ipv6 mode router
set interface trust ipv6 ip 2aaa::/64
set interface trust ipv6 interface-id 0000000000000001
set interface trust ipv6 enable
set interface trust ipv6 ra transmit
set interface trust route
set interface trust manage

set interface untrust ipv6 mode router
set interface untrust ipv6 ip 2bbb::/64
set interface untrust ipv6 interface-id 0000000000000002
set interface untrust ipv6 enable
set interface untrust ipv6 ra transmit
set interface untrust route
set interface untrust manage
```

2. トンネル

```
set interface tunnel.6 zone untrust
set interface tunnel.6 ipv6 mode host
set interface tunnel.6 ipv6 enable
set interface tunnel.6 ipv6 ip 3ddd::/64
```

3. ルート

```
set vrouter trust-vr route 3bbb::/64 interface tunnel.6
set vrouter trust-vr route::/0 interface untrust gateway 2bbb::3
```

4. IKE

```
set ike gateway ton4 address 3aaa::5 outgoing-interface untrust local-address
    2bbb::2 preshare abc sec-level standard
set ike gateway ton4 dpd interval 15
set ike gateway ton4 dpd retry 10
```

5. VPN

```
set vpn vpn1 gateway ton4 no-replay sec-level standard
set vpn vpn1 bind interface tunnel.6
```

6. ポリシー

```
set policy from untrust to trust any-ipv6 any-ipv6 any permit
set policy from trust to untrust any-ipv6 any-ipv6 any permit
```

WebUI（デバイス 2）

1. インターフェース

Network > Interfaces > Edit (for untrust)

Network > Interfaces > Edit (for untrust) > IPv6

Network > Interfaces > Edit (for trust)

Network > Interfaces > Edit (for trust) > IPv6

2. **トンネル**
   Network > Interfaces > New (Tunnel IF)

   Network > Interfaces > Edit (for tunnel.6) > IPv6

3. **ルート**
   Network > Routing > Routing Table > New (trust-vr)

4. **IKE**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > AutoKey Advanced > Gateway > Edit

5. **VPN**
   VPNs > AutoKey IKE > New

   VPNs > AutoKey IKE > Edit

6. **ポリシー**
   Policies > (From: Untrust, To: Trust) > New

   Policies > (From: Trust, To: Untrust) > New

CLI（デバイス 2）

1. **インターフェース**

```
unset zone untrust block
set interface untrust ipv6 mode host
set interface untrust ipv6 interface-id 0000000000000005
set interface untrust ipv6 enable
set interface untrust ipv6 ra accept
set interface untrust route
set interface untrust manage

set interface trust ipv6 mode router
set interface trust ipv6 ip 3bbb::/64
set interface trust ipv6 interface-id 0000000000000006
set interface trust ipv6 enable
set interface trust ipv6 ra transmit
set interface trust route
set interface trust manage
```

2. **トンネル**

```
set interface tunnel.6 zone untrust
set interface tunnel.6 ipv6 mode host
set interface tunnel.6 ipv6 ip 3ddd::/64
set interface tunnel.6 ipv6 enable
```

3. **ルート**

```
set vrouter trust-vr route::/0 interface untrust gateway 3aaa::4
set vrouter trust-vr route 2aaa::/64 interface tunnel.6
```

4. **IKE**

```
set ike gateway ton1 address 2bbb::2 outgoing-interface untrust local-address
    3aaa::5 preshare abc sec-level standard
set ike gateway ton1 dpd interval 15
set ike gateway ton1 dpd retry 5
```

5. **VPN**
   set vpn vpn4 gateway ton1 no-replay sec-level standard
   set vpn vpn4 bind interface tunnel.6

6. **ポリシー**
   set policy from untrust to trust any-ipv6 any-ipv6 any permit
   set policy from trust to untrust any-ipv6 any-ipv6 any permit

付録 A

スイッチング

パスに沿って IPv6 トラフィックを通過させるため、セキュリティデバイスをスイッチとして使用できます。これには、そのデバイスを透過モードにする必要があります。透過モードについての詳細は、*第 2 部: 基本*を参照してください。

表 4 は、IPv6 トラフィックや他の非 IP トラフィックが透過モードで動作するセキュリティデバイスを通過できるようにする、ScreenOS のコマンドを列挙しています。

表 4: 非 IP トラフィックをバイパスするための透過モードコマンド

コマンド	説明
set interface vlan1 bypass-non-ip	レイヤー 2 非 IP トラフィックすべてがセキュリティデバイスを通過することを許可します。
unset interface vlan1 bypass-non-ip	非 IP および 非 ARP ユニキャストトラフィックをすべてブロックします（デフォルトの動作）。
unset interface vlan1 bypass-non-ip-all	両方のコマンドが構成ファイルに現れた場合、**unset interface vlan1 bypass-non-ip** コマンドを上書きします。 **unset interface vlan1 bypass-non-ip-all** コマンドを実行してしまった後で、IP でも ARP でもないユニキャストトラフィックを遮断する、という初期状態の動作を反転したい場合は、まず **set interface vlan1 bypass-non-ip** コマンドを実行して、マルチキャスト、ユニキャスト、およびブロードキャストトラフィックを含む、非 IP および非 ARP トラフィックがすべて通過できるようにする必要があります。次に **unset interface vlan1 bypass-non-ip** コマンドを実行すると、IP でも ARP でもないユニキャストトラフィックのみを遮断できます。
set interface vlan1 bypass-others-ipsec	デバイスが、終了しようとしないで IPSec トラフィックを通過させるのを許可します。すると IPSec トラフィックはそのまま通過して、他の VPN 終端ポイントに向かうようになります。

索引

数字

3DES 暗号化 117
4in6 トンネリング
　基本セットアップ 111
　定義 111
6in4 トンネリング 107
　IPv4 WAN 上 115
　基本セットアップ 116
6over4 トンネリング
　アドレス、処理 96
　手動トンネリング 96
　種類 95
　使用する時 95
　定義 95
6to4
　アドレス 8, 99, 104
　トンネリング 95, 99
　トンネリング、説明 99
　ホスト 104
　リレールーター 99, 100
　ルーター 99

A

AES128 暗号化 116

C

CLI 30, 32

D

DHCPv6
　TLA と SLA 37
　委譲されたプレフィックス 38
　クライアントとサーバー 36
　目的 35
Diffie-Hellman グループ 116
DNS (ドメイン名システム) アドレス
　変換 91
Domain Name System (DNS) addresses
　分割 44, 45
dynamic IP 80
dynamic IP, from IPv6 to IPv4 81

H

Host モード 46, 112

I

ID アソシエーションプレフィックス委譲 ID
（IAPD-ID） 37, 39
Interior Gateway Protocol (IGP) 51
IPSec Access Session (IAS) 128
IPv4
　addresses, mapped 80, 84
　WAN 108
IPv4 to IPv6
　host mapping 89
　network mapping 87
IPv4/IPv6 boundaries 87
IPv4/IPv6 境界 79–84
IPv6
　addresses, SLA 37
　backbone 83, 111
　networks, island 108
　アドレス、TLA 37
IPv6 to IPv4 host mapping 86
IPv6/IPv4 boundaries 80–86

M

MAC アドレス 13, 21, 29
mapped IP (MIP)
　IPv4 ホストから単一 IPv6 ホストへの送信 89
　IPv4 ホストから複数 IPv6 ホストへの送信 87
　IPv6 から IPv4 への MIP 82
　IPv6 ホストから単一 IPv4 ホストへの送信 86
　IPv6 ホストから複数 IPv4 ホストへの送信 84
　IPv6-to-IPv4 ネットワークマッピング 84
MIP 80

N

NAT-PT 79
NAT-PT, IPSec, when to use 108
Neighbor Solicitation (NS)
　設定 30
Network Address Translation-Port Translation (NAT-PT)
79

P

Point-to-Point Protocol (PPP) 46
PPPoE - Point-to-Point Protocol over Ethernet 46

R

RA
- ルーター通知 12

RADIUSv6 126
request packets, outgoing from IPv6 to IPv4 82
RIP
- インスタンス、VR で作成 54
- インターフェースパラメータ 60
- インターフェース、稼動 55
- 近隣ノード、フィルタリング 57
- 構成 53
- 大域パラメータ 55
- フラッディングの回避 59

RIP ルート
- 再配布 58
- デフォルト、拒否 57

RIP 、表示
- 近隣ノード情報 66
- データベース 65
- プロトコル詳細 65

RIPng 49, 51
- インターフェースコストメトリック 60, 61
- オフセットメトリック 60, 61
- メトリックの計算 61
- ルート情報の再配布 51
- ルートのメトリック 60, 61

RSA 認証 116

S

service requests, outgoing 84, 86
Site-Local Aggregator (SLA) 37, 39

T

Top-Level Aggregator (TLA) 37

U

upstream routers 38

V

virtual routers, RIP 53–68

W

WebUI 32
WebUI、サンプルクライアント上、下流ルーター . 40
WINS サーバー 126

X

XAuth
- 使用する時 126
- 認証 132

あ

アクセスコンセントレータ（AC） 46
宛先ゲートウェイ 96
アドレス
- MAC 13, 21, 29
- 自動構成 11
- 分割 44
- リンクローカル 12

アドレス、処理
- 4in6 トンネリング 111
- 6to4 トンネリング 101
- IPv4 から IPv6 への DIP 82
- IPv4 ホストから単一 IPv6 ホストへの送信 108
- IPv6 から IPv4 への DIP 81
- IPv6 ホストから複数 IPv4 ホストへの送信 84
- 宛先アドレス変換 82
- 手動トンネリング 96

暗号化 107, 111
- 3DES 117
- AES128 116

い

インターネットサービスプロバイダ（ISP） . 36, 44, 96
インターフェース
- DHCPv6 35
- ND 29
- NDP 30
- NUD 29
- PPPoE 46
- デュアルルーティングテーブル 50

か

仮想ルーター 50, 99
カプセル化 100, 107, 112

く

グローバルユニキャストアドレス 99, 116

こ

構成例
- 6to4 ホスト、へのトンネリング 105
- DNS サーバー情報、要求 43
- IPv4 上で IPv6 から IPv4 ネットワークへ 108
- Ipv6 上の Ipv4 トンネリング（autokey IKE） .. 112, 116
- IPv6 要求の複数 IPv4 ホストへの送信 85
- native host, tunneling to 101
- PPPoE instance, configuring 46
- prefixes, delegating 38, 40
- アクセスリストおよびルートマップ 61
- 手動トンネリング 97
- 静的ルートの再配布 61

顧客構内装置（CPE） 39, 128
異なる IP スタック 82, 83

さ

再送信時間 31

最大送信単位（MTU）.....12

し
自動構成
　アドレスの自動構成.....11
　ステートレス.....11
　ルーター通知メッセージ.....12
手動 6over4 トンネリング.....95
手動トンネリング.....96
状態の移行
　静的なエントリ.....18
　端点ホスト.....16
　次ホップゲートウェイルーター.....16
　トンネルゲートウェイ.....17

す
ステートレスアドレス自動構成.....11

せ
精査.....31

そ
ソースアドレス変換.....81

た
端点ホスト状態
　Probe Forever 状態.....31
　Stale モード.....30
　再送信時間.....31
　重複アドレス検出（DAD）.....31
　到達可能時間.....30
　プローブ時間.....31
　ベース到着可能時間.....30

ち
重複アドレス検出（DAD）
　機能.....31
　再試行カウント.....31

つ
次ホップゲートウェイ.....31

て
デバイスユニーク ID（DUID）.....37
デュアルスタックアーキテクチャ.....50
　networks, dissimilar.....50
　WAN backbones, dissimilar.....50
　ルーティングテーブル.....50

と
到達可能性状態.....14
到達可能性状態、移行.....16
ドメイン名システム (DNS).....42, 43
　DHCPv6 検索リスト.....36
　DHCP クライアントホスト.....43
　IPv4 または IPv4 アドレス.....42
　サーバー.....126
　サーバー、トンネリング.....44
　ドメイン名の一部.....36
　ドメインルックアップ.....44
　プロキシ.....44
トンネル終端ポイント.....99

に
認証.....107, 111, 132

ね
ネイティブホスト.....99, 101
ネットワークアドレス変換 - ポート変換
　dynamic IP (DIP).....80
　DIP アドレス、変換.....82
　IPv4 から IPv6 への MIP.....83
　IPv4 ホストから単一 IPv6 ホストへの送信.....89
　IPv4 ホストから複数 IPv6 ホストへの送信.....87
　IPv6 から IPv4 への DIP.....81
　IPv6 ホストから単一 IPv4 ホストへの送信.....86
　IPv6 ホストから複数 IPv4 ホストへの送信.....84
　サービス要求送信.....80, 83
　使用する時.....80
　ソースアドレス変換.....81

は
ハッシング、セキュアハッシュアルゴリズム（SHA）
116

ふ
プレフィックス一覧.....12
プローブ時間.....31
プロトコル
　IGP.....51
　PPP.....46

ま
マッピング
　host, IPv4 to IPv6.....89
　host, IPv6 to IPv4.....86
　network, IPv4 to IPv6.....87
マップ.....82

も
モード
　Stale.....30
　ホスト.....46, 112
　ルーター.....52

り

リモート終端ポイント 101, 104
リンクローカルアドレス 12, 14
隣接ノードキャッシュテーブル 13, 14, 16, 25, 30
隣接ノードキャッシュテーブル、隣接ノードエントリのカテゴリ 14
隣接ノード通知（NA） 30
隣接ノード到達不能検出（NUD） 14
　隣接ノードキャッシュテーブル 25
隣接ノード到達不能検出（NUD）、隣接ノードキャッシュテーブル 14
隣接ノード発見（ND） 29
　Accept Incoming RAs 21
　使用可能 29
　定義 13
　到達可能性状態 29
　バイパス MAC セッションキャッシング 29
　パケット、送信のため現在キューにはいっている 13
　隣接ノードエントリのエージ 13
　隣接ノードキャッシュテーブル 13, 29
　隣接ノード到達可能性状態 13, 30
隣接ノード発見（ND）、表示 32
隣接ノード発見パラメータ（NDP） 21, 30
隣接ノード要請（NS） 14, 31

る

ルーター
　upstream 38
　仮想 50, 99
ルーターモード 52
ルーター要請（RS） 12