FortiGateVer.6.0 Patch8

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 Ver6.0 Patch8 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 Patch8 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-30D-POE, FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, 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-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3400E, FG-3401E, FG3600E, FG-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, FG-5001D, FG-5001E, FG-5001E1
FortiWiFi	FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-30D, FGR-35D, FGR-60D, FGR-90D
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VMX, FG-VM64-XEN, FG-VM64-GCP, FG-VM64-OPC, FG-VM64-GCPONDEMAND

3.1 Special branch supported models

以下のモデルは、FortiOS 6.0.8 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 0302 が表示されていることを確認します。

機種	ビルド番号
FG-30E-MG	build 5419.
FG-60F	build 6575.
FG-61F	build 6575.
FG-100F	build 6575.
FG-101F	build 6575.
FG-1100E	build 6553.
FG-1101E	build 6553.
FG-2200E	build 6587.
FG-2201E	build 6587.
FG-3300E	build 6587.
FG-3301E	build 6587.
FG-VM64-AZURE	build 5420.
FG-VM64-AZUREONDEMAND	build 5420.
FG-VM64-RAXONDEMAND	build 8569.

4. アップグレード注意事項

4.1 WAN optimization and web caching functions

WAN 最適化および Web キャッシュ機能は、ディスクサイズが限られているため、FortiOS 6.0.0 から 60D および 90D シリーズのプラットフォームから削除されました。

対象の機器は以下の通りです。

機器シリーズ	対象機器
FortiGate 60D シリーズ	FGT-60D, FGT-60D-POE, FWF-60D, FWF-60D-POE
FortiGate 90D シリーズ	FGT-90D, FGT-90D-POE, FWF-90D, FWF-90D-POE, FGT-94D-POE

4.2 FortiGuard Security Rating Service

Fortinet Security Fabric 機能をご利用されている場合、以下の機器が Fabric のルートデバイスとなることは出来ません。より上位の機器がルートデバイスとなることで、FortiGuard セキュリティレーティングサービスを利用することが出来るようになります。(※要ライセンス)

機器シリーズ	対象機器
FortiGate Rugged シリーズ	FGR-30D-A, FGR-30D, FGR-35D, FGR-60D, FGR-90D
FortiGate シリーズ	FGT-200D, FGT-200D-POE, FGT-240D, FGT-240D-POE, FGT-280D-POE, FGT-30D, FGT-30D-POE, FGT-30E, FGT-30E-MI, FGT-30E-MN, FGT-50E, FGT-51E, FGT-52E, FGT-60D, FGT-60D-POE, FGT-70D, FGT-70D-POE, FGT-90D, FGT-90D-POE, FGT-94D-POE, FGT-98D-POE
FortiWiFi シリーズ	FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-MI, FWF-30E-MN, FWF-50E-2R, FWF-50E, FWF-51E, FWF-60D, FWF-60D-POE, FWF-90D, FWF-90D-POE, FWF-92D

4.3 Using FortiManager as a FortiGuard server

FortiManager を FortiGuard サーバとして使用し、FortiManeger に対して安全な接続を使用したい場合、HTTPS とポート 8888 を使用する必要があります。HTTPS とポート 53 はサポートされていません。

4.4 Built-in certificate

FortiGate および FortiWiFi の D シリーズ以上には、DH グループの 14 、2048 ビット証明書を使用する組み込みの Fortinet_Factory 証明書がございます。

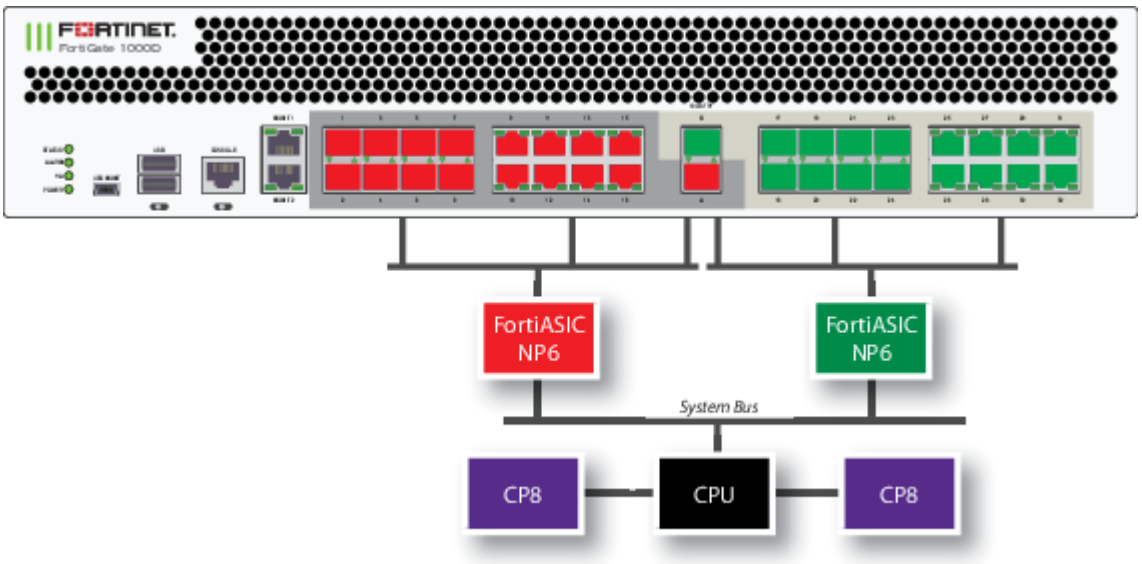
4.5 FortiGate and FortiWiFi-92D hardware limitation

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。

4.6 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

4.7 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。

4.8 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。

4.9 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。

4.10 Using FortiAnalyzer units running older versions

FortiOS 6.0 Patch8 と FortiAnalyzer の 5.6.5 以下または FortiAnalyzer 6.0.0～6.0.2 をご利用されている場合、2 分以上続くセッションがありと FortiAnalyzer との帯域幅およびセッション数の増加が発生する事象が報告されております。
正確な値を得るためには、FortiAnalyzer を最新バージョンにアップグレード頂く必要がございます。

4.11 Changes in default behavior

FortiOS 6.0.0 でファイアウォールポリシーの SNAT のデフォルトの動作が変更されました。 以下は、変更前後の SNAT の動作の比較です。

■変更前(FortiOS 5.6 以前)
NAT 制御は Firewall ポリシーの設定に依存します。
・Central-NAT が無効になっている場合、NAT の動作はファイアウォールポリシーによって決定されます。
・Central-NAT が有効の場合、以下のパターンに分けられます。
ファイアウォールポリシーで NAT が有効になっている場合
FortiGate は Central-NAT テーブルを確認し、一致する場合は Central-NAT テーブルに従います。
Central-NAT テーブルに一致しない場合、FortiGate はインタフェースの IP で NAT を行います。
ファイアウォールポリシーで NAT が無効になっている場合、NAT 処理は実行されません。

■変更後(FortiOS 6.0.0)
Central-NAT の設定が有効になっている場合、NAT の設定は Firewall ポリシーから Central-NAT テーブルへ移動されます。
・Central-NAT が無効になっている場合、NAT の動作はファイアウォールポリシーによって決定されます。
・Central-NAT が有効になっている場合、NAT の設定がファイアウォールポリシーでは設定できません。
NAT の動作はすべて Central-NAT テーブルで決定されます。

5. アップグレードに関して

5.1 Upgrading to FortiOS 6.0.8

FortiOS 6.0 Patch8 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。

※バージョン 5.6.2 または 5.6.3 からアップグレードする場合、この注意は適用されません。

5.2 FortiGuard protocol and port number

FortiOS 6.0.8 では脆弱性「CVE-2018-9195」に対するワークアラウンドとして FortiGate ユニットと FortiGuard の間で使用されるプロトコルを更新しました。それに伴い、FortiOS 6.0.8 以前のバージョンからアップグレードした場合、FortiGuard への接続に使用するプロトコルとポートを手動で変更する必要があります。

```
config system fortiguard
    set protocol https
    set port 8888
end
```

なお、FortiOS 6.0.8 で工場出荷時設定にリセットすると、デフォルトの FortiGuard 設定が上記の設定（プロトコル HTTPS およびポート 8888）に変更されます。

5.3 Physical interface inclusion in zones

FortiOS 5.6.3 以降の OS からアップグレードすると、ゾーンに物理インタフェースが含まれているかつ、その物理インタフェースの VLAN インタフェースの少なくとも 1 つ以上含まれている場合、そのゾーンのすべてのメンバーが削除されます。

■アップグレード前

```
config system zone
   edit "Trust"
      set interface "port1" "Vlan01" "Vlan02" "Vlan03"
next
```

■アップグレード後

```
config system zone
   edit "Trust"
next
```

Zone の設定から「port1」を削除すると、アップグレード後も VLAN の設定が維持されます。
削除された場合、再度 Zone の設定を行ってください。

5.4 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 6.0.0
FortiClient	FortiClient 6.0.0
FortiClient EMS	FortiClient EMS 6.0.0
FortiAP	FortiAP 5.4.4 以降
FortiSwitch	FortiSwitch 3.6.4 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/6.0.6/security-fabric-upgrade-guide
※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。
※2019/12/03 現在 FortiOS 6.0.7、6.0.8 の「Security Fabric Upgrade Guide」は公開されておりません。内容に大きな差異はございませんので、現時点では 6.0.6 の資料をご参照ください。

5.5 Minimum version of TLS services automatically changed

セキュリティを向上させるために、FortiOS 6.0.8 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 6.0.7 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)

5.6 Downgrading to previous firmware versions

FortiOS 6.0 Patch8 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。

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 6.0.0
FortiClient for MacOS X	FortiClient 5.6.0 以降
FortiClient for Linux	FortiClient 5.4.2 以降
FortiClient for iOS	FortiClient 5.6.0 以降
FortiClient for Android and VPN Android	FortiClient 5.4.2 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)	3.6.4 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 41
Mozilla Firefox	Version 59
Google Chrome	Version 65
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)	Mozilla Firefox version 61 Google Chrome version 68
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 61 Google Chrome version 68
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54
Mac OS EI Capitan 10.11.1	Apple Safari version 11 Mozilla Firefox version 61 Google Chrome version 68
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 41
Microsoft Internet Explorer	Version 11
Mozilla Firefox	Version 59
Google Chrome	Version 65
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。

7.4 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, 2016
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