NGX R65.4

Including NGX R65.2.100 Gateway & SmartProvisioning NGX R65.4

Release Notes

Check Point
SOFTWARE TECHNOLOGIES LTD.

October 26, 2009

This Release Notes document provides essential operating requirements and describes known issues for the NGX R65.4 Release, including SmartProvisioning NGX R65.4, and the NGX R65.2.100 Check Point gateway. Review this information before setting up NGX R65.4 or NGX R65.2.100.

Note - Before beginning the installation, read the latest available version of these Release Notes at: http://supportcontent.checkpoint.com/documentation_download?ID=8758

In This Document

Introduction to NGX R65.4

Check Point NGX R65.4 delivers new features to further unify and expand Check Point's enterprise security solutions. Check Point's NGX is the only platform that delivers a unified security architecture, enabling the sharing of common security technologies managed via a single management console across Check Point solutions. This unified security architecture enables enterprises of all sizes to reduce the cost and complexity of security management and ensure that their security systems can be easily extended to adapt to new and evolving threats.

This release adds new capabilities and features and enables unified management for many pre-existing Check Point plug-ins.

NGX R65.4 includes the following components:

- VPN-1 NGX R65.2.100, the latest VoIP aware Check Point gateway offering comprehensive security for Enterprise, Telecom network, and Service Provider VoIP environments.
- The ability to manage VPN-1 NGX R65.2.100 gateways with the NGX R65.2.100 management (VoIP) plug-in.
- SmartProvisioning, which enables you to manage large-scale deployments of Check Point gateways from a single SmartCenter server.
- The HFA_40 Hotfix Accumulator (HFA).
- The ability to manage Connectra gateways with the Connectra NGX R66 plug-in.
- The ability to manage VSX gateways with the VPN-1 Power VSX NGX R65 management plug-in.
- The ability to manage Messaging Security on VPN-1 UTM and VPN-1 UTM Edge gateways, with the VPN-1 NGX R65 with Messaging Security management plug-in.
- Support for Endpoint Connect, the new IPSec remote access client for seamless VPN connectivity to corporate resources.
- The NGX R65.4 SmartConsole and Multi Domain GUI, which enables the management of all features and components listed above.

What's New

New VoIP Features

The following is a summary of the new VoIP features found in NGX R65.2.100 and managed with the NGX R65.2.100 management plug-in. A more detailed list of VoIP features supported NGX R65.2.100 is available in "Newly Supported Features in NGX R65.2.100" on page 23.

- Enhanced management for VoIP security solution including quick setup. A new SmartDashboard VoIP tab helps manage VoIP, provides application policy configuration, and provides overview pages for SmartDefense VoIP protections, VoIP application Policy, and VoIP entities status.
- Enhanced and granular security for maximum flexibility in deployment and enforcement.
- Session Border Controller functionality for large enterprises, providing Far-end NAT traversal functionality, QoS for gateways and servers, and call admission control.
- Enhanced troubleshooting including monitor mode globally or per protection.
- Enhanced logging with detailed VoIP information.
- New RTP and RTCP security defenses are included and accelerated with SecureXL.
- Gateway can securely inspect TLS-Encrypted SIP Traffic, perform NAT translation (including on SIP payload), and dynamically open pinholes for data.
- Vendor Interoperability with
  - Cisco CallManager 6.1 with NAT (SIP).
  - Avaya ACM and SES R5.0
  - Universal Alcatel R6.2 UA/NOE and IPlink protocols.

For more information see the *NGX R65.2.100 Administration Guide* at http://supportcontent.checkpoint.com/file_download?ID=8690 and the "NGX R65.2.100 Limitations and Clarifications" on page 26.

SmartProvisioning

Check Point SmartProvisioning NGX R65.4 enables you to manage large-scale deployments of Check Point gateways from a single SmartCenter server, with features to define, manage, and provision gateways. For example, you can configure the DNS servers, RADIUS servers, domain name, and host list that a VPN-1 gateway should use, and then provide this configuration to a number of gateways, by assigning the gateways to the Provisioning Profile that holds this configuration.

SmartProvisioning NGX R65.4 provides all the features of SmartLSM NGX R65, with the addition of the following:

- Manage remote VPN-1 UTM Edge devices with profiles and individual settings for: date and time, routing, RADIUS servers, and HotSpots.
- Manage remote VPN-1 Power/UTM gateways with profiles and individual settings for: DNS servers, host list, domain, backup servers and schedules, host name, and network interfaces.
- Manage complex interface configurations, VPN tunnels, and routing for remote gateways.
- Automatic calculation of Anti-Spoofing information for SmartLSM gateways.
- Tracking logs for gateways based on static IDs, with local logging for reduced logging load.
- Run scripts on VPN-1 Power/UTM gateways or sets of gateways.

- Manage package distribution and installation on VPN-1 Power/UTM gateways.
- Manage ports, topology, VPNs, and configuration scripts on VPN-1 UTM Edge devices.
- Protect VPN-1 Power/UTM gateways from changes while in Maintenance Mode.
- Support for complex internal networks.
- Manage Dynamic Objects, enabling you to create Check Point Security Policies with variables.

For more information, see the *SmartProvisioning NGX R65.4 Administration Guide* at http://supportcontent.checkpoint.com/file_download?ID=8691 and the "SmartProvisioning NGX R65.4 Limitations and Clarifications" on page 30.

Enhanced Provider-1 High Availability and New Features

- Provider-1 commands can be executed without root permissions, in a new Provider-1 shell (P1Shell)
- New High Availability capabilities:
  - High Availability deployments can now be across different platforms.
  - High Availability deployments can now include more than two CMAs per Customer.
  - New failure recovery capabilities in High Availability deployments.
- New search capability for objects and rules across CMA databases.

For more information see the *Provider-1 NGX R65.4 Administration Guide* at http://supportcontent.checkpoint.com/file_download?ID=8694

New Endpoint Connect Features

Endpoint Connect is Check Point's new lightweight remote access client. Providing seamless, secure (IPSec) VPN connectivity to corporate resources, the client works transparently with VPN-1 and Connectra gateways. Resident on the users desktop or laptop, Endpoint Connect provides various capabilities for connectivity, security, installation and administration.

To learn how to configure a gateway to accept the new Endpoint Connect client, see the *Endpoint Connect NGX R65.4 Administration Guide* at:
http://supportcontent.checkpoint.com/file_download?ID=8631

To learn how to use the Endpoint Connect client, see the *Endpoint Connect NGX R66 HFA01 User Guide* at: http://supportcontent.checkpoint.com/file_download?ID=8632

VPN-1 UTM Edge

- Messaging Security for VPN-1 UTM Edge gateways can be centrally managed with NGX R65.4.
- New support for firmware 8.0.34.

Support for Plug-ins

- The NGX R65.4 SmartConsole and Multi-Domain GUI provides support for new NGX R65.2.100 VoIP features.
- The NGX R65.4 SmartConsole and Multi-Domain GUI supports previous Check Point Plug-ins for NGX R65, including:
  - VPN-1 Power VSX NGX R65 management plug-in
  - Connectra NGX R66 management plug-in

- VPN-1 NGX R65 with Messaging Security management plug-in

Other Integrated Plug-ins and HFAs

Hotfix Accumulator NGX R65 HFA_40

NGX R65.4 includes Hotfix Accumulator R65 HFA 40. This HFA resolves various issues and contains improvements for various Check Point products.

The VPN-1 NGX R65_HFA_40 Release Notes are available at http://supportcontent.checkpoint.com/file_download?ID=8684

The Provider-1 NGX R65_HFA_40 Release Notes are available at http://supportcontent.checkpoint.com/file_download?ID=8764

NGX R65 with Messaging Security Plug-in

NGX R65.4 includes a management plug-in allowing you to manage NGX R65 with Messaging Security gateways. Gateway capabilities include Anti Spam, Mail Anti Virus, Zero Hour Malware protection, and additional content inspection reporting options in Eventia Reporter.

For more information, see the *NGX R65 with Messaging Security* guide at http://supportcontent.checkpoint.com/file_download?ID=7891.

Connectra NGX R66 Plug-in

NGX R65.4 includes a plug-in allowing you to manage Connectra NGX R66 gateways.

For more information, see the *Connectra Central Management NGX R66 Administration Guide* at http://supportcontent.checkpoint.com/file_download?ID=8397

VPN-1 Power VSX NGX R65 Plug-in

NGX R65.4 includes the plug-in allowing you to manage VPN-1 Power VSX NGX R65 gateways.

For more information, see the *VPN-1 Power VSX NGX R65 Administration Guide* at http://supportcontent.checkpoint.com/file_download?ID=7944

Supported Platforms and Versions

In This Section

Supported Platforms and Versions

NGX R65.4 Supported Platforms

NGX R65.4 must be installed on top of an NGX R65 SmartCenter server or Provider-1 MDS. If you do not already have NGX R65 installed:

- For a new installation see the *NGX R65 Internet Security Products Getting Started Guide* at http://supportcontent.checkpoint.com/file_download?ID=7249
- To upgrade to NGX R65, see the *NGX R65 Upgrade Guide* at http://supportcontent.checkpoint.com/file_download?ID=7259

The following platforms are supported for installing NGX R65.4 on the SmartCenter server or MDS:

Platform	Version	Required Free Disk space
SecurePlatform	NGX R65	1 GB
Linux	Red Hat Enterprise Linux 3.0	1 GB
Solaris	5.8, 5.9, 5.10	700 MB
Windows	Windows Server 2000, Windows Server 2000 with SP1- SP4, Windows Server 2003, Windows Server 2003 with SP1 and SP2	700 MB
Nokia IPSO (disk)	4.1, 4.2	500 MB

Note - Nokia IPSO platform supports only the VPN-1 Power VSX NGX R65 management plug-in and the NGX R65 HFA 40

NGX R65.2.100 Gateway Supported Platforms

The following platforms are supported for installing the NGX R65.2.100 gateway:

Platform	Version
SecurePlatform	NGX R65, NGX R65 HFA01, NGX R65 HFA02
Linux	Red Hat Enterprise Linux 3.0
Solaris	5.8, 5.9, 5.10
Nokia	IPSO 4.2

Note - The NGX R65.2.100 gateway is not supported on the Windows platform.

NGX R65.4 SmartConsole and Multi Domain GUI Supported Platforms

NGX R65.4 SmartConsole and Multi Domain GUI can manage any NGX R65 SmartCenter or Provider-1 MDS.

Install the SmartConsole on any of the following platforms:

- Microsoft Windows Server 2003 (SP1-2)
- Microsoft Windows 2000 Advanced Server (SP1-4)

- Microsoft Windows 2000 Server (SP1-4)
- Microsoft Windows XP Home and Professional (SP1-3)
- Microsoft Windows Vista and Vista SP1 (32 bit only)

SmartProvisioning Supported Platforms

The following platforms support SmartProvisioning NGX R65.4.

Provisioning Gateways:

- SecurePlatform NGX R65 VPN-1 Power/UTM
- SecurePlatform NGX R65 on Power-1/UTM-1 appliances
- Firmware 7.5 and higher on VPN-1 UTM Edge

Supported Upgrade Paths

Supported Upgrade Paths for NGX R65.4

Upgrading to NGX R65.4 is supported from the following versions of Check Point management:

- NGX R65
- NGX R65 with HFA 01
- NGX R65 with HFA 02
- NGX R65 with HFA 30
- NGX R65 with HFA 30 with the Connectra NGX R66 plug-in
- NGX R65 with Messaging Security
- NGX R65 with the VPN-1 Power VSX NGX R65 Plug-in
- NGX R65 UTM-1
- NGX R65 on VMware ESX Server versions 3.0.2, 3.5 or 3i

To upgrade from earlier versions, first upgrade to NGX R65 and then upgrade to NGX R65.4.

Supported Upgrade Paths for NGX R65.2.100

Upgrades to the NGX R65.2.100 gateway are supported from the following versions of Check Point gateways:

- NGX R65
- NGX R65 with HFA 01
- NGX R65 with HFA 02

To upgrade from earlier versions, first upgrade to NGX R65 and then upgrade to NGX R65.2.100.

Supported Builds

The following builds are included in this release:

Component	Build Number	Verify Command and Output
NGX R65.2.100 Gateway	526	The output of **`fw ver`**: **`This is Check Point VPN-1(TM) & Firewall-1 (R) NGX R65.2.100 - Build 526`** The output of **`fw ver -k kernel`**: **`This is Check Point VPN-1(TM) & FireWall-1(R) NGX R65.2.100 - Build 526`** **`kernel: NGX R65.2.100 - Build 526`**
NGX R65.4 SmartConsole	620640131	Go to **Help > About Check Point SmartDashboard** a window opens that says: SmartDashboard NGX R65.4 (Build 620640131)
NGX R65 HFA 40 for VPN-1		See the VPN-1 NGX R65_HFA_40 Release Notes at http://supportcontent.checkpoint.com/file_download?ID=8684
NGX R65 HFA 40 for Provider-1		See the Provider-1 NGX R65_HFA_40 Release Notes at http://supportcontent.checkpoint.com/file_download?ID=8764

Installing NGX R65.4

NGX R65.4 must be installed on top of an NGX R65 SmartCenter server or Provider-1 MDS. If you do not already have NGX R65 installed:

- For a new installation see the *NGX R65 Internet Security Products Getting Started Guide* at http://supportcontent.checkpoint.com/file_download?ID=7249
- To upgrade to NGX R65, see the *NGX R65 Upgrade Guide* at http://supportcontent.checkpoint.com/file_download?ID=7259

Note - Check Point has found an issue with installing VPN-1 Power/UTM NGX R65.4 for Windows plug-ins on top of HFA 50 or above, on a Windows SmartCenter server. For more details, see sk42965.

In This Section

Included Components

When you install NGX R65.4, the following components are installed on your SmartCenter server or Provider-1 MDS:

Table 1 NGX R65.4 Components

Component	Description
NGX R65 HFA 40	Resolves previously existing issues and adds new Provider-1 and Endpoint Connect features and other enhancements.
Connectra NGX R66 management plug-in	Adds a secure remote access gateway with unified SSL VPN, IPSec VPN, and integrated intrusion prevention.
SmartProvisioning NGX R65.4 management plug-in	Adds the ability to manage thousands of remote gateways from a single SmartCenter server.
VPN-1 NGX R65.2.100 (VoIP) management plug-in	Enables all VoIP capabilities of the NGX R65.2.100 gateway.
VPN-1 NGX R65 with Messaging Security management plug-in	Adds comprehensive protection for an organization's email infrastructure.
VPN-1 Power VSX NGX R65 management plug-in	Uses software virtualization and utilization of VLAN technology to make VPN-1 scalable for up to 250 separate virtual systems on a single hardware platform.
SmartConsole NGX R65.4	Adds the ability to manage all of the included products.

To find further information on the various NGX R65.4 components, see "What's New" on page 4.

Installing NGX R65.4 on SecurePlatform

Important - The default idle timeout on SecurePlatform is ten minutes. After this time, the user is logged out. To ensure that installation is not interrupted by this timeout, before entering **expert** mode, type: **idle 60** in the command line.

Before installing this package on SecurePlatform, make sure to take a snapshot of the machine. This is necessary to avoid issues with removal of packages.

To install NGX R65.4 on a SecurePlatform SmartCenter server or Provider-1 MDS:

1. Create a snapshot. Run **snapshot** and go through the options of the CLI snapshot wizard.
2. Verify that there is enough free disk space to install NGX R65.4.
3. Download **Check_Point_NGX_R65_4.SPLAT.UTM-1.linux.tgz** from the Check Point Download Center,
   http://supportcenter.checkpoint.com/file_download?id=8796
4. Log in to the SmartCenter server or Provider-1 MDS using your administrator username and password.
5. Copy **Check_Point_NGX_R65_4.SPLAT.UTM-1.linux.tgz** to the **/var/log** directory on the SmartCenter server or Provider-1 MDS.
6. Open the .tgz package by running the command:
   tar -zxvf Check_Point_NGX_R65_4.SPLAT.UTM-1.linux.tgz
7. Run the extracted executable file using the command:
   ./UnixInstallScript
8. Follow the on-screen instructions to install all of the NGX R65.4 components and NGX R65 HFA 40. When the installation completes, it says **succeeded** for each component. Follow the prompt to reboot the machine.

Installing NGX R65.4 on Linux

To install NGX R65.4 on a Linux SmartCenter server or Provider-1 MDS:

1. Verify that there is enough free disk space to install NGX R65.4.
2. Download **Check_Point_NGX_R65_4.SPLAT.UTM-1.linux.tgz** from the Check Point Download Center
   http://supportcenter.checkpoint.com/file_download?id=8796
3. Log in to the SmartCenter server or Provider-1 MDS using your administrator username and password.
4. Open the .tgz package by running the command:
   tar -zxvf Check_Point_NGX_R65_4.SPLAT.UTM-1.linux.tgz
5. Run the extracted executable file using the command:
   ./UnixInstallScript
6. Follow the on-screen instructions to install all of the NGX R65.4 components and NGX R65 HFA 40. When the installation completes, it says **succeeded** for each component. Follow the prompt to reboot the machine.

Installing NGX R65.4 on Solaris

To install NGX R65.4 on a Solaris SmartCenter server or Provider-1 MDS:

1. Verify that there is enough free disk space to install NGX R65.4.
2. Download **Check_Point_NGX_R65_4.solaris2.tgz** from the Check Point Download Center, http://supportcenter.checkpoint.com/file_download?id=8798
3. Log in to the SmartCenter server or Provider-1 MDS using your administrator username and password.
4. Open the .tgz package by running the command:
   tar -zxvf Check_Point_NGX_R65_4.solaris2.tgz
5. Run the extracted executable file using the command:
   ./UnixInstallScript
6. Follow the on-screen instructions to install all of the NGX R65.4 components and NGX R65 HFA 40. When the installation completes, it says **succeeded** for each component. Follow the prompt to reboot the machine.

Installing NGX R65.4 on Windows

Important - Installation of R65.4 on top of a Windows SmartCenter with R65 HFA 50 or above is blocked. To enable installation of R65.4 on top of R65 HFA 50 or above see sk42965.

To install NGX R65.4 on a Windows SmartCenter server:

1. Verify that there is enough free disk space to install NGX R65.4.
2. Download **Check_Point_NGX_R65_4.windows.tgz** from the Check Point Download Center, http://supportcenter.checkpoint.com/file_download?id=8799
3. Extract the .tgz package.
4. Run the extracted executable file using the command:
   setup.bat
5. Follow the on-screen instructions to install all of the NGX R65.4 components and NGX R65 HFA 40. When the installation completes, it says **succeeded** for each component. Follow the prompt to reboot the machine.

Activating NGX R65.4 on Provider-1

If you want to use any of the NGX R65.4 plug-ins on a Provider-1 Customer, you must activate the plug-in on all of that Customer's Customer Management Add-ons (CMAs).

To activate plug-ins on a CMA:

1. In the MDG, right-click on a customer and select **Configure Customer**.
2. In the Customer Configuration window, select the **Plug-ins** tab.
3. Select each plug-in you want to activate on the CMA and click **Add**.
4. Click **OK** to confirm changes.

Installing the NGX R65.4 SmartConsole or MDG

The NGX R65.4 SmartConsole or Multi-Domain GUI (MDG) can be installed on a machine in addition to the NGX R65 SmartConsole or MDG. The SmartConsole that opens on your machine will be determined by the SmartCenter server or Provider-1 MDS to which you connect.

The SmartConsole package comes in .NET Framework 2.0, which is automatically installed.

To obtain the NGX R65.4 SmartConsole, do one of the following:

- Start an existing Check Point NGX R65 SmartConsole and connect to the SmartCenter server that has NGX R65.4 installed or to a CMA that has NGX R65.4 Plugin activated. In the window that opens, click **Update**. Follow the on-screen instructions to download and install the Check Point NGX R65.4 SmartConsole.

  Or

- Download and install the Check Point NGX R65.4 SmartConsole from http://supportcenter.checkpoint.com/file_download?id=8794.

To obtain the NGX R65.4 MDG:

- Download and install the Check Point NGX R65.4 MDG from http://supportcenter.checkpoint.com/file_download?id=8793.

Installing NGX R65.4 SmartConsole on Windows Vista with NGX R65 HFA01

00428392 If you have the NGX R65.4 SmartConsole installed on a Windows Vista machine and you want to install NGX R65 HFA01, you must:

1. Uninstall the NGX R65.4 SmartConsole.
2. Install NGX R65 HFA 01.
3. Reinstall the NGX R65.4 SmartConsole.

Installing the NGX R65.2.100 Gateway

When you install NGX R65.2.100, the following products will install on your machine:

- Check Point NGX R65.2.100 gateway
- Check Point NGX R65.2.100 Performance Pack (on SecurePlatform and Solaris)
- CPinfo

Installing the NGX R65.2.100 Gateway as a New Installation

The NGX R65.2.100 gateway is installed like a regular VPN-1 gateway. Below are brief instructions. For additional details, see the *NGX R65 Internet Security Products Getting Started Guide* at http://supportcontent.checkpoint.com/file_download?ID=7249. NGX R65.2.100 is not supported as a standalone installation. To manage the NGX R65.2.100 gateway, you will need an NGX R65.4 SmartCenter.

Installing the NGX R65.2.100 Gateway on SecurePlatform

Important - The default idle timeout on SecurePlatform is ten minutes. After this time, the user is logged out. To ensure that installation is not interrupted by this timeout, before entering **expert** mode, type: **`idle 60`** in the command line.

To install the NGX R65.2.100 gateway on SecurePlatform:

1. Download **`Check_Point_NGX_R65.2.100.splat_linux.iso`** from the Check Point Download Center, http://support.checkpoint.com.
2. Burn a CD with the **`.iso`** image and insert the CD into the CD drive.
3. Reboot.
4. Follow the on-screen instructions to install and configure SecurePlatform. At the end you will be told that the next stage will format your hard drive. Select **OK** and remove the CD.

   The machine restarts.
5. Log in using **admin** as your username and password.
6. When prompted, change the default username and password. Ensure that the new password contains more than six characters and has a combination of upper and lower case letters and numbers.
7. Run: `cpconfig`.

   A first-time configuration wizard opens, and displays a **Welcome** message.
8. Follow the on-screen instructions to automatically install the NGX R65.2.100 gateway and associated products.

Installing the NGX R65.2.100 Gateway on Linux

To install the NGX R65.2.100 gateway on a Linux platform:

1. Download **`Check_Point_NGX_R65.2.100.splat_linux.iso`** from the Check Point Download Center, http://support.checkpoint.com.

1. Mount the **`.iso`** file on the relevant subdirectory.

2. Run **./UnixInstallScript** from the mounted directory.

3. Follow the on-screen instructions to automatically install the NGX R65.2.100 gateway and associated products.

Installing the NGX R65.2.100 Gateway on Solaris

To install the NGX R65.2.100 gateway on a Solaris platform:

1. Download **Check_Point_NGX_R65.2.100.solaris.iso** from the Check Point Download Center, http://support.checkpoint.com.

2. Log in to the gateway machine using your administrator username and password.

3. Mount the **.iso** file on the relevant subdirectory.

4. Run **./UnixInstallScript** from the mounted directory.

5. Follow the on-screen instructions to automatically install the NGX R65.2.100 gateway and associated products.

Installing the NGX R65.2.100 Gateway on Nokia

You can install the NGX R65.2.100 Gateway on the Nokia platform using the CLI.

To install the NGX R65.2.100 gateway on Nokia using the CLI:

1. Download **Check_Point_NGX_R65.2.100.ipso.tgz** from the Check Point Download Center, http://support.checkpoint.com.

2. Copy the package to the gateway machine.

3. Run: `newpkg`

4. Select an installation method and the path name to the package you want to install.

5. Follow the on-screen instructions to automatically install the NGX R65.2.100 gateway and associated products. For a new installation, select **Install this as a new package**.

   The package installs.

6. When the installation is complete, reboot the machine.

7. Run: `cpconfig` to perform the initial configuration.

Upgrading a Gateway to NGX R65.2.100

Upgrades to NGX R65.2.100 are supported from NGX R65, NGX R65 with HFA 01, and NGX R65 with HFA 02. To upgrade from earlier versions, first upgrade to NGX R65 and then upgrade to NGX R65.2.100. For more information on upgrading to NGX R65, see the *NGX R65 Upgrade Guide* at http://supportcontent.checkpoint.com/file_download?ID=7259.

Upgrading on SecurePlatform

Important - The default idle timeout on SecurePlatform is ten minutes. After this time, the user is logged out. To ensure that upgrade is not interrupted by this timeout, before entering **expert** mode, type: **idle 60** in the command line.

Upgrading to NGX R65.2.100 on a SecurePlatform operating system requires updating both operating system and software products installed. The process described in this section upgrades all components (Operating System and software packages) in a single upgrade process. No further upgrades are required.

To upgrade a SecurePlatform gateway to NGX R65.2.100:

1. Download **Check_Point_NGX_R65.2.100.splat_linux.iso** from the Check Point Download Center, http://support.checkpoint.com.
2. Log in to the gateway machine using your administrator username and password.
3. Mount the **.iso** file.
4. Run: **patch add cd**.
5. Select the SecurePlatform upgrade package.
6. Enter y to accept the MD5 checksum calculation.
7. When prompted, create a backup image for automatic revert.

A Safe Upgrade will be performed. Safe Upgrade automatically takes a snapshot of the entire system so that the entire system (operating system and installed products) can be restored if something goes wrong during the Upgrade process (for example, hardware incompatibility). If the Upgrade process detects a malfunction, it automatically reverts to the Safe Upgrade image. When the Upgrade process is complete, upon reboot you are given the option to manually start the SecurePlatform operating system using the upgraded version image or using the image created prior to the Upgrade process.

8. After you complete the upgrade process, do the following:
   a. Using R65.4 SmartDashboard, log in to the NGX R65 SmartCenter server that

      controls the upgraded gateway.
   b. Open the gateway object properties window for the upgraded gateway and click **Get Version** to change the version to NGX R65.2.100.
   c. Install Policy on the upgraded gateway.

Upgrading on a Linux Platform

To upgrade a gateway on a Linux platform to NGX R65.2.100:

1. Download **Check_Point_NGX_R65.2.100.splat_linux.iso** from the Check Point Download Center, http://support.checkpoint.com.
2. Log in to the gateway machine using your administrator username and password.
3. Mount the **.iso** file.
4. Run: **./UnixInstallScript** from the mounted directory.
5. Select the Linux upgrade package.
6. Enter y to accept the MD5 checksum calculation.
7. After you complete the upgrade process, do the following:
   a. Using the NGX R65.4 SmartDashboard, log in to the NGX R65 SmartCenter server that

controls the upgraded gateway.

b. Open the gateway object properties window for the upgraded gateway and click **Get Version** to change the version to NGX R65.2.100.

c. Install Policy on the upgraded gateway.

Upgrading on a Solaris Platform

This section describes the upgrade process using the **Check_Point_NGX_R65.2.100.solaris.iso** file. It is recommended that you back up your current configuration before you perform an upgrade process.

To upgrade a gateway on a Solaris platform:

1. Download **Check_Point_NGX_R65.2.100.solaris.iso** from the Check Point Download Center, http://support.checkpoint.com.
2. Log in to the gateway machine using your administrator username and password.
3. Mount the **.iso** file on the relevant subdirectory.
4. From the mounted directory, run: **./UnixInstallScript**.

   A welcome message is displayed.
5. Follow the on-screen instructions to continue.
6. Select **upgrade** and type **n**.
7. Select a source for the upgrade utilities.
8. The pre-upgrade verification process runs automatically. View the results and follow any recommendations. Then, run the pre-upgrade verifier again. The following message is displayed: "The pre-Upgrade Verification was completed successfully. Your configuration is ready for upgrade".
9. Select **Upgrade installed products** or, to install additional products, select **Upgrade installed products and install new products**. You are prompted to select the products from a list. Type **n**.
10. Type **n** to validate the products to install.

    The products are upgraded. Wait until the successful message is displayed.
11. Type **e** to exit
12. Reboot.
13. After you complete the upgrade process, do the following:
    a. Using R65.4 SmartDashboard, log in to the NGX R65 SmartCenter server that controls the upgraded gateway.
    b. Open the gateway object properties window for the upgraded gateway and click **Get Version** to change the version to NGX R65.2.100.
    c. Install Policy on the upgraded gateway.

Upgrading on a Nokia Platform

You can upgrade to the NGX R65.2.100 Gateway on Nokia using the CLI.

To upgrade to the NGX R65.2.100 gateway on a Nokia platform using the CLI:

1. Download **Check_Point_NGX_R65.2.100.ipso.tgz** from the Check Point Download Center, http://support.checkpoint.com, and copy the package to the gateway machine.

2. Run: `newpkg`

3. Select an installation method and the pathname to the package you want to install.

4. Follow the on-screen instructions to automatically install the NGX R65.2.100 gateway and associated products. Select **Upgrade from an old package**.

5. Select the package to upgrade from.

   The upgrade installs.

6. When the installation is complete, reboot the machine.

Updating Customized INSPECT Files

Updating Customized VPN-1 INSPECT Files

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

For environments using only original Check Point INSPECT files, the updated INSPECT files are installed automatically: the previous *.def files are replaced with the new ones.

If even one INSPECT file was manually customized, none of the new INSPECT files replace the previous ones. The following message appears:

```
The updated inspect files were NOT installed due to signature mismatches
or errors.
To complete the installation replace the inspect files.
Inspect files that were not replaced may lead to unexpected behavior!
To force update of the inspect files run: update_inspect_files -f
```

If the files were not replaced (signature mismatch message displayed), you must force the INSPECT files to be updated.

Important - You **must** replace the previous files. If you do not, unexpected behavior may result.

To force INSPECT files to be updated:

1. Make note of the customized INSPECT files.

   To see which INSPECT were not replaced, see the log:

   - **Unix - /opt/CPInstLog/update_inspect_files_40.log**
   - **Windows - C:\Program Files\CheckPoint\CPInstLog\update_inspect_files_40.log**

   If the files were not replaced because of customizations, the log shows:
   <filename>.def was changed by user, signature didn't match!

2. Open the files that are listed in **update_inspect_files_40.log** and note the customized lines.

3. Run: **update_inspect_files -f**

   The log will show: <filename>.def was replaced.

4. Merge the customized content that you noted in step 2 into the new INSPECT file(s).

5. Re-install the Security Policy to enable the new INSPECT files.

Updating Customized Provider-1 INSPECT Files

The MDS contains several INSPECT (*.def) files, typically located in the **$FWDIR/lib** directory. The MDS may include one or more updated INSPECT files, which replace the files currently in use.

The installation routine automatically updates INSPECT files for all CMAs **only** if **all** INSPECT files are unmodified for that CMA.

If all CMAs were updated successfully (none had modified INSPECT files), the following message appears:

```
The updated Inspect files have been installed successfully.
To complete the installation, please re-install the Security Policy on all
your gateway for the CMAs.
```

If any INSPECT files in a CMA were previously modified, no INSPECT files are updated for this CMA. The following message appears:

```
Signature mismatches were found for some CMAs. This indicates that manual
change were made to the Inspect files. These affected CMAs are listed in:
$MSDIR/tmp/manually_modified_cmas.txt
Please note that the specified Inspect files were NOT updated for these
CMAs. If you wish to update them, execute the following command:
hf_propagate o --override_manual
```

If the files were not replaced (signature mismatch message displayed), you must force the INSPECT files to be updated.

Important - You **must** replace the previous files. If you do not, unexpected behavior may result.

To force INSPECT files to be updated:

1. On the MDS, open **$MSDIR/tmp/manually_modified_cmas.txt** and note the CMAs that have modified INSPECT files.

   For each of these CMAs, do the following.

2. Go to the CMA: **mdsenv** <CMA_Name>

3. On the CMA, open **$FWDIR/lib/update_inspect_files_40.log** and note the INSPECT files that were modified.

   If the files were not replaced because of customizations, the log shows:
   <filename>`.def was changed by user, signature didn’t match!`

4. Open the files that are listed in **update_inspect_files_40.log** and note the customized lines.

5. Run: **hf_propagate o --override_manual**

6. Merge the customized content that you noted in step 4 into the new INSPECT file(s).

7. Re-install the Security Policy to enable the new INSPECT files.

Uninstallation

While NGX R65.4 is installed along with HFA 40, they are uninstalled separately.

It is possible to either uninstall both NGX R65.4 and HFA 40 and revert to NGX R65, or to uninstall only NGX R65.4, and revert to NGX R65 with HFA 40.

If you want to uninstall both NGX R65.4 and HFA 40, you must run the uninstall command twice.

Before Uninstalling NGX R65.4

If you managed an NGX R65.2.100 gateway, you must perform the following steps before uninstalling NGX R65.4.

Before uninstalling NGX R65.4, from the SmartDashboard VoIP tab:

1. *Delete* all Version NGX R65.2.100 gateways (from the **Enforcing Gateways** page).
2. *Delete* all VoIP servers (from the **VoIP Entities and Topology > VoIP Servers** page).
3. *Remove* all VoIP endpoints (from the **VoIP Entities and Topology > VoIP Endpoints** page).
4. *Delete* the External Trusted CAs for VoIP as follows:
   a. In SmartDashboard, go to the **Advanced > External Trusted CAs** page of the VoIP tab.
   b. Select an External Trusted CA where VoIP appear in the **Purpose List**.
   c. Click **Delete**.

Uninstalling NGX R65.4 On SecurePlatform, Linux, and Solaris

To uninstall both NGX R65.4 and HFA 40, and revert to NGX R65, perform the following steps on the SmartCenter server:

1. To uninstall NGX R65.4, run the following command from the **/opt/CPUninstall/R65.4** directory: **UnixInstallScript -u**
2. To uninstall HFA 40, run the following command from the **/opt/CPUninstall/R65_HFA_40** directory: **UnixInstallScript -u**

To uninstall only NGX R65.4, and revert to NGX R65 with HFA 40, perform the following steps on the SmartCenter server:

1. To uninstall NGX R65.4, run the following command from the **/opt/CPUninstall/R65.4** directory: **UnixInstallScript -u**
2. Start the Check Point processes. Run: **cpstart**

Uninstalling NGX R65.4 On Windows

To uninstall both NGX R65.4 and HFA 40, and revert to NGX R65, perform the following steps on the SmartCenter server:

1. To uninstall NGX R65.4, run the following command from the **Program Files\CheckPoint\CPUninstall\R65.4** folder: **Setup.bat -u**
2. To uninstall HFA 40, run the following command from the **Program Files\CheckPoint\CPUninstall\R65_HFA_40** folder: **Setup.bat -u**

To uninstall only NGX R65.4, and revert to NGX R65 with HFA 40, perform the following steps on the SmartCenter server:

1. To uninstall NGX R65.4, run the following command from the **Program Files\CheckPoint\CPUninstall\R65.4** folder:
   Setup.bat -u

2. Start the Check Point processes. From the command line, run: **cpstart**

Newly Supported Features in NGX R65.2.100

NGX R65.2.100 has advanced VoIP connectivity, security and management capabilities in addition to all features supported in earlier VPN-1 versions.

Session Border Controller

NGX R65.2.100 can be configured to act as a Session Border Controller (SBC).

An essential requirement for deploying VoIP infrastructures is to allow VoIP connectivity across NAT devices and firewalls, together with strong security and Quality of Service.

The SBC makes it possible to deliver VoIP services across network boundaries, without NAT and firewall devices limiting that capability, and without changing the established IP infrastructure.

The firewall component of NGX R65.2.100 acts as a Back-to-Back SIP user agent (B2BUA), and handles all signaling and media traffic from the enterprise, branch offices and home users.

The issue of NAT traversal is a major problem for the widespread deployment of VoIP. Far-end NAT traversal functionality enables secure VoIP communication even though it does not control the NAT devices at the customer premises, and performs the modifications to the incoming and outgoing signaling and media packets from a centralized location.

Quality of Service (QoS) for gateways and VoIP servers can be monitored and controlled. QoS includes call admission control and traffic bandwidth shaping.

Security Features

- Many new VoIP-specific SmartDefense protections are available.
- Sophisticated inspection of VoIP signaling and media protocols protects voice and video networks from potential threats. Deep protocol inspection using Check Point Application Intelligence™ technologies ensures RFC compliance of the traffic.
- Denial of Service (DoS) protections include rate-limiting of traffic to SIP servers and internal VoIP networks. Limiting the rate of traffic is one of the techniques that can help protect against denial of service attacks. Rate limiting is accomplished by configuring traffic thresholds. Traffic that exceeds the thresholds is blocked.
- Prevention of unsupported message types (methods) from reaching SIP and MGCP servers. Service levels are guaranteed by stopping messages at the gateway.
- Highly granular configuration of connectivity and security per phone-network (whether internal or external) or server type (proxy, registrar or presence) makes it possible to fine-tune security settings to the needs of the organization.
- Topology awareness allows NGX R65.2.100 to optimally secure each network element. It is also possible to define the phones that each server controls (media access control).
- Information disclosure protections prevent hackers from tailoring attacks that exploit vulnerabilities in vendor equipment. This is achieved by removing vendor-specific fingerprint information from SIP packets.
- New RTP/RTCP RFC security enforcements are included and accelerated with SecureXL. Management Enhancements
- Quick setup for VoIP connectivity is made possible through simple and intuitive installation and configuration. The administrator need only define the VoIP network, and default protections are automatically activated.
- A new SmartDashboard GUI tab is available for managing VoIP.

- Summary pages are available in the SmartDashboard VoIP tab, showing the configuration of the VoIP system at a glance:
  - **SmartDefense VoIP Protections** overview, showing the settings for each SmartDefense VoIP protection.
  - **VoIP Application Policy** overview, showing the settings for each VoIP Application Policy option.
  - **Entity Protection Summary** showing the protection status of a VoIP entity when it is protected by a specific gateway.

Full Stateful Inspection of TLS-Secured SIP Traffic

TLS is increasingly being used as the standard way of protecting SIP signaling from eavesdropping and tampering. TLS can be used to provide encryption and/or authentication of the SIP signaling messages. NGX R65.2.100 gateways are able to inspect and modify SIP signaling secured by TLS, thereby providing full security and connectivity for TLS-secured SIP traffic.

- **Inspection of TLS-Encrypted SIP Traffic**—In many VoIP deployments that secure SIP with TLS, malicious endpoints may nevertheless be able to establish a TLS connections with the SIP server. The reason is that either the server does not require the endpoint to present a trusted client certificate, or because the attacker can easily obtain such a certificate. In those cases, DoS attacks against the SIP server could be carried out over the TLS connection. By having the ability to inspect SIP traffic secured by TLS, even if the traffic is encrypted, the gateway can protect the SIP server from such attacks.
- **Dynamic Pinholing of TLS-Encrypted SIP Traffic**—By inspecting encrypted SIP signaling, the gateway can dynamically open pinholes for data (e.g., voice, video), eliminating the need to statically open a large range of high UDP ports in the firewall.
- **NAT for TLS-Encrypted SIP Traffic**—Most SIP signaling messages contain IP addresses and ports of VoIP entities. Therefore, when NAT is applied, SIP messages are usually modified by the NAT device. By being able to securely modify SIP messages which are secured by TLS, the gateway can apply NAT to SIP messages over TLS.

Troubleshooting

- A monitor-only mode inspects traffic without actually blocking it. This is useful for observing traffic during the deployment process in order to create appropriate definitions, and also for debugging connectivity problems. Monitor-only can be configured globally or per protection.
- New enhanced logs contain more details about the VoIP packets inspected by the firewall. These logs provide better troubleshooting capabilities.

Vendor Interoperability

Universal Alcatel R6.2

NGX R65.2.100 can be placed anywhere in an Alcatel VoIP environment. This is because dynamic pin-holing can be performed for Alcatel systems, which is made possible because two new flavors of the Universal Alcatel (UA) protocol are supported. The supported protocols are:

- UA/NOE, which handles signaling between the IP phone set and the Call Server.
- IPlink, which handles signaling between the media gateway (or voice mail system) and the Call Server.

Cisco CallManager

NGX R65.2.100 and gateway versions enable secure connectivity for CallManager 6.1 and lower versions. NGX R65.2.100 supports NAT for the endpoints and for the CallManager server for the SIP protocol.

Avaya SES and ACM

NGX R65.2.100 enables secure connectivity for ACM and SES Release 5.0 for SIP and H.323 protocols.

Known Limitations and Clarifications

In This Section

NGX R65.4 SmartConsole and MDG Limitations and Clarifications

- The NGX R65.4 SmartConsole does not support the Connectra Central Management plug-in for Connectra NGX R62.
- **00424967** Installation of Connectra NGX R62 Central Management plug-in is not supported on an NGX R65 SmartCenter server or MDS with certain other plug-ins. For a list of plug-in compatibility, see

  http://www.checkpoint.com/ngx/upgrade/plugin/index.html

NGX R65.2.100 Limitations and Clarifications

In This Section

Installation and Upgrade

- The NGX R65.2.100 gateway can be installed on appliances such us UTM-1 and Power-1, but only as an open platform without any appliance features (such as interface naming).
- **00366494** Windows limits the length of the "path" environment variable to 1 Kbytes in Windows 2000 and up to 2 Kbytes in Windows 2003/XP, after the addition of a special patch. Installing version NGX R65 may fill the "path" variable, depending on which Check Point products are installed. The result of this is that the path of the VoIP plug-is not recorded in the "path" variable, thereby preventing the plug-in from installing properly. To prevent this problem, ensure the "path" is not full before installing the VoIP plug-in. Do this by deleting unnecessary paths from the "path" variable, and by not installing Check Point products that are not required.

ClusterXL Gateway Clusters

- **00338423** Incoming connections are lost if a failover occurs on a ClusterXL cluster member gateway with all of the following:
  - VoIP is SIP over TCP.
  - SIP proxy is in the external network.
  - Gateway is configured as Hide NAT.
  - Gateway is running SecureXL.
- **00422950** In a ClusterXL gateway cluster, failover of SIP over TLS connections is not supported when the inspection is done by the sip_tls_with_server_certificate service.

SmartCenter Server

- **00373946** When using a URI resource, do not configure a URI Match Specification type: File. Use the other URI match specification types instead (Wildcards or UFP). This is because the imported file does not arrive at the gateway when the policy is installed, and so relevant traffic does not match a service with this type of URI resource.

Provider-1

- **00354835** If the NGX R65.2.100 VoIP management plug-in is installed on an MDS, then CMAs that are subscribed to Global SmartDefense in Override mode, and have the NGX R65.2.100 management plug-in activated on them, cannot be assigned a Global Policy. Subscription to Global SmartDefense in Override mode is still supported for CMAs on which the NGX R65.2.100 management plug-in is not activated. In addition, NGX R65.2.100 management plug-in configuration is not supported via the Global Policy.
- **00427078** If you uninstall HFA 40 from an MDS, you will not be able to restore a database revision version in the global database from a revision created when HFA 40 was still installed.

SmartConsole Applications

- **00379251** When creating or editing a version NGX R65.2.100 gateway in the Advanced > VoIP page of SmartDashboard, it is not possible to delete the signaling host defined in the “Translate source IP for signaling channel to” section. To delete the host, use the Network Objects tree.
- **00427539** In SmartDefense VoIP protections for which a maximum value is configured (for example, the protection SIP Protocol Anomaly > Max allowed Call-ID length), SmartDashboard verifies and enforces an absolute maximum value by means of a pop-up warning. If an exception is configured with a higher value than the absolute maximum value allowed for the protection, the exception is enforced with the absolute maximum value that is allowed for the protection, not the higher value that is configured as the exception. In addition a warning is generated when the policy is installed.

Logging

- **00438748** When monitor only is used for VoIP traffic (as configured in SmartDefense, under VoIP > Protections for R65.2.100 > Monitor-only for protections, or in the VoIP tab under Enforcing Gateways for VoIP application policy), when a monitor log is generated for a VoIP Security event or for Policy events, an additional "DROP" log is created on the corresponding rule. This "DROP" log can be ignored. It is only generated for the first packet of a connection which is logged as a violation event.

Media Admission Control

- **00381034** H.323 Media Admission Control logs appear in SmartView Tracker in the Security Events query and not, as for other VoIP protocols, in the Policy Events query.
- **00405549** In several scenarios, when a SIP phone places a call on hold, the Media Admission Control drops the packet and the call is lost. This happens if the source IP address and the IP address in the SDP body are not the same (they belong to different phones), and neither contains the server IP address. This behavior has been observed when an Avaya phone places a call on hold during a conference. To allow this behavior, deactivate the Media Admission Control checks on the specific server (in the VoIP tab, under VoIP Entities and Topology > Media Admission Control.)

Far End NAT Traversal

- **00352665** Far End NAT Traversal is not supported within an IPSEC VPN. Note however that Far End NAT Traversal is not required within VPNs between Check Point VPN-1 Power/UTM gateways, because they are VoIP-aware.
- **00373020** Far End NAT is not supported when the extension name is an IP address.
- **00403370** Far Far End NAT Traversal only works if the SIP packets contain the following headers (defined as mandatory by RFC 3261): Call-ID, CSeq, From, To, and at least one of Via or Contact. Therefore, when using Far End NAT Traversal, the SmartDefense protection SIP > SIP Protocol Anomaly > General Header Security > Enforce mandatory fields existence is always enforced, even if it is configured as Inactive. Examine the SmartDefense logs to locate packets dropped by this protection.
- **00353751** The Far End NAT Traversal signaling IP address (configured in the Advanced > VoIP page of the Check Point gateway) must be different from any of the gateway IP addresses.
- **00375594** Far End NAT Traversal does not support registration of users at the firewall gateway IP address. Far End NAT Traversal users must register at the signaling IP address (configured in the Advanced VoIP page of the Check Point gateway).
- **00406267** When establishing a SIP call between a user whose address is translated using Far End NAT Traversal (FEN), and a non-FEN user, Call Admission Control (configured in the SmartDashboard VoIP tab, in the QoS > Per Gateway page) is not supported.
- **00355842** In SIP traffic that uses Far End NAT Traversal, the 'Replaces' header field is not always properly translated. This can cause connectivity issues.
- **00367208** In SmartView Tracker, the SIP connection logs for Far End NAT Traversal traffic is logged differently for registration sessions and call sessions. Registration session logs are associated with the real connection, which means that the connection is between the user IP address and the signaling IP address, or between SIP server IP and the signaling IP. Call session log are associated with the signaling virtual connection, which means that the connection is between the user IP and SIP server IP.
- **00375617** Call session and Registration logs for Far End NAT Traversal connections over TCP are sometimes logged with the sip_any-tcp-ipv6 service instead of the sip-tcp service
- **00427538** In Far End NAT Traversal, when two users are behind the same NAT device and the proxy acts as a Back-to-back user agent (B2BUA), the RTP media is not directed between the two users, but is transferred via the gateway.
- **00422935** Far End NAT Traversal is not supported for SIP over TLS.
- **00368273** The NGX R65.2.100 gateway does not reply to ping requests to the Far End NAT signaling IP. It can only handle SIP traffic.
- **00429744** When establishing a SIP call between a user whose address is translated using Far End NAT Traversal (FEN), and a non-FEN user, NAT is not supported on the non-FEN user's address (neither static nor hide).

RTP/RTCP

- **00355904** Some VoIP products change the Synchronization Source (SSRC) field in RTP and RTCP media packets during the session. This behavior has been observed in Avaya H.323 and SIP equipment. To allow this behavior, deactivate the Enforce Single Synchronization Source (SSRC) protections for such objects. These protections are located in the SmartDefense tab > **Application Intelligence > VoIP > Protections for R65.2.100 > RTP and RTCP**.

SIP

- **00376741** In site to site VPN environment with a star community topology, SIP communication is only supported if the SIP proxy is behind the central gateway. When the SIP proxy is behind one of the satellites. SIP communication between the satellite gateways is not supported
- **00405778** In a Security Rule that allow SIP over UDP with Hide NAT, the destination must not include the Hide NAT IP address.
- **00411760** The “Hide NAT changes source port for VoIP traffic over UDP” in the VoIP server works only if the port in the Contact field of the REGISTER message sent by the phone behind Hide NAT is the same as the source port of the message.

  In some SIP clients, it is possible to configure whether the source port is equivalent to the client port. For example in Cisco phones, setting NAT Enabled to "Yes" makes the source port the same as the client port. In Cisco phone7970, this is configured from Settings -> Device Configuration -> SIP Configuration -> SIP General Configuration -> NAT Enabled.
- **00429873** When the SmartDashboard option "Hide NAT changes source port for VoIP traffic over UDP" is enabled on the SIP server, if the NAT configuration is changed on the endpoints that register to the SIP server, then after a policy is installed, new connections from the endpoints can be made only after:

  1. Connections from these endpoints have expired from the connections table on the Check Point gateway, and
  2. The registration of these endpoints have expired from the SIP server (proxy).

  In general, the connection expires after the period that the endpoint has registered in the proxy.

  Alternatively, solve the problem by restarting the Check Point gateway and the endpoints.
- **00368889** An empty NAT log is generated in SmartView Tracker when SIP over TCP with Hide NAT is used, and the relevant rule is logged. This empty log is generated in addition to the VoIP log, which has all relevant details.
- **00409894** When working with Cisco Call Manager v.5 and higher, VoIP call session logs sometimes appear with a string instead of the real user. This occurs because Cisco Call Manager sometimes sends a unique session string in From or To headers, instead of a real user.
- **00413805** In VoIP logs, when the connection is over UDP, the source port is sometimes incorrectly shown as UDP/10000 or higher.
- **00370661** In some VoIP systems it is possible to define several aliases for the same username. It is recommended, where possible, to avoid defining aliases. For example, it is possible to define in the VoIP server "John" as a username and "1234" as its alias. With this configuration, the server may write "1234" instead of "John" in the SIP messages. Since the IP phones register with the name at the server, the firewall is not aware of the association between the alias and the name. This behavior may therefore cause some of firewall features, such as NAT and logging to work incorrectly.
- **00350509** In a SIP packet Via header field, having several URIs is not supported. Only multiple Via header fields are supported.

- **00349512** In a SIP packet Contact header field, having several URIs is not supported. Only multiple Contact header fields are supported.
- **00440435** The SIP services sip_dynamic_ports and sip_tls_with_server_certificate cannot be used on the same NGX R65.2.100 gateway. Using both services for the same gateway causes connectivity problems for SIP traffic over TLS which is inspected by the sip_tls_with_server_certificate service.

H.323

- **00379989** In H.323 deployments where the Gatekeeper is connected to a gateway DMZ interface, multiple logs can appear for the same event. For example, when the Gatekeeper is in a DMZ, two logs are created for a single call session. This is because the firewall sees the packets twice: once from the caller endpoint to the Gatekeeper, and second time from the Gatekeeper to the callee endpoint.
- **00381115** H.323 Avaya logging: Two of the call session log fields in SmartView Tracker are not updated: The State field (shown permanently as OPEN) and the Duration field.
- **00405648** Cluster failover is not supported for H.323 Avaya equipment unless the phones support gratuitous ARP.
- **00410142** The endpoint normally initiates the H.323 (H.225) TCP connection to the Gatekeeper or server. In scenarios where the Gatekeeper initiates the TCP connection to the endpoint, set the global parameter "h323_gk_init_tcp_conn", by running the command "fw ctl set int h323_gk_init_tcp_conn 1". Note that when running Avaya Communication Manager (ACM), the TTS (Time to service) feature may be enabled by default. When TTS is enabled, the Gatekeeper initiates the TCP connection to the endpoint, and so the "h323_gk_init_tcp_conn" parameter must be set.
- **00421931** If H.323 TCP keepalive messages are sent for a period of an hour or more, the call may be terminated. To prevent this problem, increase the timeout of the relevant H.323 service in SmartDashboard to the same timeout as the keepalive message.

SCCP

- **00405890** Video calls over SCCP (Skinny) are not supported.

Unicast Routing

- **00380629** When running the drouter start or drouter stop command, error messages are printed to the console. These messages can be ignored.

SmartProvisioning NGX R65.4 Limitations and Clarifications

- SmartProvisioning does not support SmartPortal or the Eventia Suite.
- **00379226** Gateway provisioning is supported only on SecurePlatform NGX R65 and later, or VPN-1 UTM Edge with Firmware 7.5 and later.
- **00421659** Installing NGX R65 HFA 30 or SmartProvisioning NGX R65.4 takes time. If the installation process takes longer than the idle time of the machine (default 10 minutes), the shell of the machine exits during the installation and the installation is not successful.

  To solve this problem, before running the installation application, increase the idle time of the SecurePlatform shell to 60 minutes using the command `idle <number of minutes>`, so that the installation application will not exit in the middle of the installation. After the installation is complete and the machine is rebooted, return the idle time to it's original value.
- **00409264** All LSMcli `Convert` commands reset the device's provisioning settings.

- **00411840** The Open SSH feature supports only SSH clients (such as Putty) that can be run from a command line with the following format: <ssh_name.exe> <IP>
- **00417180** If two instances of SmartProvisioning are open, and an object is open for editing in one instance while being deleted in the other, the editing instance may shut down.
- **00404926** SmartProvisioning and Endpoint Security server can coexist on SmartCenter or Provider-1 only if Endpoint Security server is installed before SmartProvisioning.
- **00378021** The VPN Domain of a SmartLSM gateway will include only the IP address used for the SIC between the SmartLSM gateway and the SmartCenter server or CMA; it appears in the Last Known IP column of gateway lists. Other external interfaces that are defined in the Interfaces of the gateway are not included in the VPN Domain.
- **00416624** The Internet Explorer browser must be installed on the SmartConsole machine to enable the VPN-1 UTM Edge Portal to be opened from within SmartProvisioning (right-click an Edge device and select **Launch VPN-1 UTM Edge Portal**).
- **00421620** Some gateway configurations (RADIUS, certain Port settings, and Bridge Interface) are not supported in T1.0 VPN-1 UTM Edge; if configured on a T1.0 device, no settings will be pushed to the device as long as the unsupported configuration remains. There is no notification.
- **00422369** If a VPN-1 UTM Edge device has a local configuration for a DMZ port to be a WAN2 interface, and interfaces are managed centrally from VPN-1 Power/UTM, provisioning settings will not be enforced on the device. To make sure central management through VPN-1 Power/UTM is performed as expected, change the DMZ port to Internet network in SmartProvisioning.
- **00410554** PPTP, PPOE, and ISDN interfaces are not supported on SecurePlatform NGX R65.
- **00370494** Windows limits the length of the PATH environment variable to 1 KB in Windows 2000 and up to 2Kbytes in Windows 2003/XP, after the addition of a patch (`Userenv.dll`; refer to **Microsoft Help and Support** site, Article **906469**). Installing version NGX R65 may fill PATH, resulting in the path of the SmartProvisioning plug-in to not be recorded, and preventing the plug-in from installing properly.

  To prevent this issue, delete duplicate or unnecessary paths from PATH and do not install non-required products.

  If you cannot prevent the issue, fix it with the following procedure:

  a. Change PATH so that `C:\Program Files\CheckPoint\PIprov\R65\lib` is included.
  b. In a command window, type: `cpwd_admin stop -name FWM`
  c. Run: `C:\Windows\fw1\R65\fw1\bin\fwm`
     (If using non-default installation, change the path of this command.)
- **00419680** If, after running the SmartProvisioning wizard, there is no indication that the "Get Actual Settings" action was run (in the actions table no "Get Actual Settings" line was added), wait until all distributed actions are finished, and then run **Get Actual Settings** manually on each gateway by right-clicking.
- **00419547** When managing the routing on a VPN-1 Edge device, if you want to use the routing data defined on the Profile page, you must select the 'Overriding profile settings' option of 'Denied' because the "use profile settings" options is not available from the Device page.

VPN-1 UTM Edge Limitation

- **00437995** When first connecting VPN-1 UTM Edge to the SmartCenter, Anti Spam cannot be turned on for centrally managed VPN-1 UTM Edge devices, ignoring the SmartDashboard configuration. As a workaround, upgrade to VPN-1 UTM Edge firmware 8.0.38 or above; or:

  1. In SmartDashboard double click a VPN-1 UTM Edge object.
  2. Clear the Anti Spam checkbox.

3. Install the policy on that VPN-1 UTM Edge object.
4. Open the VPN-1 UTM Edge object again and now check the Anti Spam checkbox.
5. Install the policy on the VPN-1 UTM Edge object again.

After implementing a workaround, Messaging Security will work on centrally managed VPN-1 UTM Edge, as configured in SmartDashboard.

Resolved Limitation for NGX R65.2.100

How VPN-1 Gateways Handle DiffServ Traffic

00368273

When VPN-1 gateway acts as a proxy for a TCP connection between a client and server, the connection is split into two separate TCP connections: a connection between the client and the VPN-1 gateway and a connection between the VPN-1 gateway and the server.

The VPN-1 gateway, when acting as a proxy for a connection, preserves the QoS tagging between the two separate connections. To achieve that, the TOS tag (if it exists) used by the client which initiates the connection, is used by the VPN-1 gateway for all traffic that the gateway generates both for the client and for the server connections.

In previous versions, the TOS tag was used only for the client side of the connection.

Note: When the SmartDefense TCP > SYN Attack Configuration protection is enabled and detection of SYN attack has triggered Active Defense mode, the TOS tagging is not applied to the TCP 3-way-handshake between the VPN-1 gateway and the client/server.

Related Documentation

Table 2 and Table 3 contain links and brief descriptions of documentation that is related to NGX R65.4, NGX R65.2.100.

Table 2 Documentation Specific to the NGX R65.4 Release, Related HFA, and Plug-ins

Title	Description
VPN-1 NGX R65 HFA 40 Release Notes	Contains the details of VPN-1 NGX R65 HFA_40 (Hotfix Accumulator) including improvements and issues resolved.
Provider-1 NGX R65 HFA 40 Release Notes	Contains the details of Provider-1 NGX R65 HFA_40 (Hotfix Accumulator) including improvements and issues resolved.
NGX R65.2.100 Administration Guide	Describes how to administer VPN-1 Power/UTM NGX R65.2.100, a VoIP aware Check Point gateway offering comprehensive security for Enterprises, Telecom Networks, and Service Provider VoIP environments.
Provider-1/SiteManager-1 Administration Guide NGX R65.4	Explains the Provider-1/SiteManager-1 security management solution. This guide provides details about a three-tier, multi-policy management architecture and a host of Network Operating Center oriented features that automate time-consuming repetitive tasks common in Network Operating Center environments.
SmartProvisioning Administration Guide NGX R65.4	Explains how to manage and use the SmartProvisioning management plug-in to manage large-scale deployments of Check Point gateways from a single SmartCenter server, with features to define, manage, and provision gateways.
Connectra Administration Guide NGX R66	Explains how to manage and use Check Point Connectra, a complete Web Security gateway that provides SSL VPN access and integrated endpoint and application security in a single unified solution.
NGX R65 with Messaging Security Guide	Explains how to manage and use Messaging Security, a comprehensive solution for protecting a company's messaging infrastructure.
VPN-1 Power VSX Administration Guide NGX R65	Explains how to manage and use VPN-1 Power VSX, a virtualized security gateway. VPN-1 Power VSX allows you to manage service providers and enterprises with virtualized networks to create up to 250 virtual security systems-including firewall, VPN, and intrusion prevention-on a single hardware platform.
Endpoint Connect Administration Guide NGX R65.	Describes how to configure a gateway to accept the Endpoint Connect client for lightweight remote access. Providing seamless, secure (IPSec) VPN connectivity to corporate resources, the client works transparently with VPN-1 and Connectra gateways.
Endpoint Connect User Guide NGX R66 HFA 01	Describes how to use the Endpoint Connect client for lightweight remote access. Providing seamless, secure (IPSec) VPN connectivity to corporate resources, the client works transparently with VPN-1 and Connectra gateways.

Table 3 Relevant NGX R65 Documentation

Title	Description
Internet Security Product Suite Getting Started Guide NGX R65	Contains an overview of NGX R65 and step by step product installation and upgrade procedures. This document also provides information about What's New, Licenses, Minimum hardware and software requirements, etc.
High End Security Products Getting Started Guide NGX R65	Contains an overview of NGX R65 High End Security Applications, including Provider-1 and VPN-1 Power VSX and their installation procedures.
NGX R65 Upgrade Guide	Explains all available upgrade paths for Check Point products from VPN-1/FireWall-1 NG forward. This guide is specifically geared towards upgrading to NGX R65.

Title	Description
SmartCenter Administration Guide NGX R65	Explains SmartCenter Management solutions. This guide provides solutions for control over configuring, managing, and monitoring security deployments at the perimeter, inside the network, at all user endpoints.
Firewall and SmartDefense Administration Guide NGX R65	Describes how to control and secure network access; establish network connectivity; use SmartDefense to protect against network and application level attacks; use Web Intelligence to protect web servers and applications; the integrated web security capabilities; use Content Vectoring Protocol (CVP) applications for anti-virus protection, and URL Filtering (UFP) applications for limiting access to web sites; secure VoIP traffic.
Virtual Private Networks Administration Guide NGX R65	This guide describes the basic components of a VPN and provides the background for the technology that comprises the VPN infrastructure.
Eventia Reporter Administration Guide NGX R65	Explains how to monitor and audit traffic, and generate detailed or summarized reports in the format of your choice (list, vertical bar, pie chart etc.) for all events logged by Check Point VPN-1 Power, SecureClient and SmartDefense.
SecurePlatform™/ SecurePlatform Pro Administration Guide NGX R65	Explains how to install and configure SecurePlatform. This guide will also teach you how to manage your SecurePlatform machine and explains Dynamic Routing (Unicast and Multicast) protocols.

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