FortiGateVer.6.0 MR2 Patch5

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 MR2 Patch5 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 MR2 Patch5 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-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-30E-MG, FG-40F, FG-40F-3G4G, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-92D, FG-100D, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140D, FG-140D-POE, 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, FG800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG2000E, 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-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F
FortiGate Rugged	FGR-30D, FGR-35D, FGR-90D
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM, FOS-VM64-XEN

3.1 Special branch supported models

以下のモデルは、FortiOS 6.0 MR2 Patch5 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
FG-80F	is released on build 6801.
FG-80F-BP	is released on build 6801.
FG-81F	is released on build 6801.
FG-400E-BP	is released on build 5848.
FG-1800F	is released on build 5878.
FG-1801F	is released on build 5878.
FG-2600F	is released on build 5884.
FG-2601F	is released on build 5884.
FG-4200F	is released on build 5878.
FG-4201F	is released on build 5878.
FGR-60F	is released on build 5761.
FGR-60F-3G4G	is released on build 5883.

4. アップグレード注意事項

4.1 New Fortinet cloud services

FortiOS 6.2 以降、以下のクラウドベースのサービスが追加されました。

・Overlay Controller VPN
・FortiGuard Cloud-Assist SD-WAN Interface Bandwidth Monitoring
・FortiManager Cloud
・FortiAnalyzer Cloud

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, FGR-35D
FortiGate シリーズ	FGT-30E, FGT-30E-MN, FGT-30E-MI, FGT-50E, FGT-51E, FGT-52E
FortiWiFi シリーズ	FWF-30E, FWF-30E-MI, FWF-30E-MN, FWF-50E-2R, FWF-50E, FWF-51E

4.3 Using FortiManager as a FortiGuard server

FortiManager を FortiGuard サーバとして使用し、安全な接続を使用するように FortiGate を設定する場合 FortiManager では、ポート 8888 で HTTPS を使用する必要があります。ポート 53 での HTTPS はサポートされていません。

4.4 FortiGate hardware limitation

FortiOS 5.4.0 において FortiWiFi-92D（日本未発売製品）の port1～port14 における以下の問題がございました。

・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。

これらの問題は FortiOS 5.4.1 で改善されましたが、デフォルトで有効になっている以下の新しいコマンドの導入によるいくつかの副作用がございます。

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

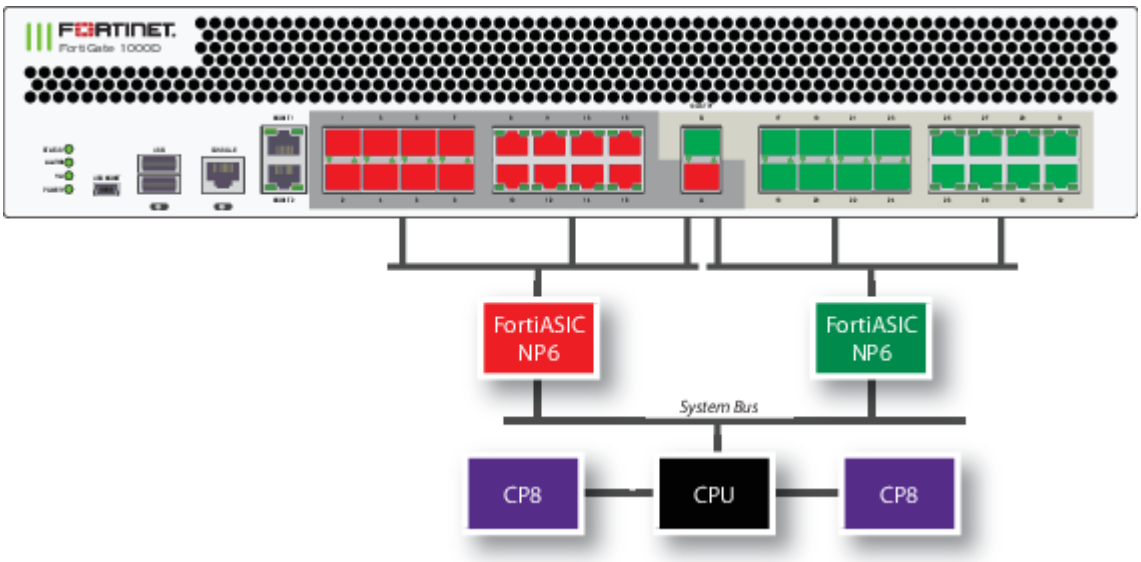
コマンドが有効な場合：
・ARP（0x0806）、IPv4（0x0800）、および VLAN（0x8100）パケットが許可される。
・BPDU はドロップされるため、STP ループは発生しない。
・PPPoE パケットはドロップされます。
・IPv6 パケットはドロップされます。
・FortiSwitch デバイスは検出されません。
・ネットワークトポロジによっては、HA の形成に失敗する場合がある。

コマンドが無効な場合：
・すべてのパケットタイプが許可されるが、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。

4.5 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

4.6 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。

4.7 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 NP4lite platforms

FortiOS 6.2 以降、NP4lite 搭載のモデルはサポートされません。

4.9 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

4.10 L2TP over IPsec on certain mobile devices

Bug ID	Description
459996	L2TP over IPsec が接続された後、Samsung Galaxy Tab A8 と Android9.0 がクラッシュします。

4.11 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。

4.12 Proxy web filter with SSL inspection may fail for websites that allow TLS versions below 1.3 after upgrading to FortiOS 6.2.5

Bug ID	Description
617934	SSL インスペクションも有効にしたプロキシベースのファイアウォールポリシーを使用して Web フィルタリングが有効になっている場合、安全性の低い TLS バージョンをまだサポートしているサーバへの接続が失敗する可能性があります。 見られるブラウザエラー： Chrome：ERR_CONNECTION_CLOSED Firefox：PR_END_OF_FILE_ERROR 回避策：影響を受けるファイアウォールポリシーをフローベースの検査に切り替えます。

5. New features or enhancements

以下の機能が追加されました。

Bug ID	Description
480717	mgmt、mgmt1、mgmt2 ポートを持つすべての FortiGate モデルに config system dedicated-mgmt コマンドが追加されます。
641990	WAN 最適化をサポートしていないモデルでも diagnose wad session list コマンドを使用できるようになります。

6. Changes in default behavior

以下の機能が変更になります。

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した。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評価されます。このオーバーライドは、webfilter プロファイル、ssl-exempt、および proxy-address に適用できます。 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 プロファイル、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 プロファイルのみが関与し、IPS エンジンでの変更とは異なる動作をします。6.2.5 および 6.4.2 では、ローカル/リモートの評価は、カテゴリが WebFilter プロファイル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/リモートの評価はまだグローバルまたは 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。

7. Changes in default values

以下の内容が変更されます。

Bug ID	Description
613730	Azure SDN 構成のルートテーブルに subscription-id 属性を追加し、異なるサブスクリプションのルートテーブルを更新できるようになります。 config system sdn-connector edit "azsdn" config route-table edit "xxxxxxxxx-rtb1" set subscription-id "xxxxxxxxxxxxxxx" <==added set resource-group "xxxxxxxxx" config route edit "internal-forword" set next-hop "172.28.5.4" next end next end end
613876	ipsec phase1-interface の下に dhcp-ra-giaddr が追加されます。 config vpn ipsec phase1-interface edit "1" set type dynamic set peertype any set net-device disable set mode-cfg enable set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1 set dpd on-idle set assign-ip-from dhcp set dhcp-ra-giaddr <==added next end

8. アップグレードに関して

8.1 FortiClient Endpoint Telemetry license

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

8.2 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 6.2.0
FortiClient	FortiClient 6.2.0
FortiClient EMS	FortiClient EMS 6.2.0
FortiAP	FortiAP 5.4.4 以降
FortiSwitch	FortiSwitch 3.6.9 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。

セキュリティファブリックをアップグレードする際には、他の機器を管理する機器を先にアップグレードする必要がございます。各機器のファームウェアを以下の順序でアップグレードしてください。これにより、手動による手順を踏まなくても、ネットワークの接続性が維持されます。

1. FortiAnalyzer
2. FortiManager
3. FortiGate devices
4. Managed FortiSwitch devices
5. Managed FortiAP devices
6. FortiClient EMS
7. FortiClient
8. FortiSandbox
9. FortiMail
10. FortiWeb
11. FortiADC
12. FortiDDOS
13. FortiWLC

8.3 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 MR2 Patch5 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)

8.4 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

8.5 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 MR2 Patch5 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 MR2 Patch5 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。

8.6 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 6.2.0 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。6.2.0 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
```

8.7 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。

8.8 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
```

8.9 FortiView widgets

FortiView ウィジェットは 6.2.0 で大きく変更されました。 以前のバージョンで作成された FortiView ウィジェットは、アップグレードで削除されます。

9. 各 Fortinet 製品とのサポートについて

9.1 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。

9.2 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

※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。

9.3 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 6.2.0
FortiClient for MacOS X	FortiClient 6.2.0
FortiClient for Linux	FortiClient 6.2.0
FortiClient for iOS	FortiClient 6.2.0 以降
FortiClient for Android and VPN Android	FortiClient 6.2.0 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。

9.4 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。

9.5 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。

9.6 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。

10. 動作環境

10.1 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 44
Mozilla Firefox	Version 76
Google Chrome	Version 81

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。

10.2 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
Microsoft Internet Explorer	Version 11
Mozilla Firefox	Version 76
Google Chrome	Version 81

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。

10.3 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 76 Google Chrome version 81
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 76 Google Chrome version 81
Linux CentOS 7/8	Mozilla Firefox version 68
OS X Catalina 10.15	Apple Safari version 13 Mozilla Firefox version 76 Google Chrome version 81
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

10.4 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 Express 8.1, build 2019-12-04
Linux KVM	Ubuntu 18.04.3 LTS l QEMU emulator version 4.4.4 (Debian 1:4.0+dfsg-0ubuntu9.4) libvirtd (libvirt) 4.0.0
Microsoft	Hyper-V Server 2019
Open Source	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 (サポートされる NIC のチップセット)	Intel X520