NGX R65 with Messaging Security

In This Document

Introduction: page 1
What's New: page 2
Installing NGX R65 with Messaging Security: page 3
Upgrading to NGX R65 with Messaging Security: page 6
Messaging Security: page 11
UTM-1 Clustering: page 26
Tracking and Reporting Options: page 39
Uninstalling NGX with Messaging Security: page 41
Uninstalling the Connectra Central Management Plug-in: page 43
Known Limitations: page 44
Documentation Feedback: page 51

Introduction

Thank you for updating your Check Point products with NGX R65 with Messaging Security. NGX with Messaging Security is a recommended update that contains improvements for VPN-1 UTM. Read this document carefully prior to installation. We recommend that you refer to the appropriate Check Point user documentation and release notes, which contain hardware requirements, software requirements and version recommendations.

The most updated version of this document is available at:

http://support.checkpoint.com
What’s New

NGX R65 with Messaging Security offers:

- Anti Spam capabilities for NGX R65 SecurePlatform.
- Anti Spam plus UTM-1 clustering (gateway and SmartCenter server) on UTM-1 appliances.
- Provider-1/SiteManager-1 support for messaging security.
- Additional content inspection reporting options in Eventia Reporter.
- Zero Hour Malware protection.
- Mail Anti Virus

Anti Spam

The relentless and unprecedented growth in unwanted email now poses an unexpected security threat to the network. As the amount of resources (disk space, network bandwidth, CPU) devoted to handling unsolicited emails increases from year to year, employees waste more and more time sorting through unsolicited bulk email commonly known as spam.

NGX R65 with Messaging Security provides network administrators with an easy and central way to eliminate most of the spam reaching their networks.

NGX R65 with Messaging Security provides:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content based Anti Spam</td>
<td>The core of the Anti Spam functionality is the content based classification engine.</td>
</tr>
<tr>
<td>IP reputation</td>
<td>Using an IP reputation service, most of the incoming spam is blocked at connect time.</td>
</tr>
<tr>
<td>Customized disclaimer notice</td>
<td>Suspected spam is labelled as such, either in the header or subject of the email, so that employees do not waste their time reading it.</td>
</tr>
<tr>
<td>Directional scans</td>
<td>Email can be scanned according to three parameters: incoming, outgoing, or internal.</td>
</tr>
<tr>
<td>Network exceptions</td>
<td>Networks can be excepted from the scan by selecting the relevant gateway.</td>
</tr>
<tr>
<td>Granular exception lists</td>
<td>Block and allow lists, allowing the administrator to manually block or allow specific senders based on IP address, sender’s country, sender’s domain, or sender’s email address.</td>
</tr>
</tbody>
</table>

Anti Spam functionality is supported for UTM-1 appliances, and VPN-1 UTM on SecurePlatform. To implement Anti Spam detection, users need a valid service contract attached to their account at the Check Point User Center.

UTM-1 Clustering

Using NGX R65 with Messaging Security, UTM-1 devices can now be clustered to provide a High-availability solution. UTM-1 appliances contain both the firewall gateway and SmartCenter server. Both the gateways and the SmartCenter servers can be clustered to provide a high availability solution.

Note - UTM-1 clustering is only supported on UTM-1 appliances. By default, a UTM-1 cluster solution supports High Availability and Load Sharing. (For Load Sharing, the appropriate license is required)
Provider-1/SiteManager-1 Support

After installation of a special MDS hotfix, NGX R65 with Messaging Security fully supports Provider-1/SiteManager-1.

Additional Reporting options

New counters have been added to the reporting programs for Web Filtering, Anti Virus, and Anti Spam, and three new express reports added to Eventia Reporter.

Installing NGX R65 with Messaging Security

In This Section

Installing NGX R65 with Messaging Security on an Existing Gateway page 5
Installing NGX R65 with Messaging Security on an Existing SmartCenter Server page 5
Allowing WebUI Access page 5
Installing Additional HFAs page 5

To obtain Anti Spam or clustering functionality, you can either:

- Upgrade an existing UTM-1 appliance (see: “Upgrading to NGX R65 with Messaging Security”).
- Install the plug-in on existing SecurePlatform NGX R65 firewalls and SmartCenter servers (see: “Installing NGX R65 with Messaging Security on an Existing Gateway”, and “Installing NGX R65 with Messaging Security on an Existing SmartCenter Server”).
- Purchase new UTM-1 appliances with NGX R65 with Messaging Security already installed. Note - New UTM-1 appliances with NGX R65 with Messaging Security contain a factory default images for NGX R65.

To enable clustering and Anti Spam functionality, the NGX R65 with Messaging Security package needs to be installed on both gateways and SmartCenter servers. NGX R65 with Messaging Security is supplied as a single package that identifies the underlying operating system and installed Check Point products on the target machine. If the NGX R65 with Messaging Security package identifies a gateway on an open server (not an appliance), a gateway hotfix is installed. If the NGX R65 with Messaging Security package identifies a SmartCenter server, a management hotfix and then a plug-in is installed. If the NGX R65 with Messaging Security package identifies a UTM-1 appliance, the appliance is upgraded. The UTM-1 WebUI is replaced to show the new clustering configuration options.


It is also recommended to create a backup image using the image management options in the SecurePlatform WebUI, as shown in Figure 1:
Installing NGX R65 with Messaging Security

Figure 1: Image Management options

Image Management

Available Images

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Created</th>
<th>Size</th>
<th>Version</th>
</tr>
</thead>
</table>
| Factory defaults | NGX R65 with Messaging Security factory defaults | Tue Dec 11 19:38:56 2007 | 1.92G | NGX R6
Installing NGX R65 with Messaging Security on an Existing Gateway

To install NGX R65 with Messaging Security on an existing gateway:
1. Transfer the package to the gateway.
2. Install the package: on SecurePlatform, run UnixInstallScript -splat.

Installing NGX R65 with Messaging Security on an Existing SmartCenter Server

To install NGX R65 with Messaging Security on an existing SmartCenter server:
1. Transfer the package to SmartCenter server.
2. Install the package:
   - On SecurePlatform, run UnixInstallScript -splat
   - On the Windows platform, run setup.exe
   - For Solaris and Linux, run UnixInstallScript.
3. Open SmartConsole, and connect to SmartCenter server.
4. When prompted, download the new version of SmartConsole
5. Install the new SmartConsole and connect again to SmartCenter server
   If the SmartCenter server is installed on a UTM-1 appliance, the first time cluster configuration wizard opens. Cancel the wizard if you do not wish to cluster your gateways at this point.
   See “Configuring Anti Spam” on page 14 to setup up messaging security.

Allowing WebUI Access

During the installation process, an initial default policy allows access to the gateway or appliance via the UTM-1 WebUI. However, there is no default WebUI access after the first policy install. As part of the first policy, be sure to include a rule that enables WebUI access on port 4434.

Installing Additional HFAs

NGX R65 with Messaging Security already contains R65 HFA01 and HFA02. Installing these HFA packages again will result in unpredictable behavior.
Upgrading to NGX R65 with Messaging Security

In This Section:

In-Place Upgrades  page 6
SmartUpdate  page 10

In-Place Upgrades

Only a UTM-1 appliance (based on NGX R65) can be upgraded to NGX R65 with Messaging Security.

Upgrading a UTM-1 Appliance

A UTM-1 appliance will either be

• Locally managed
• Centrally managed

Upgrading a Locally Managed UTM-1 Appliance

To upgrade a locally managed UTM-1 appliance, perform an in-place upgrade using the UTM-1 WebUI. This method is possible when NGX R65 with Messaging Security is installed on top of either NGX R65 or NGX R65 with the Connectra Central Management plug-in (Connectra NGX R62CM, or CCM for short). The in-place upgrade process consists of:

• Uploading the new package
• Decompressing and extracting the package
• Taking a snapshot of the system for roll-back purposes
• Upgrading and rebooting.

To perform an in-place upgrade to NGX R65 with Messaging Security:

1. Open a browser and connect to the UTM-1 WebUI.
2. Open the **Appliance > Upgrade** window:

3. Download the upgrade package from the Check Point Download Center by clicking on the **Check Point Download Center** link.

4. Click **Upload upgrade package to appliance**.
   
The **Upload package to appliance** window opens.

5. Browse to the upgrade (.tgz) package and select it.
6. Click **Upload**, and wait until the package uploads.

![Upgrade Status](image)

7. Click **Start Upgrade**.

8. The **Start Upgrade** wizard opens.

![Start Upgrade Wizard](image)

It is recommended to save an image of the current running system before the upgrade.

9. Click **Next**, select **Safe Upgrade**, and enter an expiration interval (15 minutes is the default).
Upgrading to NGX R65 with Messaging Security

10. Click **Next**, and **Start**.

The upgrade package is extracted and a snapshot taken of the system. The system is upgraded and rebooted. At the end of the process, the Upgrade Status window looks like this:

11. Log in to the UTM-1 appliance.

If you do not log in within the expiration interval you set in step 9, the UTM-1 appliance reverts to the previous version.

**Note** - If you left the browser window open, you do not have to log into the appliance again.

**Upgrading a Centrally Managed UTM-1 Appliance**

In this kind of deployment, the UTM-1 appliance is managed either by another locally managed UTM-1 appliance, or by SmartCenter server/Provider-1.

- Upgrade the SmartCenter server
  - If the SmartCenter server is on a windows platform:
    i. Obtain NGX R65 with Messaging Security
    ii. Run setup.exe
  - If the SmartCenter server is on SecurePlatform:
    i. Obtain NGX R65 with Messaging Security
    ii. Run UnixInstallScript - splat
  - If the SmartCenter is on Linux
    i. Obtain NGX R65 with Messaging Security
    ii. Run UnixInstallScript
- Upgrade the gateway
  i. Transfer the upgrade package to the gateway.
ii. Perform an in-place upgrade using the UTM-1 WebUI.

**Upgrading VPN-1 UTM**

For both gateways and SmartCenter servers:

- For Windows platforms:
  a. Obtain NGX R65 with Messaging Security
  b. Run `setup.exe`

- For SecurePlatform:
  a. Obtain NGX R65 with Messaging Security
  b. Run `UnixInstallScript-splat`

- For Linux
  a. Obtain NGX R65 with Messaging Security
  b. Run `UnixInstallScript`

12. **Provider-1 INSPECT Files**

If INSPECT files were manually edited on one of the CMAs (for example `vpn_table.def` in the `$FWDIR/lib/` directory), and you wish to preserve these changes through the upgrade, simply backing up these files is insufficient. To retain manual modifications to `.def` files, record these changes elsewhere before the upgrade, and manually reapply them after the upgrade is complete.

**SmartUpdate**

SmartUpdate is supported for all gateways. Install NGX R65 with Messaging Security from the CD.
Messaging Security

In This Section

Messaging Security Overview  page 11
Anti Spam  page 11
Architecture  page 13
Configuring Anti Spam  page 14
Configuring Anti Virus  page 21
Logging and Monitoring  page 24
Reporting False Positives to Check Point  page 24

This section covers Messaging Security. Messaging security is composed of both Anti Spam and Anti Virus protections for incoming, outgoing, and internal corporate email.

Messaging Security Overview

On the Messaging Security Overview page, select:

- Select gateways that enforce Anti Virus checking
- Select gateways that enforce Anti Spam protection
- Enable automatic updates

You can also view settings and logs, as shown in Figure 2:

Figure 2  Messaging Security Overview

Anti Spam

A typical spam outbreak lasts only a few hours but during that time, many millions of unsolicited messages bombard the corporate mail server. To generate a maximum return on investment, the spammer will have varied the content of each message to prevent its identification as spam.
Nonetheless, all messages within the same outbreak share at least one and often more than one unique, identifiable value which can be used to distinguish the outbreak — for example a link to a specific commercial web site. Different spam attacks are often launched from the same network of zombie machines — this constitutes a characteristic, a recurring pattern or value that can be logged and analyzed.

NGX R65 with Messaging Security's Anti Spam functionality employs unique licensed technology. Unlike many Anti Spam applications that rely on searching for keywords and a lexical analysis of the content of an email message, this Anti Spam solution classifies spam by analyzing known and emerging distribution patterns. By avoiding a search for key words and phrases that might classify a legitimate email as spam and instead focusing on other message characteristics, this solution offers a high spam detection rate with a low number of false positives.

To preserve personal privacy and business confidentiality, only select characteristics are extracted from the message envelope, headers, and body (no reference to actual content or attachments are included). Hashed values of these message characteristics are sent to a Detection Center for pattern analysis. The Detection Center identifies spam outbreaks in any language, message format, or encoding type. Responses are returned to the enterprise gateway within 300 milliseconds.

Key benefits of an active Anti Spam policy configured in SmartDashboard:

- Real-time protection
- High spam-detection rate.
- Spam detection in any language across all message formats.

Once identified, the network of zombie machines is blacklisted. If the network changes it behavior, for example no longer launches spam attacks, the network is removed from the black list.
Architecture

Figure 3 shows the process by which spam is identified by NGX R65 with Messaging Security:

Figure 3  NGX R65 with Messaging Security Architecture

1. Proxy SMTP server on the gateway receives incoming mail
2. The SMTP proxy forwards the mail to an Anti Spam daemon to extract selected message characteristics, and produce a hash fingerprint.
3. Using a special Anti Spam protocol, the Anti Spam daemon queries the Detection center. The hashed fingerprint is compared to other fingerprints in the pattern repository to determine whether the email is spam.
4. The detection classifies the email as either spam or not spam, and returns the result to the gateway.
5. If the email has been classified as spam, the email is flagged as such (in the header or subject) and forwarded to the enterprise mail server.
6. The mail server forwards the email to its recipient on the network. Because the header or subject has been flagged as spam, recipients can use that tag or marker to set up filtering rules in their native mail program — for example in Microsoft Outlook a rule can be configured to delete all emails with the word SPAM in either the subject line or header.

To prevent delays while large email files are scanned for Spam, a feature known as Adaptive Continuous Download transfers email to the recipient while Anti Spamilng detection takes place.

Adaptive Continuous Download

For emails that need to be scanned, the Anti Spam engine acts as a proxy which caches the file before delivering it to the recipient. If an email happens to be a large file, the recipient may experience delays before the file is delivered. To avoid delays, Adaptive Continuous Download starts delivering the email to the recipient while Anti Spam scanning is still in progress. If the email is designated as Spam, the email is flagged as spam before it is completely transferred to the recipient. SMTP and POP3 protocols support Adaptive Continuous Download for the entire email message.
Configuring Anti Spam

In This Section

Configuring a Content Anti Spam Policy
Configuring an IP Reputation Policy
Configuring a Block List
Configuring Anti Spam SMTP
Configuring Anti Spam POP3
Configuring Network Exceptions
Configuring an Allow List
Selecting a Customized Server
Anti Spam on VPN-1 UTM Edge Devices
Bridge Mode and Anti Spam

Configuring a Content Anti Spam Policy

A content Anti Spam policy is set on the Messaging Security tab of SmartDashboard, as shown in Figure 4:

Figure 4

1. Use the slider to select an Anti Spam policy protection level.
2. Select flagging options.
3. In the VPN-1 UTM Engine settings section, set a maximum data size to scan.
4. In the VPN-1 UTM Edge Engine settings section, set a confidence level for spam and suspected spam.

A spam confidence level is a grade or rating (usually between zero and a hundred) used decide whether a particular email message should be treated as spam. For example, if the confidence level is set to 70, then all email messages rated at 70 or above will be treated as spam.
SofaWare UTM-1 Edge devices contain their own Anti Spam engines. Values entered in the VPN-1 UTM Edge Engine settings section are used to correlate SofaWare Anti Spam engine ratings with Check Point Anti Spam engine ratings. For example if a particular email message is rated by the SofaWare Anti Spam engine as 90, and this value, once translated into Check Point ratings, means the email should be treated as spam, then the Actions defined for Spam or Suspected spam on the Anti Spam Policy page are enforced.

5. Select Tracking Options for Spam, Suspected Spam, or Non Spam. Tracking options include:
   - None (no logging)
   - Log
   - Popup Alert
   - Mail Alert
   - SNMP trap alert
   - Three custom user-defined scripts.

Configuring an IP Reputation Policy

This window enables IP reputation, an Anti Spam mechanism that checks the IP address of the message sender (contained in the opening SYN packet) against a dynamic database of suspect IP addresses. If, according to the IP reputation service, the originating network has a reputation for sending spam, then the spam session is blocked at connect time. In this way, the IP reputation feature creates a list of trusted email sources.

1. Use the slider to select an IP Reputation Policy:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>No IP Reputation service</td>
</tr>
<tr>
<td>Monitor Only</td>
<td>Monitors spam and suspected spam</td>
</tr>
<tr>
<td>Medium Protection</td>
<td>Rejects spam and monitors suspected spam</td>
</tr>
<tr>
<td>High Protection</td>
<td>Rejects spam and suspected Spam</td>
</tr>
</tbody>
</table>

2. Select tracking options for Spam, Suspected Spam, or Non spam. Tracking options include
   - None (no logging)
   - Log
   - Popup Alert
   - Mail Alert
   - SNMP trap alert
   - Three custom user-defined scripts.
Configuring a Block List

As shown in Figure 5, a list of email sources to block can be configured according to either the senders name, domain name, or IP address.

1. Use the slider to select a Block Policy:

<table>
<thead>
<tr>
<th>Block Policy</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>No blocking</td>
</tr>
<tr>
<td>Monitor Only</td>
<td>Monitors sends by IP and email address</td>
</tr>
<tr>
<td>Block</td>
<td>Blocks senders by IP address and email address</td>
</tr>
</tbody>
</table>

2. In the Blocked senders/domains section, click Add and enter the name of a sender or domain to be rejected.

3. In the Blocked IPs section, click Add and enter an IP address that should be blocked.

4. From the drop-down list in the Tracking section, select a tracking option for either blocked mail or non spam.

Configuring Anti Spam SMTP

SMTP traffic can be scanned according to direction, as shown in Figure 6:
1. Select a scanning direction for:
   - Incoming files
   - Outgoing files
   - Internal files through the gateway

2. Select **Activate Continuous download**... to avoid client time-outs when large files are scanned.
   See “Adaptive Continuous Download” on page 13 for further information.
Configuring Anti Spam POP3

POP3 traffic can be scanned according to direction, as shown in Figure 7:

Figure 7  POP3 Scanning directions.

1. Select a scanning direction for:
   - Incoming files
   - Outgoing files
   - Internal files

2. Select **Activate Continuous download**... to avoid client time-outs when large files are scanned.
   See “Adaptive Continuous Download” on page 13 for further information.
Configuring Network Exceptions

As shown in Figure 8, an Anti Spam policy can be enforced on all email traffic or only on traffic that has not been deliberately excluded from the policy.

Figure 8 Networking exceptions

To exclude sources and destinations:

1. Click Add..

   The **Network Exceptions** window opens.

   **Network Exceptions**
   - Enforce the Anti Spam policy on all traffic.
   - Enforce the Anti Spam policy on all traffic except for traffic from the following sources and destinations.

2. Select Source and Destination gateways for which the Anti Spam policy will not be applied, and click **OK**.
Configuring an Allow List

As shown in Figure 9, a list of email sources to allow can be configured according to either the senders name and domain name, or IP address.

1. In the **Allowed senders\domains** section, click **Add** and enter the name of a sender or domain to be allowed.
2. In the **Allowed IPs** section, click **Add** and enter an allowed IP address.
3. From the drop-down list in the **Tracking** section, select a tracking option.

Selecting a Customized Server

As shown in Figure 10, an alternative data center for Anti Spam analysis can be selected.

If appropriate, select **Use Customized Server**, and select an alternative data center from the drop-down list.
**Anti Spam on VPN-1 UTM Edge Devices**

Anti Spam protection is available on VPN-1 UTM Edge devices. To configure Anti Spam, on the General Properties window of the VPN-1 UTM Edge gateway, select the Anti Spam option, as shown in Figure 11:

Figure 11 Enabling Anti Spam on VPN-1 UTM Edge devices.

### Bridge Mode and Anti Spam

If an UTM-1 appliance is configured to run in bridge mode, Anti Spam is supported providing that:

- The bridge interface has an IP address
- The bridge interface has a default gateway

### Configuring Anti Virus

In This Section:

- Configuring Mail Anti Virus page 21
- Configuring Zero Hour Malware Protection page 22
- Configuring File Types page 22
- Configuring Settings page 23
- Configuring a Disclaimer page 24

### Configuring Mail Anti Virus

The Mail Anti Virus policy prevents email from being used as a virus delivery mechanism. To configure a mail anti virus policy:

1. Set the slider to block
2. Select tracking options for either all POP3 and SMTP mail, or just blocked mail. As shown in fig:
**Configuring Zero Hour Malware Protection**

By proactively scanning the Internet, the DataCenter identifies massive virus outbreaks as soon as they occur. This Zero-Hour solution provides protection during the critical time it takes to discover a new virus outbreak and assign it a signature.

1. Using the slider, select a Zero hour malware protection level:
   - Off
   - Monitor Only
   - Block

2. Select tracking options for SMTP and POP3 mail, as shown in Figure 13

**Configuring File Types**

On this page, set an action to take place when a file of a certain type passes through the gateway. Certain file types can pass through the gateway without being scanned for viruses. For example, picture and video files are normally considered safe. Other formats can be considered safe because they are relatively hard to tamper with. Update the list as necessary.

On this window you can also configure Continuous Download options. (See “Adaptive Continuous Download” on page 13 for more information.)
Figure 14  File types

File Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>.ps</td>
<td>PostScript file</td>
<td>Scan</td>
</tr>
<tr>
<td>.pdf</td>
<td>Adobe Acrobat PDF</td>
<td>Scan</td>
</tr>
<tr>
<td>.zip</td>
<td>ZIP compressed archive</td>
<td>Scan</td>
</tr>
<tr>
<td>.af</td>
<td>AFF archive file data</td>
<td>Scan</td>
</tr>
<tr>
<td>.arc</td>
<td>ARC archive data</td>
<td>Scan</td>
</tr>
<tr>
<td>.ar</td>
<td>Archive data</td>
<td>Scan</td>
</tr>
<tr>
<td>.sbr</td>
<td>SBR archive data</td>
<td>Scan</td>
</tr>
<tr>
<td>.class</td>
<td>Compiled Java class file</td>
<td>Scan</td>
</tr>
<tr>
<td>Unknown</td>
<td>Default Scan Values for Unknown File Types</td>
<td>Scan</td>
</tr>
<tr>
<td>.eps</td>
<td>EPS (Encapsulated PostScript) file</td>
<td>Scan</td>
</tr>
<tr>
<td>.gif</td>
<td>GIF image data</td>
<td>Pass</td>
</tr>
</tbody>
</table>

Configuring Settings

On this page, define maximum sizes for files and archives that should be scanned. Configure actions to take if the set limits are exceeded, or when a scan fails.
Configuring a Disclaimer

A shown in Figure 15, a custom disclaimer notice can be created.

Figure 15   Disclaimer notice

1. Select Add disclaimer to email scanned by Anti Virus and Anti Spam engines.
2. In the text box, type your disclaimer notice.

Logging and Monitoring

Logs derived from Anti Spam scanning are sent to SmartCenter server, and viewed using SmartView Tracker.

Anti Spam status is monitored using SmartView Monitor. The Anti Spam status appears under the Firewall product. The status contains information such as the Anti Spam engine version. Anti Spam status also includes statistics regarding scanned files. See also: Tracking and Reporting Options page 39.

Reporting False Positives to Check Point

A small number of genuine emails will inevitably be classified as spam. To help Check Point fine-tune the Anti Spam service, please report them to Check Point support.

The sender of an email that is falsely classified as spam will receive an email notification that the email could not be delivered. This email contains an Email session ID.

1. Request the email session ID from the sender.
2. Open SmartView Tracker.
3. On the Log tab > Content-based Anti Spam section locate the email session ID.
4. Open the Record Details and click Copy.
5. At the Check Point Support Center, open a Service Request and paste in the record details.

For more information on how to create and view Service Requests, consult sk31615 at the Check Point Support Center:

http://support.checkpoint.com
Figure 16  Record details

![Record Details](image_url)
UTM-1 Clustering

In This Section

Overview
Configuring a Cluster on New Appliances
Adding an Existing UTM-1 Appliance to a Cluster
Removing a Cluster Member
Upgrading to a UTM-1 Cluster
Importing a Database to a Primary Cluster Member
Migrating a SmartCenter Server Database to a UTM-1 Cluster
Supported Logging Options for UTM-1 Clusters

Overview

A pair of UTM-1 appliances can be clustered for high-availability. Each UTM-1 appliance becomes a single member in the cluster. High availability refers to the fact that both the gateway components and the SmartCenter server management components are fully synchronized. If one component fails, a complete replication of the data exists on the member’s peer in the cluster. Connections through the appliance continue uninterrupted.

Unlike between the gateway components, there is no fail-over between the SmartCenter server components. If the primary SmartCenter server goes down, the secondary SmartCenter server does not take over. However, the secondary SmartCenter server’s database is fully synchronized with the Primary, so no data is lost. Before setting up a UTM-1 cluster, note that:

- The members of UTM-1 Cluster can either be configured together (both appliances are linked before the UTM-1 WebUI wizard is opened) or separately (the user chooses to figure a UTM-1 Cluster consisting of a single, primary member, and configure the secondary member at a later date).
- Even if you decide not to install a secondary cluster member, it is worthwhile to configure a cluster composed of a single primary member. A UTM-1 cluster is visible to the external network through its virtual IP addresses, not the actual physical addresses of its members. If at some point you do decide to add a secondary member, you will not have to alter the layer 3 topology of the network.

Configuring a Cluster on New Appliances

To configure a cluster on appliances with NGX R65 with Messaging Security already installed:

1. Power up the UTM-1 appliance.
   The PWR/Status LED on the front panel starts blinking. When the LED ceases to blink, the appliance is ready for login.

2. Using the supplied Ethernet cable, connect the UTM-1 appliance’s internal interface to a PC.

3. Configure the PC to be on the same subnet as the UTM-1 appliance. For Windows XP operating systems:
   a. Click Start > Settings > Control Panel > Network Connections.
   b. Double-click Local Area Connection.
   c. On the General tab, click Properties.
   d. In the Local Area Connection Properties window, scroll down to and double-click Internet Protocol (TCP/IP).
e. In the Internet Protocol (TCP/IP) Properties window that opens, select Use the following IP address.

f. In the IP address field, enter 192.168.1.2.

g. In the Subnet Mask field, enter 255.255.255.0.

h. Leave the Default gateway settings empty.

i. Select Use the following DNS server addresses, and leave the Preferred DNS server and Alternate DNS server fields empty. The window should look like this:

![Internet Protocol (TCP/IP) Properties window with settings filled in]

j. Click OK.


   The UTM-1 Appliance login window appears.

   If you receive a certificate error page notice, click Continue to this Web site. If you are using a popup block, allow all popups.

5. Log in with the default system administrator login name and password: admin/admin.
6. Change the default login name and password:

7. Click **Save and Login**.

   The first time configuration wizard opens.

8. Click **Next**.
The **Appliance Date and Time Setup** page opens.

9. Set up the appliance date and time and click **Apply**.

The **Network Connections** page opens.

10. Add an interface for the cluster SYNC/LAN1 interface, and click **Next**.

The **Routing Table** page opens.
11. Add or delete routes as necessary, and click Next.

The DNS and Domain Settings page opens.

12. Configure a hostname, domain name, and DNS servers, and click Next.

The Management Type page opens.

13. Select Locally Managed, and click Next.

The UTM-1 High Availability Cluster page opens.

14. Select UTM-1 Primary cluster member, and click Next.
If you are configuring the secondary management, select **UTM-1 Secondary Cluster member** and click **Next**. The **Secure Internal Communication (SIC) setup** page opens:

Enter an activation key (one-time password), and make a note of it. You will need this activation key when initializing SIC in SmartCenter server. Click **Next**.

The **Web/SSH and GUI clients** page opens.

15. Add or remove remote machines from which Web, SSH, or SmartConsole Clients can connect to the SmartCenter server, and click **Next**.

The **Download SmartConsole Applications** page opens.

16. Download SmartConsole to your PC, and click **Next**.
A summary page is displayed.

![First Time Configuration Wizard - Summary](image)

To access SmartDashboard application use the same Username and Password you use for the Web Administration Interface.

After successfully configuring Check Point UTM-1, you have a 15 day trial period in which you can use UTM-1.

### Summary
- **Check Point UTM-1** will be configured as:
  - Management Type: Locally Managed
  - Cluster Configuration: UTM-1 Primary cluster member
  - GW Clients: Any
  - Internal Interface: 192.168.1.1/205.255.255.0
  - Default Routes: 192.168.1.254
  - Hostname: Primary-HMVT

In order to complete the configuration wizard, click on 'Finish' button. This will initiate the appliance, it will take several minutes to complete.

17. Click **Finish**.

   The configuration process runs.

18. Wait until the completed message appears, and click **OK**.

19. **Reboot**.

   The gateway must be rebooted at this point.

20. Repeat the procedure for the secondary management device, but at step 14 on page 30, select **UTM-1 Secondary cluster member**, and enter an activation key when prompted.

   **Note** - Remember the activation key. You will need it later when configuring the cluster in SmartDashboard. Remember to configure the cluster SYNC interface on the same subnet as the SYNC interface on the Primary management device.

   You now have two UTM-1 appliances, one configured as a primary management, the other as secondary.

   **Note** - IP addresses need to be configured on both cluster members before opening SmartDashboard and running the first-time cluster configuration wizard, as described in step 23.

21. Using a cross cable, connect the SYNC/LAN1 ports.

22. Install the SmartDashboard you downloaded in step 16 on page 31.

23. Open SmartDashboard and connect to the IP address of the UTM-1 appliance that has been configured as the primary cluster member.

   The cluster configuration wizard starts automatically. If the UTM-1 Cluster wizard does not start automatically, double click the network cluster object in SmartDashboard and select the **Simple mode** option.
Click **Next** on the welcome page. The Cluster’s general properties window opens:

![General Properties Window](image)

24. Enter the cluster name.

The name entered here will replace the provisional name that already appears in the network objects tree. (If you cancel the wizard at this point and examine the network objects tree, a cluster object is shown with only the primary member defined).

**Note** - If you choose to define the UTM-1 Cluster in classic mode, when entering the IP address of the cluster, enter the Virtual IP.

25. Click **Next**.

The **Secondary member’s properties** window opens.

![Secondary Member Properties](image)

The UTM-1 appliance acting as the primary management server has been defined automatically, so only the secondary management server needs to be configured.

26. Enter:

   a. the Secondary cluster’s name and IP address, the same name that you entered during the SecurePlatform first-time configuration wizard.
b. the activation key.

If you choose to define the secondary member later, then each time SmartDashboard is opened, the UTM-1 first-time wizard runs automatically.

27. Click Next.

Clicking Next initiates SIC. The SmartCenter server on the primary management retrieves a list of interfaces (and therefore networks) the secondary cluster member is connected to: the topology of the UTM-1 cluster.

Once SIC is initiated, the **Cluster topology** window opens:

![Cluster topology window](image)

Define member interfaces here, and also enter the Cluster interface IP address.

- **Configure Cluster topology for interface (SYNC, DMZ, EXT, INT, LANs)**

The LAN1 interface serves as the SYNC interface between cluster members. If not configured, SYNC interfaces are automatically set to 10.231.149.1 and 10.231.149.2. If these addresses are already in use, their values can be manually adjusted. If you manually adjust the default IP SYNC addresses, verify that both reside on the same subnet.

**Note** - All interfaces in the cluster must have unique IP addresses. If the same IP address is used twice, policy installation will fail. A **Load on module failed** error message is displayed. See also: "Changing Cluster IP Addresses" on page 48.

- **Configure Cluster Virtual Interface.**

In addition to the UTM-1 cluster having its own unique IP address, which is visible to the network, each member interface also has a unique IP address. These unique IP addresses are used for internal communication between the cluster members as well as for accessing the cluster member directly. It is the Virtual IP address which makes the cluster visible to the external network, and populates the network routing tables — not the actual
IP addresses of the individual members. If you chose to define a secondary member at a later date, but still configure the Virtual Cluster IP address, secondary members can later be added without changing the layer 3 topology of the network.

**Note** - The external Virtual IP address of the cluster must be unique.

28. Click **Next**, and in the following windows configure IP addresses for the **External**, and **Internal** interfaces on each cluster member.

29. Click **Next**, and **Finish**.

**Note** - After completing the first-time cluster wizard, the main IP address, as shown in the UTM-1 Cluster **General properties** window, will be the Virtual IP address of the cluster.

The new cluster of UTM-1 appliances appears in the network objects tree:

---

**Adding an Existing UTM-1 Appliance to a Cluster**

A single standalone UTM-1 appliance can easily be added to a UTM-1 cluster once a second UTM-1 device has been added to the network.

To add an existing UTM-1 device to a Cluster:

1. Open the SecurePlatform WebUI.
2. On the **Product Configuration, Cluster** page, select **Make this Appliance the primary member of a UTM-1 High Availability Cluster**.
3. Click **Apply**.
4. Reboot the appliance.
5. Using SmartDashboard, connect to the primary SmartCenter server.

The first-time cluster configuration wizard opens.
6. Complete the wizard in order to configure the secondary cluster member.

In SmartDashboard, the network object representing the former standalone UTM-1 device is converted to a cluster object. If the standalone UTM-1 device appeared in the:

- **INSTALL ON** column of any rule (Security, QoS, NAT)
- **Participating Gateways** list for a VPN community

the new cluster object is now shown. In all other columns (Source, Destination, Groups) the standalone UTM-1 object needs to be manually changed to the cluster object.

Manually changing this network object may have implications for your Security, NAT, and QoS rules. To understand how and where the new primary cluster member is being used, right-click the cluster object and select **Where used**...

It is also recommended to use the **Search > Query Rules...** option on the File Menu.

1. Select the Stand Alone object and make sure it appears in the **In List** section.
2. Select the **Explicit** option.
3. Click **Apply**.

For the remaining rules that still contain the standalone object, replace by drag-and-dropping the new cluster object.

In addition, if you have a group that contains a standalone UTM-1 gateway, which has since been promoted to a primary cluster member, a policy install for that group will fail. To successfully install a policy, replace the standalone UTM-1 gateway with the object for the cluster.

**Note** - While the icon in SmartDashboard has changed to reflect the UTM-1 device’s new status as a primary cluster member, the **Name** and **UID** of the object in the database remains unchanged.

### Removing a Cluster Member

Although a UTM-1 Cluster consists of only two members, it is still possible to remove one of the members without erasing the cluster. A UTM-1 cluster can exist with only a single (primary) member until a new secondary member is added. This means that either member can be easily taken offline for maintenance.

A cluster member is removed in two stages: first in the UTM-1 WebUI, second on the command line of the appliance. To remove a cluster member:

1. Open the **UTM-1 WebUI > Product Configuration > Cluster** page, as shown in **Figure 17**:

   ![Figure 17](remove_peer.png)

2. Click **Remove Peer**.

   Clicking **Remove Peer** results in a UTM-1 Cluster with a single member.
• If the current machine is the primary member of the cluster, the secondary member is deleted.

• If the current machine is the secondary member, the secondary member is first promoted to a primary and then the peer is deleted.

Note - Services running on the appliance are restarted.

3. On the appliance command line, run: cp_conf fullha disable. This command reverts the primary cluster member to a standalone configuration.

4. Reboot.

After reverting to a standalone configuration, the former cluster is shown in SmartDashboard as a locally managed gateway consisting of gateway module and SmartCenter server. Before installing a new policy:

• See “Deleting a UTM-1 Cluster” on page 48, and

• See “Adding a New Secondary Member to a UTM-1 Cluster” on page 48.

Upgrading to a UTM-1 Cluster

If you have a single UTM-1 appliance in production, and want to upgrade to NGX R65 with Messaging Security and configure a UTM-1 Cluster:

1. Perform a standard in-place upgrade to NGX R65 with Messaging Security using the UTM-1 WebUI.

2. Using the UTM-1 WebUI, on the Cluster page, convert the appliance to a primary member.

3. Connect a second UTM-1 appliance to the network.
   a. If this second appliance is based on an earlier version, obtain the relevant upgrade package from the Download Center, save it to a USB stick, and reinstall the appliance as a secondary cluster member.
   b. If the second appliance is already NGX R65 with Messaging Security, run the first-time wizard and select “secondary cluster member.”

Importing a Database to a Primary Cluster Member

To import an older SmartCenter database to the primary member of a new UTM-1 cluster:

1. Install the primary as a standard management (not a cluster)

2. Import the older SmartCenter server database

3. Using the UTM-1 WebUI, convert the standard management to a primary cluster member.

Note - If the older database is from another primary member of a UTM-1 Cluster, the above procedure is not required.

Migrating a SmartCenter Server Database to a UTM-1 Cluster

To migrate a SmartCenter server database to a UTM-1 Cluster, go to the Check Point Support Center at:

http://support.checkpoint.com
and consult:

**sk33896**

### Supported Logging Options for UTM-1 Clusters

The standard logging options for a regular cluster are also available in UTM-1. In UTM-1, the primary cluster member can send logs to the secondary, and the secondary to the primary. Both can also send logs to an external log server. However, while a regular cluster cannot save logs locally, a UTM-1 Cluster member also functions as a log server. When logs are saved locally on the UTM-1 cluster member, implications exist for High Availability and Load Sharing scenarios.

#### Recommended Logging Options for High Availability

In a High Availability scenario, one of the UTM-1 cluster members is active while the other cluster member remains in standby. Log files are not synchronized between the two UTM-1 cluster members. For this reason it is recommended to:

- Configure logging so that logs are always sent to the primary UTM-1 cluster member, but to the secondary UTM-1 cluster member when the primary is unreachable.
- Set scheduled log forwarding to the primary UTM-1 cluster member.

Alternatively:

- Configure logging so that logs are sent to both UTM-1 cluster members. (Eventia Analyzer and Eventia Reporter with standard reports should use only one of the cluster members as a source for log file correlation and consolidation). Or:
  - Use an external log server.

**Note** - These logging options can also be applied to new NGX R65 with Messaging Security gateways.

#### Load Sharing

To enable load sharing on a UTM-1 Cluster, you must first deselect the **Save logs locally on each cluster member** option on the Log Servers page.

When load sharing is enabled for a UTM-1 Cluster, a connection initiated to the primary member may terminate with the secondary. If logs were saved locally on each cluster member, only partial logs would be produced on each member for connections that were handled by both members. Saving logs locally would result in partial log data being displayed in Smartview Tracker.

If possible, when load sharing is enabled, configure log files to be sent to an external log server.
Tracking and Reporting Options

Anti Spam tracking and reporting options are available in:

- SmartView Tracker
- SmartView Monitor
- Eventia Reporter

SmartView Tracker

SmartView Tracker now logs Anti Spam activity, as shown in Figure 18:

Figure 18  SmartView Tracker monitoring Anti Spam

Record details exist for Number, Date, Time, Product, Interface, Origin, Type, Action, Service, Source, Source country, Destination, Sender, Original sender, Recipients, Original recipients, Spam category, Control, and Information.

Right-clicking on a row displays a new Follow Email Session ID option. Following the session provides granular information, as shown in Figure 19:

Figure 19  Followed session
SmartView Monitor

For NGX R65 with Messaging Security, SmartView Monitor now reports on Web Filtering, Anti Spam, and Anti Virus activity.

Eventia Reporter

As shown in Figure 20, three new express reports for content inspection have been added to Eventia Reporter:

- Anti Virus
- Web (URL) Filtering
- Anti Spam

![Express Report - Anti Spam Activity](image)

Figure 20  Eventia Reporter Express reports:

MIB

To facilitate reporting and logging, additional objects have been added to the Check Point MIB.
Uninstalling NGX with Messaging Security

This section covers uninstalling R65 NGX with Messaging Security on various supported platforms. Before uninstalling the NGX R65 with Messaging Security plug-in, see “SmartView Tracker” on page 49 of the Known Limitations section.

Uninstalling the Plug-in

This section covers uninstalling the plug-in.

Before Uninstalling the Plug-in

For Provider-1:
1. Deactivate the R65 with Messaging Security plug-in on all CMAs.
2. Remove all NGX R65 with Messaging Security objects from all the CMAs.
   On the General Properties window of each object, deselect the Anti Spam option in the Check Point Products area.
3. If you are using CMA/SmartCenter server High Availability, synchronize all CMAs.

For SmartCenter Server:
1. Remove all NGX R65 with Messaging Security objects
   On the General Properties window of each object, deselect the Anti Spam option in the Check Point Products area.
2. If you are using SmartCenter server High availability, synchronize all SmartCenter servers.

Uninstalling the Plug-in

From Windows
1. Run the pre-uninstall verifier in C:\program files\CheckPoint\Plutm1\R65\bin. Double click plugin_preuninstall_verifier.exe
   Follow any instructions presented by the pre-uninstall verifier.
2. If you have Eventia Reporter enabled, terminate the consolidator process:
   a. Run rmdstop -lc.
   b. Using either the windows Task Manager, or by running cpwd_admin list on the command line, terminate the:
      i. log_consolidator process.
      Verify that no consolidation sessions are running. (The PID column for the log_consolidator process should show 0).
      ii. mysqld-nt.exe process.
   c. Stop the Database service by running: net stop RTDatabase.
   d. Stop the SNMP service.
      i. Use the Services applet in Control panel > Administrative Tools, stop the SNMP service or:
      ii. From the command line run: net stop snmp.
3. Using the Add or Remove programs option in Control Panel
   a. Remove the Check Point NGX R65 with Messaging Security Plug-in.
b. Remove all Check Point packages that contain **Messaging Security** in their names.

4. Reboot the machine.

**From Other Platforms**

**For gateways only:**

1. Remove the FireWall-1 HotFix:
   
   `/opt/CPsuite-R65/uninstall_fw1_HOTFIX_R65_25`

2. Reboot the machine.

**For SmartCenter Server:**

1. Run the preuninstall verifier for the plug-in:

   `/opt/CPPIutm1-R65/bin/plugin_preuninstall_verifier`

   Follow any instructions presented by the pre-uninstall verifier, then:

2. Using the appropriate command (rpm -e for SecurePlatform, pkgrm for Solaris), remove the plug-in from the Operating System. For example:

   `rpm -e CPPIutm1-R65`

3. Remove the FireWall-1 HotFix:

   `/opt/CPsuite-R65/uninstall_fw1_HOTFIX_R65_25`

4. Remove the VPN-1 UTM Edge compatibility package HotFix:

   `/opt/CPEdgecmp-R65/uninstall_edge_cmp_HOTFIX_R65_25`

5. Remove (if installed) the Eventia Reporter HotFix:

   `/opt/CPrt-R65/uninstall_ReportingServer_HOTFIX_R65_25`

6. Reboot the machine.

**For Provider-1:**

1. Run the preuninstall verifier for the plug-in:

   `/opt/CPPIutm1-R65/bin/plugin_preuninstall_verifier`

   Follow any instructions presented by the pre-uninstall verifier, then:

2. Using the appropriate command (rpm -e for SecurePlatform, pkgrm for Solaris), remove the plug-in from the Operating System. For example:

   `rpm -e CPPIutm1-R65`

3. Remove the FireWall-1 HotFix:

   `/opt/CPsuite-R65/uninstall_fw1_HOTFIX_R65_25`

4. Remove the VPN-1 UTM Edge compatibility package HotFix:

   `/opt/CPEdgecmp-R65/uninstall_edge_cmp_HOTFIX_R65_25`

5. On the command line, run: `hf_propagate u`.

6. Remove the MDS HotFix:

   `/opt/CPmds-R65/uninstall_mds_HOTFIX_R65_25`

7. Reboot the machine.
Uninstalling the Connectra Central Management Plug-in

To remove the Connectra Central Management Plug-in:

1. In the Provider-1 MDS, deactivate the Connectra Central Management Plug-in (PIConnectra) on all customers.

2. On the command line, run:
   ```bash
   rm -f /opt/CPPIconnectra-R65/conf/PluginTableTypePairs.conf ; touch /opt/CPPIconnectra-R65/conf/PluginTableTypePairs.conf
   ```

3. Run the pre-uninstall verifier:
   ```bash
   /opt/CPPIconnectra-R65/bin/plugin_preuninstall_verifier
   ```

4. Remove the Connectra Central Management Plug-in:
   - Use `rpm -e CPPIconnectra-R65` on Linux and SecurePlatform
   - Use `pkgrm CPPIconnectra-R65` on Solaris

5. Run `mdsstop/mdsstart`.

From UTM-1 Devices:

UTM-1 Devices only supports image management, and not the command line work flow covered in this section.
Known Limitations

This sections covers known limitations for NGX R65 with Messaging Security. For Known limitations and resolved issues related to R65 only, see the full R65 release notes at:

http://support.checkpoint.com

Firmware Restrictions on Edge page 45
VPN-1 UTM-1 Edge Connectivity page 45
SmartCenter Advanced Upgrades page 45
Restoring an Appliance page 45
Managing UTM-1 Devices Through SmartDashboard page 45
Installation on Windows Platforms page 45
Using SmartUpdate to Install NGX R65 with Messaging Security page 46
Installing Through the Command Line page 46
CPSM Process on Secondary Member page 46
Detaching a Member From a Cluster page 46
Advanced Upgrade Issues page 46
Quality of Service page 46
SmartCenter Server Fingerprint After Cluster Failover page 46
SmartDashboard Server objects page 46
SmartConsole Issues page 46
Controlling the Number of Security Servers page 47
Anti Spam page 47
Editing Cluster Properties page 47
Enlarging the Log Partition Size. page 47
Backup and Restore page 47
Editing Web Applications page 47
Syslog Messages page 48
Deleting a UTM-1 Cluster page 48
Deleting a Member From a Cluster page 48
Adding a New Secondary Member to a UTM-1 Cluster page 48
Changing Cluster IP Addresses page 48
Installing Licenses for Web Intelligence page 48
NGX R65 with Messaging Security Installation time page 48
SmartView Tracker page 49
Dynamic Objects in VPN-1 Edge and UTM-1 Devices page 49
Removing a Peer page 49
Image Management Issue in UTM-1 WebUI page 49
Upgrading SecurePlatform page 49
Eventia Reporter Issues page 49
SMTP Traffic page 50
USB Key Factory Defaults page 50
Firmware Restrictions on Edge

On UTM-1 Edge devices, only Firmware 8.0 and above supports NGX R65 with Messaging Security.

VPN-1 UTM-1 Edge Connectivity

When managing VPN-1 UTM Edge devices using NGX R65 with Messaging Security in a full HA deployment, connectivity problems may arise between a VPN-1 UTM Edge device and SmartCenter server. The VPN-1 UTM Edge device might fail over to the standby SmartCenter server then fail over again to the active SmartCenter. To prevent this, on both SmartCenter servers:

1. Open \$FWDIR/conf/sofaware/SWManagementServer.ini for editing.
2. Change BindAny=true to BindAny=false.
3. Save the file.
4. Restart the SMS process by running smsstop and smsstart.

SmartCenter Advanced Upgrades

- An exported configuration that includes settings for a UTM-1 cluster cannot be imported to another UTM-1 appliance during the installation process. The resulting configuration will be inconsistent.

- To import an existing database to the SmartCenter Server on the UTM-1 device:
  1. Complete the UTM-1 WebUI first-time configuration wizard.
  2. Login to the UTM-1 device, and run the upgrade_export command from \$FWDIR/bin.

Restoring an Appliance

When restoring an appliance using the WebUI option, the process might hang indefinitely. To prevent this from happening, restore using the command line options.

Managing UTM-1 Devices Through SmartDashboard

When attempting to manage a UTM-1 device through SmartDashboard by right-clicking the network object and selecting Manage Device, the browser attempts to connect using port 443 instead of 4434. Manually adjust the port to 4434.

Installation on Windows Platforms

NGX R65 with Messaging Security must not be installed from a directory that has spaces in the directory name. The installation program will abort with error messages.
Using SmartUpdate to Install NGX R65 with Messaging Security

SmartUpdate can be used to install NGX R65 with Messaging Security providing each package is installed separately.

Installing Through the Command Line

When installing NGX R65 with Messaging Security through the command line, do not use the patch add cd command. Use the ./UnixInstallScript -splat option.

CPSM Process on Secondary Member

After installing a UTM-1 Cluster, the CPSM process (responsible for SmartView Monitor) always appeared as terminated on the secondary member.

Detaching a Member From a Cluster

Using SmartDashboard to detach a member of UTM-1 Cluster is currently not supported.

Advanced Upgrade Issues

If policy install fails after performing an advanced upgrade, and Skype error messages are displayed, perform an online update using SmartDashboard, then install the policy again.

Quality of Service

- After running etmstop/etmstart or cpstop/cpstart on the standby member of a UTM-1 Cluster, QoS policy installation fails. If the connection passes through the standby member, then the QoS policy will not be enforced.
- When deleting a UTM-1 Cluster in SmartDashboard, the QoS configuration (which was associated with the cluster's virtual IP address) is lost on the standalone gateway. Reconfigure QoS for the standalone gateway.

SmartCenter Server Fingerprint After Cluster Failover

When connecting with SmartDashboard to a UTM-1 cluster’s virtual IP address, the user is prompted (after a failover event) to approve a new fingerprint. To avoid approving a new fingerprint each time, do not connect to the Virtual IP address of the cluster. Instead, connect to the actual IP address of the management server.

SmartDashboard Server objects

In a UTM-1 Cluster configuration, SmartDashboard Mail/Web/DNS server objects are not supported.

SmartConsole Issues

- Verify that you connect to UTM-1 using SmartConsole NGX R65 build B620000380. You will then be prompted to upgrade to a SmartConsole suitable for NGX R65 with Messaging Security.
• Installing SmartConsole Plug-ins on Windows Vista platform is not supported. If you already have a SmartConsole R65 HFA01 installed on Windows Vista, you will not be able to connect with it to the SmartCenter with this plug-in. To workaround the problem, install SmartConsole R65 HFA01 on any other supported platform.

Controlling the Number of Security Servers

After installing NGX R65 with Messaging Security, it is possible to adjust the number of processes engaged in HTTP, POP3 and SMTP processing. To adjust the number of security servers:

1. Using GuiDBedit, connect to the primary SmartCenter server.
2. On the Tables tab, select Other > content_security.
3. Open the Global_security_server_settings object.
4. Change http_process_num, pop3_process_num and smtp_process_num properties to the desired value.
   Values are between 1 and 12. The higher the value, the greater the number of processes run in parallel. However, a higher number consumes greater system resources.
5. Save changes.
6. Install policy.

Anti Spam

Internet connectivity is required for Anti Spam functionality. If Internet connectivity is not immediately available, perform cpstop and cpstart.

Editing Cluster Properties

When editing cluster properties (using the classic view, not the first-time wizard) in SmartDashboard, verify that the Virtual IP address of the cluster is unique. If you supply an IP address that is not unique, a error message warning you of this fact will not be generated. The duplicate IP address will be accepted.

Enlarging the Log Partition Size.

The default size of the UTM-1 log partition is 10GB. To enlarge it, follow the instructions in: sk33179. See:
http://support.checkpoint.com

Backup and Restore

A backup operation performed using the SecurePlatform WebUI (saving the files to the local desktop) will also save the files on the UTM-1 device in: /opt/spwm/www/html. These duplicate files have the same name and size as those backed up to the desktop.

Editing Web Applications

When editing a web application on the Connectra tab of a UTM-1 SmartCenter server, a Check Point Gateway cannot be converted to a Check Point Host. Create a separate host for the application that is using the current host.
Syslog Messages

By default, syslog messages are not accepted by members of UTM-1 Cluster. To accept syslog messages, use GuiDBedit to alter the value of the Enable_CPSyslogD property.

Deleting a UTM-1 Cluster

After deleting a UTM-1 cluster and reverting to a standalone deployment:

1. Double-click the new standalone object in SmartDashboard to open the object's properties window.
2. Click OK.
   Clicking OK generates a new IKE certificate.
3. Install a policy.

Deleting a Member From a Cluster

A SmartDashboard error occurs after removing a secondary cluster member and then editing the cluster object. To prevent the SmartDashboard error occurring, EITHER edit the cluster object, and then select the Logs and Masters page, followed by the Masters page, OR save, close and then reopen SmartDashboard.

Adding a New Secondary Member to a UTM-1 Cluster

After detaching a member from a UTM-1 Cluster, and adding it again, you need to re-initialize the SIC before installing a policy. To re-initialize SIC, on the command line of the secondary member, run: cp_conf sic init <password>.

Changing Cluster IP Addresses

After changing the IP address of a cluster member, the SIC connection with the secondary member may be lost, or installation of a new policy fail. To resolve this issue:

2. Install the policy (on both members)
4. Install the policy again.

Installing Licenses for Web Intelligence

Because Web Intelligence licenses are not synchronized on the SmartCenter servers of a UTM-1 Cluster, verify that the license are installed on both the primary and secondary appliances.

NGX R65 with Messaging Security Installation time

The default IDLE time for cpshell is 10 minutes. The installation of R65 with Messaging Security may take longer. It is recommended to increase IDLE time to 30 minutes before switching to expert mode and running the installation script. At the command line, run: idle 30.
SmartView Tracker

Anti Spam and Messaging Security directories remain listed in SmartView Tracker after the UTM-1 plug-in is removed, even though they are no longer relevant. This happens because TrackerTree objects are marked as undeletable. To resolve this issue:

1. Stop Check Point services by running the cpstop command.
2. Open the $FWDIR/conf/TrackerTree.C file for editing.
3. Remove the objects that have the following names:
   - AD1D67CB4A5138A47FAAB2FCAC168D2BF00CCA
   - AED963818A3BA0A4C1CAA30DA84CD4B32F140A
5. Start Check Point services by running the cpstart command.

This solution is also available as sk33682. See:

http://support.checkpoint.com

Dynamic Objects in VPN-1 Edge and UTM-1 Devices

Dynamic objects are not supported in an Anti Spam policy for VPN-1 Edge and VPN-1 UTM Edge devices.

Removing a Peer

When using the Remove Peer option in the UTM-1 WebUI, wait five minutes before running the cp_conf fullha disable command on the primary cluster member.

Image Management Issue in UTM-1 WebUI

The second time you use the image management page of the UTM-1 WebUI to revert to a previous image, a "revert successful" message appears a few seconds after you click Apply. The revert operation is not yet complete. It is recommended to wait until the UTM-1 device has rebooted. Monitor the reboot process through the console, or by watching the green power light.

Upgrading SecurePlatform

After upgrading SecurePlatform from NGX R65 to NGX R65 with Messaging Security, delete all files from the var/log/cpupgrade/web directory.

Eventia Reporter Issues

When exporting the database (advanced upgrade) from an R65 SmartCenter server with Eventia Reporter enabled to R65 with Messaging security (clean install), the internal HFA01 hotfixes for Eventia Reporter are no longer enforced. To reapply the HFA:

1. Run: cpstop
2. Change directory to $RTDIR/bin
3. Run: srv_install -hfa
4. Run: cpstart
When exporting the database (advanced upgrade) from an R65 SmartCenter server with Reporter disabled to R65 with Messaging Security, all Content Inspection Express reports are lost. To recover Express reports:
1. Run: cpstop
2. Change directory to $RTDIR/bin
3. Run: srv_install -hfa
4. Run: cpstart

SMTP Traffic
If SMTP traffic is dropped after installing NGX R65 with Messaging Security on a specific CMS where Anti Spam is enabled:
1. Deactivate and then reactivate the client.
2. Reinstall the security policy.

USB Key Factory Defaults
USB keys containing factory default images are not supplied with this appliance. Previously supplied USB keys will not work with the new appliance.

RFD Button
The Reset Factory Default (RFD) button on the appliance does not function.

Restrictions on the Solaris Platform
URL filtering, and Anti Virus functionality is not available on the Solaris Platform.

Restrictions on the Nokia Platform
Messaging Security is not available on the Nokia platform.
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