Forcepoint Web Security Cloud
トライアル実施時の
初期セットアップに関するご案内

2019年12月
フォースポイント・ジャパン株式会社

FORCEPOINT WEB SECURITY CLOUD 導入手順

サービスをご利用いただくための導入の流れ

必須項目　任意項目

1. ファイアウォール設定

当社クラウドサービスを使用できるように、クラウドサーバとの管理用通信ならびにPACファイルを取得するための通信経路を確保します。

2. 既存機器との接続 プロキシ・チェーン

既存プロキシサーバと親子関係を構築することができます。※ 必須ではありません。親子関係がない導入方法が障害ポイントの少ないベストソリューションです。

3. エンドユーザ登録

当社クラウドサービスのポリシーを適用、ログを記録するにあたり、接続ユーザを特定する必要があります。そのためのユーザ登録を行います。

※ クライアント設定にてエンドポイント・ソフトウェアを導入する場合は必須ではありません。ただし、ユーザ・クライアント特定を明確化したい場合には、設定いただくことを推奨します。

4. クライアント設定・エージェント導入

当社クラウドサービスを利用するためのクライアント端末へのエージェントソフトウェアの導入を行います。

FORCEPOINT WEB SECURITY CLOUD 導入手順

1. ファイアウォール設定

各クライアントからのウェブ通信を、強制的にフォースポイントのクラウドサービスへ通過させるためのネットワークおよびクライアントへの設定を行います。

クラウドサービス上のPACファイルを取得できるように、ファイアウォールや経路上のルータのACL、クライアント端末に導入されているファイアウォール・ソフトウェアに対して公開しているIPレンジの通信を許可する設定を行ってください。

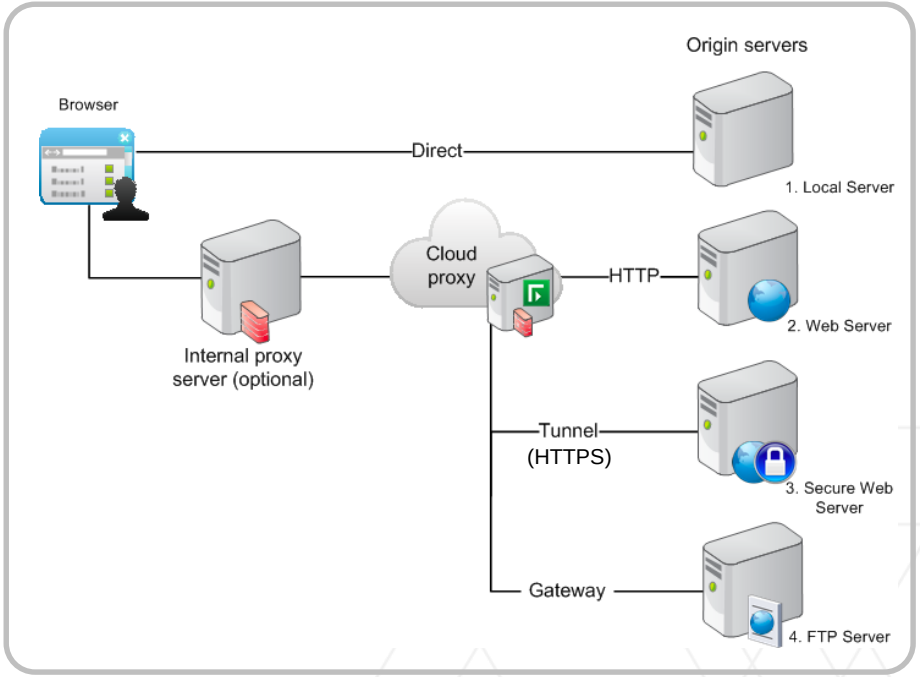
- PACファイルのアドレスおよびポート番号

http://pac.webdefence.global.blackspider.com:8082/proxy.pac

- IPレンジ

http://www.websense.com/content/support/library/web/hosted/admin_guide/wiz_firewall_setup.aspx

(詳細版) *Cloud service data center (cluster) IP addresses and port numbers*
https://support.forcepoint.com/KBArticle?id=Cloud-service-data-center-IP-addresses-port-numbers



クライアントからのウェブサーバ接続概念図

FORCEPOINT WEB SECURITY CLOUD 導入手順

1. ファイアウォール設定

- ポート番号

ポート番号	目的
80　443	クラウド管理サーバとの通信
8081　8082	PACファイルの取得、HTTPプロキシ通信
8006	シングル・サインオン (SSO使用時のみ)
8089	セキュアフォーム認証、HTTPSプロキシ通信

- IPレンジ

主要エリア	CIDR	IPレンジ	サブネット	マスク
ヨーロッパ	85.115.32.0/19	85.115.32.0 - 85.115.63.255	85.115.32.0	255.255.224.0
アジア (日本を含む)	116.50.56.0/21	116.50.56.0 - 116.50.63.255	116.50.56.0	255.255.248.0
北米	208.87.232.0/21	208.87.232.0 - 208.87.239.255	208.87.232.0	255.255.248.0

Cloud service data center (cluster) IP addresses and port numbers
https://support.forcepoint.com/KBArticle?id=Cloud-service-data-center-IP-addresses-port-numbers

FORCEPOINT WEB SECURITY CLOUD 導入手順

2. 既存機器との接続 プロキシ・チェーン

現在導入済みのプロキシサーバとの 親子関係 を構築することが出来ます。

以下の例ではSquidとの連携ですが、Basic Chaining構成、もしくは NTLM pass-through AD認証情報の転送をサポートしております。

※あくまでも連携構成が必要なときのみ。原則は当社クラウドサービスとの直接接続を推奨します。

Using Chained Proxies > Squid Proxy

https://www.websense.com/content/support/library/web/hosted/proxy_chaining/squid_ntlm.aspx

FORCEPOINT WEB SECURITY CLOUD 導入手順

3. エンドユーザ登録

クラウドサービスを利用するユーザ = エンドユーザを登録します。
ユーザ登録方法には、次の3つがございます。

1) Active Directory等 ディレクトリ情報を同期

ユーザ情報、コンピュータ・アカウント情報を同期させることにより、OUなどに基づくポリシー適用、ログへのユーザ・コンピュータ情報の記録ができるようになります。

Directory synchronization
https://www.websense.com/content/support/library/web/hosted/dsc_admin/first.aspx

2) 個別登録 (1台ずつ、もしくは 複数台まとめて登録)

個別でのユーザ登録、パスワード管理が必要となります。OUなどを活用したポリシー設定はできませんが、管理コンソールでグループの設定が出来ます。

End-user self registration and bulk registration
https://www.websense.com/content/support/library/web/hosted/admin_guide/wd_policy_enduser_upload.aspx

3) NTLM透過認証登録

プロキシ親子関係構築時に、NTLM認証チェーンを設定いただく際には、簡便な設定方法です。ブラウザにも透過認証のための設定が必要です。

NTLM transparent identification registration
https://www.websense.com/content/support/library/web/hosted/admin_guide/ntlm_id.aspx

FORCEPOINT WEB SECURITY CLOUD 導入手順

4. クライアント設定・エージェント導入

エンドポイント・ソフトウェアの導入

1. 導入する

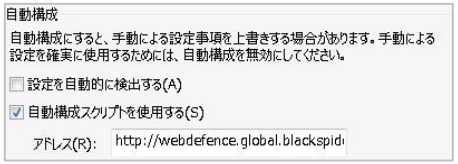
クライアントへ、エンドポイント・ソフトウェアを配布、導入します。

導入済みクライアントへのPACファイルのブラウザ設定は不要です。自動的にPACファイルが強制的に設定・適用されます。

※ HTTP(S)プロキシとの通信時にはユーザ認証情報をHTTPヘッダに含めて通信を行うため、個別での認証ログインが不要、透過認証となります。エンドポイント・ソフトウェアのアンインストール時にも、アンインストールパスワードが必要となり、ユーザが任意にアンインストールすることが出来ず、ウェブポリシーの強制力を働かせることができます。

2. 導入しない

ブラウザに http://pac.webdefence.global.blackspider.com:8082/proxy.pac?p=XXXXXX を設定します。設定情報はADの機能 GPO などをお使いになり、配布いただくことを推奨いたします。



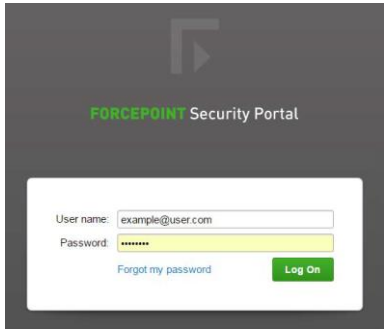
セキュアフォーム認証やSSO認証を利用する場合には、クラウドサービスの認証情報を保存するためのクッキー情報の保存を有効化してお使いください。最大1年まで保存が有効となります。

セキュアなクラウド・サービスをお試しください。

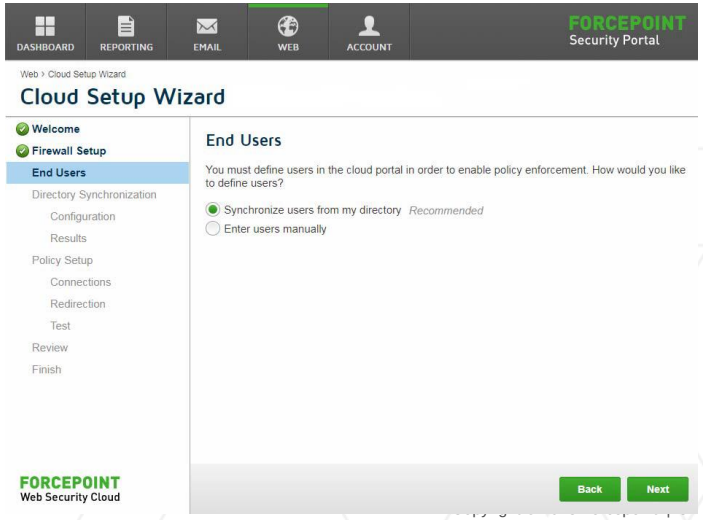
FORCEPOINT WEB SECURITY CLOUD 初期セットアップ 1

前提 ▶ ファイアウォールの設定が済んでいること

1) 管理ウェブサイトへアクセス
https://admin.forcepoint.net/portal



2) 初期セットアップ ウィザードに基づき設定
・レポートデータセンターなどの設定は
デフォルトのままでお願いします。



FORCEPOINT WEB SECURITY CLOUD 初期セットアップ 2

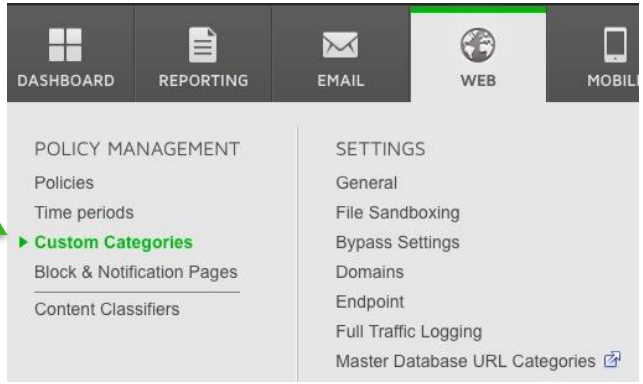
3) ウェブポリシーの編集

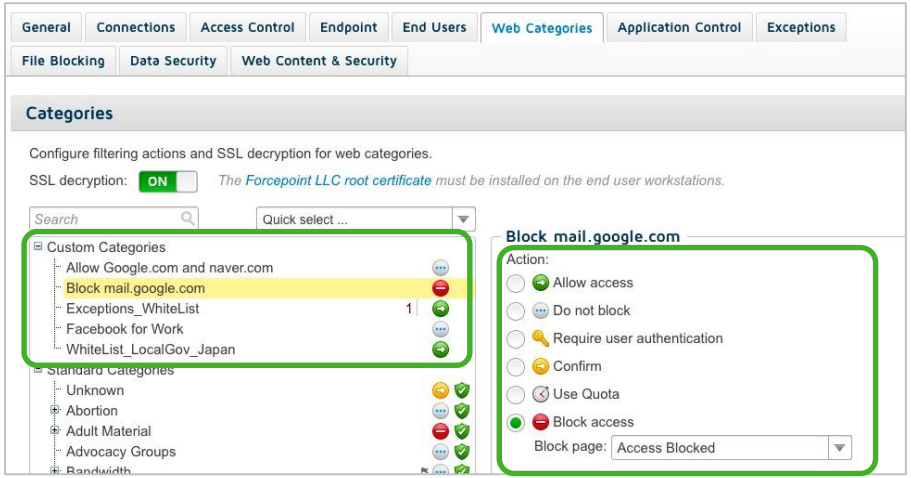
3-1. ブラックリスト、ホワイトリストの登録は
「Custom Categories」から CSVファイルで一括登録

その後、ウェブポリシー (Policies) から、各ポリシー毎に
カスタムカテゴリを設定

ブラックリスト ▸ ブロック (Block)

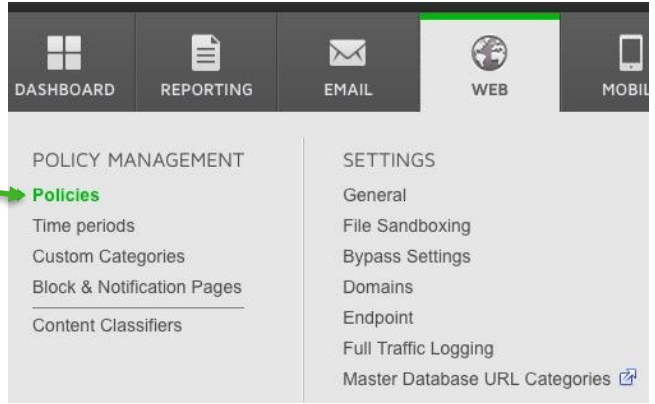
ホワイトリスト ▸ ブロックしない (Do not block) もしくは
アクセス許可 (Allow access)

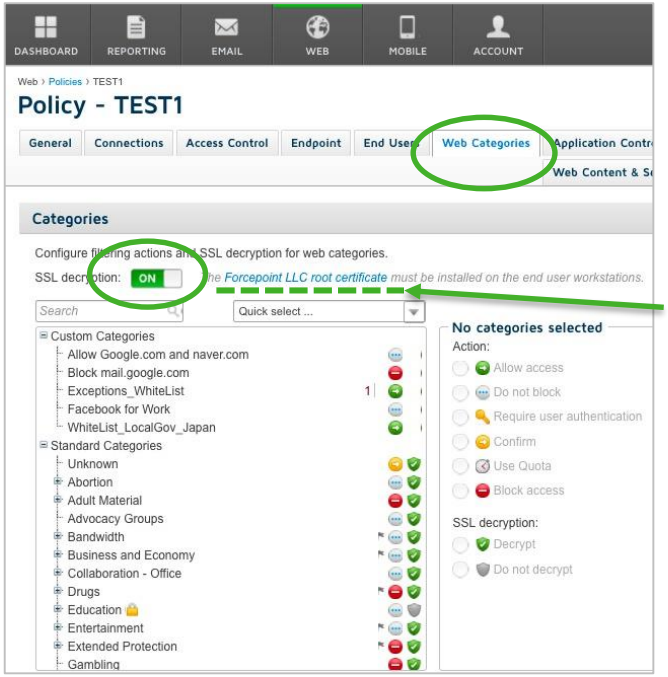




FORCEPOINT WEB SECURITY CLOUD 初期セットアップ 3

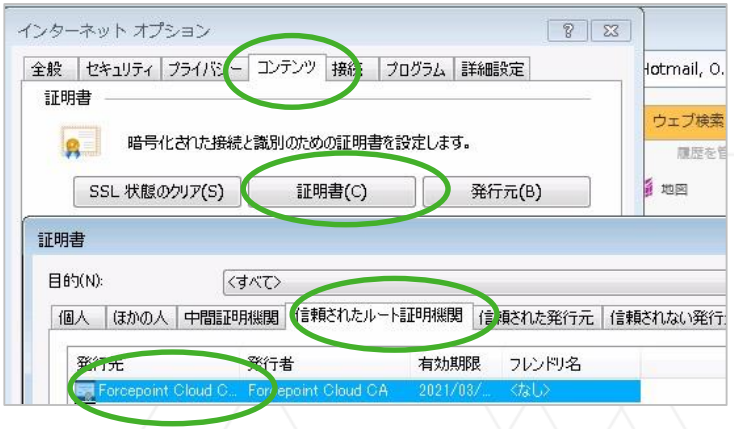
3) ウェブポリシーの編集
3-2. SSL復号化を実施する場合
ウェブポリシー設定画面から有効へ変更





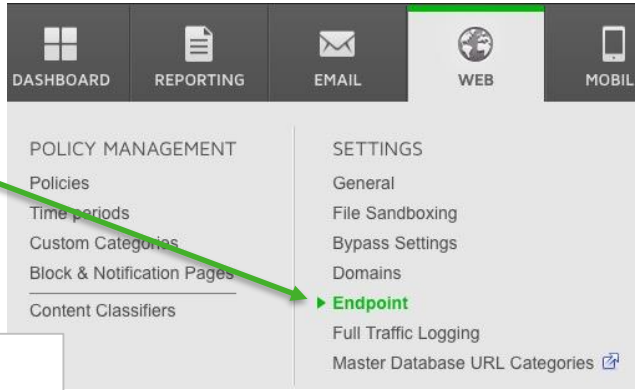
- ユーザのプライバシーを保護するため、カテゴリ毎のSSL非復号化設定も同時に設定を推奨

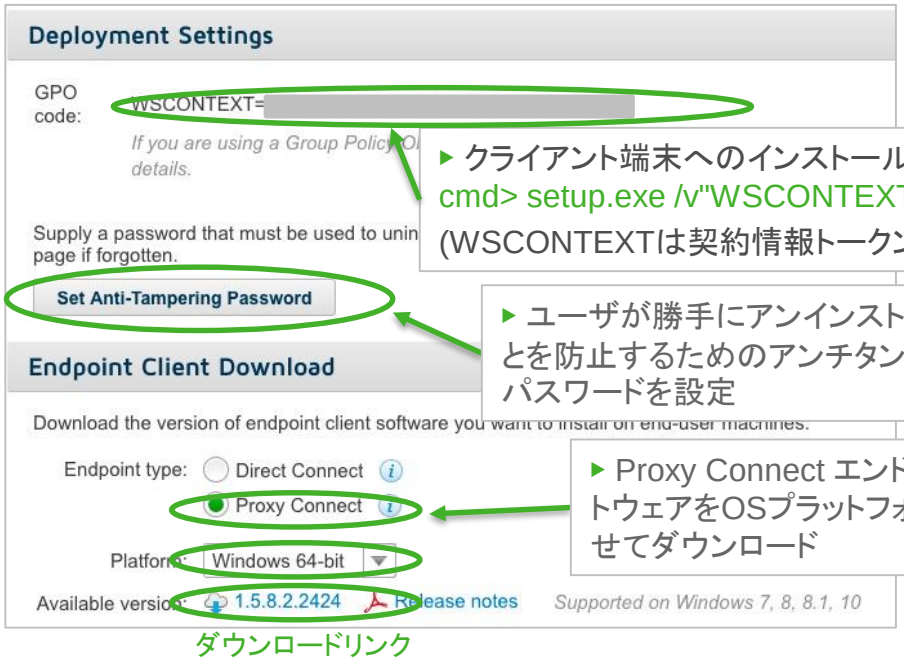
- SSL証明書を「http://www.mailcontrol.com/crl/wbsnca.crt」からcrtファイルをダウンロードしていただき、ブラウザの“ルート証明書”への登録してください



FORCEPOINT WEB SECURITY CLOUD 初期セットアップ 4

4) エンドポイントソフトウェアの導入
  4-1. エンドポイントソフトウェアのダウンロード
  4-2. クライアントへのインストールと確認



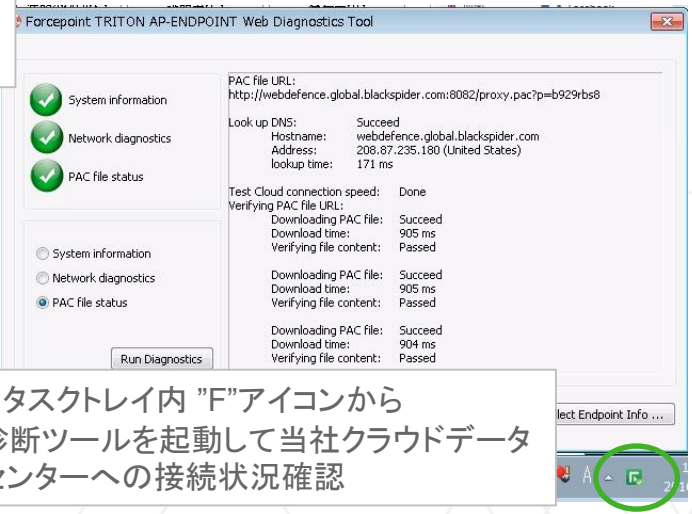


ダウンロードリンク

▸ クライアント端末へのインストールコマンド
cmd> setup.exe /v"WSCONTEXT=xxx-x"
(WSCONTEXTは契約情報トークンコードです)

▸ ユーザが勝手にアンインストールすることを防止するためのアンチタンパリング・パスワードを設定

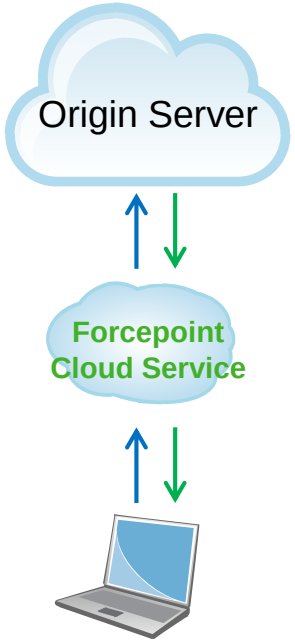
▸ Proxy Connect エンドポイントソフトウェアをOSプラットフォームにあわせてダウンロード



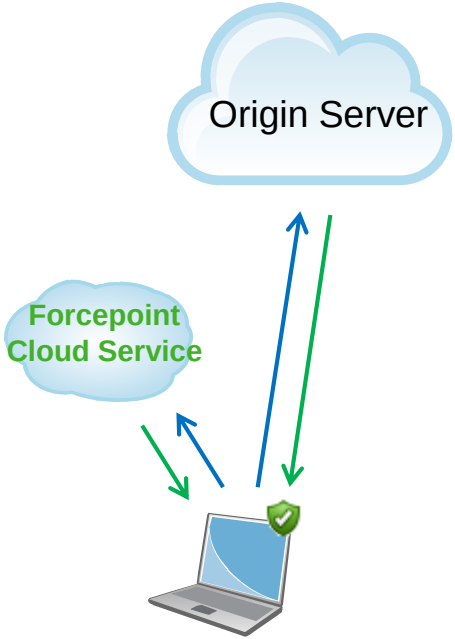
▸ タスクトレイ内 ”F”アイコンから診断ツールを起動して当社クラウドデータセンターへの接続状況確認

ご参考情報 FORCEPOINT 2種類の接続タイプ別 エンドポイント クライアント

プロキシ接続型 Proxy Connect (PCEP)



ウェブサイト直接続型 Direct Connect (DCEP)



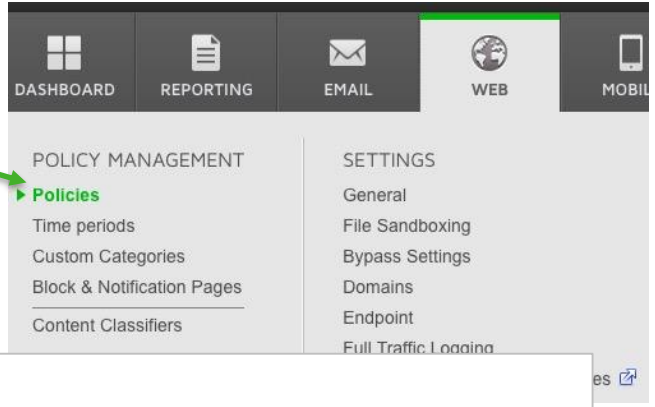
DCEPの特徴・制限事項

- PACファイル指定不要
- ポリシーはクラウドサービスから取得
- 不審なコンテンツのみクラウドサービスにアップロードして分析、悪性コンテンツはブロック
- ブラウザ以外は80・443ポートのみ対応
- ウイルススキャンなし
- DLP未対応 (別ソリューションのDLP Endpoint のご利用を推奨)
- Windows および macOS 対応

※ 通常は制限の少ない【Proxy Connect】のご使用を推奨しております。

FORCEPOINT WEB SECURITY CLOUD 初期セットアップ 5

5) ポリシーへのユーザ登録状況の確認



▸ このウェブポリシーの登録ユーザを確認

Web › Policies › TEST1

Policy - TEST1

General | Connections | Access Control | Endpoint | End Users | Web Categories | Application Control | Exceptions | File Blocking | Data Security | Web Content & Security

User Management

You can invite users who are unable to register themselves (for example, if they do not have email addresses in

Currently there are 4 registered users on this policy.

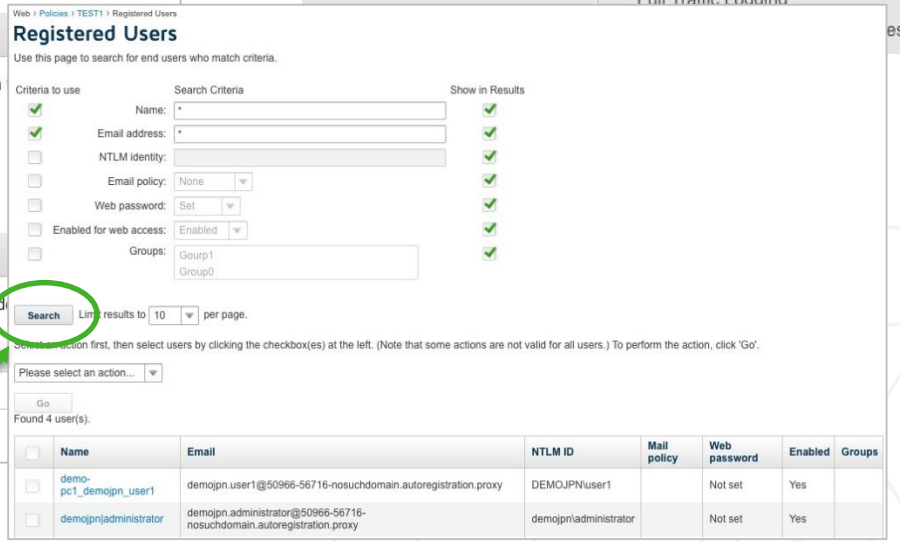
Invite an end-user | Bulk register end-users

Self Registration

Your end-users can register themselves with this policy if they have an email address on one of the configured d

Domain	Include Subdomains	All Policies
fp-jp.com	✔	

Add



▸ ”Search“から登録されているユーザを確認

テスト用 URL

- デフォルトのウェブポリシー設定でブロックされるウェブサイト

Gambling (ギャンブル)	hxxp://777 [dot] com/
Adult Content (アダルト)	hxxp://playboy [dot] com/
Malicious Web Sites (悪性ウェブサイト)	hxxp://www.eicar [dot] org/download/eicar.com.txt

- サンドボックスの動作確認サイト

hxxp://testdatabasewebsense [dot] com/threatscope/wbsn-ts-test-1_sbx_test.exe

Web Security Cloud サービスご利用いただける環境にある端末にて、ブラウザからこちらのURLへアクセスします。
アクセスするとファイルはダウンロード成功しますが、サンドボックスへ送付された通知メールならびに解析結果の通知メールが届くことをご確認ください。
ご注意: 不正プログラム検出プログラムが動作している場合は、ダウンロードされた時点で、ウイルスとして検出されます。検出プログラムを事前に停止、もしくはアンインストールした端末にてテストしてください。

- ご参考: 当社カテゴリテストサイト

hxxp://testdatabasewebsense [dot] com/

※ 悪性サイトのため、httpをhxxpへ変更しております。また、一部 ”.” を [dot] へ変更しております。実際のアクセス時には変更してアクセスしてください。

目的どおりに動作しない場合はご相談ください。

ENDPOINTソフトウェアの導入が出来ない端末への対応 1

▸ Linuxサーバ プロキシ設定

エンドポイント製品を導入できないLinuxなどのサーバには、環境変数にプロキシサーバのアドレス、ならびにアクセスユーザ名・パスワードを設定し、サービス利用時にはベーシック認証を利用します。

Yumなど動作するアプリケーションでOSの環境変数を参照することができない場合は、個別に設定します。

- /etc/environment に追加
http_proxy="http://ユーザ名:パスワード@webdefence.global.blackspider.com:8081/"
https_proxy="https://ユーザ名:パスワード@webdefence.global.blackspider.com:8081/"

- /etc/yum.conf に追加
proxy=http://ユーザ名:パスワード@webdefence.global.blackspider.com:8081

Tips: ユーザ名 = メールアドレスです。@ は “&40” に置き換えて設定します
例) maobara@forcepoint.com
→ tamano&40forcepoint.com

【ご参考 確認方法】
$ curl -v --proxy http://ユーザ名:パスワード@webdefence.global.blackspider.com:8081 -L http://www.hostname.com

【ユーザ名:パスワード@ を含むプロキシを設定できない場合】
ユーザ名がログに記録されなくなるため、発信者の特定ができなくなりますが、Web Security Cloudのポリシー設定において、認証を迂回させることが可能です。認証迂回設定をご参照ください。

ENDPOINTソフトウェアの導入が出来ない端末への対応 2

▶ 認証迂回設定

未登録ユーザなど認証できない社内からのアクセス時には、Firewallの出口IPを登録いただくことで、特定のウェブポリシーを適用することが出来ます。

注意点

・IPアドレス 1つあたりの適用可能なウェブポリシー数は1つとなります。

・エンドポイント利用時、ベーシック認証やセキュアフォーム認証などでユーザが特定できる場合は、そのエンドユーザが割り当てられたポリシーが優先されます。

【設定方法】

1) 特定のGlobal IP (通常はFirewallのインターネット側のIPアドレス) を Web > Policies > “特定のポリシー名” > Connection タブ内、Proxied Connections に登録

2) Web > Policies > “特定のポリシー名” > Access Control タブ内、ラジオボタンを次の項目に設定

Only authenticate when:

Connection is from an unknown IP address.

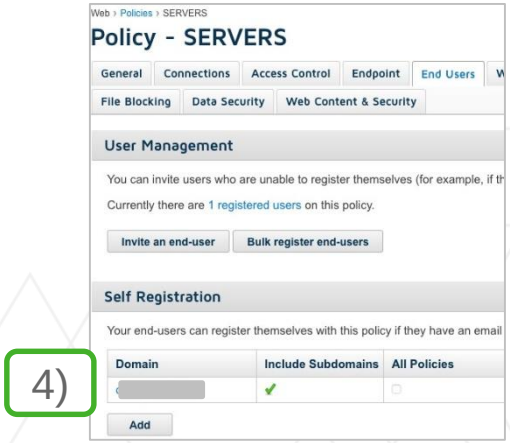
Requested site is in a Web category that requires user authentication.

他のチェックボタン外す

3) Web > Policies > “特定のポリシー名” > Endpoint タブ内、Endpoint Installation

Deploy endpoint software on user machines for: のチェックを外す

4) Web > Policies > “特定のポリシー名” > End Users タブ内、Self Registration に Windows ドメイン名 (例 xxx.local など) を登録



ENDPOINTソフトウェアの導入が出来ない端末への対応 3

▸ ベーシック認証やセキュアフォーム認証を利用するユーザの登録

先にご紹介しましたLinuxサーバなどENDPOINTソフトウェアの導入ができない端末向けに、ユーザ追加とパスワードの設定をお願いいたします。

【前提】ベーシック認証のユーザにパスワードを設定するためには、パスワード設定を通知するメールアドレスが必要です。

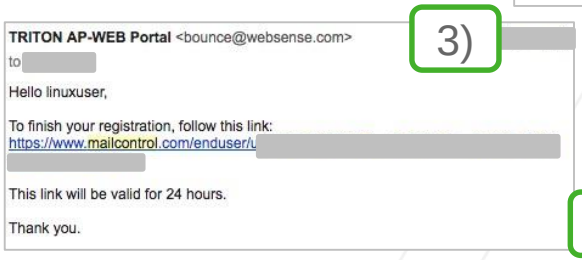
【設定方法】

1) Web > Policies > “特定のポリシー名” > End Users タブ内、
User Management から Invite an end-user を選択します
(複数ユーザを一度に登録する際には Bulk register end-users を選択)

2) Name: (登録名 (スペースなしが望ましい))、
Email Address: (メールアドレス) を入力し ”Save” 保存します

3) 2) で設定したメールアドレス宛てに パスワード設定画面が届きます

4) 届いたワンタイムURLにアクセスしてパスワードを設定します
※ ここで設定したパスワードをプロキシサービス利用時のパスワードとしてお使いいただきます
※ 3) 4) は日本語表示へ設定いただくことが出来ます
Web > Block and Notification Pages から設定します



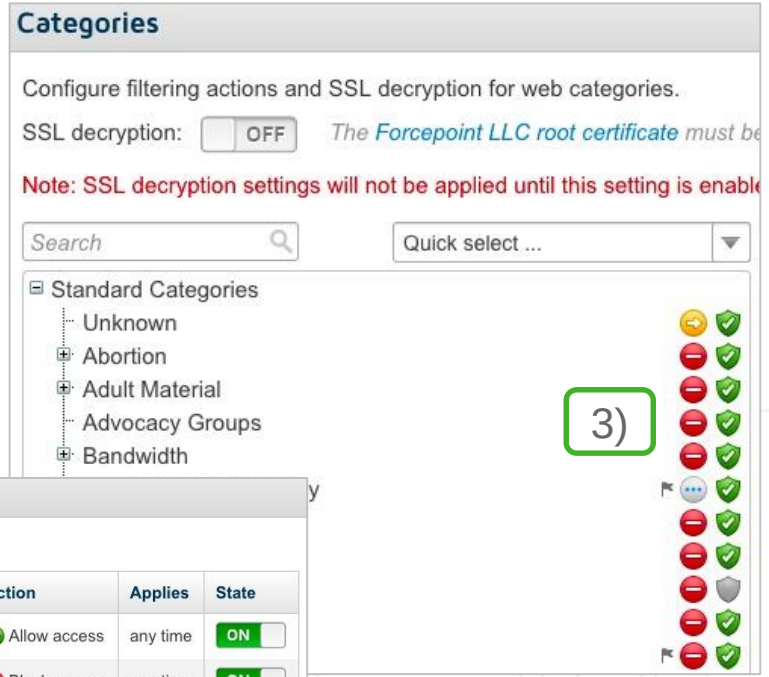
ユーザ毎の個別ウェブポリシー設定も出来ます

ユーザ認証ができる環境では、個別にアクセス先を設定することが出来ます。「Exception」(例外) 設定 と呼びます。サーバからのアクセスは原則禁止にしたいが、特定の業務サイトやソフトウェア等の更新に必要なサイトへのアクセスを許可したい、といった使用方法に有効です。

【設定方法】
1) Web > Custom Categories へ “ホワイトリスト” を作成、登録

2) Web > Policies > “特定のポリシー名” > Web Categories タブ内、
Category Exceptions にユーザ別の除外設定内容を入力
- アクションに アクセスを許可 Allow access を指定
- 1) で設定した カスタム・カテゴリ名を指定
- 例外設定対象の「ユーザ」もしくは「グループ」を指定

3) Web > Policies > “特定のポリシー名” > Web Categories タブ内、
Categories の Standard Categories は ブロック Block Access を選択



[Tips] ”Allow access” として設定されたサイトも、セキュリティ上の問題の有無をリアルタイムにコンテンツをチェックしますので、突然のサイト改ざんなどのセキュリティ・インシデント時にはブロックされます。

製品ドキュメント ご参考情報

ご紹介した内容は、一般的なトライアル環境でのご評価時に必要な設定情報をまとめたものです。
その他にも様々な設定がございます。あわせて製品ドキュメントもご参照ください。

- 製品ドキュメント・FAQなど

当社サポートサイト https://support.forcepoint.com
Documentation > All Documents > WEB SECURITY > Forcepoint Web Security Cloud
All versions からご確認いただけます

直リンク:
https://support.forcepoint.com/DocumentsDisplayed?version=All%20versions&name=Forcepoint%20Web%20Security%20Cloud

お困りなことがございましたら、遠慮なく当社営業・SEまでご相談ください。

www.forcepoint.com/ja

fb.com/ForcepointJapan

@ForcepointJP