



We Secure the Internet.

Check Point VPN-1/FireWall-1™

Version 4.1 SP6 Release Notes

First published: April 2002

Introduction

Thank you for using Check Point VPN-1/FireWall-1 4.1 SP6. This document contains important information not included in the VPN-1/FireWall-1 documentation. Please review this information before installing VPN-1/FireWall-1 4.1 SP6.

This service pack can be applied to VPN-1/FireWall-1 Version 4.1 SP1, Version 4.1 SP2, Version 4.1 SP3, Version 4.1 SP4, and Version 4.1 SP5.

The latest version of the VPN-1/FireWall-1 Release Notes can be found at
<http://www.checkpoint.com/techsupport>

Service Pack Availability

This Service Pack is available for the DES and Strong (3DES) editions for all supported product platforms (HPUX/PA, Solaris/SPARC, Solaris/x86, Windows NT/x86, Windows 2000, Linux, IPSO and AIX). For more information, see "Installation Instructions" on page 5.

In This Document

<i>Supported Platforms</i>	<i>page 1</i>
<i>Build Numbers</i>	<i>page 2</i>
<i>Fixes and Improvements</i>	<i>page 2</i>
<i>Known Limitations</i>	<i>page 3</i>
<i>Installation Instructions</i>	<i>page 5</i>

IMPORTANT — For information about upgrading clusters in a High Availability configuration, see "Cluster Members" on page 7.

Supported Platforms

The supported platforms for VPN-1/FireWall-1 Version 4.1 SP6 are listed in TABLE 1:

TABLE 1 Platform Summary

Component	Platforms
GUI Client	■ Windows 9x, Windows NT 4.0 (SP6a), Windows 2000, Windows 2000 (SP1 and SP2)
X/Motif GUI Client	■ Solaris 2.6, 2.7 and 8, Solaris 7/SPARC, Solaris 8/SPARC ■ IBM AIX 4.1.5, 4.2, 4.3.0 ■ HPUX 10.20 (in 32 bit installation mode only)
Management Module, VPN/FireWall Module	■ Windows NT 4.0 (SP6a), Windows 2000 Server/Advanced Server (SP1 and SP2) ■ Solaris 2.6/SPARC, Solaris 7/SPARC, and Solaris 8/SPARC (in 32 bit installation mode only), Solaris 2.6/x86, Solaris 7/x86 ■ HPUX 10.20, HPUX 11.0 (in 32 bit installation mode only) ■ Red Hat Linux 6.2 (SMP kernel) — kernel version 2.2.x, Red Hat Linux 7.0 (SMP Kernel) ■ IPSO 3.4.1, IPSO 3.5 ■ IBM AIX 4.2.1, 4.3.2, 4.3.3

Build Numbers

The build numbers for the VPN-1/FireWall-1 Version 4.1 SP6 components are given in TABLE 2.

TABLE 2 Build Numbers

Product	Build Number	To verify, see ...
VPN-1/FireWall-1 Management and Module (Windows)	41618	<code>fw ver -k</code>
VPN-1/FireWall-1 Management and Module (Linux, Nokia, AIX, Solaris)	41617	<code>fw ver -k</code>
VPN-1/FireWall-1 Management and Module (HP)	41617	<code>fw ver -k</code>
VPN-1/FireWall-1 GUI Client	41608	Help_About
VPN-1/FireWall-1 GUI Client (Motif)	41608	Help_About

Note – The kernel version of the Solaris installations is 41512.

Fixes and Improvements

The following limitations were relevant in Version 4.1 SP5:

VPN-1

- 1 When exchanging keys using IKE, certificates, and IKE over TCP, Quick Mode is also performed over TCP. This happens only if Phase 1 is Main Mode and may cause connectivity problems when using VPN clusters.
- 2 The command line `fw isakmpd_debug on` will not take effect (i.e., will not create the `isakmpd.elg` file) until VPN-1/FireWall-1 is restarted.
- 3 Memory leak may occur when a VPN/FireWall Module is under heavy load with SecuRemote connections and is using an LDAP server for authentication.
- 4 A policy installation on a VPN/FireWall Module (using FWZ) may cause a heavy load on the Management Server.
- 5 IKE over TCP is not supported if the VPN/FireWall Module and the Management Server are not installed on the same machine.

FireWall-1

- 1 After upgrading the Management Server from an earlier Service Pack, traffic is not passed after installing a policy on a cluster running SBFC 2.0 SP3a.
- 2 Policy installation may make the Module unstable when FLOWS is enabled.
- 3 When FLOWS is enabled it is possible that connections will not be removed from the connection table. These connections will appear in the connections table with a negative timeout value.
- 4 The files `loggers` and `dnsinfo.C` are lost after upgrading from an earlier version.
- 5 The problems related to the following message in the Event Viewer application log have been fixed: **“Firewall-1: SwOpen: failed to open C:\WINNT\FW1\4.1\database\fwauthtmp.NDB: The system cannot find the file specified.”**
- 6 The **HA** tab in the `cpconfig` Configuration Tool appears blank when FireWall-1 is installed on a non-English version of Windows NT.
- 7 A StoneBeat configuration on a dual CPU machine may cause a system panic.
- 8 Policy installation from a Solaris 8 Management Server can sometimes fail.
- 9 The `fwstart` command may fail on non-Intel machines.
- 10 On a Windows machine, several ICMP connections with NAT to a single destination are not supported. In version 4.1 SP6 they can be supported by enabling the `enable_nated_icmp` property in `objects.C`.
- 11 Communication problems with Axent servers cause authentication failures.
- 12 URLs that contain the character `@` are not handled correctly by the HTTP security server.
- 13 Mails are stuck in the SMTP Security Server spool when working with eSafe CVP Server.
- 14 The HTTP Security Server sends cacheable headers when redirecting client authentication connections. Proxy servers that cache user-passwords will therefore serve the same user-password to the FireWall. If the authentication method is “one time password” then every authentication after the first one will fail.

In version 4.1 SP6 this behavior is controlled by the `http_allow_store_reply` property in `objects.c`. When this property is enabled, the Security Server will send no-store in the Cache-Control header. For an explanation of the AOL caching method, see <http://webmaster.info.aol.com/index.cfm?article=12&expand=0&sitenum=2>.

- 15** UFP fails under stress conditions with the error message “**Unknown error while trying to connect to UFP**”.
- 16** In the log Viewer, when more than 20000 logs are displayed, there is a problem closing the Log Viewer properly.
- 17** Log files larger than 512 MB are not properly handled.
- 18** Installing a policy with a large NAT rule base may fail because of memory allocation problems.
- 19** Installing a policy on a SecureServer with **Gateways** in the **Install On** field of a rule, fails.
- 20** ACL Downloads on 3Com routers are not supported.
- 21** HSSI (High Speed Serial Interfaces) NICs for Cisco routers are not supported.
- 22** Under load conditions, the FireWall-1 Alert subsystem may stop functioning on the Windows platforms. Connections in the Log Viewer are still marked as Alert but no actual alerts are sent. The following error appears in the Event Viewer application log: “**firewall-1: T_evenet_NT_mainloop: wait failed: The handle is invalid**”.
- 23** IKE over TCP is not supported if the VPN/FireWall Module and the Management Server are not installed on the same machine.
- 24** In previous versions, SNMP queries sent to the FireWall-1 SNMP daemon requesting non-Check Point MIBs may have resulted in high CPU utilization (Only on Unix platforms and only if the OS SNMP daemon is not running). In version 4.1 SP6 (and in future versions) FireWall-1 SNMP daemon serves requests only for Check Point MIBs. Other requests are sent to an OS daemon.
- 25** There is a memory leak in the HTTP Security Server when client authentication is used.
- 26** Incorrect DNS resolution results under load.
- 27** Fixed problems related to the error message “**Can’t retrieve the cao from hash**” with RADIUS authentication.
- 28** Memory leak when client authentication is used in the HTTP Security Server and there are a number of rules with different user groups.
- 29** The `fw tab -t <remote module>` connections may display negative timeout values when the module is in a different time zone.
- 30** The following commands are not supported: `fwall stat`, `fwall load`, `fwall unload`.

Known Limitations

FireWall-1

General

- 1** FTP resources are not supported with FTP servers that have extensive welcome messages.
- 2** The command **fw getver** may display wrong version information.
- 3** FTP resources are not supported when SYN Defender Gateway is enabled.
- 4** Some H.323 UDP media connections may fail if **Accept UDP Replies** is disabled in the **Security Policy** tab of the policy's properties.
- 5** After upgrading from SP2, `polsvrd` and `netsod` processes may crash. These processes are part of the DTM package and are not required for normal FireWall-1 operation.
It is recommended to disable these DTM processes as described in Secure Knowledge solution sk13408 (available at <http://support.checkpoint.com/kb/>).
If your configuration requires DTM, this problem is corrected by applying the following packages (available from CheckPoint's support site <http://support.checkpoint.com>)
 - UAG SP4
 - DTM SP5
 Please note that is important to apply the UAG SP4 package first.
- 6** More than one Log Viewer can be connected to the same Management Server or CLM in Read/Write mode at the same time.

- 7** When importing an ACL from a Cisco or 3Com router, the policy name of the previous policy is displayed. To show the correct policy name, close and reopen the Policy Editor, or open the imported policy from the **File** menu.
- 8** Upgrading to SP6 may cause DTM (polsrzd) to exit with exceptions. Explanation: DTM is required for checking the SCV status of SecureClient communicating from the protected LAN outwards. This product was automatically installed and activated in SP2. In most configurations it is not required at all, and can be deactivated by remarking the polsrd line in the \$FWDIR/conf/fwauthd.conf file. If you do need this product, make sure you upgrade it to SP5, which is compatible with FireWall-1 SP6.
- 9** The HTTP Security Server handles proxy and tunneled connection request differently than earlier FireWall-1 versions. Starting from FireWall-1 SP6, such requests are not allowed if they are matched with an **Accept** rule, they are still allowed if the request is matched with an authentication or a resource rule. This change was introduced in order to tighten security and prevent the CONNECT looping to the Security Server and then to another destination. This behavior can be reverted to the old behavior by modifying the following global properties (in objects.C) to true and installing the policy:
 - http_connection_method_proxy
 - http_connection_method_tunneling
 These properties were added only for compatibility reasons and it is not recommended to change their default values.

Motif GUI

- 10** A memory leak occurs in the Log Viewer.
- 11** Running fwstop/fwstart causes the System Status to generate application failure.

Platform Specific - Windows 2000

- 12** 802.1q (VLAN) virtual interfaces are not supported.
- 13** default.bin can only be read from the drive that the system is installed on. For default security to be enforced, it is necessary that the value of FW1\Parameters\DefaultPolicy in the registry point to a copy of default.bin in the same drive as the system.
- 14** fw kill is not supported.
- 15** Only 13 interfaces are supported.
- 16** Cannot install an Access List on a Bay router if it contains a rule with the ICMP service.

Platform Specific - Solaris

- 17** Changes made to the control.map file are lost after FireWall-1 is upgraded.
- 18** plx interface is not supported.

Platform Specific - Linux

- 19** Segmentation fault when removing 802.1Q virtual interfaces when the FireWall is running. The following workaround is available: stop the module before modifying virtual interfaces and then restart.
- 20** Running tcpdump with 802.1q VLANs is not supported.

Platform Specific - Nokia

- 21** After installing this Service Pack, you must reboot the system in order for the Service Pack to take effect, even though Voyager does not require that you reboot.
- 22** FireWall-1 supports up to 8 IP addresses for each 4-port Ethernet card.

Platform Specific - HPUX 11

- 23** The Madge Smart 16/4 EISA Ringnode Token Ring interface is not supported.

Platform Specific - AIX

- 24** Policy installation may fail with large policies with more than 350 rules.

VPN

IKE, Interoperability

- 1** An IPSec tunnel will not open if the IKE Scheme uses the following parameters: for Phase 1: 3DES+MD5; for Phase 2: AES256+SHA1 (+PFS).

VPN-1 and SecuRemote/SecureClient Issues

- 2** Removing the internal CA certificate in the **VPN** tab of a VPN/FireWall Module's **Workstation Properties** window does not disable the Hybrid mode support (in the same tab). As a result, when a 4.1 client attempts to download the topology, it tries to use Hybrid mode and the negotiation fails. To avoid this

scenario, before removing the internal CA certificate from a 4.1 VPN/FireWall Module, disable the Hybrid mode support and make sure that all clients have downloaded the topology. Only then the internal CA certificate can be safely removed.

High Availability, Load Sharing (MEP/SEP), Load Balancing

- 3 When using VRRP with SecuRemote that is configured to work with FWZ, RDP packets sent from SecuRemote to the cluster's virtual IP address receive responses from the physical IP address of the active gateway. This may cause connectivity problems for SecuRemote clients located behind a VPN/FireWall Module.
- 4 When defining a cluster, multiple interface resolving mechanisms are not supported with any Load Sharing or High Availability solution.
- 5 Upgrading a 4.1 SP4 Management Server to SP5 or SP6 may cause connectivity problems due to a wrong upgrade of the following properties in the `objects.C` file: `IPSec_cluster_nat` (related to VPN-1 cluster members) and `IPSec_main_if_nat` (related to VPN/FireWall Modules with multiple interfaces).

Both properties were global in SP4 and have been modified to be per object in SP5. In case there is a discrepancy while upgrading from SP4 to a more advanced SP:

- `IPSec_cluster_nat` should be modified to match its global value before upgrade for all the cluster members;
- `IPSec_main_if_nat` should be modified to match its global value before upgrade for all the VPN/FireWall Modules with multiple interfaces.

PKI, PKCS

- 6 The combination of a Nokia VPN/FireWall Module and an Entrust CA server (4/5) may not function properly when viewing the `Entrust.ini` file in the GUI. The problem occurs when in the end of this INI file the line `Talk30=0` appears, which may lead to the configuration's failure.

To resolve this problem, proceed as follows:

- edit `Entrust.ini` and remove the line `Talk30=0`, *or*
- import `Entrust.ini` but avoid viewing it using the **View** option. Note, that pressing **View** will cause the `Talk30=0` entry to appear.

Miscellaneous

- 7 When a VPN/FireWall Module is located behind another VPN/FireWall Module which performs static NAT for the internal Module, SecuRemote VPN connections with the internal Module will fail.

Installation Instructions

Note – Existing users running the non-VPN and VPN editions of these versions should install the DES version. No new license is required.

Windows Platforms

Note –

- The VPN-1/FireWall-1 4.1 SP6 GUI clients package automatically detects whether the FCS version is installed on your computer. If yes, only the Service Pack 6 will be installed. If no, the full installation process will be initiated.
- Before installing VPN-1/FireWall-1 Version 4.1 SP6 on Windows NT, stop the NT performance monitor.

Installing

- 1 Download the .TGZ file to a temporary directory and extract the files.
- 2 Double-click on `setup.exe`.
This will start the Service Pack installation.

Uninstalling

- 1 In the **Control Panel**, click on **Add/Remove Programs** and choose “FireWall-1 Service Pack 6”.
- 2 In the **Control Panel**, click on **Add/Remove Programs** and choose “Check Point Management Client 4.1 SP6”.

Nokia

Installing

The SP6 package can be installed and upgraded either from the Voyager GUI or by running newpkg from the command line.

An example of the installation command line is:

```
newpkg -m LOCAL -n fw1_41_SP6_nokia_41616.tgz -o $FWDIR
```

General Installation Notes

- 1 Installation on IPSO from the Voyager must be performed with pressing Apply and Save after each step. When installing through the Voyager or command line, reboot after installation.
- 2 When uninstalling Check Point products, delete one package at a time and press Apply and Save after un-activating the package and after deleting it.
- 3 An attempt to install the same product twice will fail and result in the product's removal. If this happens, start the installation process from scratch.

Note – The active package does not change after upgrading. It is necessary to switch between SP6 and SP5 manually.

UNIX platforms

- 1 Download both tg'zipped files (VPN/FireWall Module and GUI), each to a different temporary directory.
- 2 Gunzip and untar each file in the different temporary directories.
- 3 Install according to the following platform specific instructions.

Solaris 2.8

Installing

Change to the CPFWSP410006-01 directory and run the patchadd command, giving as an argument the name of the CPFWSP410006-01 directory:

```
patchadd CPFWSP410006-01
```

or for the Motif GUI:

```
patchadd CPGUISP410006-01
```

Uninstalling

From the root directory, run the patchrm command, giving as an argument the name of this upgrade:

```
patchrm CPFWSP410006-01
```

or for the Motif GUI:

```
patchrm CPGUISP410006-01
```

Linux

Installing

Change to the directory where the untarred installation file is located and run the following command:

```
rpm -i --replacefiles CPfw1-41.6-SP6.i386.rpm
```

Uninstalling

Run the following command:

```
rpm -e CPfw-41.6
```

HPUX

Installing

This Service Pack includes two packages for HP-UX. One package contains installations for VPN/FireWall Module+Management Module and for Management Module only. The other package contains the GUI installation. Install the packages one after the other, using `swinstall`.

You must choose **ONLY ONE** from the first two installations and also the Motif GUI if required:

- **CPfw1-41_SP6** — to be installed on VPN/FireWall Module+Management Module or on VPN/FireWall Module only
Enter the following command, giving as an argument the name of the directory in which you have opened the package:

```
swinstall -s <absolute_path_to_package_directory> CPfw1-41_SP6
```

- **CPfw1-41_SP6_mgm** — to be installed on Management Module only
Enter a line command as follows, giving as an argument the name of the directory in which you have opened the package:

```
swinstall -s <absolute_path_to_package_directory> CPfw1-41_SP6_mgm
```

- **CPgui-41_SP6** — GUI installation
Enter a line command as follows, giving as an argument the name of the directory in which you have opened the package:

```
swinstall -s <absolute_path_to_package_directory> CPgui-41_SP6
```

Note – `<absolute_path_to_package_directory>` is the path to the catalog directory.

Uninstalling

Uninstall the packages using `swremove`.

Note – Before uninstalling VPN-1/FireWall-1 Version 4.1 SP6 on HP-UX, ensure that you have at least 15 MB free in the `/stand` directory.

Cluster Members

State synchronization is not supported (that is, it may crash) between Version 4.1 SP6 Modules and Modules of any previous version in a cluster. When upgrading the entire cluster to 4.1 SP6, state synchronization must be turned off until all cluster members have been upgraded.

To ensure connectivity during the upgrade to Version 4.1 SP6, proceed as follows:

- 1 On each of the standby machines:

- a. Stop VPN-1/FireWall-1 (fwstop).
 - b. Save the file `$FWDIR/conf/sync.conf` under a different name and create a new `sync.conf` file containing only the string `"SyncMode=no sync"`.
 - c. Start VPN-1/FireWall-1 (fwstart).
- 2** On the active machine:
- a. Stop VPN-1/FireWall-1 (fwstop).
 - b. Save the file `$FWDIR/conf/sync.conf` under a different name and create a new `sync.conf` file containing only the string `"SyncMode=no sync"`.
 - c. Start VPN-1/FireWall-1 (fwstart).
- Failover will occur, and existing connections will break.
- 3** Perform the software upgrade procedure on each of the standby machines.
Make sure that at the end of the upgrade, each standby machine is in the standby state.
- 4** Perform the software upgrade procedure on the active machine.
Failover will occur, and existing connections will break.
- 5** On each of the standby machines:
- a. Stop VPN-1/FireWall-1 (fwstop).
 - b. Restore the original `sync.conf` file in place of the new one created during the cluster upgrade.
 - c. Start VPN-1/FireWall-1 (fwstart).
- 6** On the active machine:
- a. Stop VPN-1/FireWall-1 (fwstop).
 - b. Restore the original `sync.conf` file in place of the new one created during the cluster upgrade.
 - c. Start VPN-1/FireWall-1 (fwstart).

Remote Installation

VPN-1/FireWall-1 Next Generation, the next major release, includes a new management tool called SecureUpdate. SecureUpdate enables FireWall administrators to easily upgrade software, major versions and Service packs on remote VPN/FireWall Modules from the Management Server. In order to leverage SecureUpdate to upgrade existing Version 4.1 VPN/FireWall Modules to NG, the Check Point Remote Installation package must first be installed on the 4.1 VPN/FireWall Module. It is therefore recommended to install and configure the Check Point Remote Installation package when installing FireWall-1 4.1 or installing a service pack onto an existing 4.1 VPN/FireWall Module; the upgrade to NG may then be done remotely, without any manual administration on the Module itself.

For installation and configuration instructions, see the Remote Installation Release Notes at <http://www.checkpoint.com/techsupport>

Note – You must reboot after installing and configuring CPUtil.

"Backing Out"

VPN-1/FireWall-1 Version 4.1 SP6 can be "backed out" or downgraded. When you uninstall VPN-1/FireWall-1 Version 4.1 SP6, the previously installed package or service pack will be fully restored. All new configuration updates or objects created in VPN-1/FireWall-1 Version 4.1 SP6 will be lost.