Express5800/FirewallServer ユーザーズガイド

改訂表

2001年8月

2001年7月、FirewallServerに採用しているファイアウォールエンジンであるFireWall-1に2件のセキュリ ティホールが発見され、その対応策としてCheck Point社よりHotFixが提供されています。

http://www.checkpoint.com/techsupport/alerts/rdp.html

http://www.checkpoint.com/techsupport/alerts/format_strings.html

これにともない、FirewallServerにおいてもHotFix適用(HotFixを適用するには先にSP4の適用が必要となります)が必須となり、インストール手順が同梱の「Express5800/FirewallServer ユーザーズガイド」の 内容から一部変更になります。

下記に示す新しいインストール手順に従い、必ずSP4とHotFixを適用するようにお願いいたします。

ページ	改訂前	改訂後
P.54	システムのセットアップ	
	4. <u>FireWall-1 SP3 の適用</u>	4. <u>FireWall-1 SP4+HotFix の適用</u>
P.62	FireWall-1 SP3の適用	別紙1差し替え
P.68	FireWall-1のカーネルバージョンの確認	別紙2差し替え
P.88	再インストールの手順	別紙3差し替え
P.147	FirewallServerのセットアップ	
	3. <u>FireWall-1 SP3 の適用</u>	3. <u>FireWall-1 SP4+HotFix の適用</u>
P.152	SP3のインストール	別紙4差し替え

別紙1

FireWall-1 SP4 + HotFixの適用

2001年8月末現在の最新パッチはSP4(CPfw1-41.4-SP4.i386.rpm)+HotFixです。 管理コンピュータから以下の手順でSPパッケージとHotFixを展開してください。

重要

FireWall-1 のパッチは定期的に発行されています。パッチの入手にあたっては、保守型番(ULH)製品を購入する必要があります。詳細につきましては「保守サポート/保守サービスについて(16ページ)」を参照してください。



ディレクトリを変更する。 rpm コマンドでSP4パッケージを展開する。 この例では表示を省略しています。 rpm コマンドでHotFixパッケージを展開する。 終了後、rebootする。

別紙2

FireWall-1 のカーネルバージョンの確認

再起動後、再度コンソールから root ユーザでログインして fw ver -k コマンドでFireWall-1のカーネ ルバージョンが「41862」になっていることを確認してください。

fw ver -k
This is Check Point VPN-1(TM) & FireWall 1(R) Version 4.1 Build 341418 [VPN + DES]
kernel: Version 4.1 [VPN + DES] Build 41862

これでFirewallServer の設定が終了しました。

今後、FirewallServer が立ちあがると自動的にFireWall-1 が起動するようになります。

再インストールの手順

次の手順に従って再インストールします。

- 本体前面にあるフロッピーディスクドライブに再インストール用ディスクをセットし FirewallServer を再起動する。
 管理コンピュータのディスプレイに [boot:]の表示が出るまで待ってください。
- 本体前面にあるCD-ROM ドライブに OS CD-ROM をセットする。
 自動的にプログラムCD-ROM からのインストールが始まります。インストールは約10分で完了します。
 インストールを完了すると、ディスプレイにインストールの完了を通知するメッセージが表示されます。
- <Ctrl>-<D>キーを押す。
 自動的に再起動が開始されます。再起動を開始したら、セットしたフロッピーディスクとCD-ROM を
 本体から取り出してください。

>> install finish. press Ctrl+D bash# 、 ここで<Ctrl>-<D>キーを押す

- 4. 再起動開始から約3分程度経過したら、管理コンピュータの<Enter>キーを押す。
- Iogin プロンプトが表示されたら、「root」と入力し、Password に添付品の「root パスワード」に 書かれているパスワードを入力する。 ログインに成功すると[#]のプロンプトが表示されます。
- 6. CD-ROMドライブにバックアップCD-ROM をセットし、以下の手順でESMPRO/ServerAgentなどの追加パ ッケージを展開する。

$\left(\right)$	#	mount /dev/cdrom	
	#	/mnt/cdrom/nec/Linux/necsetup	
L	#	umount /dev/cdrom	

- 7. CD-ROMドライブからバックアップCD-ROM を取り出す。
- <あらかじめバックアップしておいた設定をリストアする場合> 以下のコマンドを実行して基本設定をする。

設定をバックアップしたフロッピーディスクを本体にセットしてください。

/	<pre># /opt/necfws/bin/fwrestore -i</pre>	\backslash
	Please insert backup floppy disk. (#1)	
	Press enter key バックアップディスクをセッ	トして <enter>を押す</enter>
	restore fws.ini	
	restore caeconf.ini 二重化構成を使用していない	場合は表示されない
	restore completed.	
	After turned off FDD access light, Press enter key. \diagdown	
	<pre># /opt/necfws/bin/fwsetup -i /opt/necfws/etc/fws.ini</pre>	、 フロッピーディスクドライプの
		アクセスランプが消えたら
	# shutdown -r now 終了後、再起動する	<enter>キーを押し、その後</enter>
		フロッピーディスクを取り出す
1	×	

<バックアップのリストアをしない場合> 「設定ツールによる基本設定(58ページ)」を参照して基本設定をする。

9. CD-ROM ドライブにCheck Point 2000 のCD-ROM をセットし、FireWall-1 のモジュールを以下の手順 で展開する。

10. Check Point 製品パッチのCD-ROM に入れ換え、FireWall-1 のSPとHotFix を以下の手順で適用する。

mount /dev/cdrom # cd /tmp # gtar xvzf /mnt/cdrom/fw141/sp4/vpndes/linux/fw1_41862_5_sp4_linux_des.tgz # rpm -i --replacefiles CPfw1-41.4-SP4.i386.rpm # cd /opt/CPfw1-41/lib # gtar xvzf /mnt/cdrom/fw141/rdp/is_fw1_41_sp4_rdphf_tar.gz # chown root crypt.def table.def # chgrp root crypt.def table.def # chmod 670 crypt.def table.def # cd /opt/CPfw1-41/bin 804-091639-017-A

(#	gtar xvzf /mnt/cdrom/fw141/fs/des/sp4/linux/fw41sp4_fshf_linux_des_tar.gz	
	#	chown root fw	
	#	chgrp root fw	
	#	chmod 770 fw	
	#	umount /dev/cdromここでCD-ROMを取り出す	
Ĺ	#	shutdown -r now	

二重化構成をとるためにFireWall-1を分散型構成でインストールしている場合、この後の手順は「二重化構成について」の分散構成の再インストール(4章)に従ってください。

11. <あらかじめバックアップしておいた設定をリストアする場合>

以下のコマンドを実行してFireWall-1 の設定をする。

cpconfig については「FireWall-1 のコンフィグレーション(63ページ)」を参照してください(ラ イセンス、管理者の登録、クライアントマシンのIPアドレスはバックアップデータに含まれているため省 略することができます)。

# cpconfig	
<pre># /opt/necfws/bin/fwrestore -f</pre>	
Please insert backup floppy disk. (#1)	
Press enter key.	パックアップディスクをセットして
There is 1 floppy disk for restore.	<enter>キーを押す</enter>
restore fw config files (1/1)	
restore completed.	
After turned off FDD access light, Press enter	r key.
# shutdown -r now 終了後、再起動する	フロッピーディスクのアクセスランプが
\backslash	消えたら <enter>キーを押し、その後 /</enter>
	フロッピーディスクを取り出す

<バックアップのリストアをしない場合>

「FireWall-1 のコンフィグレーション(63ページ)」を参照して設定をする。

12. GUI クライアントからポリシーをインストールする。

SP4 + HotFixの適用

2001年8月末現在の最新パッチはSP4+HotFixです。 FireWall-1管理モジュールのSPとHotFixは同梱されているCHECKPOINT製品パッチのCD-ROMから以下の手 順でインストールします。

- 1. FireWall-1管理モジュールがインストールされているコンピュータのCD-ROMドライブにCHECKPOINT製 品パッチのCD-ROMをセットする。
- モジュール「fw1_41862_2_sp4_win32_des.tgz」をコンピュータの適当なフォルダへコピーする。
 モジュールはCD-ROMの[fw141]フォルダ [sp4]フォルダ [vpndes]フォルダ [win32]フォルダ内にあります。
- WinZip7.0などのツールを使いモジュールを解凍する。
 モジュールは圧縮されています。解凍されると[Disk_Images]フォルダ [Disk1]フォルダが形成され、
 [Disk1]フォルダの中にモジュールが展開されます。
- [Disk1]フォルダの中にあるSetup.exeをダブルクリックする。
 インストールプログラムが起動し、画面の指示に従い[Next]ボタンをクリックします。
 使用許諾書が表示されます。
- 問題がなければ[Yes]ボタンをクリックする。
 [Yes]ボタンをクリックするとSP4のインストールが開始されます。
 [No]ボタンをクリックした場合は、インストールは中断されます。
- インストール完了後、コンピュータを再起動する。 CD-ROMはセットしたままにしておきます。
- FireWall-1サービスを停止する。
 コマンドプロンプトから*\$FWD1R*#bin¥fwstopコマンドを実行するか、サービス一覧から[Check Point VPN-1/FireWall-1]を停止します。(*\$FWD1R*はFireWall-1管理モジュールをインストールしたフォルダ です。通常はC:¥winnt¥fw1¥4.1になります。)
- モジュール「is_fw1_41_sp4_rdphf_tar.gz」をコンピュータの適当なフォルダへコピーする。
 モジュールはCD-ROMの[fw141]フォルダ [rdp]フォルダ内にあります。
- 9. WinZip7.0などのツールを使いモジュールを解凍する。 モジュールは圧縮されています。解凍するとcrypt.def,table.defの2つのファイルが展開されます。

804-091639-017-A

- 10. crypt.def,table.defファイルを*\$FWD1R*4libフォルダにコピー(上書き)する。
- モジュール「fw41sp4_fshf_win32_des.zip」をコンピュータの適当なフォルダへコピーする。
 モジュールはCD-ROMの[fw141]フォルダ [fs]フォルダ [des]フォルダ [sp4]フォルダ [winnt]フォルダ内にあります。
- 12. WinZip7.0などのツールを使いモジュールを解凍する。 モジュールは圧縮されています。解凍するとfw.exeファイルが展開されます。
- 13. fw.exeファイルを*\$FWDIR*4binフォルダにコピー(上書き)する。
- 14. FireWall-1サービスを開始する。 コマンドプロンプトから*\$FWD1R*#bin¥fwstartコマンドを実行するか、サービス一覧から[Check Point VPN-1/FireWall-1]を開始します。