FortiGateVer.6.0 MR4 Patch2

Information 資料

株式会社ネットワークバリューコンポネンツ
NETWORK VALUE COMPONENTS

目次

1. はじめに ..... – 1 –
2. アップグレードパス ..... – 1 –
3. サポート機種 ..... – 2 –
3.1 SPECIAL BRANCH SUPPORTED MODELS ..... - 2 -
4. アップグレード注意事項 ..... – 3 –
4.1 CAPWAP TRAFFIC OFFLOADING ..... - 3 -
4.2 FORTICLIENT (MAC OS X) SSL VPN REQUIREMENTS ..... - 3 -
4.3 USE OF DEDICATED MANAGEMENT INTERFACES (MGMT1 AND MGMT2) ..... - 3 -
4.4 TAGS OPTION REMOVED FROM GUI ..... - 4 -
4.5 SYSTEM ADVANCED MENU REMOVAL (COMBINED WITH SYSTEM SETTINGS) ..... - 4 -
4.6 PCI PASSTHROUGH PORTS ..... - 4 -
4.7 FG-80E-POE AND FG-81E-POE POE CONTROLLER FIRMWARE UPDATE ..... - 5 -
4.8 AWS-ON-DEMAND IMAGE ..... - 5 -
4.9 POLICY ROUTING ENHANCEMENTS IN THE REPLY DIRECTION ..... - 5 -
5. CHANGES IN CLI ..... – 6 –
6. CHANGES IN GUI BEHAVIOR ..... – 8 –
7. CHANGE IN DEFAULT BEHAVIOR ..... – 9 –
8. CHANGE IN DEFAULT TABLE SIZE ..... – 10 –
9. NEW FEATURES OR ENHANCEMENTS ..... – 11 –
10. アップグレードに関して ..... – 16 –
10.1 DEVICE DETECTION CHANGES ..... - 16 -
10.2 FORTICLIENT ENDPOINT TELEMETRY LICENSE ..... - 16 -
10.3 SECURITY FABRIC UPGRADE ..... - 16 -
10.4 MINIMUM VERSION OF TLS SERVICES AUTOMATICALLY CHANGED ..... - 17 -
10.5 DOWNGRADING TO PREVIOUS FIRMWARE VERSIONS ..... - 18 -
10.6 AMAZON AWS ENHANCED NETWORKING COMPATIBILITY ISSUE ..... - 18 -
10.7 FORTILINK ACCESS-PROFILE SETTING ..... - 19 -
10.8 FORTIGATE VM WITH V-LICENSE ..... - 19 -
10.9 FORTIGUARD UPDATE-SERVER-LOCATION SETTING ..... - 20 -
10.10 FORTIVIEW WIDGETS ..... - 20 -
10.11 WANOPT CONFIGURATION CHANGES IN 6.4.0 ..... - 20 -

10.12 IPSEC INTERFACE MTU VALUE ..... - 21 -
10.13 VIRTUAL WAN LINK MEMBER LOST ..... - 21 -

11. 各 FORTINET 製品とのサポートについて ..... – 22 –

11.1 FORTIANALYZER ..... - 22 -
11.2 FORTIMANAGER ..... - 22 -
11.3 FORTICLIENT ..... - 22 -
11.4 FORTISWITCH ..... - 23 -
11.5 FORTIAP/FORTIAP-S ..... - 23 -
11.6 FORTISANDBOX ..... - 23 -

12. 動作環境 ..... – 24 –

12.1 推奨 WEB ブラウザについて ..... - 24 -
12.2 EXPLICIT WEB PROXY のブラウザサポートについて ..... - 24 -
12.3 SSL-VPN (WEB モード)のサポートについて ..... - 25 -
12.4 VM プラットフォーム ..... - 26 -

1. はじめに

本マニュアルは FortiGate の OS バージョンを弊社提供バージョンの Ver6.0 MR4 Patch2 へアップグレードする際の注意事項について記載しています。
具体的なアップグレード手順については、以下の手順書を参照ください。
https://gold.nvc.co.jp/document/fortinet/tech/tech_doc/FortiGate アップグレード手順書.pdf

2. アップグレードパス

現在ご利用の OS バージョンによっては、バージョンアップを段階的に行う必要がございます。下記のアップグレードパスサイトをご参照いただき、ご利用バージョンに合わせたアップグレード手順を行ってください。

https://docs.fortinet.com/upgrade-tool
※FortiOS 5.2.9 以前の OS からアップグレードする際は、一度 5.2.9 までアップグレード頂いた後、アップグレードパスに従いバージョンアップを実施ください。

3. サポート機種

FortiOS Ver6.0 MR4 Patch2 をサポートしている機種は下記の通りです。

機器シリーズ	機器
FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-5001D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
FortiWiFi	FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-61E
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

3.1 Special branch supported models

以下のモデルは、FortiOS 6.0 MR4 Patch2 の特別ブランチでリリースされています。 正しいビルドを実行されていることを確認するには、CLI コマンド「get system status」を実行して、Branch point フィールドに該当のビルド番号が表示されていることを確認します。

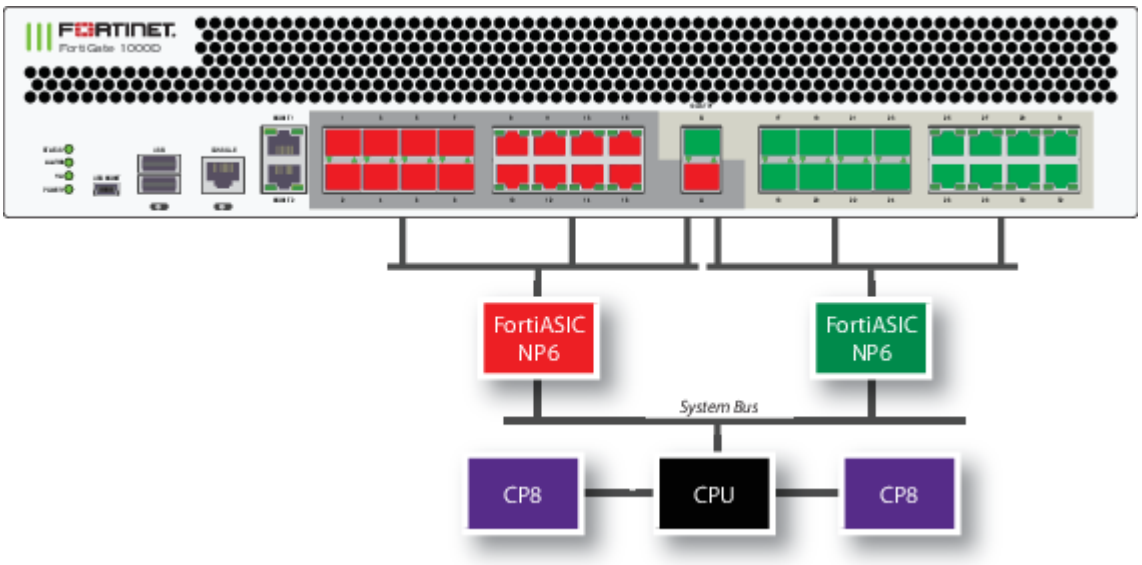
機種	ビルド番号
FWF-40F	is released on build 5323.
FWF-40F-3G4G	is released on build 5323.
FWF-60F	is released on build 5323.
FWF-61F	is released on build 5323.

4. アップグレード注意事項

4.1 CAPWAP traffic offloading

入力インタフェースと出力インタフェースが異なる NP6 チップ上にある場合、CAPWAP トラフィックは NP にオフロードされません。以下のモデルが影響を受ける可能性がございます。

機器シリーズ	対象機器
FortiGate シリーズ	FGT-900D, FGT-1000D, FGT-2000E, FGT-2500E



FortiGate-1000D の SPU 配置

4.2 FortiClient (Mac OS X) SSL VPN requirements

Mac OS X 10.8 で SSL VPN を使用するときは、FortiOS で SSLv3 を有効にする必要があります。

4.3 Use of dedicated management interfaces (mgmt1 and mgmt2)

最適な安定性を得るために、管理トラフィック専用の管理ポート（mgmt1 および mgmt2）を使用してください。 一般のトラフィック処理用途で管理ポートを使用しないでください。

4.4 Tags option removed from GUI

タグオプションは GUI から削除されます。これには次のものが含まれます。
・「システム > タグ」ページを削除
・「タグ」セクションがすべてのページから削除
・「タグ」カラムがあったすべてのページから削除

4.5 System Advanced menu removal (combined with System Settings)

Bug ID	Description
584254	・[システム]> [詳細]メニューを削除しました（ほとんどの機能を[システム]> [設定]ページに移動しました） ・構成スクリプトのアップロード機能をトップメニュー>構成>スクリプトページに移動しました。 ・自動スクリプト構成の GUI サポートを削除しました（この機能は引き続き CLI でサポートされます)。 ・すべてのコンプライアンステストをセキュリティレーティングテストに変換しました。

4.6 PCI passthrough ports

Bug ID	Description
605103	PCI パススルーポートの順序は、アップグレード後に変更される場合があります。 SR-IOV ポートはデフォルトで MAC オーダーであるため、これは VMXNET3 および SR-IOV ポートには影響しません。

4.7 FG-80E-POE and FG-81E-POE PoE controller firmware update

FortiOS 6.4.1 はバグ 570575 を解決し、ポートに電力を供給できない FortiGate を修正しました。 解決された問題のセクションを参照してください。ただし、PoE ハードウェアコントローラーでは、CLI を使用して実行する必要のある更新が必要になる場合があります。 このコマンドが正常に実行されると、PoE ハードウェアコントローラーのファームウェアが最新バージョン 2.18 に更新されます。

diagnose poe upgrade-firmware

4.8 AWS-On-Demand image

Bug ID	Description
589605	FortiOS 6.4.0 以降、FGT-VM64-AWSONDEMAND イメージは提供されなくなりました。 AWSPAYG モデルと AWSBYOL モデルの両方が、同じ FGT-VM64-AWS イメージを共有します。

4.9 Policy routing enhancements in the reply direction

応答トラフィックが FortiGate に入り、ポリシールートまたは SD-WAN ルールが設定されている場合、出力インタフェースは次のように選択されます。

・構成システム設定で補助セッションが有効になっている場合

6.4.0 以降、応答トラフィックは、出力インタフェースとネクストホップを決定するためのポリシールートまたは SD-WAN ルールと一致しなくなります。

この変更の前は、応答トラフィックは、出力インタフェースとネクストホップを決定するためにポリシールートまたは SD-WAN ルールと一致します。

・構成システム設定で補助セッションが無効になっている場合

応答トラフィックは、元の着信インタフェースで出力されます。

5. Changes in CLI

以下の内容が変更されています。

Bug ID	Description
614892	wtp-profile の spectrum-analysis と wtp の override-analysis が削除されます。
621751	FortiSwitch LACP トランクは、同じ速度にネゴシエートされたポートがアグリゲーターにグループ化されます。 aggregator-mode 設定を使用すると、ユーザは帯域幅またはリンク数に基づいてアグリゲーターを選択できるようになります。 config switch-controller managed-switch edit <serial_number> config ports edit <port> set mode lacp-passive set aggregator-mode {bandwidth | count} next end next end
639237	EMS サーバは、IP アドレスに加えて MAC アドレスを使用して動的アドレスを生成できるようになります。 スイッチコントローラの NAC ポリシーは、一致条件として EMS からの MAC ベースの動的ファイアウォールアドレスを参照できます。 config firewall address edit <name> set type dynamic set sub-type ems-tag set obj-type [ip | mac] next end config user nac-policy edit <ID> set category ems-tag set ems-tag <address> next end

643514	hold-time オプションを使用すると、ユーザは FortiGuard IPS シグニチャの更新後にシグニチャを保持するための保留時間を時間または日単位で設定できます。 保留期間中、シグニチャのアクションはモニターになります。 config system ips set signature-hold-time <##d##h> set override-signature-hold-by-id <enable|disable> end
643831	ユーザが CVEID（CVE-YYYY-NNNN）または CVE ワイルドカード（CVE-YYYY）に基づいて IPS シグニチャをフィルタリングできるようになります。 config ips sensor edit "cve" config entries edit 1 set cve <CVE ID or Wildcard> next end next end

6. Changes in GUI behavior

以下の内容が変更されています。

Bug ID	Description
516031	セキュリティプロファイルに関する次の動作が変更されます。 ・Feature Visibility>Multiple Security Profiles オプションを削除します。 ・すべてのセキュリティプロファイルは、デフォルトで複数のプロファイルを許可します。 ・すべてのセキュリティプロファイルページは、プロファイルのリストになります。
634719	Optimal ダッシュボード設定と comprehensive ダッシュボード設定を切り替えるオプションが追加されます。 このオプションは、古い FortiOS ビルドからアップグレードするとき、または新しいユーザとしてログインするときに、ログインプロンプトで使用できます。 その後は、左側のナビゲーションバーにあるすべてのダッシュボードをリセットオプションからいつでもアクセスできます。 Optimal は、一連のデフォルトダッシュボードと、簡素化された FortiView ページの選択が提供されます。 comprehensive は、ダッシュボードのセットと、以前の FortiOS バージョンに存在していたすべてのモニターページと FortiView ページで構成されます。
643505	ハブアンドスポーク VPN ウィザードで、複数のローカルインターフェイスを選択する機能、変更を確認する手順、およびトンネルの作成時にリアルタイムの更新を追加します。 VPN ダイアログ内に、ハブアンドスポークトポロジセクションを追加して、各スポークの簡単なキーと、スポークを追加する機能を表示します。

7. Change in default behavior

以下の内容が変更されています。

Bug ID	Description
630433	ローカルカテゴリとリモートカテゴリのオーバーライドをプロファイルレベルで制御できるようになります。プロキシモードでは、webfilter プロファイル、ssl-exempt、および proxy-address は、ローカルカテゴリとリモートカテゴリの処理で同様の動作をします。たとえば、ローカルカテゴリでは次のようになります。 ・6.0.x、6.2.x、6.4.0、および 6.4.1 では、ホストがローカル評価でカテゴリ 140 として構成されると、ホストは常にグローバルレベルまたは VDOM レベルで 140 として評価されます。それを制御するためのプロファイルレベルのオプションはありません。 ・6.4.2 では、ホストは、そのカテゴリが Web フィルタプロファイルで明示的に設定されている場合にのみ、設定されたローカルレーティングとしてレーティングされます。このオーバーライドは、webfilter profile, ssl- exempt、および proxy-address に適用できます。 次に、Web フィルタプロファイルの設定例を示します。 config webfilter profile edit webf-use-local-rating config ftgd-wf config filters edit 1 set category 140 set action monitor next end end next end webfilter profile, ssl- exempt、および proxy-address の評価は、互いに独立しています。 GUI では、Web フィルタプロファイルを編集するときにローカル/リモートカテゴリの許可アクションは、ローカル/リモートカテゴリのオーバーライドを無効にするためのショートカットです。 フローモードの場合、webfilter profile のみが関係し、変更が IPS エンジンにあるため、動作が異なります。 ・6.2.5 および 6.4.2 では、ローカル/リモート評価は、カテゴリが webfilter profile で有効になっている場合にのみ有効になります。 ・6.2.1-6.2.4 および 6.4.0-6.4.1 では、現在、ローカル/リモートの評価はグローバルレベルまたは VDOM レベルです。次の IPS エンジンの公開リリース後、動作は 6.2.5 /6.4.2 と同じになるように変更されます。

	フローモードおよび NGFWURL カテゴリを使用する FortiGuard の ssl-exempt に変更はありません。

8. Change in default table size

以下の内容が変更されています。

Bug ID	Description
609785	FG-1100E / 1101E プラットフォームの switch-controller.managed-switch スケール番号を 128 から 196 に変更されます。
626765	FG-60F / 61F および FWF-60F / 61F の合計 WTP サイズが 64 に増加されます。

9. New features or enhancements

以下の内容が変更されています。

Bug ID	Description
480717	mgmt、mgmt1、および mgmt2 ポートを備えたすべての FortiGate モデルに configure system dedicated-mgmt が追加されます。
555169	FortiToken Cloud GUI の機能強化： ・FortiToken Cloud のバランスがマイナスの場合の警告メッセージが追加されます。 ・FortiToken Cloud ユーザ数がクォータを超えたときの警告メッセージが追加されます。 ・メールと SMS の設定を 2FA セクションに移動されます。 ・ユーザ定義、ユーザーグループ、TACACS +、および FortiToken の CSF サポートが追加されます。
556054	CIFS メッセージで使用される新しく追加された圧縮方法により、FortiGate はこれらの圧縮メッセージをプロキシモードでスキャンできるようになりました。
562031	ファイアウォールセキュリティポリシーの下で設定できるセキュリティポリシーsrcaddr-negate および dstaddr-negate オプションをサポートします。 config firewall security-policy edit <policyid> ... set srcaddr-negate[enable|disable] set dstaddr-negate [enable|disable] ... next end
573076	FortiGate は、管理対象の FortiAP（WTP エントリ）ごとに UUID を生成します。新しい BLE プロファイルである fortiap-discovery は、FortiAP デバイス上での iBeaconUUID の展開を容易にします。
589621	新しい Azure オンデマンドインスタンスとアップグレードされたインスタンスは、FortiCare サーバから FortiGate のシリアル番号とライセンスを取得できます。シリアル番号を使用して、ユーザはデバイスを自分のアカウントに登録し、FortiToken および FortiGate クラウドサービスの使用を開始できます。
596002	FortiOS エンタープライズ MIB に 2 つの新しいテーブルが追加されます。接続された FortiSwitch の詳細については FgSwDeviceEntry、ポート関連の情報については FgSwPortEntry を参照してください。

596870	IEEE 802.1ad（QinQ）標準のカーネルサポートが追加されます。以前は、802.1Q 標準では、単一の VLAN ヘッダーをイーサネットフレームに挿入できました。新機能により、もう 1 つの VLAN タグを 1 つのフレームに挿入できます。
597301	シリアル番号、IP アドレス、インスタンス ID、トランジットゲートウェイ（AWS のみ）など、自動スケールメンバーに関する情報を GUI および CLI に表示されます。
600037	FAP-U431F / U433F（802.11ax AP）での BSS カラーリングがサポートされます。
606167	スイッチコントローラでネットワークモニタ機能が有効になっている場合、update-user-device オプションを使用すると、デバイス情報を収集するソースをきめ細かく制御できます。情報は FortiGate デバイスリストに入力されます。
608557	プッシュサービス用のプロキシサーバーがサポートされます。
610596	ユーザは IPv6MAC アドレスを定義し、ファイアウォールポリシー、仮想ワイヤペアポリシー、およびその他のポリシータイプに適用できます。
610990	FortiOS Carrier で GTPv1 と GTPv2 の IPv6 のみと IPv4v6 デュアルスタックサポートが追加されます。
614924	ユーザは、侵害されたホストまたは着信 Webhook のトリガーを設定するときに、FortiNAC アクションを介して隔離を使用して自動化を構成できます。自動化がトリガーされると、クライアント PC は、構成された FortiNAC で MAC アドレスが無効になっている状態で隔離されます。
617640	動的ファイアウォールアドレスで Azure SDN コネクタに新しいフィルターキーservicetag と region を追加して、サービスタグの IP 範囲をフィルターで除外が適用できます。
620994	3 つの無線を備えた FortiAP モデルの場合、スペクトル分析は、2.4GHz および 5GHz 帯域のすべてのチャネルの 3 番目の無線で実行できます。 AP モードで動作する 2 つの無線を備えた FortiAP では、動作チャネルでスペクトル分析を実行できます。
621714	両端間でタイミング精度を通信するために、トランスペアレントクロックを有効にして全体的なパス遅延を測定できます。この機能により、FortiGate はサポートされている FortiSwitch モデルに対してこの設定を構成できます。
621742	単一の RADIUS アクセス要求内で複数の RADIUS 属性値を送信するように FortiSwitch を構成するためのサポートが追加されます。
621746	管理対象の FortiSwitch の explicit congestion notification（ECN）構成がサポートされます。
621757	管理対象の FortiSwitch で高速 PVST＋との相互運用性を有効にするようにスイッチポートを構成するためのサポートが追加されます。
622291	ヘルスメトリクスの計算はバックエンドで標準化されており、一貫した色を使用して、good, fair、および poor のメトリックを表します。さらに、ヘルスデータが REST API を介して利用できるようになります。
623821	FortiGate のイーサネットインターフェースに接続されている FortiAP のブリッジ SSID に関連付けられている WiFi クライアントの場合、DHCP モニターウィジェットは、それらのクライアントの IP リースのインタフェース列に AP ブリッジと SSID 名を示すことができます。 config wireless-controller vap

	edit VAP01 set dhcp-option43-insertion {enable | disable} next end デフォルトでは、dhcp-option43-insertion は有効に設定されています。 FAP-U に必要な最小バージョンは 6.0.3 です。 FAP-W2 に必要な最小バージョンは 6.4.1 です。
629530	IBM Cloud プラットフォームの BYOL FortiGate VM の実行がサポートされます。
630238	system standalone-cluster で最大 16 の FGSP スタンドアロンピアの設定が許可されます。
630881	FortiSwitch ネットワークをテストし、セットアップを最適化するための推奨事項を作成するために、さまざまな新しいシナリオがセキュリティ評価に追加されます。
631818	新しい OID を追加して、IPv4 および IPv6 IPsec トンネルの SNMP クエリ、およびライセンスの詳細の SNMP クエリがサポートされます。
635717	FortiAP アンテナ（Rx チェーンごと）のステータスを監視し、アンテナの欠陥が検出されたときにワイヤレスイベントをログに記録します。
635795	ARRP プロファイルは、FortiAP 間のチャネル選択を最適化するために考慮できる要素を増やすことにより、DARRP が改善されます。
637508	CLI コマンドを追加して、WAD デバッグが改善されます。 ・diagnose wad memory report は、diagnose test app wad {2 3 803 21 22 23 25 27 70 120123}に示されている統計を含むすべてのワーカーのメモリ関連の統計を出力します。 ・diagnose wad memory monitor はワッドメモリ使用量を監視します。 WAD メモリ使用量は定期的にチェックされ、WAD メモリ使用量がしきい値を超えた場合にレポートが生成されます。 ・diagnose wad debug crash {enable | disable}は、WAD がクラッシュしたときに表示され、デバッグメッセージにファイルを保存します。 ・diagnose wad debug crash list には、すべてのクラッシュログが一覧表示されます。 ・diagnose wad debug crash read <proc_type> <id>は特定のクラッシュログを読み取ります。
637829	FortiMail の証明書を使用した標準の認証手順で、セキュリティファブリックへの FortiMail の追加がサポートされます。セキュリティファブリックの一部として、FortiMail はファブリックナビゲーション、トポロジ、ファブリックウィジェット、およびセキュリティ評価の配下に表示されます。
637946	以前の slide-out ターミナルをフルページマスキングターミナルと置き換えられます。管理者が最小化できる複数の CLI コンソールを開くことを許可します。
638975	SD-WAN とポリシールートにより、ユーザはデバイスの MAC アドレスオブジェクトをソースとして選択できるようになります。さらに、FABRIC_DEVICE オブジェクトは SD-WAN およびポリシールートでも使用できます。
639590	NGFW モードでは、セキュリティポリシーでアプリケーション、アプリケーションカテゴリ、またはアプリケーショングループが選択され、ログトラフィックが UTM またはすべてに設定されている場合、アプリケーション制御ログが生成されます。さらに、セキュリティポリシーの下で 1 つ

	の署名が受け入れられると、すべての子シグネチャーが評価され、それに応じてログに記録されます。
640563	FortiLink インタフェースを 1 つのインタフェースに制限するデフォルトのコマンドが削除されます。 CLI から複数のインタフェースで Fort インタフェースになっている場合、GUI は複数の FortiLink インタフェースを表示するようになります。
641152	新しい帯域幅制限付き VM ライセンスにより、インタフェースごとの帯域幅使用量が制限された VM 展開が可能になります。専用の管理インタフェースは計算から免除されます。
641928	BGP の ECMP ネクストホップが再帰的距離を使用して、インストールする必要があるものを決定できるかどうかを制御するオプションが追加されます。 config router bgp set multipath-recursive-distance {enable | disable} end ネクストホップが接続されたルートによって解決される場合、その距離は 0 になります。別のルートによって解決される場合、その距離はそのルートと同じになります。このオプションを有効にすると、最短のネクストホップのみが ECMP ルートを形成し、カーネルにインストールできます。
641990	diagnose wad session list コマンドは、WANopt をサポートしていないモデルで使用できます。
642898	次のオプションは、NGFW ポリシーモードのフローベースの Web フィルタセキュリティプロファイルで設定可能であり、セキュリティポリシーに適用できます。 ・無効な URL をブロック ・静的 URL フィルター ・FortiSandbox で発見された悪意のある URL をブロック ・コンテンツフィルタ
643616	FortiAP をサポートして、FortiGate を介して FortiGuard IoT サービスにクエリを実行し、デバイスの詳細が決定されます。
643912	VIP を FQDN アドレスにマップする必要がある場合、GUI から設定できます。
644049	SSID ごとの複数の事前共有キーの拡張機能には、MPSK キーのバッチ生成またはインポート、CSV へのキーのエクスポート、使用される MPSK に基づく VLAN の動的割り当て、および GUI での MPSK スケジュールの適用が含まれます。
645140	セッションを相互に関連付けるために、GTP 関連トラフィックのトラフィックログと GTP ログにトンネル ID が追加されます。
648568	6.4.0 で追加されたサーバに加えて、GeoIP、DDNS、および FortiToken Mobile 登録用の FortiGuard サーバは、OCSP ステープリングを使用したサードパーティの CA 署名付き証明書をサポートするようになります。
648604	GTP のユーザーロケーション情報（ULI）の場合、異なるタイプの ID が複数含まれている可能性があります。このログ拡張により、GTP ログ内のすべての ID 情報が表示されます。
651206	ダウンストリームの FortiGate の GUI を使用すると、ユーザはファブリックルートデバイスにログインして、保留中の参加要求を承認できます。

	CLI では、この機能をサポートするために、VAP 構成の下に dhcp-option43-insertion が追加されています。

10. アップグレードに関して

10.1 Device detection changes

FortiOS 6.0 ではデバイス検知機能に以下の構成が含まれています。
・Visibility：検出された情報は、トポロジの可視性とロギングに利用できます。
・FortiClient endpoint compliance：FortiClient から学習した情報を使用して、これらのエンドポイントのコンプライアンスを実施できます。
・Mac-address-based device policies：検出されたデバイスは、カスタムデバイスとして定義し、デバイスベースのポリシーで使用できます。

FortiOS 6.2 では以下のように変更されます。
・Visibility：変更はありません。
・FortiClient endpoint compliance：新しいファブリックコネクタに置き換わります、動的ポリシーのために他のすべてのエンドポイントコネクタと整合します。（FortiClient EMS）
・Mac-address-based device policies：FW アドレスに Mac アドレス範囲が設定できるようになります。これにより、以前のデバイスポリシー機能は、通常のポリシーで実現できるようになります。
6.0.x でデバイスポリシーを使用していた場合は、アップグレード後にこれらのポリシーを通常のポリシーテーブルに手動で移行する必要があります。
6.4.0 では、デバイス検出に関連する GUI 機能が再配置されます。

10.2 FortiClient Endpoint Telemetry license

FortiClient Endpoint Telemetry License が廃止され、FortiClient EMS に統合されます。

10.3 Security Fabric upgrade

Fortinet Security Fabric を構成している場合、以下の OS がサポート対象となります。

機器	OS
FortiAnalyzer	FortiAnalyzer 6.4.1
FortiManager	FortiManager 6.4.1
FortiClient	FortiClient 6.4.1
FortiClient EMS	FortiClient EMS 6.4.0
FortiAP	FortiAP 6.4.0 以降
FortiSwitch	FortiSwitch 6.4.1 以降

※複数の FortiGate で Security Fabric 構成されている場合、ファブリック内のすべての FortiGate デバイスは同一である必要がございます。

10.4 Minimum version of TLS services automatically changed

セキュリティを向上させるために、FortiOS 6.2.0 は ssl-min-proto-version オプション（config system global）を使用して、FortiGate とサードパーティの SSL および TLS サービス間の通信に使用される最小 SSL プロトコルバージョンを制御するようになっております。
FortiOS 6.0 MR4 Patch2 以降にアップグレードした場合、デフォルトの ssl-min-proto-version オプションは TLS v1.2 になります。
以下の SSL および TLS サービスは、デフォルトとして TLS v1.2 を使用するためにグローバル設定を継承します。 これらの設定は個別の設定で上書き可能です。

・Email server (config system email-server)
・Certificate (config vpn certificate setting)
・FortiSandbox (config system fortisandbox)
・FortiGuard (config log fortiguard setting)
・FortiAnalyzer (config log fortianalyzer setting)
・LDAP server (config user ldap)
・POP3 server (config user pop3)

10.5 Downgrading to previous firmware versions

以前のファームウェアバージョンにダウングレードすると、すべてのモデルで設定が失われます。 以下の設定のみ保持されます。

・operation mode
・interface IP/management IP
・static route table
・DNS settings
・admin user account
・session helpers
・system access profiles

10.6 Amazon AWS enhanced networking compatibility issue

この拡張機能では、5.6.2 以前のバージョンの AWS 用 FortiGate VM との互換性の問題があります。 FortiOS 6.0 MR4 Patch2 イメージを 5.6.2 以前のバージョンにダウングレードすると、ネットワーク接続が失われます。 AWS はコンソールアクセスを提供しないため、ダウングレードされたイメージを復元することはできません。
FortiOS 6.0 MR4 Patch2 から 5.6.2 以前のバージョンにダウングレードする場合、拡張 NIC ドライバーの実行は許可されません。 次の AWS インスタンスが影響を受けます。

C5 / C5d / C5n / F1 / G3 / G4 / H1 / I3 / I3en / Inf1 / m4.16xlarge / M5 / M5a / M5ad / M5d / M5dn / M5n / P2 / P3 / R4 / R5 / R5a / R5ad / R5d / R5dn / R5n / T3 / T3a / u-6tb1.metal / u-9tb1.metal / u-12tb1.metal / u-18tb1.metal / u-24tb1.metal / X1 / X1e / z1d

回避策は、インスタンスを停止し、タイプを非 ENA ドライバーNIC に変更することです。

10.7 FortiLink access-profile setting

新しい FortiLink ローカルアクセスプロファイルは、FortiGate によって管理される FortiSwitch の物理インタフェースへのアクセスを制御します。FortiGate を 6.4.0 にアップグレードすると、すべての管理対象 FortiSwitch のインタフェースの allowaccess の設定が、デフォルトの FortiGate ローカルアクセスプロファイルによって上書きされます。6.4.0 にアップグレードした後、ローカルアクセスプロファイルにプロトコルを手動で追加する必要があります。

■ローカルアクセスプロファイルを設定する場合

```
config switch-controller security-policy local-access
    edit [Policy Name]
        set mgmt-allowaccess https ping ssh
        set internal-allowaccess https ping ssh
    next
end
```

■ローカルアクセスプロファイルを管理対象の FortiSwitch に設定する場合

```
config switch-controller managed-switch
    edit [FortiSwitch Serial Number]
        set switch-profile [Policy Name]
        set access-profile [Policy Name]
    next
end
```

10.8 FortiGate VM with V-license

FortiOS6.2 から V ライセンスを備えた FortiGate-VM で Split-vdom が有効にできます。

■split-vm の有効方法

```
config system global
    set vdom-mode [no-vdom | split vdom]
end
```

※split-vdom の詳細については https://docs.fortinet.com/document/fortimanager/6.2.0/new-features/744923/split-task-vdom-mode-support をご確認ください。

10.9 FortiGuard update-server-location setting

FortiGuard のシグネチャアップデート等で利用される FortiGuard サーバに接続する際に、update-server-location のデフォルト設定は、ハードウェアプラットフォームと VM で異なります。ハードウェアプラットフォームの場合、デフォルトは any です。 VM の場合、デフォルトは usa となります。
遅延を少なくするためには手動で「any」に設定頂く必要があります。

```
config system fortiguard
    set update-server-location [usa | any]
end
```

10.10 FortiView widgets

モニターウィジェットは、スタンドアロンのダッシュボードとして保存できます。
デフォルトのダッシュボード設定には、次の 2 つのタイプがあります。
Optimal：6.4.1 のデフォルトのダッシュボード設定
Comprehensive：6.4.1 より前のデフォルトのモニターおよび FortiView 設定

10.11 WanOpt configuration changes in 6.4.0

ポート設定はプロファイルプロトコルオプションで行われます。 HTTPS 設定は、ファイアウォールポリシーで certificate inspection の設定する必要があります。
FortiOS 6.4.0 では、set ssl-ssh-profilecertificate-inspection をファイアウォールポリシーに追加する必要があります。

```
config firewall policy
    edit 1
        select srcintf FGT_A:NET_CLIENT
        select dstintf FGT_A:WAN
        select srcaddr all
        select dstaddr all
        set action accept
        set schedule always
        select service ALL
        set inspection-mode proxy
        set ssl-ssh-profile certificate-inspection
        set wanopt enable
        set wanopt-detection off
```

```
        set wanopt-profile "http"
        set wanopt-peer FGT_D:HOSTID
    next
end
```

10.12 IPsec interface MTU value

IPsec インタフェースは、6.2 からのアップグレード後に異なる MTU 値を計算する場合があります。
この変更により、アップグレード後に OSPF ネイバーが確立されなくなる可能性があります。 回避策は、OSPF インタフェースの設定で有効になるように mtu-ignore を設定することです。

Interface 設定：

```
config router ospf
    config ospf-interface
        edit "ipsce-vpnx"
            set mtu-ignore enable
        next
    end
end
```

10.13 Virtual WAN link member lost

mgmt インタフェースがアップグレード前に dedicated-to management の設定されている場合、virtual-wan-link のメンバーはアップグレード後に失われます。

11. 各 Fortinet 製品とのサポートについて

11.1 FortiAnalyzer

FortiAnalyzerとFortiOSの互換性については、下記ページに最新情報がございます。
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/0955b58b-a143-11eb-b70b-00505692583a/fortianalyzer-compatibility_-_caveats.pdf

※FortiGate のアップグレード前に FortiAnalyzer のアップグレードを行う必要がございます。

11.2 FortiManager

FortiManagerとFortiOSの互換性については、下記ページに最新情報がございます。
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/61c2bba0-a142-11eb-b70b-00505692583a/fortimanager-compatibility_-_caveats.pdf
FortiOS 6.4.1は、FortiManager6.4.1以降で動作させる必要があります。

※FortiGate のアップグレード前に FortiManager のアップグレードを行う必要があります。

11.3 FortiClient

FortiClient と FortiOS の互換性は以下の通りです。

プラットフォーム	OS バージョン
FortiClient for Windows	FortiClient 6.4 FortiClient Endpoint Telemetry ライセンスおよびフォーティネットセキュリティファブリックのアップグレードの重要な互換性情報を参照してください。
FortiClient for MacOS X	FortiClient 6.4 FortiClient Endpoint Telemetry ライセンスおよびフォーティネットセキュリティファブリックのアップグレードの重要な互換性情報を参照してください。
FortiClient for Linux	FortiClient for Linux は、Ubuntu 16.04 以降、Red Hat 7.4 以降、および CentOS7.4 以降でサポートされています。 FortiClient を IPsecVPN または SSLVPN にのみ使用している場合は、FortiClient バージョン 6.0 以降がサポートされています。
FortiClient for iOS	FortiClient 6.4.0 以降
FortiClient for Android and VPN Android	FortiClient 6.4.0 以降

※FortiOS のリリース時点での情報ですので、FortiClient の Release Notes も合わせてご確認ください。

11.4 FortiSwitch

FortiSwitch (FortiLink モード)と FortiOS の互換性は以下の通りです。

プラットフォーム	OS バージョン
FortiSwitch (FortiLink)	3.6.9 以降

※FortiOS のリリース時点での情報ですので、FortiSwitch の Release Notes も合わせてご確認ください。

11.5 FortiAP/FortiAP-S

FortiAP および FortiAP-S と FortiOS の互換性は以下の通りです。

プラットフォーム	OS バージョン
FortiAP	5.4.2 以降
	5.6.0 以降
FortiAP-S	5.4.3 以降
	5.6.0 以降

※FortiOS のリリース時点での情報ですので、FortiAP/FortiAP-S の Release Notes も合わせてご確認ください。

11.6 FortiSandbox

FortiSandbox と FortiOS の互換性は以下の通りです。

プラットフォーム	OS バージョン
FortiSandbox	2.3.3 以降

※FortiOS のリリース時点での情報ですので、FortiSandbox の Release Notes も合わせてご確認ください。

12. 動作環境

12.1 推奨 Web ブラウザについて

FortiGate の WebUI を表示する際の推奨ブラウザとなります。

プラットフォーム	OS バージョン
Microsoft Edge	Version 83
Mozilla Firefox	Version 76
Google Chrome	Version 83

他の Web ブラウザは正しく機能する可能性がありますが、Fortinet ではサポートされていません。

12.2 Explicit Web Proxy のブラウザサポートについて

FortiGate の Explicit Proxy 機能を利用する際のサポートブラウザの一覧です。

プラットフォーム	OS バージョン
Microsoft Edge	Version 44
Mozilla Firefox	Version 74
Google Chrome	Version 80

他の Web ブラウザは正しく機能する可能性がありますが、Fortinet ではサポートされていません。

12.3 SSL-VPN (Web モード)のサポートについて

FortiGate の SSL-VPN(Web モード)でサポートされているブラウザの一覧です。

プラットフォーム	ブラウザバージョン
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 78 Google Chrome version 84
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 78 Google Chrome version 84
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54
OS X Catalina 10.15	Apple Safari version 13 Mozilla Firefox version 78 Google Chrome version 84
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

12.4 VM プラットフォーム

FortiGate-VM の動作可能なプラットフォームとなります。

プラットフォーム	ブラウザバージョン
Citrix	Hypervisor 8.1 Express Edition, Dec 17, 2019
Linux KVM	Ubuntu 18.0.4 LTS, 4.15.0-72-generic, QEMU emulator version 2.11.1(Debian 1:2.11+dfsg-1ubuntu7.21)
Microsoft	Windows Server 2012R2 with Hyper-V role Windows Hyper-V Server 2019
Open Source	XenServer version 3.4.3 XenServer version 4.1 and later
VMware	ESX versions 4.0 and 4.1 ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, and 6.7
VM Series - SR-IOV 次の NIC チップセットカードがサポートされています。	Intel 82599 Intel X540 Intel X710/XL710