FortiGate アップグレード手順書

NVC
NETWORK VALUE COMPONENTS

改訂履歴

発行年月	版 数	改版内容
H30.1	第 1.0 版	初版発行

目次

1. はじめに

本マニュアルは FortiGate の OS バージョンのアップグレードを行うための各種操作方法について記載しています。

※注意①
アップグレードを行う際は、必ずアップグレードするバージョンの Information 資料も読んでから実施するようにして下さい。

Information 資料は下記の通りです。

資料名：FortiGate Ver.x.0 MRy Patchg Information
“Ver.x.0”がメジャーバージョン、”MRy”がマイナーバージョン、”Patchg”が Patch に該当致します。

OSver5.0 MR4 patch1 へアップグレードする場合は、”FortiGate Ver.5.0 MR4 Patch1 Information”をご確認ください。
OSver5.0 MR2 patch7 へアップグレードする場合は、”FortiGate Ver.5.0 MR2 Patch7 Information”をご確認ください。
OSver5.0 Patch13 へアップグレードする場合は、”FortiGate Ver.5.0 Patch13 Information”をご確認ください。

資料は下記 URL よりダウンロードを行ってください。

http://gold.nvc.co.jp/supports/fortinet/OS/fgt/infomation/

2. アップグレード手順概要

2.1 WebUI と CLI の違い

FortiGate のアップグレード・ダウングレードは、WebUI による操作と CLI による操作で行うことが出来ます。

<アップグレード>

[WebUI]

設定情報を引き継ぎつつ OS の Version を上げる事が可能です。通常のアップグレード時は WebUI での操作を推奨します。

*一部引き継がれない設定がございます。詳細は各 OS の Information 資料を参照ください。

[CLI]

工場出荷状態になり、設定情報は引き継がれません。OS を入れ直す必要がある場合や特別な操作が必要な場合などに CLI での操作を実施します。

<ダウングレード>

[WebUI]

一部の設定が失われる場合がございます。そのため、ダウングレードは CLI から行うことを推奨します。

[CLI]

工場出荷状態になり、設定情報は引き継がれません。

2.2 アップグレード手順概要

[WebUI からのアップグレード]

順番	手順	注意点	参照
1	Config のバックアップ		3.Config のバックアップ、リストア
2	WebUI からのアップグレード	※機器が再起動するため通信断が発生します。	4.WebUI でのアップグレード
3	(必要な場合)Config の修正およびリストア		3.Config のバックアップ、リストア

[CLI からのアップグレード]

順番	手順	注意点	参照
1	Config のバックアップ		3.Config のバックアップ、リストア
2	CLI からのアップグレード	※機器が再起動するため通信断が発生します。	5. CLI でのアップグレード、ダウングレード
3	Config のリストア		3.Config のバックアップ、リストア

3. Config のバックアップ、リストア

注意 1 :Config のリストア時には機器の再起動が発生するため通信断が発生します。

3.1 準備

以下のものを準備します。

- ネットワーク接続可能な PC(対応ブラウザ情報はアップグレードするバージョンの ReleaseNote をご確認ください。)

3.2 PC の設定

WebUI では、PC のブラウザを利用して Config のバックアップを行います。

その為、作業は FortiGate に対してアクセスが許可されている PC で行います。

3.3 接続

(1) FG の HTTP/HTTPS のアクセスを許可しているインタフェースに、PC を直接またはネットワーク経由で接続します。

(2) PC のブラウザにて FortiGate へアクセスします。
(ブラウザに URL https://xxx.xxx.xxx.xxx もしくは http://xxx.xxx.xxx.xxx を指定します。x は FortiGate の IP アドレスを指定します。)

(3) ログイン画面が表示されるので、ユーザー名・パスワードを入力してログインをクリックします。

3.4 Config のバックアップ

(1) トップ画面左の システム > ダッシュボード > Status(ステータス) にある『バックアップ』をクリックします。

(図 3-4-1-1. Dashboard の status 画面)

(図 3-4-1-2. Dashboard の status 画面(ver5.0 MR6))

(2) バックアップ画面の『バックアップ』をクリックして、ファイル名を指定し、バックアップファイルをダウンロードします。

※OSver5.0 MR4、OSver5.0 MR6 の場合は『OK』をクリックします。

(図 3-4-2. バックアップ画面)

3.5 Config のリストア

※注意:Config のリストアを実施する際は再起動が発生するため、通信断が発生します。

(1) 左上のシステム > ダッシュボード > Status(ステータス)にある『リストア』をクリックします。

(図 3-5-1-1.Dashboard の status 画面)

(図 3-5-1-2. Dashboard の status 画面(ver5.0 MR6))

(2)　ファイル名の右側にある『参照』をクリックし、リストアするファイルを選択します。
※OSver5.0 MR4、OSver5.0MR6 の場合は『アップロード』をクリックします。

(3)　画面の『リストア』をクリックすると、リストアが始まります。
※OSver5.0MR4、OSver5.0MR6 の場合は『OK』をクリックします。

(図 3-5-2.リストア画面)

4. WebUI でのアップグレード

注意 1 :アップグレード時には機器の再起動が発生するため通信断が発生します。
注意 2:アップグレード時には、必ずアップグレードするバージョンの Information 資料も読んでから実施するようにして下さい。Information 資料は下記 URL よりダウンロード可能です。

http://gold.nvc.co.jp/supports/fortinet/OS/

資料名 : FortiGate Ver.x.0 MRy Patchg Information

“Ver.x.0”がメジャーバージョン、”MRy”がマイナーバージョン、”Patchg”が Patch に該当致します。

4.1 準備

以下のものを準備します。

- ネットワーク接続可能な PC (対応ブラウザ情報はアップグレードするバージョンの ReleaseNote をご確認ください。)
- アップグレードするファームウェアファイル

4.2 PC の設定

WebUI では、ブラウザを利用してアップグレードを行います。
その為、作業は FortiGate に対してアクセスが許可されている PC で行います。

4.3 接続

(1) FG の HTTP/HTTPS のアクセスを許可しているインタフェースに、PC を直接またはネットワーク経由で接続します。

(2) PC のブラウザにて FortiGate へアクセスします。
(ブラウザに URL https://xxx.xxx.xxx.xxx もしくは http://xxx.xxx.xxx.xxx を指定します。x は FortiGate の IP アドレスを指定します。)

(3) ログイン画面が表示されるので、ユーザー名・パスワードを入力してログインをクリックします。

4.4 アップグレード

(1) トップ画面左の システム > ダッシュボード > Status(ステータス)の中央にある ファームウェアバージョンで現在のバージョンを確認します。

※OSver5.0MR6 の場合は ダッシュボード > Main のファームウェアバージョンで現在のバージョンを確認します。

（図 4-4-1-1.バージョン情報確認画面）

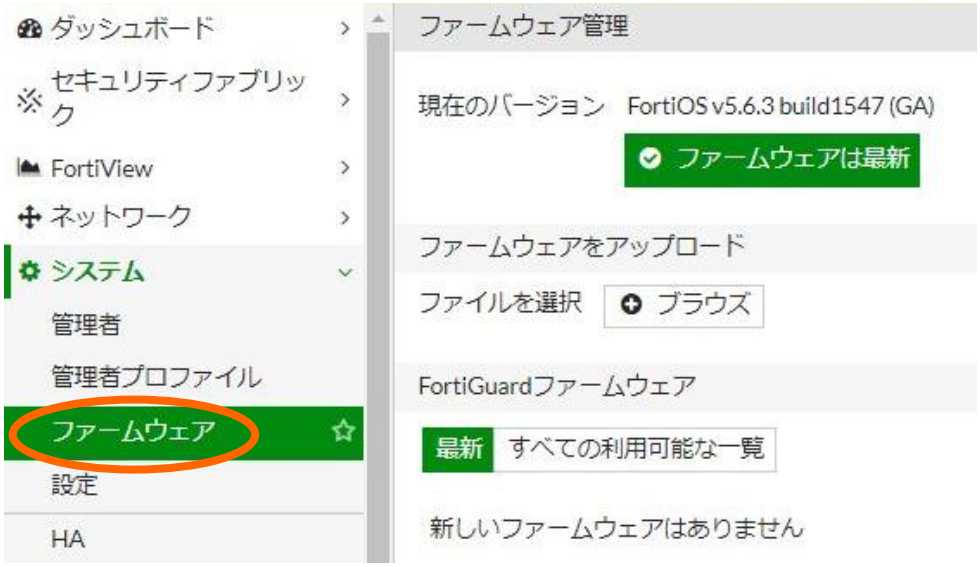
（図 4-4-1-2.バージョン情報確認画面(ver5.0 MR6)）

(2) 現在の Config のバックアップを取得します。 3.Config のバックアップ、リストア参照

(3) ファームウェアバージョンの右にある『アップデート』をクリックします。

※OSver5.0MR6 の場合は『ファームウェア』をクリックします。

（図 4-4-2.アップデートボタン確認画面）



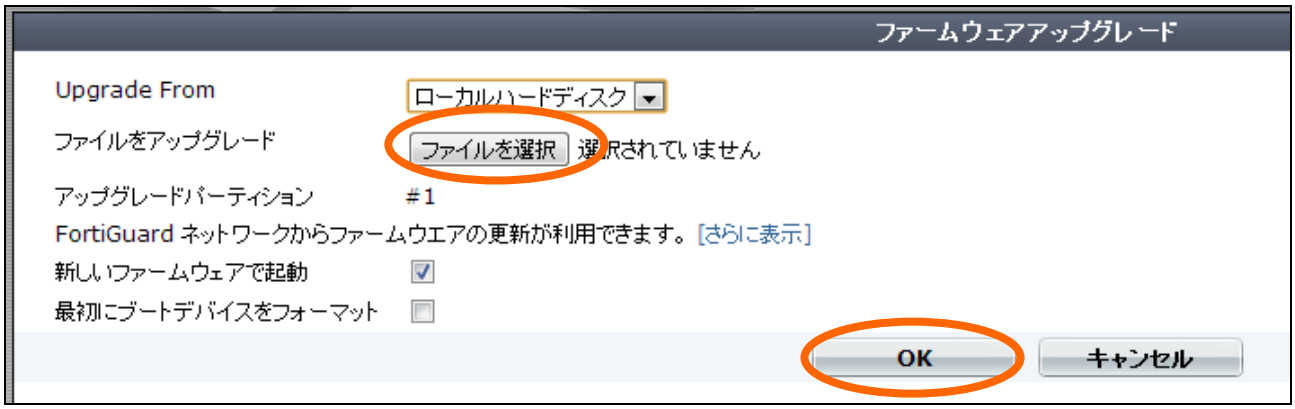
（図 4-4-2.アップデートボタン確認画面(ver5.0 MR6)）

(4)　画面が切り替わった後アップデートするファームウェアを選択します。

➢　ver4.0 MR2, ver4.0 MR3, ver5.0 の場合

①　『ファイルをアップグレード』の右にある『ファイルを選択』をクリックしアップグレードするファームウェアファイルを選択します。

②　『OK』をクリックするとアップグレードが始まり、自動的に機器が再起動します。
※機器の再起動が発生するため、通信断が発生します。



（図 4-4-3.アップグレードボタン確認画面）

➢ ver5.0 MR2 の場合

① 『ファームフェアをアップロード』をクリックしアップグレードするファームウェアファイルを選択します。

（図 4-4-4.v5.2 アップロードボタン確認画面 1）

② その後、『アップグレード』をクリックするとアップグレードが始まり、自動的に再起動します。
※機器の再起動が発生するため、通信断が発生します。

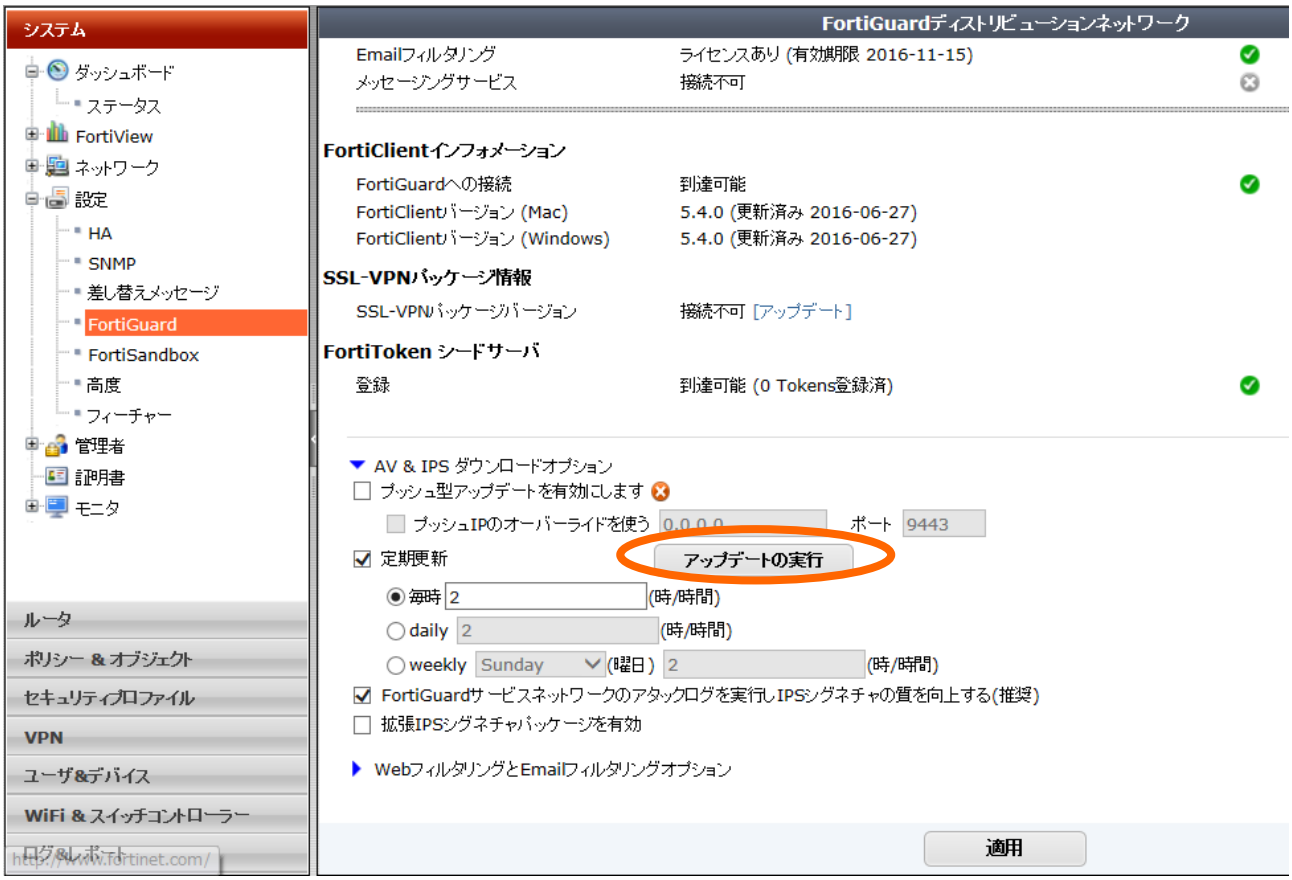
（図 4-4-5.v5.2 アップグレードボタン確認画面 2）
※補足：ビルド 1064 は FortiOS Ver5 MR4 Patch1

(5) 再起動後、再度 WebUI へ接続します。
(6) 項番(1)と同様にして、ファームウェアバージョンの確認を行います。
(7) コンフィグをバックアップします。（「3.Config のバックアップ、リストア」参照）
(8) 実通信に問題が発生していないことを確認します。
アップグレードによる問題の有無を確認します。
問題が発生した場合は設定等を見直し問題の修正または切り戻しを行います。
切り戻し方法は、CLI でのダウングレード(「5. CLI でのアップグレード、ダウングレード」参照)を実行後に、手順(2)にてバックアップした Config をリストアします(「3.Config のバックアップ、リストア」

参照)。

(9) アンチウィルス、IPS をご利用されている場合は、シグネチャのアップデートを実施します。

(10) システム > 設定 > FortiGuard にて画面下部の『AV & IPS ダウンロードオプション』をクリックして展開し、『アップデートの実行』をクリックして最新シグネチャのアップデートを実行します。シグネチャアップデート時には機器に多少の負荷がかかります。



(図 4-4-6.シグネチャアップデートの画面)

※FortiOS4.0 MR2 から FortiOS4.0 MR3 以上のバージョンへアップグレードする場合に、
Web フィルタリングのコンテンツブロック機能をご利用しているお客様は
「FortiGate Ver.4.0 MR3 Patch12 Information」をご確認ください。

➢ ver5.0 MR4 の場合

① 『ファームフェアをアップロード』をクリックしアップグレードするファームウェアファイルを選択します。

（図 4-4-7.v5.4 アップロードボタン確認画面 1）

② その後、『アップグレード』をクリックするとアップグレードが始まり、自動的に再起動します。

※機器の再起動が発生するため、通信断が発生します。

（図 4-4-8.v5.4 アップグレードボタン確認画面 2）

(5) 再起動後、再度 WebUI へ接続します。

(6) 項番(1)と同様にして、ファームウェアバージョンの確認を行います。

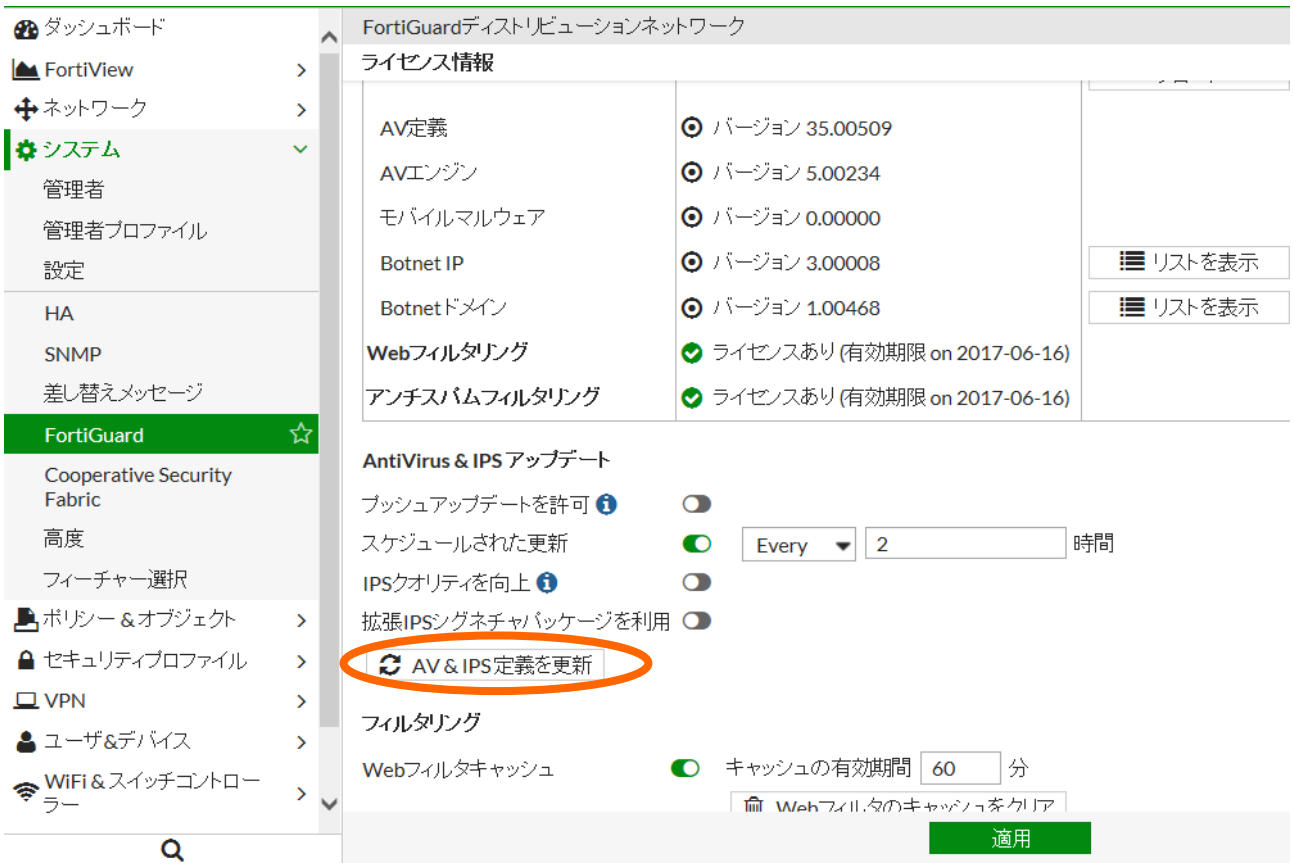
(7) コンフィグをバックアップします。（「3.Config のバックアップ、リストア」参照）

(8) 実通信に問題が発生していないことを確認します。

アップグレードによる問題の有無を確認します。
問題が発生した場合は設定等を見直し問題の修正または切り戻しを行います。
切り戻し方法は、CLI でのダウングレード(「5. CLI でのアップグレード、ダウングレード」参照)を実行後に、手順(2)にてバックアップした Config をリストアします(「3.Config のバックアップ、リストア」参照)。

(9) アンチウィルス、IPS をご利用されている場合は、シグネチャのアップデートを実施します。

(10) システム > FortiGuard にて画面下部の『AV & IPS 定義を更新』をクリックして最新シグネチャのアップデートを実行します。シグネチャアップデート時には機器に多少の負荷がかかります。



(図 4-4-9.シグネチャアップデートの画面)

※FortiOS4.0 MR2 から FortiOS4.0 MR3 以上のバージョンへアップグレードする場合に、
Web フィルタリングのコンテンツブロック機能をご利用しているお客様は
「FortiGate Ver.4.0 MR3 Patch12 Information」をご確認ください。

➢ ver5.0 MR6 の場合

① 『ブラウズ』をクリックしアップグレードするファームウェアファイルを選択します。

（図 4-4-10.v5.6 アップロードボタン確認画面 1）

② 『設定のバックアップとアップグレード』をクリックしアップグレードするファームウェアファイルを選択します。

（図 4-4-11.v5.6 アップグレードボタン確認画面 2）

(5) 再起動後、再度 WebUI へ接続します。

(6) 項番(1)と同様にして、ファームウェアバージョンの確認を行います。

(7) コンフィグをバックアップします。（「3.Config のバックアップ、リストア」参照）

(8) 実通信に問題が発生していないことを確認します。
アップグレードによる問題の有無を確認します。
問題が発生した場合は設定等を見直し問題の修正または切り戻しを行います。

切り戻し方法は、CLI でのダウングレード(「5. CLI でのアップグレード、ダウングレード」参照)を実行後に、手順(2)にてバックアップした Config をリストアします(「3.Config のバックアップ、リストア」参照)。

(9) アンチウィルス、IPS をご利用されている場合は、シグネチャのアップデートを実施します。

(10) システム > FortiGuard にて画面下部の『AV & IPS 定義を更新』をクリックして最新シグネチャのアップデートを実行します。シグネチャアップデート時には機器に多少の負荷がかかります。

5. CLI でのアップグレード、ダウングレード

注意 1 :アップグレード時には機器の再起動が発生するため通信断が発生します。
注意 2: CLI でアップグレードを実施する場合、Config やユーザー名、パスワードは工場出荷時状態になります。必ず Config のバックアップを行うようにしてください。

5.1 準備

以下のものを準備します。

- PC(TeraTerm 等のターミナルソフト、TFTPServer ソフトがインストールされているもの)
- LAN ケーブル
- シリアルケーブル (FortiGate に付属)
- アップグレード(またはダウングレード)するファームウェアファイル
- リストアする Config ファイル(事前にバックアップしたファイルをリストアする場合)

現在の Config の保存を必ず行います。 3.Config のバックアップ、リストア参照

5.2 PC の設定

CLI では、TFTP サーバを利用してアップグレードを行います。そのため、PC の IP アドレスの設定とターミナルソフトの設定が必要になります。

(1) PC の IP アドレスを設定します。(例:192.168.1.168/24)
(2) ターミナルソフトを起動して設定を以下の通りに設定します。
  - ボーレート:9600
  - データ :8 ビット
  - パリティ :なし
  - ストップ :1
  - フロー制御:なし
(3) TFTPServer ソフトを起動して、ファームウェアを保存してあるフォルダを指定します。

5.3 ネットワークからの切り離し

FortiGate をネットワークから切り離します。

5.4 CLI 接続

(1) PC と FortiGate のコンソールポートをシリアルケーブルで接続します。
(2) ターミナルソフトより FortiGate に CLI でアクセスします。
(3) ユーザー名・パスワードを入力してログインします。

5.5 アップグレード、ダウングレード

(1) 現在のバージョンを get sys status コマンドで確認します。

```
# get system status
Version: FortiGate-200D v5.2.7,build0718,160328 (GA)
```

(2) execute reboot と入力し、リブートを行います。
※機器の再起動が発生するため、通信断が発生します。

(3) リブート後 Press Any Key To Download Boot Image.と表示されたら何かキーを押します。
Enter G,F,B,Q,or H: と表示されるので G を入力します。
※機器によっては何かキーを押した後、G を押さず(4)へ移行するものもあります。

＊次ページは、実際に CLI からアップグレードを行なったときの CLI 画面です。

FortiGateCLI 画面

FGT200D #execute reboot

This operation will reboot the system !

Do you want to continue? (y/n)y

The system is going down NOW !!

System is rebooting...

FGT200D #

Please stand by while rebooting the system.

Restarting system.

FortiGate-200D (18:47-05.08.2013)

Ver:04000006

Serial number:FG200D[redacted]

RAM activation

CPU(00:000206a7 bfebfbff): MP initialization

CPU(02:000206a7 bfebfbff): MP initialization

Total RAM: 2048MB

Enabling cache...Done.

Scanning PCI bus...Done.

Allocating PCI resources...Done.

Enabling PCI resources...Done.

Zeroing IRQ settings...Done.

Verifying PIRQ tables...Done.

Boot up, boot device capacity: 15272MB.

Press any key to display configuration menu... ←ここで何かキーを押す

...

[G]: Get firmware image from TFTP server.

[F]: Format boot device.

[B]: Boot with backup firmware and set as default.

[I]: Configuration and information.

[Q]: Quit menu and continue to boot with default firmware.

[H]: Display this list of options.

Enter Selection [G]:

Enter G,F,B,I,Q,or H: ←G を入力する

(4) PC と FortiGate のインタフェースを LAN ケーブルで接続します。

(5) Enter tftp server address [192.168.1.168]: と表示されるので PC の IP アドレスを入力します。
(例: Enter tftp server address [192.168.1.168]: 192.168.1.10)

(6) Enter local address [192.168.1.188]: と表示されるので FG の IP アドレスを入力します。
(例: Enter local address [192.168.1.188]: 192.168.1.99)

(7) Enter firmware image file name [image.out]: と表示されるので Firmware のファイル名を入力します。
(例: Enter firmware image file name [image.out]: FGT_200D-v5-build1011-FORTINET.out)

(8) その後、Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]? と確認メッセージが表示されるので D キーを押す
*モデルによっては"B"が表示されません。

(9) 再起動したのち、ログイン(User:admin, Password:なし)をして項番(1)の手順でバージョンの確認を行います。

(10) 保存していたコンフィグをリストアします。 3.Config のバックアップ、リストア参照

(11) 実通信に問題が発生していないことを確認します。
アップグレードによる問題の有無を確認します。
問題が発生した場合は設定等を見直し問題の修正または切り戻しを行います。
切り戻し方法は、CLI でのダウングレード(「5. CLI でのアップグレード、ダウングレード」参照)を実行後に、「5.1 準備」にてバックアップした Config をリストアします(「3.Config のバックアップ、リストア」参照)。

(12) アンチウィルス、IPS をご利用されている場合は、execute update-now コマンドにより最新シグネチャのアップデートを実行します。シグネチャアップデート時には機器に多少の負荷がかかります。

6. HA 構成時のアップグレード、ダウングレード

HA 構成時における NVC 推奨アップグレード作業手順ついて解説いたします。

注意:Active-Passive の HA 構成時の手順について解説いたします。Active-Active の HA 構成の場合は弊社サポートへご連絡下さい。

6.1 準備

以下のものを準備します。

- PC(TeraTerm 等のターミナルソフト、TFTPServer ソフトがインストールされているもの)
- LAN ケーブル
- シリアルケーブル (FortiGate に付属)
- アップグレード(またはダウングレード)するファームウェアファイル
- リストアする Config ファイル(事前にバックアップしたファイルをリストアする場合)

現在の Config の保存を必ず行います。 3.Config のバックアップ、リストア参照

6.2 PC の設定

CLI では、ターミナルソフトを利用してコマンドを実行します。

(1) TeraTerm の設定を以下の通りに設定します。(コンソールから実施する場合)

- ボーレート:9600
- データ :8 ビット
- パリティ :なし
- ストップ :1
- フロー制御 : なし

6.3 HA ステータスの確認

Master の FortiGate を FortiGate01、Slave の FortiGate を FortiGate02 として説明致します。

(1) ターミナルソフトより FortiGate01 にアクセスします。
(2) ユーザー名・パスワードを入力してログインします。
(3) HA ステータスを get system ha status により確認します。(6.9 コマンド実行例 参照)
(4) ターミナルソフトより FortiGate02 にアクセスします。
(5) ユーザー名・パスワードを入力してログインします。
(6) HA ステータスを get system ha status により確認します。(6.9 コマンド実行例 参照)

6.4 FortiGate02 をネットワークから切り離す

(1) FortiGate02 の通信用ケーブルを抜線します。
(2) FortiGate02 の HA 用ケーブルを抜線します。

6.5 FortiGate02 のアップグレード

別項の「4.WebUIでのアップグレード」を参照します。

*Configの引継ぎが必要な場合はWebUIを利用したアップグレード手順にて実施願います。

6.6 FortiGate02 と FortiGate01 の入れ替え

(1) FortiGate01 の通信用ケーブルと HA 用ケーブルを抜線します。

※ケーブルの付け替えを行うので通信断が発生します。

(2) FortiGate02 の通信用ケーブルと HA 用ケーブルを結線します。

(3) 実通信に問題が発生していないことを確認します。
アップグレードによる問題の有無を確認します。
問題が発生した場合は設定等を見直し問題の修正または切り戻しを行います。
切り戻し方法は、CLI でのダウングレード(「5. CLI でのアップグレード、ダウングレード」参照)を実行後に、「6.1 準備」にてバックアップした Config をリストアします(「3.Config のバックアップ、リストア」参照)。

(4) アンチウィルス、IPS をご利用されている場合は、execute update-now コマンドにより最新シグネチャのアップデートを実行します。シグネチャアップデート時には機器に多少の負荷がかかります。

6.7 FortiGate01 のアップグレード

別項の「4.WebUIでのアップグレード」を参照します。

*Configの引継ぎが必要な場合はWebUIを利用したアップグレード手順にて実施願います。

6.8 FortiGate01 のネットワークへの導入

(1) FortiGate01 の HA 用ケーブルを結線します。

(2) get system ha status を実行して、HA が正常に組めていることを確認します。(6.9 コマンド実行例 参照)

(3) FortiGate01 の通信用ケーブルを結線します。

※ オーバーライドの設定が有効の場合は、切り戻りによる通信断が発生し、FortiGate01 が Master となります。無効の場合は、切り戻りは発生せずに FortiGate02 が Master のままとなります。FortiGate01 を Master に切り戻したい場合は、FortiGate02 のインタフェースを抜線し、切り戻りによる通信断が発生した後に FortiGate01 が Master に切り戻ります。

(4) 実通信に問題が発生していないことを確認します。

アップグレードによる問題の有無を確認します。

問題が発生した場合は設定等を見直し問題の修正または切り戻しを行います。

切り戻し方法は、CLI でのダウングレード(「5. CLI でのアップグレード、ダウングレード」参照)を実行後に、「6.1 準備」にてバックアップした Config をリストアします(「3.Config のバックアップ、リストア」参照)。

(5) アンチウィルス、IPS をご利用されている場合は、execute update-now コマンドにより最新シグネチャのアップデートを実行します。シグネチャアップデート時には機器に多少の負荷がかかります。

6.9 コマンド実行例

下記はホスト名が 「FortiGate01」と「FortiGate02」の機器でコマンドを実行した結果となります。

▼ForitGate01 # get system ha status

Model: FortiGate-200D
Mode: a-p
Group: 0
Debug: 0
ses_pickup: disable
Master:100 FortiGate01 FGT200D[redacted] 0
Slave :200 FortiGate02 FGT200D[redacted] 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Master:0 FGT200D[redacted]
Slave :1 FGT200D[redacted]

以上