

VPN-1 NGX R62_HFA_01

Release Notes

Revised: June 5, 2008

IMPORTANT

Check Point recommends that customers remain up-to-date with the latest HFAs, as they contain security enhancements and protection against new and evolving attacks.



Note - Before beginning the installation, read the latest available version of these release notes at: <http://www.checkpoint.com/support/>

In This Document

<i>Introduction</i>	<i>page 2</i>
<i>What's New</i>	<i>page 2</i>
<i>Known Limitations</i>	<i>page 2</i>
<i>Supported Versions, Platforms and Builds</i>	<i>page 3</i>
<i>Installation and Uninstallation</i>	<i>page 4</i>
<i>Resolved Issues VPN-1 NGX R62_HFA_01</i>	<i>page 9</i>
<i>Documentation Feedback</i>	<i>page 20</i>

Introduction

Thank you for updating your Check Point products with VPN-1 NGX R62_HFA_01 (Hotfix Accumulator). This HFA is a recommended update that resolves various issues and contains improvements for VPN-1 and other Check Point products on a variety of platforms.

Please read this document carefully prior to installing this HFA. We also recommended that you refer to the appropriate Check Point user documentation and release notes, which contain hardware requirements, software requirements and version recommendations.

What's New

- Enhanced firewalling features for mail security servers and for authentication servers.
- H.323 for Video over IP has improved firewall handling.
- Enhanced NAT and RTSP for improved packet handling, performance, and connectivity.
- Overall improved memory consumption for various modules in the Check Point Suite.
- New feature to allow out-of-state TCP packets per Gateway, even if disallowed in Global Policy.
- Improved installation and upgrade processes for various modules in the Check Point Suite.
- Enhanced High Availability synchronization.
- Improved logging ensure log maintenance, even if the log server cannot be reached.
- Enhanced scalability and connectivity of VPN-1 Gateways with SecureClients.
- Added support of Vista L2TP clients for IKE interoperability with Check Point VPN-1 Gateways.
- **For SecurePlatform and UTM-1 users:** Easy HFA installation through the WebUI.

Known Limitations

- Before installing the HFA wrapper on IPSO SmartCenter server or as a Standalone, verify (using Voyager) that `CPngcmp` and `R55cmp` packages are activated. If the packages are not in active state (which is the default), the installation of these packages will fail. After installation, deactivate these packages.
- When uninstalling VPN-1 NGX R62_HFA_01 using SmartUpdate from gateways on Windows platforms, you must manually reboot the gateway after the uninstallation process completes.
- Uninstallation of the SecurePlatform package from SecurePlatform machines is not supported.
- Uninstallation of VPN-1 NGX R62_HFA_01 from IPSO gateways using SmartUpdate, or from IPSO flash-based platforms, is not supported.
- After installing VPN-1 NGX R62_HFA_01 on flash-based Nokia platforms, the installation log files are automatically deleted after reboot.
- IPv6 is not supported.

Supported Versions, Platforms and Builds

In This Section

[Supported Platforms](#)

[page 3](#)

[Supported Builds](#)

[page 3](#)

Supported Platforms

The following platforms are supported for VPN-1 NGX R62_HFA_01:

Platform	Version
Solaris	8, 9, 10
IPSO	3.9, 4.1, 4.2
Linux	Red Hat Enterprise Linux 3.0
Windows	2000 Server, 2003 Server, 2003 Server SP1
SecurePlatform	NGX

Supported Builds

Take: 45

VPN-1 NGX R62_HFA_01 consists of the following builds:

Component	Build Number	Comment
Firewall & Kernel	618601048	The output of fw ver -k should appear similar to the following: This is Check Point VPN-1(TM) & Firewall(R) NGX (R62) HFA_01, Hotfix 601 - Build 048 kernel: NGX R62 HFA_01, Hotfix 601 - Build 048
SecurePlatform	618601042	
Performance Pack	618601008	The output of sim ver -k should appear similar to the following: This is Check Point Performance Pack version: NGX (R62) HFA_01, Hotfix 601 - Build 008 Kernel version: NGX (R62) HFA_01, Hotfix 601 - Build 008
Backward Compatibility R55	618601012	
Backward Compatibility R55W	618601009	

Installation and Uninstallation

In This Section

Installation Packages	page 4
Installing the HFA	page 4
Updating INSPECT Files	page 7
Uninstallation	page 8

Installation Packages

This HFA uses a wrapper that includes all installation packages required for each platform and operating system. When you expand the wrapper, the directories relevant for your platform are provided. The complete VPN-1 NGX R62_HFA_01 list of installation packages is given here, though some of the directories may not be relevant, and therefore not available, to your platform.

- **CPvpn** - Installation package for VPN-1
- **CPngcmp** - Installation package for NG versions compatibility
- **CPR55WCmp** - Installation package for VPN-1 NG version R55W compatibility
- **SecurePlatform** - Installation package for SecurePlatform gateways
- **CPppak** - Installation package for Performance Pack, for SecurePlatform and Solaris gateways

Installing the HFA

There are several methods to install the HFA. CLI and SmartUpdate installations are applicable to any platform that is supported by Check Point products. Specific vendors and operating systems offer additional installation methods.

In This Section

Installing using Wrapper	page 5
Remote Installation using SmartUpdate	page 5
Installation on SecurePlatform Platforms with WebUI	page 5
Installation on UTM-1 Appliances with WebUI	page 6
Installation on Nokia Flash-Based Platforms	page 6
Installation on Clusters	page 7

Installing using Wrapper

To install VPN-1 NGX R62_HFA_01:

1. Verify that there is enough free disk space for the installation of the HFA packages.
2. Download the HFA wrapper and extract the packages.
3. Run the installation script:
 - Windows: **Setup.bat**
 - Unix: **./UnixInstallScript**
4. Reboot the machine.

Remote Installation using SmartUpdate

You can use SmartUpdate to install this HFA on most platforms. Before using SmartUpdate, make sure that there is sufficient free disk space (140MB) on the SmartCenter server.

To install with SmartUpdate:

1. Install VPN-1 NGX R62_HFA_01 on the SmartCenter server.
2. Add the HFA wrapper to the Package Repository. This step automatically extracts the appropriate packages into the repository.
3. Make sure that SmartDashboard is closed.
4. Distribute the packages to the gateways. SmartUpdate reboots the gateway after each package installation.

Installation on SecurePlatform Platforms with WebUI

Installation of this HFA can be done through the WebUI on any device running the SecurePlatform operating system.

To install the HFA on a SecurePlatform machine with WebUI:

1. Download the HFA wrapper (**VPN-1_R62_HFA_01_wrapper.SecurePlatform.tgz**).
2. Connect to the WebUI (**https://<IP>**).
3. Click **Device > Upgrade**.
4. In the **Upgrade Steps** pane, browse to the downloaded HFA wrapper and click **Upload upgrade package to device**.
5. Click **Start Upgrade**.

At the end of the installation, the device automatically reboots.

6. Re-login to the device.

To verify HFA installation through the WebUI: check the **Version and Build** information (**Status** page) and check that it shows: **NGX R62_HFA_01**

Installation on UTM-1 Appliances with WebUI

Installation of this HFA can be done through the WebUI on any UTM-1 appliance.

To install the HFA on a UTM-1 machine with WebUI:

1. Download the HFA wrapper (`VPN-1_R62_HFA_01_wrapper.SecurePlatform.tgz`).
2. Connect to the WebUI (`https://<IP>:4434`).
3. Click **Appliance > Upgrade**.
4. In the **Upgrade Steps** pane, click **Upload upgrade package to appliance**.
5. Browse to the downloaded HFA wrapper and click **Upload**.
6. Click **Start Upgrade**.

At the end of the installation, the appliance automatically reboots.

7. Re-login to the device.

To verify HFA installation through the WebUI: open the **Version and Build** information (**Information > Appliance Status**) and check that it shows: `NGX R62_HFA_01`

Installation on Nokia Flash-Based Platforms

Installing this HFA on Nokia flash-based IPSO platforms is straightforward. However, you **must** follow all of the prerequisite and installation steps precisely to avoid installation problems.

Before installing the HFA wrapper on IPSO SmartCenter or as a Standalone, verify (by Voyager) that `CPngcmp` and `R55cmp` packages are activated.

If the packages are not in active state (which is the default), the installation of these packages will fail.

After installation, make sure to deactivate these packages.

To install the HFA on a Nokia Flash-Based platform:

1. Create a temporary directory on the **optional disk** (`/opt`).
For example, run the `mkdir /opt/hfa` command, where `/hfa` is the directory name.
2. Navigate to the temporary directory and execute the `df -k.` command (the dot is important!) and verify that there is at least 400 MB available disk space.
If you do not have sufficient space, free up space by deleting non-critical data files.
3. Download the `VPN-1_HFA_R62_01_wrapper.ipso.tgz` file to a temporary directory, and extract the contents of the file.



Important - Do not use the `/opt/admin` directory.

4. Delete the TGZ file, as it is no longer needed.
5. Run: `./UnixInstallScript`
6. Reboot the machine.

Installation on Clusters

When upgrading from the NGX R62 general release, the following upgrade options are available:

- **Minimal Effort Upgrade** - For more information, refer to the *Performing a Minimal Effort Upgrade on a ClusterXL* chapter in the Upgrade guide.
- **Zero Down Time Upgrade** - For more information, refer to the *Performing a Zero Down Time Upgrade on a ClusterXL Cluster* chapter in the Upgrade guide.
- **Full Connectivity Upgrade** – For more information, refer to the *Performing a Full Connectivity Upgrade on a ClusterXL Cluster* chapter in the Upgrade guide.

Notes:

1. When performing a Full Connectivity Upgrade, you must follow all steps described in the *Performing a Full Connectivity Upgrade on a ClusterXL Cluster* chapter in the Upgrade guide. This includes running the **fw fcu** command and understanding the relevance of the Ready state as described in step 7 of the *Performing a Zero Down Time Upgrade on a ClusterXL Cluster* section in the Upgrade guide.
2. The Full Connectivity Upgrade is not supported when upgrading a cluster from any version prior to NGX. You can only perform Minimal Effort or Zero Down-Time upgrades in this circumstance.

Updating INSPECT Files

The SmartCenter server contains several INSPECT (.def) files, typically located in the **FWDIR/lib** directory. This HFA includes one or more updated INSPECT files, which replace the files currently in use.

For those environments using only default Check Point INSPECT files, the updated INSPECT files are installed automatically.

If INSPECT files were manually customized, the new INSPECT files do not replace the customized ones.

To see which INSPECT files were not replaced, see the logs:

- Unix: **/opt/CPInstLog/update_inspect_files_01.log**
- Windows: **C:\ProgramFiles\CheckPoint\CPInstLog\update_inspect_files_01.log**

To force new INSPECT files to replace customized ones, run: **update_inspect_files -f**

Uninstallation

This section contains instructions for uninstalling VPN-1 NGX R62_HFA_01 from various platforms and configurations. You must reboot the computer after uninstalling this HFA.



Note - Uninstallation of this HFA on the SmartCenter server does not automatically restore INSPECT files that existed prior to installation of this HFA. Before uninstalling the packages, run:
update_inspect_files -restore

To uninstall this HFA:

Windows

1. Open **Control Panel > Add or Remove Programs**.
2. Remove all Check Point packages that contain **R62_01** in their names.

Other Platforms and Packages

Package	Uninstall
Firewall on Solaris, IPSO, SecurePlatform, Linux	<code>/opt/CPsuite-R62/uninstall_fw1_HOTFIX_R62_01</code>
Performance Pack	<code>/opt/CPppak-R62/uninstall_sim_HOTFIX_R62_01</code>
Backward Compatibility R55	<code>/opt/CPR55Cmp-R62/uninstall_cor_cmp_HOTFIX_R62_01</code>
Backward Compatibility R55W	<code>/opt/CPR55WCmp-R62/uninstall_trini_cmp_HOTFIX_R62_01</code>

Resolved Issues VPN-1 NGX R62_HFA_01

In This Section

<i>Firewall</i>	<i>page 9</i>
<i>SmartCenter Server</i>	<i>page 12</i>
<i>Nokia IPSO</i>	<i>page 14</i>
<i>SecurePlatform</i>	<i>page 15</i>
<i>Platform Specific</i>	<i>page 16</i>
<i>VPN-1</i>	<i>page 17</i>
<i>Web Intelligence</i>	<i>page 18</i>
<i>Miscellaneous</i>	<i>page 18</i>

Firewall

R62_01-1

Category:	General
Problem:	Specific web applications may have connectivity issues.
Resolution:	Improvements to the streaming engine ensure that these connectivity issues do not arise.
Install On:	Gateway

R62_01-2

Category:	Anti Virus
Problem:	The Anti Virus security servers do not provide an error message when the mail server does not respond.
Resolution:	Firewall-1 has been improved for mail security servers and now correctly provides notifications.
Install On:	Gateway

R62_01-3

Category:	Licensing
Problem:	With a limited license and VPN Tunnel Interface (VTI) that has Anti-Spoofing enabled, the license counting may incorrectly calculate external interfaces as internal hosts, causing connectivity issues.
Resolution:	Improved license counting ensures proper connectivity.
Install On:	Gateway

R62_01-4

Category:	NAT
Problem:	In an ISP Redundancy configuration, the firewall may have stability issues.
Resolution:	ISP Redundancy has improved stability.
Install On:	Gateway

R62_01-5

Category: NAT
Problem: In an ISP Redundancy configuration, the firewall may have a memory leak.
Resolution: Memory consumption has been improved for ISP Redundancy.
Install On: Gateway

R62_01-6

Category: NAT
Problem: In a Check Point cluster environment and a host with Windows Personal Firewall, legitimate DHCP OFFER packets may be dropped.
Resolution: Legitimate DHCP OFFER packets are correctly passed.
Install On: Gateway

R62_01-7

Category: Policy Installation
Problem: When a large number of protections are activated after performing SmartDefense update, policy installation may not succeed.
Resolution: Scalability for Firewall-1 has been enhanced.
Install On: SmartCenter server

R62_01-8

Category: Security Servers
Problem: Legitimate email messages are incorrectly identified as **Malformed MIME** and dropped.
Resolution: Legitimate emails are now passed correctly.
Install On: Gateway

R62_01-9

Category: Security Servers
Problem: A rulebase that contains a Session Authentication rule with Single Sign-on may cause stability issues.
Resolution: Enhanced Session Authentication handling.
Install On: Gateway

R62_01-10

Category: Services
Problem: The firewall may drop RTP streams.
Resolution: Enhancements to RTSP ensure that legitimate RTP streams are passed correctly.
Install On: SmartCenter server and Gateway

R62_01-11

Category: Services

Problem: During an RTSP connection, the following error may appear:
Violated Unidirectional Connection.

Resolution: Enhanced RTSP enforcement ensures this error does not occur.

Install On: SmartCenter server

R62_01-12

Category: Services

Problem: DNS Enforcement may drop legitimate traffic that contains domain names with international characters. For such traffic, the following log may appear:
Bad domain format, illegal ASCII value in domain

Resolution: This HFA disables DNS ASCII enforcement by default.
For more information, please see [sk33601](#).

Install On: Gateway

R62_01-13

Category: Stateful Inspection

Enhancement: This HFA adds an option that allows out-of-state TCP packets per Gateway, even if the global policy disallows it.

Install On: Gateway

R62_01-14

Category: Stateful Inspection

Problem: When two setup messages are used, RTSP data connections may be improperly recorded.

Resolution: Improved connectivity when using Hide NAT and RTSP for differentiating between connections.

Install On: SmartCenter server

R62_01-15

Category: VoIP

Problem: Legitimate H.323 packets may be incorrectly identified as **Malformed Packets** and dropped.

Resolution: Enhanced H.323 decoding ensures correct identification and passing of legitimate H.323 traffic.

Install On: Gateway

R62_01-16

Category: VoIP

Problem: SIP validation for domain and user names may sometimes cause legitimate packets to be dropped.

Resolution: SIP validation has been improved to ensure legitimate traffic is passed.

Install On: Gateway

R62_01-17

Category: VoIP
Problem: UDP packets may be incorrectly logged as **Unknown SIP message type**.
Resolution: Firewall now identifies UDP packets that are not SIP and correctly does not attempt SIP inspection on these packets.
Install On: Gateway

R62_01-18

Category: VoIP
Problem: Legitimate non-VoIP (SIP) traffic is incorrectly dropped.
Resolution: Legitimate SIP traffic is now correctly passed.
Install On: Gateway

R62_01-19

Category: VoIP
Problem: On Crossbeam X80 when SIP over TCP is passed, the firewall may experience stability issues.
Resolution: Enhancements to the firewall improve stability.
Install On: Gateway

SmartCenter Server

R62_01-20

Category: General
Problem: When running a Log Server on an R62 Eventia Suite machine, install database is required to update the Log Server.
Resolution: This HFA enables to install database on R62 Eventia Suite.
Install On: SmartCenter server

R62_01-21

Category: Clientless VPN Issues
Problem: After a version upgrade, Clientless VPN on Cluster may fail to function properly.
Resolution: Clientless VPN properties are now correctly added to member objects when a cluster is created, ensuring proper functionality of Clientless VPN on Clusters.
Install On: SmartCenter server

R62_01-22

Category: Database
Problem: Deleting an object from the database using the DBedit utility might cause other objects having references to the deleted object to be deleted as well.
Resolution: Database functionality has been improved to ensure referencing objects are not deleted.
Install On: SmartCenter server

R62_01-23

Category: Installation

Problem: When setting firewall group permissions via CPConfig, for a group other than root, a user of this group is unable to execute firewall commands.

Resolution: Permission functionality has been improved to ensure correct user features.

Install On: SmartCenter server

R62_01-24

Category: Internal Certificate Authority

Problem: On SecurePlatform, the internal CA database file in some cases may become corrupt, making the server unable to perform as an Internal CA.

Resolution: Improvements to the internal CA database ensure that the server can continue to perform CA operations correctly and that the certificate database is maintained.

Install On: SmartCenter server

R62_01-25

Category: Logging

Problem: Logs may be lost when connectivity between the gateway and the log server is broken.

Resolution: Enhancements to log buffering and backup ensure that logs are maintained, even if the log server cannot be reached.

Install On: Log server

R62_01-26

Category: Logging

Problem: The **Rule Name** and **Version** filters in SmartView Tracker do not function properly.

Resolution: Filters have been enhanced to ensure proper functionality.

Install On: Log server

Category: Management HA

Problem: When automatic synchronization between two servers is deactivated, the **Synchronize Me** option may sometimes get an incorrect response.

Resolution: Synchronization has been improved to ensure high availability.

Install On: SmartCenter server st

R62_01-27

Category: SmartConsole

Problem: When there are nested user groups, upon changing a nested group, an error is displayed: `Failed to save object group.`

Resolution: This HFA ensures proper nested group editing.

Install On: SmartCenter server

R62_01-28

Category: SmartDefense Updates
Problem: When updating SmartDefense, the update may sometimes fail.
Resolution: Update procedures have been improved.
Install On: SmartCenter server

Nokia IPSO**R62_01-29**

Platform: IPSO
Problem: Nokia hybrid machines (both gateways and standalones) ignore local logging configuration set in SmartDashboard because the Nokia machines are incorrectly identified as diskless machines.
Resolution: The Nokia hybrid machines are now correctly identified, providing correct functionality.
Install On: SmartCenter server and Gateway

R62_01-30

Platform: IPSO
Problem: When SecureXL is enabled, IP fragments may incorrectly be allowed.
Resolution: SecureXL on IPSO has been improved to ensure that the SmartDefense option **Forbid IP Fragments** operates correctly.
Install On: Gateway

R62_01-31

Platform: IPSO 4.1
Enhancement: Enhanced functionality and stability of internal flash due to improved log-saving algorithm.
Install On: Gateway

R62_01-32

Platform: Nokia IP2250 diskless
Problem: On IP2250 diskless machines, the following error may be seen:
The log repository quote has been exceeded. No file could be deleted.
Resolution: Improved logging performance on diskless Nokia machines for forwarding logs to the SmartCenter server.
Install On: Gateway

SecurePlatform

R62_01-33

Category: General

Enhancement: Linux openssh has been upgraded with patches.

For more information, see <https://rhn.redhat.com/errata/RHSA-2006-0738.html>

Resolution: SecurePlatform version of openssh has been upgraded.

Install On: SecurePlatform

R62_01-34

Category: General

Problem: Potential local privilege escalation by a legitimate administrator with restricted (cpshell) rights.

Resolution: Fixed relevant components. For more information, please refer to [sk33639](#).

Install On: SmartCenter server , Gateway

R62_01-35

Category: General

Enhancement: Added support for Dell 2950.

Install On: SmartCenter server and Gateway

R62_01-36

Category: General

Problem: On a Sun Microsystems 10G GBE NIC machine, the ixgb driver may be loaded instead of the correct ixge driver.

Resolution: The correct driver is now loaded on Sun machines.

Install On: Gateway

R62_01-37

Category: Hardware Certification

Enhancement: Added support for TG3 driver for PCI IDs.

Install On: SmartCenter server and Gateway

R62_01-38

Category: Hardware Certification

Enhancement: Added support for IntelPRO/1000 PT QUAD NIC 8086

Install On: SmartCenter server and Gateway

R62_01-39

Category: Firewall

Problem: System load average measurements from uptime command are inaccurate.

Resolution: VPN-1 has been enhanced to be measured correctly by the uptime command.

Install On: Gateway

Platform Specific

R62_01-40

Platform: VPN-1 Edge/Embedded

Problem: When sending or forwarding packets to an IP address that previously belonged to a ROBO gateway, VPN-1 gateway attempts to encrypt these packets.

Resolution: ROBO gateways now always have up-to-date information, ensuring these packets are handled correctly.

Install On: Gateway

R62_01-41

R62_01-42

Platform: VPN-1 Edge/Embedded

Enhancement: VPN-1 Edge Firmware 7.5.38 is now supported.

Install On: SmartCenter server

Platform: Solaris

Problem: VPN-1 gateway cannot be installed on Solaris 10 update 2 (6/06) and above.

Resolution: Installation on Solaris has been enhanced for Solaris 10 update 2 (6/06) and above. For more information about installing Solaris patches, see [sk32031](#).

Install On: Gateway

R62_01-43

Platform: PerformancePack on Solaris

Problem: When SecureXL is enabled, TCP on Solaris 10 with BGE interface may have connection issues.

Resolution: Enhancements on TCP handling on Solaris 10 with BGE interface ensure TCP connects correctly.

Install On: Gateway

R62_01-44

Platform: Crossbeam X80 and Linux

Problem: When running `ifconfig up/down` during traffic, the firewall may experience stability issues.

Resolution: These commands may now be run at any time without affecting the stability of the firewall.

Install On: Gateway

R62_01-45

Platform: Mobile VPN

Problem: Mobile SecureClients cannot stay in reconnect mode for more than a few minutes; authentication is demanded in an inconvenient interval.

Resolution: Gateway now keeps the cookie for as long as it is valid, allowing the client to remain in reconnecting state, without re-authenticating to server, during a few hours.

Install On: Gateway

VPN-1

R62_01-46

Category: IKE, Interoperability

Problem: Vista L2TP clients cannot connect to Check Point Gateways

Resolution: IKE validation procedures now allow Vista L2TP clients to connect to Check Point VPN-1 Gateways.

Install On: Gateway

R62_01-47

Category: Keys

Problem: After upgrading, the following error message may be seen: Cannot find DH pre computation for group.

Resolution: Use of Diffie Hellman pre-computation uses new keys for upgraded Check Point Suites and the error no longer occurs.

Install On: SmartCenter server

R62_01-48

Category: SecuRemote and SecureClient

Problem: When SecureClient accesses a gateway with multiple interfaces and multiple ISPs, an ISP may see that the SecureClient used the gateway's default interface and incorrectly drop the connection as spoofing.

Resolution: The VPN-1 gateway is now able to handle multiple interface connections and correct communications with ISPs for SecureClients.

Install On: Gateway

R62_01-49

Category: Services

Problem: When connecting with SSL Network Extender, Office Mode from RADIUS server does not function correctly.

Resolution: Enhanced information identification and storage ensures that Office Mode from a RADIUS server functions correctly.

Install On: SmartCenter server

R62_01-50

Category: VPN Communities

Problem: When a rule is based on a specific community, SmartDefense incorrectly drops DCERPC UID.

Resolution: Rules with communities have been improved to correctly handle traffic.

Install On: SmartCenter server

- Category:** VPN-1 and SecuRemote/SecureClient Issues
- Problem:** When a new Security Policy is installed on the Gateway, Remote Access users may experience temporary packet loss.
- Resolution:** Added option to preserve Remote Access connections while a Security Policy is being installed on the Gateway, ensuring that packets are not dropped. For more information, please see [sk32208](#).
- Install On:** SmartCenter server

Web Intelligence

R62_01-51

- Category:** General
- Enhancement:** Web Intelligence %u encoding and unicode canonization have been enhanced. For more information, see [sk32714](#).
- Install On:** Gateway

R62_01-52

- Category:** HTTP Protocol Enforcement
- Enhancement:** Added support for HTTP Response Code 304 according to [RFC 2616](#).
- Install On:** Gateway

Miscellaneous

R62_01-53

- Category:** FloodGate-1
- Problem:** When attempting to load or unload a policy to/from a large number of servers, FloodGate-1 may have stability issues.
- Resolution:** FloodGate-1 scalability has been improved to no longer experience instability when loading/unloading policies to/from a large number of servers.
- Install On:** Gateway

R62_01-54

R62_01-55

- Category:** Performance Pack: Accelerated Features
- Problem:** The gateway may lose synchronized traffic. The following message may be seen in logs: `Dead loop on virtual device sync`
- Resolution:** PerformancePack has been enhanced to resolve this issue and ensure that synchronized traffic is not lost.
If the message appears, set `sim_cflush_outbound=0` in `simkern.conf`
Change will take place after reboot.
- Install On:** Gateway

- Category:** SSL Network Extender
- Enhancement:** SSL Network Extender now supports the 5-License SKU.
- Install On:** SmartCenter server

R62_01-56

Category: SSL Network Extender

Enhancement: SSL Network Extender now supports Microsoft Vista.

Install On: Gateway

Documentation Feedback

Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments to:

cp_techpub_feedback@checkpoint.com