FortiGateVer.5.6 Patch3

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

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 Ver5.6.3 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 Ver5.6.3 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-30D, FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-30D-POE, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG- 200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240D-POE, FG-280D-POE, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, FG-5001C, FG-5001D
FortiWiFi	FWF-30D, FWF-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-30D-POE, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-30D, FGR-35D, FGR-60D, FGR-90D
FortiGate VM	FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-SVM, FG-VMX, FG-VM64-XEN

3.1 Special branch supported models

以下のモデルは特別ビルドで提供されています。

機種	ビルド番号
FG-90E	build 7719.
FG-91E	build 7719.

3.2 VXLAN supported models

以下のモデルで VXLAN がサポートされています。

機器シリーズ	機器
FortiGate	FG-30E, FG-30E-MI, FG-30E-MN, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-MC, FG-60E-MI, FG-60E-POE, FG-60EV, FG-61E, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-91E, FG-92D, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, FG-5001D
FortiWiFi	FWF-30E, FWF-30E-MI, FWF-30E-MN, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60E, FWF-60E-MC, FWF-60E-MI, FWF-60EV, FWF-61E
FortiGate Rugged	FGR-30D, FGR-30D-A, FGR-35D
FortiGate VM	FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-NPU, FG-VM64-OPC, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN

4. アップグレード注意事項

4.1 Built-In Certificate

FortiGate および FortiWiFi の D シリーズ以上には、DH グループ 14 の 2048 ビット証明書を使用する組み込みの Fortinet_Factory 証明書があらかじめインポートされています。

4.2 FortiGate and FortiWiFi-92D Hardware Limitation

FortiGate-92D および FortiWiFi-92D（日本未発売製品）では、HA 関連の機能に問題があります。以下の機能が影響を受けます。

・PPPoE での取得が失敗し、HA が形成されない
・IPv6 のパケットがドロップしてしまう。
・FortiSwitch デバイスが検出されない。
・ネットワークトポロジによっては、STP(スパニングツリー)のループが発生する可能性がある。

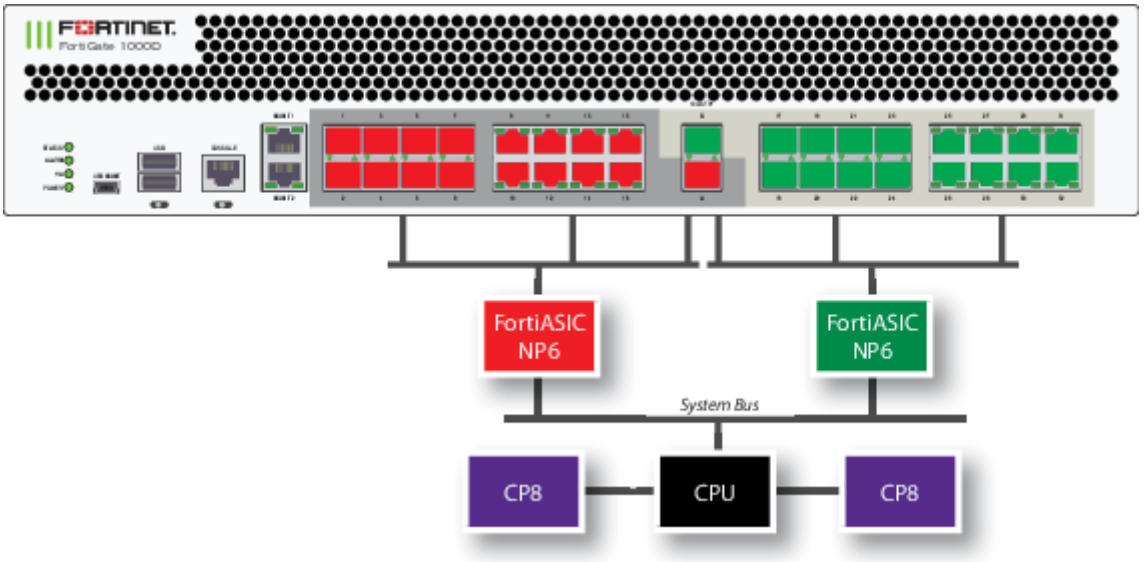
また、FortiGate-92D および FortiWiFi-92D は STP をサポートしません。これらの問題は FortiOS 5.4.1 で改善されましたが、新しいコマンドの導入に伴い、いくつかの制限事項があります。デフォルトは有効です。

```
config global
 set hw-switch-ether-filter <enable | disable>
```

■enable の場合
・ARP（0x0806）、IPv4（0x0800）、および VLAN（0x8100）パケットが許可されます。
・BPDU はドロップされるため、STP ループが発生しません。
・PPPoE のパケットはドロップされます。
・IPv6 パケットはドロップされます。
・FortiSwitch デバイスは検出されません。
・ネットワークトポロジによっては HA が形成されない場合があります。
■disable の場合
・すべてのパケットタイプが許可されていますが、ネットワークトポロジによっては、STP ループが発生する可能性があります。

4.3 FG-900D and FG-1000D

FortiGate-900D(日本未発売)および FortiGate-1000D では、複数の NP6 のチップが搭載されていますが、入力と出力のトラフィックが異なる場合、CAPWAP トラフィックのオフロードが実施できません。
入力と出力が同じ NP6 で処理されている場合、オフロードされます。



FortiGate-1000D の SPU 配置

4.4 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。

4.5 FortiGate-VM 5.6.3 for VMware ESXi

VMware ESXi 用 FortiGate-VM v5.6.3（すべてのモデル）は VMXNET2 vNIC ドライバをサポートしておりません。

4.6 FortiClient Profile Changes

Fortinet セキュリティファブリックの導入することにより、FortiClient プロファイルは FortiGate で更新されるようになります。FortiClient プロファイルと FortiGate は現在、エンドポイントコンプライアンスに主に使用されており、FortiClient Enterprise Management Server（EMS）は FortiClient の配備とプロビジョニングに使用されます。
FortiGate の FortiClient プロファイルは、アンチウイルス、Web フィルタ、脆弱性スキャン、アプリケーションファイアウォールなど、コンプライアンスに関連する FortiClient 機能です。

これらの機能は、Non-Compliance Action 設定を Block または Warn に設定することができます。
FortiClient ユーザーは、FortiGate のコンプライアンス基準を満たすように機能をローカルに変更できます。
FortiClient EMS を使用してエンドポイントを集中的にプロビジョニングすることもできます。 EMS には、VPN トンネルやその他の高度なオプションなどの追加機能のサポートも含まれています。

詳細は、FortiOS ハンドブック - セキュリティプロファイルを参照してください。

4.7 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。

4.8 Using ssh-dss algorithm to log in to FortiGate

バージョン 5.4.5 以降では、SSH 経由で FortiGate にログインするための ssh-dss アルゴリズムの使用はサポートされなくなりました。

4.9 DLP, AV

FortiOS 5.2 以前では、ブロックページはデフォルトで HTTP ステータスコード 200 OK がクライアントに送信されていました。FortiOS 5.4 以降では、ブロックページは、HTTP ステータスコードの 403 Forbidden がクライアントに送信されます。

4.10 FortiExtender support

OpenSSL のアップデートにより、FortiOS 5.6.3 では FortiExtender を管理できなくなりました。 FortiOS を FortiExtender と一緒に実行する場合は、3.2.1 以降などの新しいバージョンの FortiExtender を使用する必要があります。

5. アップグレードに関して

5.1 Upgrading to FortiOS 5.6.3

FortiOS 5.6.3 にアップグレードする際は、アップグレードパスに従ってアップグレードを行ってください。
アップグレードする前に、ポート 4433 が admin-port または admin-sport（設定システムグローバル内）、または SSL VPN（設定 vpn ssl 設定内）に使用されていないことを確認してください。
ポート 4433 を使用している場合は、アップグレードする前に admin-port、admin-sport、または SSL VPN ポートを別のポート番号に変更する必要があります。

FortiOS 5.4.5、5.4.6、または 5.4.7 からアップグレードする場合は、IPsec phase 1 の psksecret 設定が失われる可能性があります。 このような場合は、アップグレード後に psksecret 設定を再設定してください。

また、OS のアップグレード後、FortiLink モードが有効になっている場合は、FortiSwitch から（FortiLink インタフェースからのような）802.1x 認証用の RADIUS トラフィックが FortiGate を介して RADIUS サーバーに送信されるように明示的なファイアウォールポリシーを手動で作成する必要があります。

5.2 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 5.6.1
FortiClient	FortiClient 5.6.0
FortiClient EMS	FortiClient EMS 1.2.2
FortiAP	FortiAP 5.4.2 以降
FortiSwitch	FortiSwitch 3.6.2 以降

※Security Fabric 構成時、アップグレードには順序がございます。以下の URL をご参照ください。
https://docs.fortinet.com/document/fortigate/5.6.0/fortinet-security-fabric
※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。

5.3 FortiClient Profiles

FortiOS 5.4.0 から 5.4.1 以降の OS からアップグレードした後、FortiClient プロファイルは、サポートされなくなったいくつかのオプションを削除するように変更されます。
アップグレード後、FortiClient プロファイルを見直して、要件に合わせて適切に設定されていることを確認し、必要に応じてそれらを変更するか、新しいプロファイルを作成します。

以下の FortiClient プロファイル機能は FortiOS5.4.1 以降でサポートされていおりません。
・高度な FortiClient プロファイル（XML 設定）
・CA 証明書の設定、オプションの登録解除、FortiManager の更新、ダッシュボードなどの高度な設定
バナー、オンネットの場合はクライアントベースのロギング、および SSO モビリティエージェント
・VPN プロビジョニング
・スケジュール検索、FortiSandbox で検索、除外パスなど、AntiVirus の詳細設定
・オンネット時のクライアントサイド Web フィルタリング
・FortiOS GUI を使用した iOS および Android の設定

FortiOS 5.6.3 では、セキュリティファブリックのエンドポイントには FortiClient 5.6.0 が必要です。
FortiOS 5.6.3 への VPN（IPsec VPN、または SSL VPN）接続には FortiClient 5.4.3 を使用できますが、Security Fabric 機能には使用できません。

詳細なエンドポイントの展開とプロビジョニングには、FortiClient エンタープライズ管理サーバ（EMS）を使用することをお勧めします。

5.4 FortiGate-VM 5.6 for VMware ESXi

FortiOS 5.6.3 にアップグレードすると、VMware ESXi 用 FortiGate-VM v5.6（すべてのモデル）は VMXNET2 vNIC ドライバをサポートしていないためご注意ください。

5.5 Downgrading to previous firmware versions

FortiOS 5.6.3 より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
・VDOM parameters/settings
・admin user account
・session helpers
・system access profiles
長い VDOM 名がある場合は、ダウングレード前に長い VDOM 名（最大 11 文字）を短くする必要があります。

5.6 Amazon AWS Enhanced Networking Compatibility Issue

古い AWS VM バージョンとの互換性の問題があります。
FortiOS 5.6.3 のイメージを古い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ていないため、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。

5.6.0 から以前のバージョンにダウングレードするときは、Enhanced nic ドライバを実行することはできません。 以下の AWS インスタンスが影響を受けます。

・C3
・C4
・R3
・I2
・M4
・D2

6. 各 Fortinet 製品とのサポートについて

6.1 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/ea69b693-91cb-11e8-a49a-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。

6.2 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/171deb22-91cc-11e8-a49a-00505692583a/fortimanager-compatibility_-_caveats.pdf

※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。

6.3 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 5.6.0
FortiClient for MacOS X	FortiClient 5.6.0
FortiClient for iOS	FortiClient 5.4.3 以降
FortiClient for Android and VPN Android	FortiClient 5.4.1 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。

6.4 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)	3.6.2 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。

6.5 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。

6.6 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。

7. 動作環境

7.1 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 38
Microsoft Internet Explorer	Version 11
Mozilla Firefox	Version 54
Google Chrome	Version 59
Apple Safari	Version 9.1 (for Mac OS X)

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。

7.2 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) Microsoft Windows 8/8.1 (32-bit & 64-bit)	Microsoft Internet Explorer version 11 Mozilla Firefox version 54 Google Chrome version 59
Microsoft Windows 10 (64-bit)	Microsoft Edge Microsoft Internet Explorer version 11 Mozilla Firefox version 54 Google Chrome version 59
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54
Mac OS 10.11.1	Apple Safari version 9 Mozilla Firefox version 54 Google Chrome version 59
Apple iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

7.3 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 40
Microsoft Internet Explorer	Version 11
Mozilla Firefox	Version 53
Google Chrome	Version 58
Apple Safari	Version 10 (for Mac OS X)

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。

7.4 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	XenServer version 5.6 Service Pack 2 XenServer version 6.0 and later
Linux KVM	RHEL 7.1/Ubuntu 12.04 and later CentOS 6.4 (qemu 0.12.1) and later
Microsoft	Hyper-V Server 2008 R2, 2012, 2012 R2
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, and 6.5
VM Series - SR-IOV (サポートされる NIC のチップセット)	Intel 82599 Intel X540 Intel X710/XL710

※VMware ESXi 用 FortiGate-VM v5.6（すべてのモデル）は、VMXNET2 vNIC ドライバをサポートしていません。