puresecurity™

Check Point® SOFTWARE TECHNOLOGIES LTD.

VPN-1 NGX R60_HFA_06 Release Notes

Revised: October 30, 2007

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

Introduction

Thank you for updating your Check Point products with VPN-1 NGX R60_HFA_06 (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

- **SSL Network Extender** - MS Vista operating system is now supported.

- **VPN-1 Edge** - Firmware 7.5.38 is now supported.
- **VoIP** - Enhancements have been made to the MGCP parser for improved handling of RSIP, and the Hash Algorithms have been enhanced for improved SIP and MGCP handling.

Known Limitations

- The HFA wrapper does not overwrite existing packages on the target machine if the existing packages are up to date.
- When uninstalling the HFA from Windows gateways using SmartUpdate, a manual reboot should be initiated independently of the uninstall process.
- SecurePlatform Operating System HFA uninstallation is not supported.
- Uninstallation of HFA on IPSO gateways through SmartUpdate is not supported.
- In a cluster environment, you must execute the `cphastop` command on each cluster member, prior to installing this HFA. For more information, refer to SK: sk31434.
- After installing this HFA on flash based Nokia machines, the installation log files will be deleted after the reboot.
- Before installing the comprehensive package for IPSO via Voyager the `CPngcmp-R60` package must be activated. If this is not done the ng_bc package installation will fail.
- Uninstalling the HFAs from an IPSO flash based-machine is not supported.
- Before applying this HFA on the Windows platform, stop the Windows SNMP service.
- Installing this HFA overwrites the $FWDIR/lib/vpn_table.def file. If this file was manually modified, create a copy of it and perform the modification again in the new vpn_table.def file.

The following limitations are relevant only for SIP and MGCP users:

- Static NAT can be used in both automatic and manual NAT rules.
- Hide NAT can be used in both automatic and manual rules for outgoing VoIP calls. For incoming calls, automatic rules must be used.
- For security reasons, when using Hide NAT for incoming calls, the destination of a VoIP call in the appropriate rule in the Rule Base cannot be **Any**.
- Bidirectional NAT for VoIP calls is not supported.
- Internal calls cannot be made from the same source to two endpoints, where one endpoint uses NAT (of either kind) and the other does not.
- When using NAT, the SIP proxy/Call Agent must reside in the external network in order to enable VPN-1/FireWall-1 to track the registration messages.
- NAT on SIP proxy/ Call Agent is not supported.
- When using Hide NAT behind a Gateway (on the phones), Cluster XL failover is not supported for SIP-TCP/H323 with Secure XL.
- Call-ID maximum length is 63 characters. Username maximum length is 39 characters. Call-ID maximum length is 31 characters. Endpoint maximum length is 100 characters.

- SIP/MGCP connections are not accelerated. Only RTP and RTCP connections are accelerated.

Special Notes

HFA installation does not automatically overwrite modified `*.def` files. Manual modifications made to these files are not lost. The `*.def` files are copied to the directory `$FWDIR/lib` under the name `*_HFA.def`. In order to complete the HFA installation, you will need to replace the existing files (`*.def`) with the new HFA modified files (`*_HFA.def`). If you have made manual changes to your `*.def` files, you will also need to make these changes to the new HFA version of the files.

Please refer to the instructions for activating changes to INSPECT files on page 8.

Supported Versions, Platforms and Builds

In This Section

Supported Platforms

The following platforms are supported for R60_HFA_06:

Platform	Version
Solaris	8,9,10 (see **Note**)
IPSO	3.9, 4.0, 4.1
Linux	RedHat Enterprise Linux 3.0
Windows	2000 Server, 2003 Server, 2003 Server SP1
SecurePlatform	NGX

Note - R60_HFA_06 can be installed on top of special installation package of VPN-1 R60 GA for Solaris 10.

Supported Builds

Take: 10

VPN-1 NGX R60_HFA_06 consists of the following builds:

Component	Build Number	Comment

Firewall & Kernel	591606007	The output of `fw ver -k` should appear similar to:
		`This is Check Point VPN-1(TM) & Firewall(R) NGX (R60) HFA_06, Hotfix 606 - Build 007`
		`kernel: NGX R60 HFA_06, Hotfix 606 - Build 007`

SecurePlatform	591606007	

Performance Pack	591606001	The output of `sim ver -k` should appear similar to:
		`This is Check Point Performance Pack version: NGX (R60) HFA_06, Hotfix 606 - Build 001`
		`Kernel version: NGX (R60) HFA_06, Hotfix 606 - Build 001`

R55 Backwards Compatibility (BC)	541847009	

Supported Builds History

The following table displays the build history for Firewall and Kernel, SecurePlatform, Performance Pack and R55 Backwards Compatibility.

	R60_HFA_05	R60_HFA_04	R60_HFA_03	R60_HFA_02	R60_HFA_01
Firewall	591605020	591604028	591603015	591602015	591601011
SecurePlatform	591605005	591604036	591603003	591602004	591601003
Performance Pack	591605003	591604003	591603002	591602004	
R55 BC	541847009	541847002	541768001	541663001	541663001

Installation and Uninstallation

In This Section

Preliminary Tasks

Prior to installing this HFA, you **must** uninstall VoIP Hotfix 1 or VoIP Hotfix 2. The following sections present the procedures for uninstalling these hotfixes.

Uninstalling VOIP Hotfix 1

SecurePlatform/Linux/Solaris/IPSO Platforms: `./uninstall_fw1_HOTFIX_NGX_VOIP_HF_ONE_HFA`.

Windows Platforms: Use the **Add/Remove Programs** feature in the Windows **Control Panel**.

Uninstalling VOIP Hotfix

SecurePlatform/Linux/Solaris/IPSO Platforms: `./uninstall_fw1_HOTFIX_NGX_VOIP_HF_2_HFA`.

Windows Platforms: Use the **Add/Remove Programs** feature in the Windows **Control Panel**.

HFA Wrapper - Automatic Installation

This HFA employs a package wrapper that includes all installation packages for each platform It is bundled and zipped for your convenience.

Download this wrapper, extract it and run the installation script:

- On Windows run `setup.bat` and then reboot the machine.
- On Unix run `UnixInstallScript` and then reboot the machine.

Inside each wrapper for R60_HFA_06 - NGX (R60), you will see following installation packages:

- **SecurePlatform**. This package is only included in the SecurePlatform OS package and is available under the directory `SecurePlaform`.
- **VPN-1 POWER/UTM**. This package can be found under the directory `CPvpn`.
- **NG Compatibility Package Hotfix**. This package is relevant for SmartCenter only and can be found under the directory `CPngcmp`.
- **Performance Pack** is available for SecurePlatform and Solaris gateways. This package can be found under the directory `CPppak`.

The automatic installation log file is `/opt/CPInstLog/wrapper_HOTFIX__R60_06.elg`.

Verify that there is enough free disk space for the installation of these HFA packages.

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 in order to avoid installation problems.

Prerequisites for Nokia IP265 Machines

- IP265 flash-based machine with an external flash (optional disk) that has been configured for type `Packages`.
- Install the latest NG.X R60 bootstrap script according to the instructions in sk31660. You must run this bootstrap script before beginning the HFA installation.

Installation Steps

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 200 MB available disk space.

   If you do not have sufficient space, you will need to free up space by deleting non-critical data files.
3) Download the R60_HFA_06 package file (`VPN-1_R60_HFA_05_wrapper.ipso.tgz`) to the temporary directory.

   IMPORTANT NOTE: Do not use the `/opt/admin` directory.
4) Extract the contents of `VPN-1_R60_HFA_05_wrapper.ipso.tgz`.
5) Remove the R60_HFA_06 package (.tgz) file, as it is no longer needed.
6) Run the `UnixInstall` script.
7) Reboot the machine.

Remote Installation

You can use SmartUpdate installation for most platforms. Before using SmartUpdate, however, make certain that there is sufficient free disk space (140MB) on the SmartCenter server. It is recommended that you update the SmartCenter server prior to the gateways.

Using SmartUpdate

Perform the following steps to add the R60_HFA_06 packages to the SmartUpdate repository:

1) Extract the VPN-1 R60_HFA_05 package to a temporary directory.
2) Open SmartUpdate from SmartDashboard.
3) Select **Packages > Add > From File**.
4) Navigate to the directory into which the wrapper was extracted and choose the Applicable package from the following locations:
   - **SecurePlatform** is located in the SecurePlatform directory.
   - The **Firewall** package is located in the **CPvpn** directory.
   - The **Performance Pack** is located in the **CPpack** directory.
5) Select the target object (gateway) and install the relevant packages in the order listed above.

It is also possible to uninstall the previous HFA packages via SmartUpdate (except on IPSO platforms and SecurePlatform OS package).

Using the Web UI

You can now install this HFA on SecurePlatform using the Web UI.

Uninstallation

VPN-1 Pro/Express

Platform	Procedure
Windows	In **Start > Settings > Control Panel**, use the **Add/Remove** option.
Solaris IPSO SecurePlatform Linux	1. Change directory to `/opt/CPsuite-R60` 2. Run: `./uninstall_fw1_HOTFIX_R60_06`

NG Compatibility Package

Platform	Procedure
Windows	In **Start > Settings > Control Panel**, use the **Add/Remove** option.
Solaris IPSO SecurePlatform Linux	1. Change directory to `/opt/CPngcmp-R60/` 2. Run: `./uninstall_ng_bc_HOTFIX_R60_05`

Performance Pack NGX R60 HFA 05

Platform	Procedure
Windows	In **Start > Settings > Control Panel**, use the **Add/Remove** option.
Solaris IPSO SecurePlatform Linux	1. Change directory to `/opt/CPppak-R60` 2. Run: `./uninstall_sim_HOTFIX_R60_06` 3. Reboot

Special Instructions

In This Section

Installing R60_HFA_06 on NGX R60 Clusters

When upgrading ClusterXL from NGX R60 or NGX R60 with previous HFA to R60_HFA_06 the following upgrade options are available:

- Minimal Effort Upgrade - for more information see the chapter *Performing a Minimal Effort Upgrade on a ClusterXL* in the *Upgrade* guide.
- Zero Down Time Upgrade - for more information see the chapter *Performing a Zero Down Time Upgrade on a ClusterXL Cluster* in the *Upgrade* guide.
- Full Connectivity Upgrade – for more information follow the steps specified in the chapter *Performing a Full Connectivity Upgrade on a ClusterXL Cluster* in the *Upgrade* guide.

You should note the following:

1) When performing Full Connectivity Upgrade, it is necessary to follow all the steps described in the chapter *Performing a Full Connectivity Upgrade on a ClusterXL Cluster* 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 section *Performing a Zero Down Time Upgrade on a ClusterXL Cluster* in the *Upgrade* guide.
2) Full Connectivity Upgrade is not supported when upgrading a cluster from any version prior to NGX. To upgrade, follow the steps outlined in *Performing a Zero Down Time Upgrade on a ClusterXL Cluster* in the *Upgrade* guide, or P*erforming a Minimal Effort Upgrade on a ClusterXL* in the *Upgrade* guide.

Activating Updated INSPECT Files

The HFA installation process does not automatically overwrite modified `*.def` files, ensuring that manual modifications made to these files are not lost. The `*_HFA.def` suffix is appended to each file. Following installation of this HFA, you must activate the modified `INSPECT` files.

To activate changes to INSPECT (.def) files, perform the following steps:

1. Run `cpstop to` stop the SmartCenter Server.
2. Change the directory to `$FWDIR/lib/`.
3. Backup the relevant `*.def` file.
4. Rename the `*_HFA.def` file to `*.def`, (make sure that you verify file permissions).
5. Change directory to `$FWDIR/hash/`
6. Backup the relevant `*.def.hash`.
7. Rename the `*_HFA.def.hash` to `*.def.hash`. For example, rename `base_HFA.def.hash` to `base.def.hash`.
8. Repeat step 2 to step 7 to replace any other relevant `*.def` files.
9. Start the SmartCenter Server by running `cpstart`.
10. Install a Security Policy.

Advanced Instructions - VOIP NAT

When a phone is configured for NAT, NAT is not performed on the outgoing packet source port by default. If you wish to use NAT on the source port perform the following steps:

1. To begin using the new features for SIP/MGCP phones, you must perform the procedure for updating INSPECT files described on page 8 to replace the following kernel INSPECT files: `base.def, fwui_head.def, mgcp.def, services.def, sip.def, table.def, user_early.def`.
2. Set the virtual session timeout in mgcp_CA and mgcp_MG services to be longer then the refresh packet interval. It is located in the '`mgcp_CA/mgcp_MG service`' Advanced properties.
3. Set `mgcp_standard_hide_nat` to `1`, and then proceed as follows:
   - For Linux - in `$FWDIR/modules/fwkern.conf` add `mgcp_standard_hide_nat =1`. Create this file if it doesn't exist and reboot the machine.
   - For Solaris - in `/etc/system`, set `fw:mgcp_standard_hide_nat =1` and reboot the machine.
   - For IPSO - run `modzap mgcp_standard_hide_nat $FWDIR/modules/fwmod.o 1` and reboot the machine.
   - For Windows - Add a DWORD value called `mgcp_standard_hide_nat` with the value 1 under the following registry key and reboot the machine: `HKLM\System\CurrentControlSet\Services\FW1\parameters`

Resolved Issues VPN-1 NGX R60_HFA_06

In This Section

ClusterXL

R60_06-1

Category: ClusterXL

Problem: VRRP members may not be able to perform full synchronization after reboot.

Resolution: Increased the number of full synchronization attempts.

Install On: Gateway

Firewall

R60_06-2

Category: General

Problem: When RADIUS servers are defined in the database, firewall sockets may inadvertently remain open. The following error may appear:
`too many open files`

Resolution: Enhanced socket handling ensures socket are closed as needed.

Install On: Gateway

SecurePlatform

R60_06-3

Category: SecurePlatform

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

SSL Network Extender

R60_06-4

Category: SSL Network Extender

Enhancement: SSL Network Extender now supports the Microsoft Vista operating system.

Install On: Gateway

VoIP

R60_06-5

Category: Firewall

Problem: Legitimate MGCP packets may be dropped, if there is more than one ASCII white space in the header.

Resolution: Enhanced MGCP parser ensures RSIP packets are correctly passed.

Install On: Gateway

R60_06-6

Category: Firewall

Problem: Legitimate SIP and MGCP packets may be incorrectly dropped.

Resolution: Enhanced hash algorithms ensure that legitimate SIP and MGCP traffic is passed.

Install On: Gateway

R60_06-7

Category: Logging

Problem: There are unnecessary error messages in the messages file.

Resolution: Errors will be printed only when the relevant SIP debug is active.

Install On: Gateway

VPN-1 Edge

R60_06-8

Category: VPN-1 Edge/Embedded

Enhancement: VPN-1 Edge Firmware 7.5.38 is now supported

Install On: SmartCenter server

Resolved Issues in Previous HFAs

In This Section

R60_HFA_05 Resolved Issues

In This Section

FireWall-1

R60_05-26 Increased the maximum header length and maximum number of headers permitted for manual client authentication.

- **Install On**: Gateway

R60_05-27 Improved stability with NAT scenarios.

- **Install On**: Gateway

R60_05-28 Hide NAT rules improved to direct traffic to Gateway IP address when Gateway is a member of a group object.

- **Install On**: Gateway

R60_05-29 Improved connectivity while using VLANs by including VLAN tags in the ARP response.

- **Install On**: Gateway

R60_05-30 Improved logging performance on diskless Nokia machines when forwarding logs to **SmartCenter server**.

- **Install On**: Gateway

R60_05-31 Enhanced Nokia 3rd Party clustering by opening MC sockets only for sync IFCs.

- **Install On**: Gateway

R60_05-32 Improved kernel stability on Nokia platforms.

- **Install On**: Gateway

R60_05-33 Added support for Tel1000 driver 7.3.15.

- **Install On**: SmartCenter server and Gateway

R60_05-34 Added support for Sun GBE PCI-X NIC 10G (Sun code 5544A).

- **Install On**: SmartCenter server and Gateway

R60_05-35 Improved kernel stability on SecurePlatform.

- **Install On**: Gateway

R60_05-36 Fixed user authentication to groups.

- **Install On**: SmartCenter server and Gateway

R60_05-37 Improved stability and enhanced security for Solaris platforms.

- **Install On**: SmartCenter server

R60_05-38 Added support for DLPI notifications.

- **Install On**: All cluster members

R60_05-39 Improved Interface binding for Solaris 10.
- **Install On**: Gateway

R60_05-40 Improved NAT for DNS traffic.
- **Install On**: SmartCenter server

R60_05-41 Improved enforcement for Monitor-Only mode and when Packet-Sanity disabled.
- **Install On**: Gateway

R60_05-42 Improved parsing for email addresses.
- **Install On**: Gateway

R60_05-43 Improved mail stripping mechanism according to RFC 2231.
- **Install On**: Gateway

R60_05-44 Improved stability for SMTP stripping.
- **Install On**: Gateway

R60_05-45 Improved stability on HTTP Security server.
- **Install On**: Gateway

R60_05-46 Fixed security server response to connect request from URI.
- **Install On**: Gateway

R60_05-47 Improved stability while deleting services from FireWall.
- **Install On**: Gateway

R60_05-48 Fixed DHCP to ensure legitimate traffic is passed.
- **Install On**: SmartCenter server and Gateway

R60_05-49 Added option to globally allow out-of-state packets for specific gateways.
- **Install On**: Gateway

R60_05-50 Improved connectivity when using Hide NAT and RTSP.
- **Install On**: SmartCenter server

R60_05-51 Resolved connectivity issues during SYN attacks.
- **Install On**: Gateway

R60_05-52 All VPN-1 NAT features are now available for SIP/MGCP phones.
- **Install On**: SmartCenter server and Gateway

R60_05-53 Added support for NAT on SIP phones.
- **Install On**: SmartCenter server and Gateway

R60_05-54 Enhanced UDP to ensure legitimate traffic is identified.
- **Install On**: Gateway

R60_05-55 MGCP traffic is correctly inspected and handled.
- **Install On**: Gateway

R60_05-56 Improved HTTP traffic connectivity.
- **Install On**: Gateway

R60_05-57 Enhanced handling of single sign on session authority.
- **Install On**: Gateway

VPN-1

R60_05-58 Improved stability for VPN.
- **Install On**: Gateway

R60_05-59 Improved gateway stability after installation of R60 HFA_02.
- **Install On**: Gateway

R60_05-60 Improved behavior of office mode assignment from the IP pool in cluster environment.
- **Install On**: Gateway

R60_05-61 Improved handling of broadcast DHCP requests in Office Mode cluster environment.
- **Install On**: SmartCenter server

R60_05-62 Improved functionality of Radius office mode assignment for SNX client.
- **Install On**: Gateway

R60_05-63 Improved OpenSSL usage to properly verify RSA signatures.
- **Install On**: SmartCenter server and Gateway

R60_05-64 Added support for OCSP signing **ExtendedKeyUsage** purpose ID.
- **Install On**: Gateway

R60_05-65 CRL expiration date may now exceed 24 days.
- **Install On**: SmartCenter server

R60_05-66 OCSP responders with long update intervals are now supported.
- **Install On**: Gateway

R60_05-67 Added support for non-CA OCSP responders with self signed certificates.
- **Install On**: Gateway

R60_05-68 Improved SecureClient access to a gateway connected to multiple ISPs.
- **Install On**: Gateway

R60_05-69 Improved connectivity after policy installation on a gateway.
- **Install On**: Gateway

R60_05-70 VPN-1 Edge firmware 6.5 is now supported.
- **Install On**: SmartCenter server

R60_05-71 Added an option to preserve remote access connections while policy is installed on a gateway.
- **Install On**: SmartCenter server

R60_05-72 Enhanced efficiency for SecuRemote/SecureClient connections when installing a policy on a gateway that has many remote users.
- **Install On**: Gateway

R60_05-73 Enhanced performance of VPN UTM Edge after CO update.
- **Install On**: Gateway

R60_05-74 Enhanced performance of VPN UTM Edge when permanent tunnels with ROBO peers are enabled.
- **Install On**: Gateway

R60_05-75 Improved VPN connectivity during policy installation for ROBO peers.
- **Install On**: Gateway

R60_05-76 Improved functionality of visitor mode in ClusterXL LS with Sticky Decision Function.
- **Install On**: Gateway

SmartCenter

R60_05-77 Resolved permissions issue that arises when changing group permissions.
- **Install On**: SmartCenter server

R60_05-78 Enhanced stability for SmartDashboard on Solaris.
- **Install On**: SmartCenter server

R60_05-79 Improved High Availability synchronization with the **Synchronize Me** option.
- **Install On**: SmartCenter server

R60_05-80 Removed licensing requirement for Web Intelligence ASCII-Only protection.
- **Install On**: SmartCenter server

R60_05-81 Disabled the option to install a policy on a standalone **SmartCenter server** without configuring topology on all the interfaces.
- **Install On**: SmartCenter server (Standalone Mode)

R60_05-82 Logs can now be saved locally on Hybrid-based NGX machines.
- **Install On**: SmartCenter server and Gateway (Requires IPSO 4.1 build 22 or above)

SmartUpdate

R60_05-83 Enhanced stability on SecurePlatform during HFA installation.
- **Install On**: SmartCenter server

Cluster XL

R60_05-84 Improved policy installation for large databases.
- **Install On**: Gateway cluster members

R60_05-85 Improved identification and handling of disconnected interfaces.
- **Install On**: Gateway cluster members

R60_05-86 Added support for non-active interfaces in third party cluster configurations. Improved cluster connectivity.
- **Install On**: Gateway cluster members

QoS

R60_05-87 Improved QoS on Clusters.
- **Install On**: Cluster members

R60_05-88 Improved QoS Policy installation.
- **Install On**: SmartCenter server

SSL Extender

R60_05-89 Added ability to define an SNX Integrity Clientless Server (ICS) policy for each individual user group.
- **Install On**: SmartCenter server and Gateway

R60_05-90 Added ability to define an encryption domain for each individual user group.
- **Install On**: VPN-1 Gateway

R60_05-91 Add an option to enable/disable the automatic proxy PAC file script.
- **Install On**: SmartCenter server

R60_05-92 Improved support of manual proxy configurations when using SNX with proxy replacement.
- **Install On**: SmartCenter server and Gateway

R60_05-93 Enhanced stability for scenarios that include non-resolvable hostnames.
- **Install On**: SmartCenter server and Gateway

R60_05-94 Enhanced performance when uploading CIFS.
- **Install On**: Gateway

Secure XL

R60_05-95 Improved SYN Defender performance in Cluster LS when SXL is active.

- **Install On**: Gateway

HFA

R60_05-96 It is now possible to install HFA packages on SecurePlatform using the Web UI upgrade feature.

- **Install On**: SmartCenter server or SecurePlatform Gateway (needs R60_HFA_04)

Clientless VPN

R60_05-97 Improved Integrity Clientless Security.

- **Install On**: Gateway

R60_HFA_04 Resolved Issues

In This Section

ConnectControl

R60_04-01 Enhanced ConnectControl usability with large number of servers.

- **Install on**: Gateway

CP ClusterXL

R60_04-02 Improved stability of a cluster whose members connect to different switches or hubs. The fix is controlled by the **fwha_enable_global_probing** global parameter, which is off by default. For more information refer to SK31655.

- **Install on**: Gateway

R60_04-03 The pnote persistent for the CPHAD and FWD processes has been enhanced.

- **Install on**: Gateway

R60_04-04 Improved ARP handling for a standby member of a High Availability ClusterXL.

- **Install on**: Gateway

R60_04-05 Special Instructions for Installing R60_HFA_04 on NGX R60 Clusters

When installing HFA_R60_03 on Clusters from version NGX (whether or not HFA_R60_02 is installed), you should refer to the chapter on ClusterXL in the Upgrade Guide for the relevant instructions.

- **Install on**: Gateway

R60_04-06 Enhanced cluster stability while the `fwha_perform_chain_forward` kernel variable is on.

- **Install on**: Gateway

R60_04-07 ClusterXL can work with switches for which the IGMP snooping feature is enabled. Refer to SK31934 for a description of this fix.

- **Install on**: Gateway

R60_04-08 Stabilized cluster failover.

- **Install on**: Gateway

R60_04-09 Improved ClusterXL stability while using more than one sync networks. Refer to SK31622 for a description of this fix.

- **Install on**: Gateway

Firewall

R60_04-10 Authentication with an unknown RADIUS attribute is now supported. You should add the `radius_ignore` property with the right attribute (sk #47.0.350678.2517298 - Configuring FireWall-1 to ignore non-standard RADIUS attributes).

- **Install on**: SmartCenter server

R60_04-11 Numerous session authentication rules can be created after authentication is complete for the first time.

- **Install on**: Gateway

R60_04-12 Improved memory handling when using several session authentication rules.

- **Install on**: Gateway

R60_04-13 Improved support for logging when the gateway is configured as a local definition and SmartCenter server is behind NAT.

- **Install on**: Gateway

R60_04-14 While the LDAP statistics collection is turned off (via the objects_5_0.C or command line), the statistics file (ldap_pid_xxxx.stat) continued to be created with the text **Stopping statistics collection**. When issuing the command line `ldapcmd -p all stat <interval>`, the interval number is now in seconds. For additional information refer to SR 1-6218839691.

- **Install on**: Gateway

R60_04-15 Improved stability when opening multiple concurrent HTTP connections.

- **Install on**: Gateway

R60_04-16 Improved performance issues when using static NAT and SYN Defender protection.

- **Install on**: Gateway

R60_04-17 The IMAP mail server object is now supported.

- **Install on**: SmartCenter server

R60_04-18 Improved stability of `fw tab -f` output.

- **Install on**: Gateway

R60_04-19 GRE and NAT are now supported. A single GRE connection between a single NATed source to a destination is now possible.

- **Install on**: Gateway

R60_04-20 GRE The kernel table memory consumption (`fwx_alloc table`) has been reduced.

- **Install on**: Gateway

R60_04-21 GRE IPPOOL with a hide NAT feature on HA mode has been enhanced.

- **Install on**: Gateway

R60_04-22 An address range can include an automatic static NAT in the security rule destination.

- **Install on**: Gateway

R60_04-23 Improved resource release during `cpstop`.

- **Install on**: SmartCenter server and Gateway

R60_04-24 Improved stability when handling heavy traffic on SecurePlatform.

- **Install on**: Gateway

R60_04-25 Improved stability of the LKCD tool.

- **Install on**: SecurePlatform

R60_04-26 New NICs are supported with FW1/VPN1 for Solaris OS:

ipge - Dual Gigabit Ethernet

ixge - 10 Gigabit fiber

- **Install on**: Gateway

R60_04-27 The maximum domain limit has been increased. As a result, the rulebase can have more than 32 domain objects.

- **Install on**: Gateway

R60_04-28 The following errors in `fwd.elg` have been resolved on the SmartCenter server: `Failed to get interface list: No such file or directory` and `Cannot get interface list: No such file or directory`

- **Install on**: SmartCenter server

R60_04-29 Resolved policy installation failure on R55 GX modules.

- **Install on**: Gateway

R60_04-30 The error **sic name does not match** no longer appears when fetching a policy from gateways from WIN32 SmartCenter servers.

- **Install on**: SmartCenter server

R60_04-31 Removed a syntax error when installing a policy that has no services of type **other** and are marked as **matched for any**.

- **Install on**: SmartCenter server

R60_04-32 Improved stability when fetching a policy from Windows SmartCenter server.

- **Install on**: SmartCenter server

R60_04-33 Improved stability between the firewall and the security servers.

- **Install on**: Gateway

R60_04-34 Improved behavior when using enhance `ufp` and enable `Ignore UFP server after connection failure`.

- **Install on**: Gateway

R60_04-35 Increased debugging errors associated with the mdq security server.

- **Install on**: Gateway

R60_04-36 Enhancements for stripping mechanism and an SMTP Security Server.

- **Install on**: Gateway

R60_04-37 Improved CPU utilization when using the security server.

- **Install on**: Gateway

R60_04-38 Improved performance when dealing with SSHv2 traffic.

- **Install on**: Gateway

R60_04-39 Enhance DCE-RPC connectivity when the IP in the port command differs from the real source.

- **Install on**: SmartCenter server

R60_04-40 DNS query and response of resource record from type TSIG is enabled.

- **Install on**: Gateway

R60_04-41 Improved stripping mechanism when using the SMTP security server.

- **Install on**: Gateway

R60_04-41 Improved connectivity when working with a SecurePlatform configured to either DHCP server or DHCP relay mode. Refer to SK31936 for additional instructions.

- **Install on**: Gateway

R60_04-42 Improved enforcement for SNMP traffic.

- **Install on**: Gateway

R60_04-43 Enhancement of SmartDefense inspections and ClusterXL LS with asymmetric routing.

- **Install on**: Gateway and SmartCenter server

R60_04-44 Improved performance in LS mode.

- **Install on**: Gateway

R60_04-45 Enhanced HTTP connectivity while Active Streaming is enabled.

- **Install on**: Gateway

R60_04-46 When using enhanced ufp, all URLs sent to the ufp are sent to the ufp with the http://.

- **Install on**: Gateway

R60_04-47 `h323` setup acknowledge message is now supported.

- **Install on**: Gateway

R60_04-48 Enhanced connectively when there are users in the from field.

- **Install on**: Gateway

Floodgate-1

R60_04-49 Sun Fire machines with AMD processors (Opteron/Athlon) can run a QoS policy.

Note: If a previous QoS Add-Hoc fix is installed, please contact Technical-Services.

- **Install on**: Sun Fire machines with AMD processors (Opteron/Athlon) running Checkpoint QoS.

SmartCenter

R60_04-50 Audit logs show the correct and real authentication method.

- **Install on**: SmartCenter server

R60_04-51 `fwm` does not crash when running SmartView Monitor.

- **Install on**: SmartCenter server

VPN-1

R60_04-54 Better support for VPN tunnels between DAIP with groups other than Diffie-Hellman group 2.

- **Install on**: Gateway

R60_04-55 After connecting with SNX client, the user can pass traffic through the VPN gateway, as a Radius group user.

- **Install on**: Gateway

R60_04-56 Installing a Security Policy with a large amount of rules will not disrupt VPN traffic.

- **Install on**: Gateway

R60_04-57 Using the `fw tab -t IKE_SA_table -f` command the data shown is coordinated with the data shown when using the command without the `-f` flag.

- **Install on**: Gateway

R60_04-58 In Simplified Mode, Remote Access rules are now by default intersected with user database restrictions. To ignore user database restrictions, the environment variable `VPN1_IGNORE_USER_DATABASE` should be set.

- **Install on**: Gateway and SmartCenter server

R60_04-59 Once the Install Database process is complete on the gateways in a Cluster environment it is now possible to immediately receive an office mode IP from the gateways.

- **Install on**: Gateway

R60_04-60 When a CRL is larger then 1 MB, VPN can fetch it via HTTP.

- **Install on**: Gateway

R60_04-61 Support has been added for Check Point Integrity SecureClient Mobile (ISCM) central management at the module side. Default policies are located in `$FWDIR/conf/` and include the files `fw_client_1.ttm`, `vpn_client_1.ttm` and `neo_client_1.ttm`. After HFA installation these policy files are placed in `$FWDIR/conf/`. Filenames are `fw_client_1_HFA.ttm`, `vpn_client_1_HFA.ttm` and `neo_client_1_HFA.ttm`. To use these files rename them by removing the `_HFA` suffix in their names.

An special add-on should be applied to the SmartCenter side for a full use of this feature. This add-on has to be applied over HFA_02. After installing HFA_04 on the modules and the add-on to SmartCenter, Integrity Secure Client Mobile management and settings can be changed using GuiDBedit.

For more information on ISCM support installation and configuration please refer to the User Guide. The User Guide as well as HFA_02 and SmartCenter add-on can be downloaded from the Download Center. Select the Integrity SecureClient Mobile product, a version is “NGX R60” and the Windows Mobile 2003/SE/5.0 operating system.

- **Install on**: Gateway.

R60_04-62 Installing a Security Policy in a VPN-1 gateway will not break disrupt existing connections for remote users.

- **Install on**: Gateway

R60_04-63 Smartview Monitor can now show Remote Users.

- **Install on**: Gateway

R60_04-64 Improved policy installation performance issues that may occur when there is a large amount of ROBO gateways.

- **Install on**: Gateway

R60_04-65 Improved performance of VPN-1 when installing a policy with a large rulebase while many SecureClient users are connected.

- **Install on**: Gateway

R60_04-66 Reduced policy installation time and resources when reloading a gateway that has many tunnels to edge devices.

- **Install on**: Gateway

R60_04-67 Tunnel Monitoring is now supported for ROBO gateways and VPN Communities that have NAT disabled.

- **Install on**: Gateway and SmartCenter server

SecurePlatform

R60_04-68 SecurePlatform can now support the following new NICs:

- The e1000 driver was upgraded to 7.0.38 version
- 10GB support - Intel PRO/10Gbe CX4
- Sun Dual Gigabit Ethernet Adapter UTP copper PCIe x 4
- Sun Dual Gigabit Ethernet Adapter MMF fiber PCIe x 4
- IntelPRO/1000 PT Dual Port server adapter UTP copper PCIe x 4
- HP NC320T Gigabit NIC single port UTP copper PCIe x 1
- IntelPRO/1000 Dual Port PCIe x 4 (82546GB based)
- HP NC340T PCI-X Quad Port Gigabit
- Sun X445A PCI-X Quad Port Gigabit
- Intel® PRO/1000 GT Quad Port Server Adapter
- **Install on**: SecurePlatform

HFA

- **R60_04-69** For fast and easy deployment use the new automatic installation script. The new Automatic Installation script enables you to quickly and effortlessly install packages relevant to your deployment. Extract the comprehensive package and run:

  - `UnixInstallScript` - for Unix platforms, or
  - `Setup.bat` - for Windows
- **R60_04-70** A new utility name hfa_ver.sh will represent the build numbers associated with the installed HFA package.

R60_HFA_03 Resolved Issues

In This Section

Firewall

R60_03-01 The `-all` flag in the command line `fwm dbload` is properly supported for NGX. The database will be loaded on all modules/targets defined in file named `sys.conf` located on management at `$FWDIR/conf`.

- **Install on**: SmartCenter server

R60_03-02 Logging can be defined to a large disk.

- **Install on**: Gateway and SmartCenter server

R60_03-03 After the NAT rulebase is changed the NAT rule base is in the correct order.

- **Install on**: SmartCenter server

R60_03-04 An address range can include an automatic static NAT in the destination of a security rule.

- **Install on**: SmartCenter server

R60_03-05 An H323 connection with NOTIFY has been improved significantly.

- **Install on**: Gateway

R60_03-06 New user and user group configurations are saved when viewing or restoring from Database Revision Control.

- **Install on**: SmartCenter server

R60_03-07 TCP keepalive packets are supported by the TCP streaming mechanism. To drop TCP keepalive packets, change the kernel global parameter `fwtcpstr_allow_keepalive` to `0`, as explained in the SecureKnowledge > How to modify kernel global parameters?.

For more information, see SK: https://secureknowledge.us.checkpoint.com/SecureKnowledge/viewSolutionDocument.do?id=sk15619

- **Install on**: Gateway

R60_03-08 The following debug commands can be used to view a message that indicates if a packet is dropped because it is too short:

fw ctl debug 0

fw ctl debug -buf 8192

fw ctl debug drop

fw ctl kdebug -f >kern.out

- **Install on**: Gateway

R60_03-09 The firewall enforces FW1_lea implied_rule when implied_rules.def is replaced with implied_ruleHFA.def. For more information, see SK: https://secureknowledge.us.checkpoint.com/SecureKnowledge/viewSolutionDocument.do?id=sk31538

- **Install on**: Gateway and SmartCenter

R60_03-10 It is now possible to cause connections blocked by SAM to be globally dropped rather than rejected. This can be done by modifying the kernel parameter fwsam_reject either temporarily or permanently, as explained in the SK item How to modify kernel parameters.

For more information, see SK:
https://secureknowledge.us.checkpoint.com/SecureKnowledge/viewSolutionDocument.do?id=sk30452

- **Install on**: Gateway

R60_03-11 Various file names can be sent by email.

- **Install on**: Gateway

R60_03-12 Session handling has improved on the http security server.

- **Install on**: Gateway

Web Intelligence

R60_03-13 Selecting Monitor only on all web server features enables traffic and retrieves a monitor only log.

- **Install on**: Gateway

InterSpect

R60_03-14 The CIFS protocol is supported.

- **Install on**: Gateway

VPN-1

R60_03-15 With RDP Protocol Optimization the number of RDP messages on the gateway is unlimited. This enables a larger number of concurrent users in an MEP configuration.

- **Install on**: Gateway

R60_03-16 When installing a policy a warning will be produced for each certificate belonging to a network object that will expire in the next 2 months. The warning message will contain the certificate DN and expiration time.

For more information, see SK:
https://secureknowledge.us.checkpoint.com/SecureKnowledge/viewSolutionDocument.do?id=sk31539

- **Install on**: SmartCenter server

R60_03-17 User names with a DN notation but which do not contain real LDAP paths, can now be used for LDAP authentication. This implementation is necessary for certain certificates whose Subject is in the form of DN. To activate, set UserNameIsNotDN on the relevant gateway:

For more information, see SK:
https://secureknowledge.us.checkpoint.com/SecureKnowledge/viewSolutionDocument.do?id=sk31545

1. Execute `ckp_regedit -a SOFTWARE\\CheckPoint\\VPN1 UserNameIsNotDN "1"`

2. Execute `cprestart`

- **Install on**: Gateway

R60_03-18 Using a generic user configuration with SecureID authentication enables you to authenticate using a username that does not exist in the VPN-1 internal database. In addition, you can also successfully perform a SecurID authenticate with a username that does exist in the VPN-1 internal database using `auth type=SecurID`.

- **Install on**: Gateway

R60_03-19 Stability has improved when using office mode and a VPN accelerator device is installed on the machine.

- **Install on**: Gateway

R60_03-20 All members of a load sharing cluster will be able to initiate IKE with a VPN-1 Edge device after the Edge-1 device has changed its IP.

- **Install on**: Gateway

R60_03-21 VPN-1 Edge Firmware 6.0 is now supported.
For more information, see SK:
https://secureknowledge.us.checkpoint.com/SecureKnowledge/viewSolutionDocument.do?id=sk31534

- **Install on**: SmartCenter server

R60_03-22 Improved stability when authenticating LDAP users when multiple LDAP groups, of different LDAP AUs, are on the same Remote Access rule and Remote Access community.

- **Install on**: Gateway

ClusterXL

R60_03-23 ClusterXL works with a Solaris server that runs IP Multipathing.

- **Install on**: Gateway

R60_03-24 Disabling a network connection (interface) is now supported on ClusterXL gateways on Windows platforms.

- **Install on**: Clusters

R60_03-25 Set the global kernel variable fwha_ospf_bypass so that the local anti-spoofing mechanism will not check OSPF packets. As a result, OSPF packets issued from one cluster member are not dropped by the other cluster members.

For more information, see SK:
https://secureknowledge.us.checkpoint.com/SecureKnowledge/viewSolutionDocument.do?id=sk31546

- **Install on**: Gateway

SSL Network Extender

R60_03-26 SNX now supports Mac OS X Tiger.

R60_03-27 Support for the following properties was added to SSL Network Extender:

```
use_cn_to_fetch_user
use_principal_name
```

For more information, see SK:
https://secureknowledge.us.checkpoint.com/SecureKnowledge/viewSolutionDocument.do?id=sk31540

- **Install on**: Gateway

SmartCenter

R60_03-28 A policy installation will be successful when the Policy Installation Targets list includes VPN-1 and QoS objects.

- **Install on**: SmartCenter server

R60_03-29 It is now possible to establish sync on Management High Availability if the `$FWDIR` of the primary management is installed on a path that includes spaces. The primary management can create a backup tar.tgz file and does not fail.

- **Install on**: SmartCenter server

R60_03-30 Authentication is enabled via a Radius server when configuring a Radius group. For more information, see SK:
https://secureknowledge.us.checkpoint.com/SecureKnowledge/viewSolutionDocument.do?id=sk31541

- **Install on**: SmartCenter server

SecureXL

R60_03-31 It is possible to perform simultaneous pings to the cluster IP address and the active member IP address.

- **Install on**: Gateway

Policy Server

R60_03-32 Resolved Policy Server stability issues when the license does not include all operation systems is supported by SecureClient.

- **Install on**: Gateway

R60_HFA_02 Resolved Issues

In This Section

Firewall

R60_02-01 Improved functionality when working with partially automatic client authentication and SSO authentication.

- **Install on**: Gateway

R60_02-02 Improved functionality of Security Server when doing Client Authentication.

- **Install on**: Gateway

R60_02-03 Resolved Anti Spoofing functionality when configuring third party cluster interfaces; specifically when the SmartCenter server which is managing a third party cluster, is being upgraded.

- **Install on**: SmartCenter server

R60_02-04 In a Nokia Cluster environment, OSPF packets issued from one cluster member were deleted by the other cluster members because they were considered “spoofed” packets.

- **Install on**: Gateway

R60_02-05 When the VPN-1 Pro service is run on a standalone gateway, the following error message used to be logged in the Event Viewer: **ps fetch: Couldn't get masters from masters file**.

- **Install on**: SmartCenter server & Gateway (in standalone deployment)

R60_02-06 The port scanning mechanism no longer blocks connections originating from the gateway.

- **Install on**: Gateway

R60_02-07 During the installation process the following error message is displayed **cp: cannot access /opt/CPngcmp-R60/svn/***. This message does not affect the installation process and can be safely ignored.

- **Install on**: SmartCenter server

R60_02-08 Resolved functionality when specifying certain SmartDefense settings.

- **Install on**: Gateway

R60_02-09 Logical Servers now function properly following a reboot operation.

- **Install on**: Gateway

R60_02-10 When Windows creates a NBT packet, the FireWall would drop the packet and the following message: **FW-1: fwscv_request_status: Failed to generate ICMP packet** used to appear on the console and in `var/ log/messages` every few minutes `/var/log/messages`.

- **Install on**: Gateway

R60_02-11 Resolved a problem of VPN-1 Pro dropping DNS packets of DNSsec.

- **Install on**: Gateway

R60_02-56 Resolved error message that appeared on the console: **cpas_tcp_pass_data: asked to transfer 89 bytes which is more than in q(88)**

- **Install on**: Gateway

R60_02-12 Long MSN messages are now supported.

- **Install on**: Gateway

R60_02-13 Resolved RTSP issues with client-initiated RDP data-connections.

- **Install on**: SmartCenter server

R60_02-14 ftp User Authentication in Non-Transparent mode from a unix client can now be successfully executed. Previously the following message (or something similar) was displayed on the ftp client: **200 Host: you can use 'quote password' or Account command ('ACCT') ftp> quote <ftp target> Not connected**.

- **Install on**: Gateway

R60_02-15 Resolved connectivity issue for Logical Servers (Connect Control) and Client Authentication in Wait Mode. The FireWall no longer sends PING packets with erroneous ICMP checksum.

- **Install on**: Gateway

R60_02-16 ftp/telnet/rlogin User Authentication in Non-Transparent mode to the Cluster virtual IP addresses can now be executed. Previously the following messages (or a similar variant thereof) were displayed:

- On the ftp client: **413 Connection to server failed Login failed. 421 Service not available, remote server has closed connection**
- On the rlogin client: **Connection to <Virtual IP Address cluster> failed rlogin: connection closed**
- On the telnet client: **Connection to <Virtual IP Address cluster> failed Connection closed by foreign host**
  - **Install on**: Gateway

R60_02-17 Resolved issues when configuring **ASCII Only Request** and using http security servers.

- **Install on**: Gateway

R60_02-18 Fixed a connectivity problem when downloading large files and using CVP servers.

- **Install on**: Gateway

R60_02-19 Resolved Policy issue where when creating a network that includes only broadcast addresses, where **disallow broadcast addresses** was checked, the policy was incorrectly enforced.

- **Install on**: SmartCenter server

R60_02-20 Performance enhancement after executing `cpstart` when a Policy has just been installed. To activate this fix define the `SIC_SERVER_DEFAULT_ TIMEOUT` value on the registry using the `cpprod` utility. From the SmartCenter command line, run:

```
# cpprod_util CPPROD_SetValue SIC SIC_SERVER_TIMEOUT 1 60 1
```

Then run `#cpstop` and finally `#cpstart`

- **Install on**: Gateway

R60_02-21 Resolved policy installation issue when CPMI implied rule is intentionally disabled. For details, see SecureKnowledge sk25867 at: https://secureknowledge.us.checkpoint.com/SecureKnowledge/viewSolutionDocument.do?id=sk25867

- **Install on**: SmartCenter server

R60_02-22 The global parameter `fw_rst_expired_conn` global parameter now works properly for NATed connections.

- **Install on**: Gateway

R60_02-23 In SmartView Monitor a negative number of un-acked SYNs was displayed. This has been resolved and is now displayed correctly.

- Install on: Gateway

R60_02-24 Resolved error log **Malformed H.225 message and Malformed RAS message** when H.235 in the H225 messages are in use.

- **Install on**: Gateway

R60_02-25 Resolved error log **IpPortMessage is out of state**.

- **Install on**: Gateway

R60_02-26 The service displayed in the SCCP logs is now SCCP, as it should be.

- **Install on**: Gateway

VPN-1

R60_02-27 Resolved Automatic certificate enrollment with Entrust CA issues.

- **Install on**: SmartCenter server

R60_02-28 False error messages are no longer logged in the OS messages log file.

- **Install on**: Gateway

R60_02-29 Keep alive INSPECT rule enhancement. In order to use the improved rule you should use `implied_rules.def`.

- **Install on**: SmartCenter server

R60_02-30 Improved support for DHCP by correctly handling of option #54 of a DHCP message

- **Install on**: Gateway

R60_02-31 Automatic assignment through DHCP when using multiple DHCP servers is now permitted, by sending the requests to a broadcast address. To use this feature, define the IP address of the DHCP server as a broadcast address.

- **Install on**: SmartCenter server and Gateway

R60_02-32 DKM automatic enrollment (for ICA only) and DKM manual enrollment are now supported.

- **Install on**: SmartCenter server

R60_02-57 Resolved authentication issue when using two or more LDAP groups with a Remote Access community.

- **Install on**: Gateway

R60_02-33 Improved stability of remote connections in a cluster environment.

- **Install on**: Gateway

R60_02-34 FQDN, DN and User_FQDN as identification payload types in IKE for ICSA 1.1D certification are now supported.

- **Install on**: Gateway

R60_02-35 The file `ikemonitor.snoop` that contains the contents of IKE packets and should only be used for debugging purposes is now properly formatted on the Windows platform.

- **Install on**: Gateway

R60_02-36 Check Point DAIP gateways, (for instance, VPN-1 Edge or a VPN-1 gateway with a dynamic IP address) can only connect with a IKE phase1 method specified in the **Global Properties**.

- **Install on**: Gateway

R60_02-37 Improved support of IPSec tunnels with 3rd party DAIP devices, (for instance IPSec in GRE with dynamic IP address device).

- **Install on**: Gateway

R60_02-38 Nokia Symbian VPN clients are now supported.

- **Install on**: Gateway

R60_02-39 Resolved IKE phase1 negotiation in an environment that includes ROBOs. You should detect and ignore all scenarios where the ROBO is erroneously identified as being in its own encryption domain.

- **Install on**: Gateway

R60_02-40 The correct state of the VPN tunnel is now displayed in SmartView Monitor.

- **Install on**: Gateway

R60_02-54 After failover and full sync, all outbound Security Associations (SAs) with Edge devices on the newly active member may be deleted. To prevent this, when installing the HFA replace the `vpn_table.def` with the new `*_hfa.def` file supplied in the HFA package, and thereafter install the policy.

- **Install on**: SmartCenter server and Gateway

SmartCenter

R60_02-41 IPSO can now use `checkpoint snmp (cpsnmpd)`.

- **Install on**: SmartCenter server and Gateway

SmartUpdate

R60_02_42 R55P HFA packages on R55P gateways with SmartUpdate can now be properly installed.

- **Install on**: SmartCenter server

SmartView Monitor

R60_02-43 The Routing table is now properly updated when entries are removed.

- **Install on**: SmartCenter server and Gateway

ClusterXL

R60_02-44 The `fwha_timer_cpha_res` kernel parameter can now be executed.

- **Install on**: Gateway

R60_02-45 Gratuitous ARP request can now be received by both Active and Standby Cluster members.

- **Install on**: Gateway

R60_02-46 SSH connections can now be opened from a standby member.

- **Install on**: SmartCenter server

R60_02-47 Improved network capabilities when several ClusterXL clusters connect to the same network segment with a monitored private interface.

- **Install on**: Gateway

R60_02-48 Logs can now be sent from the cluster's members to a NATed log server.

- **Install on**: Gateway

R60_02-49 New procedures for installing Clusters from version NGX.

- **Install on**: Clusters

R60_02-50 When the IP address is deleted from the sync interface, no messages are printed to the console.

- **Install on**: Gateway

SecurePlatform

R60_02-52 Resolved `net snmp` issues, the oid's value is now correct.

- **Install on**: Gateway and SmartCenter server

R60_02-55 `R60_HFA_02` now supports Turbocard on SecurePlatform. For more information, refer to http://www.checkpoint.com/downloads/quicklinks/downloads_tc.html.

- **Install on**: Gateway

InterSpect

R60_02-53 Resolved machine stability issues.

- **Install on**: Gateway

Performance Pack

R60_02-51 Improved handling of retransmitted TCP packets when Sequence Verifier is enabled.

- **Install on**: Gateway

R60_HFA_01 Resolved Issues

In This Section

Firewall

1) **R60_01-01** Improved handling of alerts generated by SmartView Tracker.
    - **Install on**: CLM and SmartCenter server

2) **R60_01-02** On an IPSO OS, when a packet with source IP address 0.0.0.0, passes through Firewall via a http with resource rule when SYN Defender is enabled, these packets should be blocked.
    - **Install on**: NOKIA Gateway (IPSO)

3) **R60_01-03** ISP Redundancy now supports R55 clusters when managed from NGX. This fix requires installation of the `ng_bc_COR_BC_R60_HFA_01` package.
    - **Install on**: SmartCenter server

4) **R60_01-04** Improved Enforcement when a host is defined as both web server and mail server.
    - **Install on**: Gateway

5) **R60_01-47** TKEY and TSIG Resource records are now supported in DNS traffic. For details, see SecureKnowledge sk31163 at: https://secureknowledge.us.checkpoint.com/SecureKnowledge/viewSolutionDocument.do?id=sk31163
    - **Install on**: Gateway

6) **R60_01-05** Enhanced kernel stability, (related to SSL Enforcement in SmartDefense).
    - **Install on**: Gateway

7) Improved CIFS Service enforcement. For details, see SecureKnowledge sk31196 at http://secureknowledge.us.checkpoint.com/SecureKnowledge/viewSolutionDocument.do?id=sk31196
    - **Install on**: SmartCenter server

8) **R60_01-06** When the web server is not responding or unavailable the response status codes have been changed. Response will be 502 instead of 200.
    - **Install on**: Gateway

9) **R60_01-07** Improved user experience when doing Partially automatic Client Auth on a Macintosh web browser, Apple Safari, an authentication prompt is now displayed.
    - **Install on**: Gateway

10) **R60_01-08** Enhanced Memory performance when installing a policy with multiple cluster members.
    - **Install on**: SmartCenter server

11) **R60_01-09** Make sure that your policy has no services with overlapping ports, (e.g. 1-1000, 500-1500) in order to ensure a successful outcome for the matching process.
    - **Install on**: SmartCenter server

12) **R60_01-10** Improved Certificate renewal. This ensures that StormCenter functionality and connectivity to the SANS web site is maintained.
    - **Install on**: Gateway & SmartCenter server

13) **R60_01-12** When there is a BIND request, more than one context item can now be used.
    - **Install on**: SmartCenter server

14) **R60_01-13** Enhanced stability of Firewall kernel in relation to SmartDefense protections.
    - **Install on**: Gateway

15) **R60_01-14** Improved execution of **Block Suspicious Activity** operation from SmartView Monitor.
    - **Install on**: Gateway & SmartCenter server

16) **R60_01-15** The scenario with an external Gatekeeper and hide NAT on the internal network, incoming calls with FastStart are now successful.
    - **Install on**: Gateway

17) **R60_01-16** Improved handling of H.245 packets and H.225 packets. **Malformed H.245** log is still displayed if the H.245 and H.225 packets are malformed.
    - **Install on**: Gateway

18) **R60_01-17** Some SIP sessions might be mistakenly identified as Instant Messaging. To resolve this you should allow Instant messaging in SmartDefense.
    - **Install on**: Gateway

19) **R60_01-18** SIP over TCP is now supported with Hide NAT.
    - **Install on**: Gateway

VPN

20) **R60_01-19** VPN back connections now support L2TP clients.
    - **Install on**: Gateway

21) **R60_01-20** Improved renewal of certificates generated from the Check Point internal CA. The message displayed before the fix: **Certificate with the same DN already exists**.
    - **Install on**: SmartCenter server

22) **R60_01-22** Improved behavior failover when working in an LSM environment and the Central Office is a cluster.
    - **Install on**: Gateway & SmartCenter server

23) **R60_01-23** Fixed DHCP FQDN attribute syntax.
    - **Install on**: Gateway

24) **R60_01-24** Manual enrolling for certificate enhancements when using CA hierarchies.
    - **Install on**: SmartCenter server

25) **R60_01-25** When using CA hierarchies, a trusted CA object is now created and issued with the correct certificate.
    - **Install on**: SmartCenter server

26) **R60_01-26** Improved handling of INITIAL-CONTACT messages sent in a separate informational negotiation.
    - **Install on**: Gateway

27) **R60_01-27** Improved processing of the key length attribute in IKE.
    - **Install on**: Gateway

28) **R60_01-28** For interoperable devices, improved interoperability for VPN tunnels in GRE-on-IPSec mode.

- **Install on**: Gateway

29) **R60_01-29** Safe@ users topology are now properly downloaded when the gateway is a cluster with a traditional policy.
    - **Install on**: Gateway

30) **R60_01-30** To ensure that IKE phase1 negotiation takes place successfully, make sure that the ROBO Gateway is not being detected as part of its own encryption domain.
    - **Install on**: Gateway

31) **R60_01-31** Enhanced Nokia clients support.
    - **Install on**: Gateway

32) **R60_01-32** When working with GRE over IPSec, the network object's main IP address (and not the IP address according to the link selection) is set as the IP address of the GRE header. In this case, the expected GRE endpoint on the peer side and the main IP address of the local network object should be identical.
    - **Install on**: Gateway

33) **R60_01-33** Dynamic VPN connections now have improved tolerance to policy changes.
    - **Install on**: Gateway

34) **R60_01-34** After the SmartCenter server is upgraded from version NG to version NGX, the VPN routing configuration information is properly downloaded to older (NG) components.
    - **Install on**: SmartCenter server

SmartCenter

35) **R60_01-35** In order to display the latest HTML pages you should perform a SmartDefense update from InterSpect 2.0 SmartDashboard instead of from SmartDashboard from version R60.
    - **Install on**: SmartCenter server

36) **R60_01-36** When configuring Connect on Demand for a dialup modem on a VPN-1 Edge gateway, the modem mistakenly maintained the connection when a tunnel test was the only traffic. The modem should dial only on activity traffic, and disconnect in its absence. This issue is now resolved.
    - **Install on**: SmartCenter server

37) **R60_01-37** Improved handling of passive ftp connections towards an ftp server behind a VPN-1 Edge gateway.
    - **Install on**: SmartCenter server

38) **R60_01-38** A Hide NAT rule can now be used to allow ICMP traffic to a source.
    - **Install on**: SmartCenter server

39) **R60_01-39** Improved VoIP call handling. When there is a high load of TCP and UDP connections over VPN, UDP connections experienced issues as a result of an incorrect SA being used.
    - **Install on**: Gateway & SmartCenter server1

40) **R60_01-40** Improved traffic handling when a LocalMachine Dynamic object is used in a Static NAT rule.
    - **Install on**: SmartCenter server

SmartUpdate

41) **R60_01-41** Use **Revert installation to image on failure** when you upgrade a Gateway of version R55 or higher version only. Make sure that it is not used when you upgrade a Gateway from any version below R55. Similarly, the CLI options `cprinstall snapshot`, `cprinstall revert` and `cprinstall show` will also work with SecurePlatform R55 or higher.
    - **Install on**: SmartCenter server

ClusterXL

42) **R60_01-42** 256 interfaces are now supported for a Nokia cluster. There is no need to remove the following files in order to get the cluster topology.
- `$FWDIR/bin/cxl_create_partner_topology_file`
- `$FWDIR/tmp/cxl_partner_topology_config.txt`
- **Install on**: Gateway

Internal CA

43) **R60_01-43** Improved SIC certificate renewal resulting in enhanced SIC communications between the Gateway and the SmartCenter server.
- **Install on**: Gateway & SmartCenter server

SecurePlatform

44) **R60_01-44** e1000 driver is able to auto negotiate the speed with the switch. SecureXL.
- **Install on**: Gateway & SmartCenter server

SSL Network Extender

45) **R60_01_45** Improved SNX authentication when the Client and the SNX server both use third party certificates.

For details, see SecureKnowledge sk9-1319111 at: https://secureknowledge.us.checkpoint.com/SecureKnowledge/viewServiceRequest.do?id=9-1319111
- **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