Fortigate Firmware VersionUp 手順書

Ver.4.0MR2Patch6→ Ver.4.0MR3Patch3

Ver.4.0MR3Patch1→ Ver.4.0MR3Patch3

NVC
NETWORK VALUE COMPONENTS

改訂履歴

初版：2011 年 12 月 19 日

目次

はじめに

本マニュアルは Fortigate の OS バージョンを Version4.0MR3(Patch1)もしくは、Version4.0MR2(Patch6)から弊社推奨バージョン Version4.0MR3(Patch3)へ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。

アップグレード、ダウングレード方法について

FortiGate でのアップグレード・ダウングレードは WebUI と CLI の 2 通りが使用されます。

<<アップグレード>>

[WebUI]

設定を引き継ぎつつ OS の Version を上げる事が可能。*一部引き継がれない設定がございます。

[CLI]

工場出荷状態になります。

<<ダウングレード>>

[WebUI]

ほぼ全ての設定が失われますので、ダウングレードはより確実な CLI から行うことをお勧め致します。

[CLI]

工場出荷状態になります。

1. v4.0MR3Patch1 からのアップグレード

現在使用しているバージョンがv4.0MR3Ptch1の場合、直接v4.0MR3Patch3へアップグレードすることが可能です。

※なお、config の保存、リストア　WebUI でのアップグレード・ダウングレード方法は、項番 5,6,8 を参考に行ってください。

2. 設定の引継ぎに関する情報 (v4.0MR3Patch1→v4.0MR3Patch3)

特にございません。

3. v4.0MR2Patch6 からのアップグレード

v.4.0MR2Patch6未満からv4.0MR3Patch3上へは直接アップグレードができません。
現在使用しているバージョンがv4.0MR2Patch6未満である場合は、一度v4.0MR2Patch6にアップグレードを行なった後v4.0MR3Patch3へとアップグレードを行ないます。

以下は、V4.0MR2Patch6へのアップグレード手順書のリンクです。
http://gold.nvc.co.jp/supports/fortinet/OS/FortiOSv4.0MR2p6_rev1.pdf

※なお、config の保存、リストア、WebUI でのアップグレード・ダウングレード方法は、項番 5,7,8 を参考に行ってください。

アップグレードパス

1.v4.0MR2Patch6未満→v4.0MR2Patch6にアップグレード
2.v4.0MR2Patch6→v4.0MR3Patch3 にアップグレード

4. 設定情報の引継ぎ (v4.0MR2Patch6→v4.0MR3Patch3)

注意：下記はv4.0MR2patch6からv4.0MR3patch3へアップグレードする際に発生する項目です。

- **DNS Server**

インタフェースの設定にある dns-query recursive/non-recursive オプションは、VDom ごとのシステム設定に移動します。また、FortiOSv4.0MR3Patch3 へのアップグレード後は、config system dns-server にて、このオプションの設定を行なうことが出来ます。(CLI からのみ設定可)

- **Ping Server**

インタフェース設定の Ping Server オプションにある gwdetect は、VDom ごとの router 設定に引き継がれます。FortiOSv4.0MR3Patch3 へのアップグレード後は、config router gwdetect にて、このオプションの設定を行なうことができます。(CLI からのみ設定可)

- **SNMP community**

FortiOSv4.0MR3Patch3 へのアップグレード後、SNMP ホストの IP アドレスをネットマスクで指定できます。

- **AMC slot settings**

FortiOSv4.0MR3Patch3 へのアップグレード後、config system amc-slot で設定されている ips-weight のデフォルト値が balanced から less-fw に変わります。

- **Web フィルタリング overrides**

FortiOS v4.0 MR2 Patch6 から FortiOS 4.0MR3Patch3 へアップグレード後、Web フィルタのオーバーライドのコンテンツがなくなります。

- **Firewall policy settings**

送信元インタフェースまたは宛先インタフェースに、amc-XXX インタフェースを設定している場合、FortiOS 4.0MR3Patch3 へアップグレード後、config firewall poicy の ips センサーのデフォルト値が all_default から default に変わります。

- **URL Filter**

FortiOS 4.0MR3Patch3 へアップグレード後、URL フィルタの action 設定が、Allow、Pass、Expect、Block から Allow、Monitor、 Exempt、 Block に変わります。FortiOS 4.0MR3Patch3 の Allow はログの記録をしません。新しい設定の Monitor は Allow のアクションを行ない、ログを記録します。FortiOS 4.0MR2Patch6 の Pass は、FortiOS 4.0MR3Patch3 の Exempt に吸収されます。また、CLI コマンドが set action pass から set exempt pass に変更となります。

- **FortiGuard Log Filter**

FortiOS 4.0MR3Patch3 へアップグレード後、config log fortiguard filter の設定がなくなります。

- **FortiGurar Log Setting**

FortiOS 4.0MR3Patch3 へアップグレード後、config log fortiguard setting 上の quotafull や use-hdd オプションがなくなります。

5. Config の保存、リストア

5.1 準備

以下のものを準備する。

- ネットワーク接続可能な PC (IE8 もしくは FireFox 3.5 以上がインストールされていること)

5.2 PC の設定

WebUI では、ブラウザを利用して Config の保存を行います。

その為、作業は FortiGate に対してアクセス制限の無い PC で行います。

5.3 接続

(1) FG の HTTP/HTTPS のアクセスを許可しているポートに、PC を直接またはネットワーク経由で接続する。

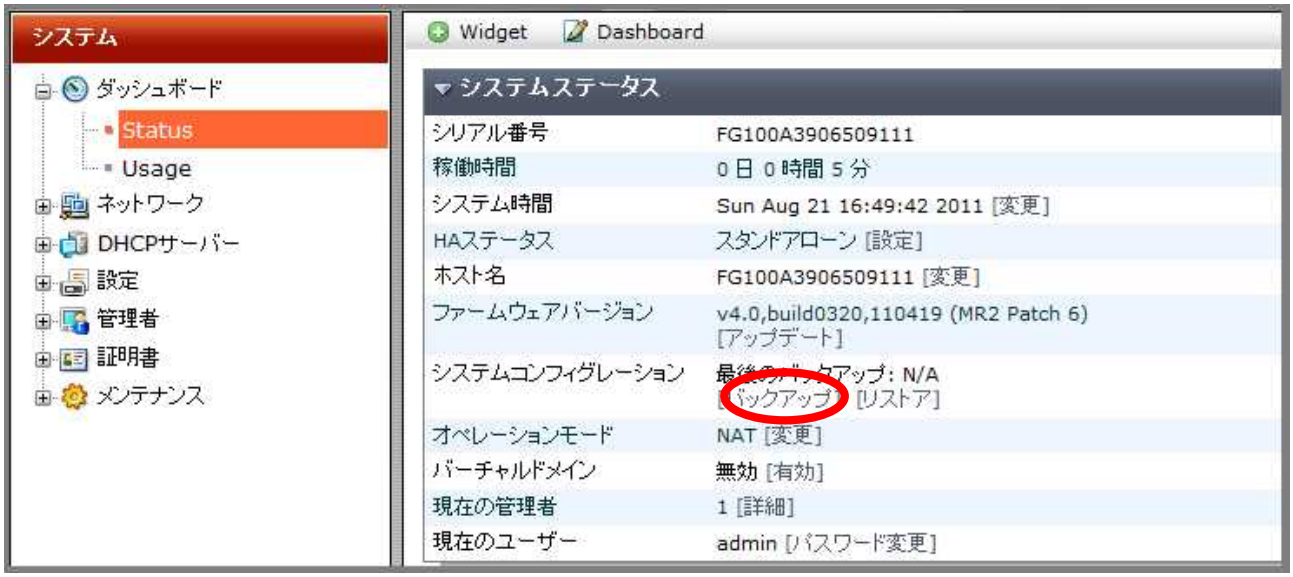
(2) PC のブラウザより FortiGate にアクセスする。

(https://xxx.xxx.xxx.xxx もしくは http://xxx.xxx.xxx.xxx x は FortiGate の IP を指定)

(3) ユーザー名・パスワードを入力してログインをします。

5.4 Config の保存(v4.0MR2Patch6)

(1) 左上のシステム>>ダッシュボード>>Status にある『バックアップ』をクリックします。



(Dashboard の status 画面 v4.0MR2Patch6)

(2) **バックアップ画面の『バックアップ』をクリックすると、バックアップがはじまります。**

(**バックアップ画面**　v4.0MR2Patch6)

5.5 Config **のリストア**(v4.0MR2Patch6)

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

(Dashboard **の** status **画面**　v4.0MR2Patch6)

(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。

(3) 画面の『復元』をクリックすると、リストアが始まります。

(リストア画面　v4.0MR2Patch6)

5.6Config の保存(v4.0MR3Patch1)

(1) 左上のシステム>>ダッシュボード>>Status にある『バックアップ』をクリックします。

（ダッシュボードの status 画面　v4.0MR3Patch1）

(2) バックアップ画面の『バックアップ』をクリックすると、バックアップがはじまります。保存するフォルダを指定して、バックアップを行なってください。

(バックアップ画面　v4.0MR3Patch1)

5.7 Config のリストア　(v4.0MR3Patch1)

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

（ダッシュボードの status 画面　v4.0MR3Patch1）

(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。

(3) 画面の『復元』をクリックすると、リストアが始まります。

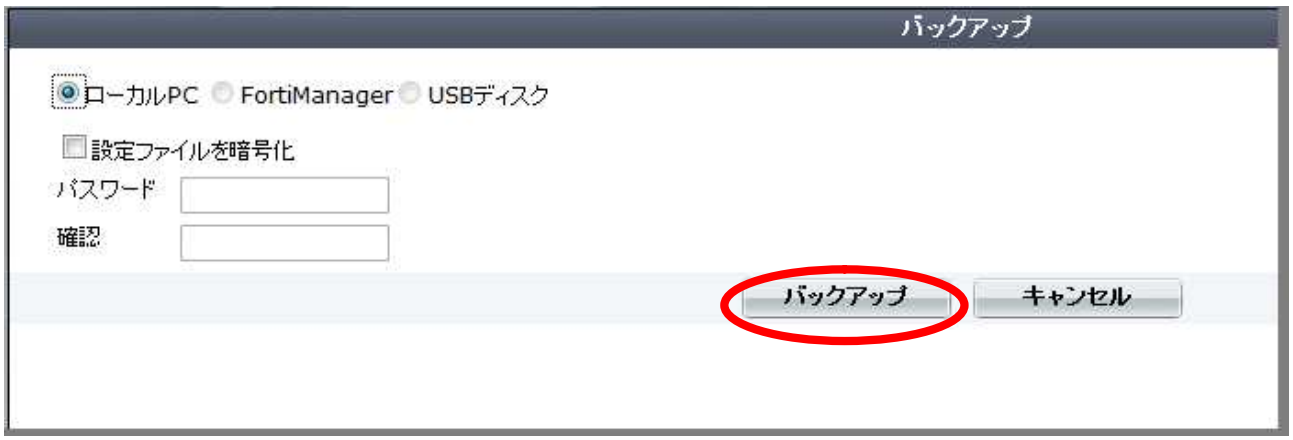
(リストア画面　v4.0MR3Patch1)

5.8 Config **の保存**(v4.0MR3Patch3)

(1) **左上のシステム>>ダッシュボード>>Status にある『バックアップ』をクリックします。**

(Dashboard の status **画面** v4.0MR3Patch3)

(2) **バックアップ画面の"バックアップ"をクリックすると、バックアップがはじまります。**



(**バックアップ画面** v4.0MR3Patch3)

5.9 Config **のリストア** (v4.0MR3Patch3)

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

(Dashboard の status **画面** v4.0MR3Patch3)

(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。

(3) リストア画面の『復元』をクリックすると、リストアが始まります。

(リストア画面　v4.0MR3Patch3)

6. WebUI でのアップグレード (v4.0MR3Patch1→v4.0MR3Patch3)

6.1 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 (IE8 もしくは FireFox 3.5 以上がインストールされていること)
- アップグレードするファームウェア

6.2 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 に対してアクセス制限の無い PC で行います。

6.3 接続

(1) PC のブラウザより FortiGate にアクセスをします。
(https://xxx.xxx.xxx.xxx もしくは http://xxx.xxx.xxx.xxx それぞれ FortiGate の IP を指定)

(2) ユーザー名・パスワードを入力してログインをします。

6.4 アップグレード

(1) 左上のシステム>>ダッシュボード>>Status の中央にある ファームウェアヴァージョンで現在のバージョンを確認します。(図 1 参照)

(2) 現在の config のバックアップを取得します。(注:p.12 参照)

(図 1．バージョン情報確認画面)

(3) ファームウェアヴァージョン の右にある『アップデート』をクリック。(図 2 参照)

(図２．アップデートボタン確認画面)

(4) 画面が切り替わった後アップグレードファイル:の右端にある『参照』をクリックしアップグレードするファイルを選択します。(図 3 参照)

(図３．アップデートボタン確認画面)

(5)　『OK』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。

(6)　再起動後、再ログインをしますと管理画面が変更されます。(図 4 参照)

(7)　項番(1)と同様にして、ファームウェアヴァージョンの確認を行います。

（図 4．v4.0MR3Patch3 の画面）

(8)　コンフィグをバックアップし作業は完了になります。(注 p.14 参照)

7. WebUI でのアップグレード (v4.0MR2Patch6→v4.0MR3Patch3)

2 バイト文字をご利用のお客様へ

v4.0MR3Patch3 へのアップグレードによって、文字コードが UTF-8 に変更となります。安全にアップグレードするために、**2 バイト文字をご利用のお客様は、すべての 2 バイト文字を半角英数字に変換してから、アップグレードをおこなってください。**なお、Web フィルタリングの禁止ワードは変換する必要はございません。

7.1 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 (IE8 もしくは FireFox 3.5 以上がインストールされていること)
- アップグレードするファームウェア
- テキストエディタ(Web フィルタリングのコンテンツブロックを使用しているお客様のみ使用)

7.2 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 に対してアクセス制限の無い PC で行います。

7.3 接続

(1) PC のブラウザより FortiGate にアクセスをします。
(https://xxx.xxx.xxx.xxx もしくは http://xxx.xxx.xxx.xxx それぞれ FortiGate の IP を指定)

(2) ユーザー名・パスワードを入力してログインをします。

7.4 アップグレード

(1) 左上のシステム>>ダッシュボード>>Status の中央にある ファームウェアヴァージョンで現在のバージョンを確認します。（図１参照）

(2) 現在の config のバックアップを取得します。(注:p.10 参照)

（図１．バージョン情報確認画面）

(3) ファームウェアヴァージョン の下にある『アップデート』をクリック。（図 2 参照）

（図２．アップデートボタン確認画面）

(4) 画面が切り替わった後、アップグレードファイル: の右端にある『参照』をクリックしアップグレードするファイルを選択します。(図 3 参照)

（図３．アップデートボタン確認画面）

(5) 『OK』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。

(6) OS v4.0MR3Patch3 のアップグレード後、再ログインをしますと管理画面が変更されます。(図 4 参照)

(7) 手順(1)と同様にして、ファームウェアヴァージョンの確認を行います。

（図 4．v4.0MR3Patch3 の画面）

(8) コンフィグをバックアップし作業は完了になります。(注:p.14 参照)

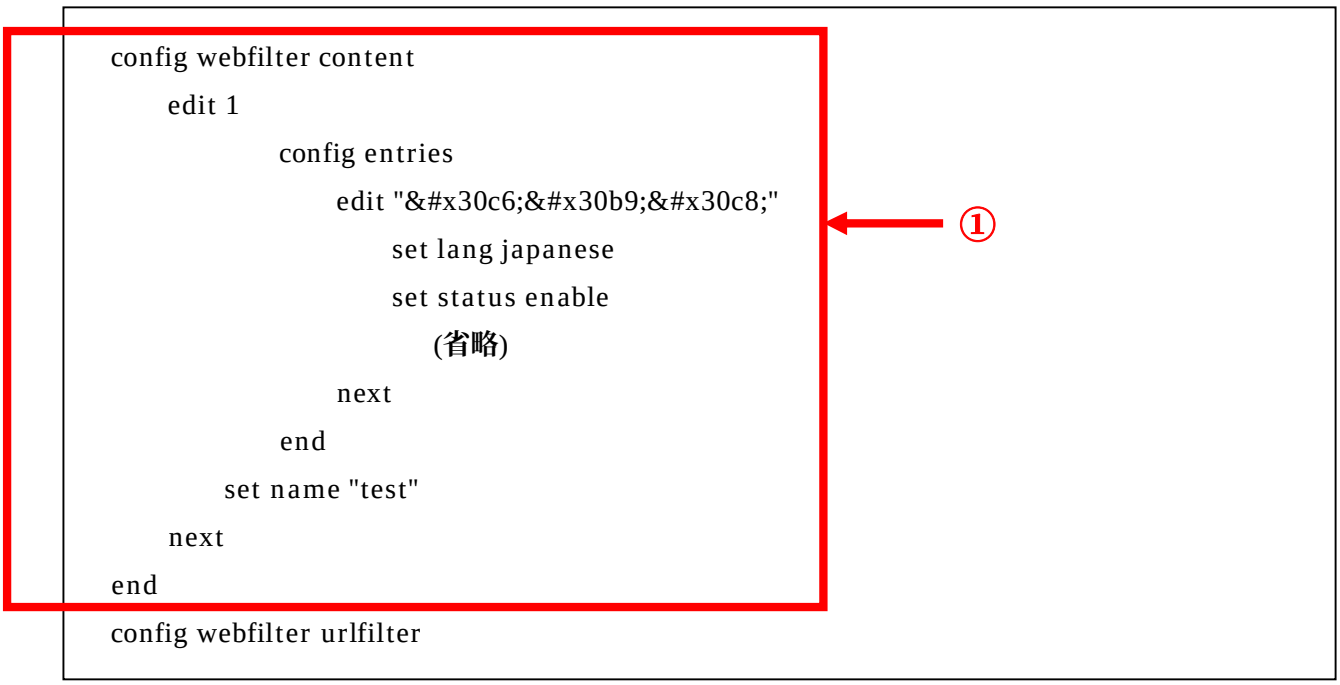
Web フィルタリングのコンテンツブロック機能をご利用しているお客様は、引き続き『7.5Config の修正』を行なってください。

7.5 Config の修正

v4.0MR2Patch6 の config では、Web フィルタリングのコンテンツブロックの禁止ワードが実態参照という表記方法で記載されています。『4.5Config の修正』では、実体参照部分を日本語に変換し、設定に反映させる方法を示します。

(1) 項番 7.4 の(8)でバックアップしたファイルをダブルクリックします。

(2) config の config webfilter content から config webfilter urlfilter の前の end までをコピーします。(図 5 の①参照)



（図 5．バックアップファイルの内容）

(3) テキストエディタを起動し、項番(2)でコピーした部分を貼り付けます。

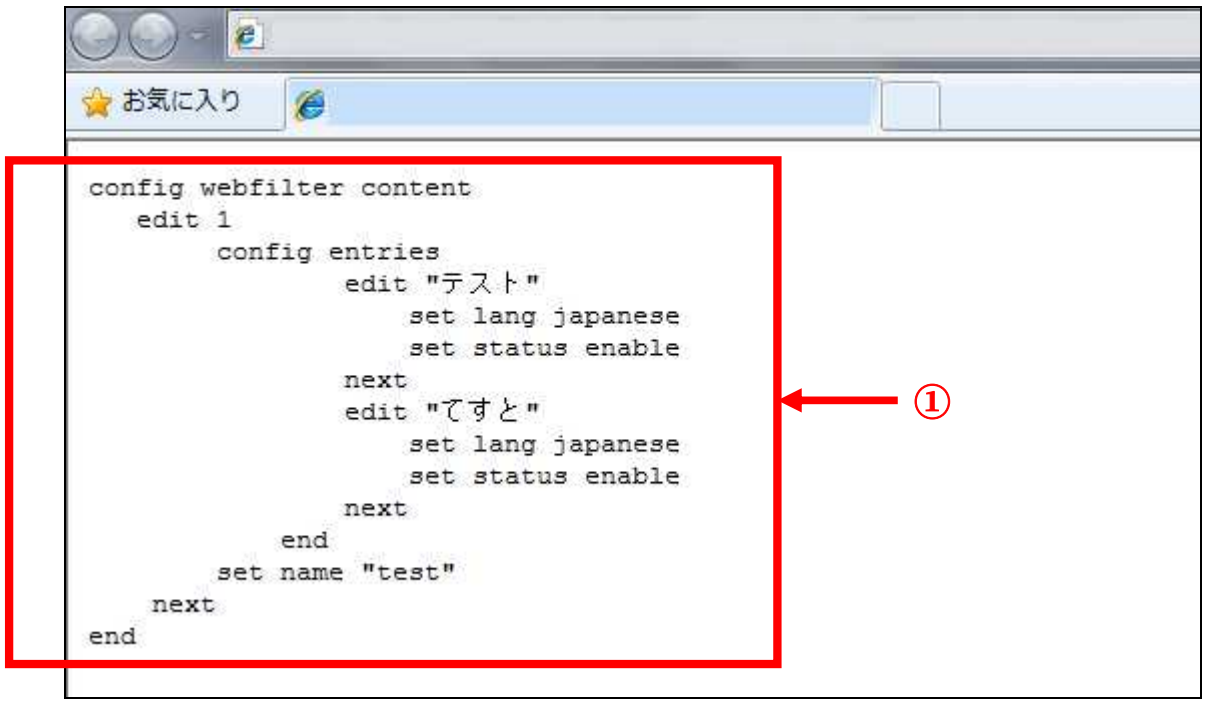
(4)　項番(3)のファイルの最初の行に<html><body><pre>を、
最後の行に</pre></body></html>を入力します。(図 6 の①、②参照)

```
<html><body><pre>                                    ①
config webfilter content
    edit 1
        config entries
            edit "&#x30c6;&#x30b9;&#x30c8;"
                set lang japanese
                set status enable
                    (省略)
            next
        end
    set name "test"
next
end
</pre></body></html>                                 ②
```

（図 6．html ファイルの内容）

(5)　項番(4)で編集したファイルを html ファイルとして保存します。

(6)　項番(5)で保存した html ファイルを開き、表示された文章をコピーします。(図 7 の①参照)



（図 7．Web ブラウザの内容）

(7) 項番(1)の config の config webfilter content から end に部分(図 5 の①参照)を、項番(7)でコピーした部分(図 7 の①参照)に置き換えます。変更後は図 8 のようになります。

```
config webfilter content
    edit 1
        config entries
            edit "テスト"
                set lang japanese
                set status enable
                    (省略)
            next
        end
        set name "test"
    next
end
config Web フィルタリング urlfilter
```

（図 8. 変更後）

(8) 文字コードを UTF-8 で、項番(1)のバックアップファイルとは別名で保存します。

(9) 項番(8)で保存した config ファイルを機器にリストアします。(注：p.14 参照)

(10) リストア後に config をバックアップして作業終了です。(注：p.14 参照)

8. CLI でのアップグレード、ダウングレード

注意: CLI でアップグレードの場合、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。

8.1 準備

以下のものを準備する

- ネットワーク接続可能な PC(TeraTerm 等のターミナルソフト、TFTPServer がインストールされていること)
- クロス LAN ケーブル
- クロスシリアルケーブル (FortiGate に付属)
- アップグレードするファームウェア
- ダウングレードするファームウェア
- 適用するコンフィグ(ある場合)

また、現在の Config の保存を行なう。(注:p.10 または p.12 参照)

8.2PC の設定

CLI では、TFTP サーバを利用してアップグレード行います。そのため、PC の設定は 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 アドレスを設定する(例:192.168.1.10/24)

(2) TeraTerm の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 ではファームウェアを保存してあるフォルダを指定します。

8.3 接続

(1) ターミナルソフトより FortiGate 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。

8.4 アップグレード、ダウングレード

(1) 現在のバージョンを確認する。get sys status で確認します。

(2) execute reboot と入力し、リブートを行います。

(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 を入力する。
※機体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。

FortiCLI 画面

FG100A3906509111 # 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...

FG100A3906509111 #
FG100A3906509111 #
Please stand by while rebooting the system.
FG100A (19:06-02.28.2006)
Ver:04000003
Serial number:FG100A3906509111
RAM activation
Total RAM: 256MB
Enabling cache...Done.
Scanning PCI bus...Done.
Allocating PCI resources...Done.
Enabling PCI resources...Done.
Zeroing IRQ settings...Done.
Verifying PIRQ tables...Done.
Disabling local APIC...Done.
Boot up, boot device capacity: 61MB.
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 G,F,B,I,Q,or H: ← G を入力する

(4) 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
(例: Enter tftp server address [192.168.1.168]: 192.168.1.10)

(5) 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
(例: Enter local address [192.168.1.188]: 192.168.1.99)

(6) 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
(例: Enter firmware image file name [image.out]: FGT_100A-v400-build0496-FORTINET.out)

(7) 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。

(8) 自動的にリブートされるのでログイン後、アップグレードの確認を行います。
ダウングレードの場合は、保存していたコンフィグをリストアします。

9. HA 構成時でのアップグレード、ダウングレード

HA 構成時に通信断を少なくするアップグレード作業の流れに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。

9.1 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(TeraTerm 等のターミナルソフト、TFTPServer がインストールされていること)
- アップグレードするファームウェア

9.2 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

9.3 HA ステータスの確認

主系の FortiGate を FortiGate01、従系の FortiGate を FortiGate02 として解説致します。
FortiGate02 の HA ステータスが Master であった場合は作業対象の機器が逆となります。

(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 ステータスの確認。diagnose sys ha status により確認します。(注:P28 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 ステータスの確認。diagnose sys ha status により確認します。(注:P28 参照)

9.4 FortiGate02 をネットワークから切り離し

(1) FortiGate02 の実通信を行っているケーブルを取り外します。
(2) FortiGate02 の HA の同期を行っているケーブルを取り外します。

9.5 FortiGate02 のアップグレード

別項のアップグレード手順を参照します。

「1. v4.0MR3Patch1からのアップグレード」または、「3. v4.0MR2Patch6からのアップグレード」を参照

*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。

*ダウングレードではCLIによる実施を推奨致します。

9.6 FortiGate02 と FortiGate01 の入れ替え

(1) FortiGate01 の実通信ケーブルと HA ケーブルを取り外します。
※通信断が発生いたします。
(2) FortiGate02 の実通信ケーブルと HA ケーブルを取り付けます。
(3) exe update-now コマンドにより自動アップデートを実行します。
(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を修正します。

9.7 FortiGate01 のアップグレード

別項のアップグレード手順を参照します。

「1. v4.0MR3Patch1からのアップグレード」または、「3. v4.0MR2Patch6からのアップグレード」を参照

*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。

*ダウングレードではCLIによる実施を推奨致します。

9.8 FortiGate01 のネットワークへの導入

(1) FortiGate01 の HA ケーブルを取り付けます。
(2) diagnose sys ha status によりネゴシエーションが行えていることを確認します。(注:P28 参照)
(3) FortiGate01 の実通信ケーブルを取り付けます。
(4) 実通信に問題が発生していないことを確認します。

以下コマンドの実行例となります。

注：diagnose コマンドはメーカ開発コマンドであるため詳細にはお答え致しかねますので予めご了承頂きたくお願い致します。

▼ForitGate01 # diagnose sys ha status

```
HA information
Statistics
        traffic.local = s:5478 p:191932 b:43865437
        traffic.total = s:5856 p:191933 b:43865497
        activity.fdb    = c:0 q:0

        Model=300, Mode=2 Group=0 Debug=0
        nvcluster=1, ses_pickup=1

        HA group member information: is_manage_master=1.
        FG500A3909601XXX, 0. Master:255 ForitGate01
        FG500A3909602XXX, 1.    Slave:128 ForitGate02

        vcluster 1, state=work, master_ip=169.254.0.1, master_id=0:
        FG500A3909601XXX, 0. Master:255 ForitGate01(prio=0, rev=0)
        FG500A3909602XXX, 1.    Slave:128 ForitGate02(prio=1, rev=1)
```

10. v4.0MR3Patch3 の不具合情報

- WebUI

不具合 ID：156208
IE9 を使用し、PDF のリポートを作成しようとすると、Web ページがフリーズします。
今後の OS リリースで修正されます。

不具合 ID：156318
『VPN』の『IPsec』の『自動鍵(IKE)』の『FortiClient VPN を作成』のページで『Enable IPv4 Split Tunnel』が有効なっている場合、『Accessible Networks』を設定することができません。この不具合は今後の OS で修正されます。

不具合 ID：156210
グラフの軸の数字がうまく表示されない可能性がございます。また、『UTM プロファイル』の『モニタ』の『アプリケーションモニタ』のページで、グラフ軸の数字が表示されません。この不具合は今後の OS で修正されます。

- UTM

フローベースの DLP 機能において、フィルタをファイルタイプ、アクションをブロックに設定した場合、出力されるログのタイプがアンチウイルスと表示されます。

以上