



We Secure the Internet.

What's New in Check Point® Enterprise Suite NGX R65

May 10, 2007



In This Document:

Introduction	page 2
Service Contracts	page 2
Firewall & SmartDefense	page 2
VPN-1 UTM Edge	page 5
Management Plug-ins	page 5
Connectra Central Management	page 6
VPN	page 7
SSL Network Extender	page 8
ClusterXL	page 8
NOKIA IPSO	page 9
SmartUpdate Enhancements	page 9
SmartView Monitor	page 10
SmartView Tracker	page 12
Eventia Analyzer	page 13
Eventia Reporter	page 14
Integrity Advanced Server	page 15
SecureClient Mobile	page 15
Provider-1/SiteManager-1	page 17
VPN-1 Power VSX	page 17

The latest version of the “What’s New” documentation is available online at <http://www.checkpoint.com/techsupport/downloads.jsp>.

Introduction

This document covers features and capabilities introduced since Check Point Internet Security Product Suite NGX R65.

Service Contracts

When upgrading your gateways to the latest version, you need to download and install a Service Contract File on your SmartCenter Server. By verifying your licensing status with the User Center, the contract file enables you to easily remain compliant with current Check Point licensing standards. Once installed on your SmartCenter server, the contract file is transferred to gateways during the upgrade process. Contract verification is now an integral part of the Check Point licensing scheme.

For more information on using contract files, see:
<http://www.checkpoint.com/ngx/upgrade/contract>.

See also “[SmartUpdate Enhancements](#)” on page 9

Firewall & SmartDefense

AMT Support for Linux and SecurePlatform

To isolate end point computers that violate the network security policy, NGX R65 supports Intel Active Management technology (AMT). AMT Quarantine installs a special security policy that restricts inbound and outbound traffic on suspect end point computers, thus protecting the larger network from malicious activity.

Aggressive Aging

Aggressive Aging helps manage the connections table capacity and memory consumption of the firewall to increase durability and stability.

Aggressive Aging introduces a new set of short timeouts called aggressive timeouts. When a connection is idle for more than its aggressive timeout it is marked as "eligible for deletion". When the connections table or memory consumption reaches a certain user defined threshold (highwater mark), Aggressive Aging begins to delete “eligible for deletion” connections, until memory consumption or connections capacity decreases back to the desired level.

Aggressive Aging allows the gateway machine to handle large amounts of unexpected traffic, especially during a Denial of Service attack.

Cooperative Enforcement

Administrators are now able to ensure that users traversing the firewall are protected by the Integrity end point shield. When configuring a Check Point Gateway, the administrator defines whether hosts accessing the network from the internal interface have to be authorized by Integrity Server. A user not authorized by Integrity server receives notification (via HTTP or E-mail) to this effect.

An administrator can define several additional parameters such as:

- Check authorization of all clients
- A white list of machines that do not have Integrity installed but can still traverse the firewall
- Tracking options for authorized or unauthorized clients
- Activating Cooperative enforcement in Monitor-Only mode

Monitor-Only Deployment Mode

In the “monitor only” deployment mode, the firewall requests authorization statuses from the Integrity server but, regardless of the received statuses, connections are not dropped. In addition (if configured by the administrator) the Cooperative Enforcement feature generates logs regardless of the deployment mode.

Handling an Unauthorized Host

Unauthorized hosts can either be added to the host’s exception list, or the administrator can take appropriate action to make these hosts compliant.

Web Filtering

In NGX R65, VPN-1 gateways with content inspection capabilities are able to inspect and control http traffic.

The Web Filtering function screens incoming URL requests against a database to determine whether the URL request should be blocked or allowed. Web Filtering takes place according to predefined categories made up of URLs. The Web Filter checks the URL of a Web page against a list of approved sites. In this way, complete sites or pages within sites that contain objectionable material (pornography, illegal software, spyware) can be blocked.

Layer-2 Firewall Deployment

Layer-2 Firewall deployment enables a VPN-1 gateway to be inserted into an internal network without affecting the existing IP address routing scheme. Traffic authorized by the Firewall is passed between bridged interfaces, which forward the traffic over Layer-2. This feature is supported only on standalone gateways.

VoIP Enhancements

New SIP features to enhance VoIP include:

- MGCP NAT support
- MGCP on dynamic ports
- SIP NAT support in a Back-to-Back User Agent (B2BUA) configuration
- Static NAT for SIP Proxy in internal network
- Extended SIP state machine
- Blocked/Allowed SIP commands
- Interoperability with Nortel, Broadsoft, Cisco, NEC, Polycom, Sylanro, Avaya and others

SYN Cookie

A SYN-cookies mode has been added to SYNDefender to prevent a Denial of Service SYN flood attack.

In a SYN flood, external hosts overwhelm a server machine by sending a constant stream of TCP connection requests. The server machine continues to allocate resources until all its resources are exhausted. With SYN cookies, the server machine does not allocate resources until the server's SYN/ACK packets receives an ACK in return, meaning that the original request for a connection was legitimate. Using SYN cookies, the TCP 3-way handshake is performed without saving state information. The connection is not registered in the connection table until the connection proves itself legitimate.

For a server, not saving any state information on an incoming SYN means the server is no longer vulnerable to backlog DoS SYN flood attacks. For a Gateway, this means that processing time spent on spoofed SYN packets is reduced, and memory consumption eliminated.

SYNDefender now has two active modes: **Relay mode** and **SYN Cookie mode**. In relay mode, when a SYN arrives, the connection table registers the connection in the usual way. In cookie mode, the firewall is not informed of the handshake with the external host or client until the client has shown itself to be legitimate. The SYN packet from the client is dropped and a cookied SYN-ACK is sent directly to the client interface. After receiving the ACK from the client, which completes the client handshake, SYNDefender transforms the ACK into a SYN and registers it in the connection table. Processing the connection then proceeds in the same way as Relay mode.

Japanese Language Support for SmartDefense Protections

When SmartConsole detects the underlying operating system to be Japanese enabled, it displays the description pages for each SmartDefense protection in Japanese. This behavior can be controlled via a new property in the database: **gui_client_lang**.

VPN-1 UTM Edge

Edge support for CLM

With VPN-1 UTM Edge you can now select the logs destination. The destination can be the SmartCenter Server or Syslog (a standard logging mechanism in Unix based machines).

Management Plug-ins

NGX R65 introduces an additional infrastructure that enables the use of management plug-ins. The new plug-ins architecture introduces the ability to dynamically add new features and support for new products. Management plug-ins offer central management of gateways and features not supported by your current NGX R65 SmartCenter or Provider-1/SiteManager-1. Management plug-ins supply new and separate packages that consist only of those components necessary for managing new gateway products or specific features, thus avoiding a full upgrade to the next release.

For more information, refer to:

- Internet Security Products Suite Getting Started Guide
- SmartCenter Administration Guide
- Provider-1/SiteManager-1 Administration Guide

or visit:

<http://www.checkpoint.com/nginx/upgrade/plugin/index.html>

Connectra Central Management

NGX R65 is the first version to manage Connectra gateways centrally. This exposes Connectra to much more configuration possibilities than were available in previous versions.

Connectra Tab

SmartDashboard has a new tab for Connectra. All Connectra related configuration is performed using the objects in this tab.

SmartDashboard and SmartDefense Update

The new Connectra tab in SmartDashboard contains a section for SmartDefense and Web Intelligence updates. SmartDefense and Web Intelligence configurations for Connectra are performed as part of “SmartDefense profiles”. A Connectra specific SmartDefense profile is used for all Connectra related SmartDefense and Web Intelligence configuration.

Provider-1 Support

Provider-1/SiteManager-1 now supports Connectra objects (Connectra gateway, Connectra cluster and Connectra cluster members). Provider-1 collects Connectra objects, their statuses, licenses and packages from the CMAs to the MDS, and displays these collected objects in the MDG.

SmartView Monitor

SmartView monitor is now able to monitor Connectra gateways, and generate reports regarding status and activities.

VPN

Same Local IP and Cluster IP Address for VTIs

Ability to configure same local IP and Cluster IP address for VTIs on the same cluster member. This new feature reduces the total amount of IP Address needed in clusters configurations.

Anti-spoofing for Unnumbered Interfaces on IPSO

Support for Anti-Spoofing on unnumbered interfaces on IPSO.

Dynamic Routing and Virtual Tunnel Interfaces

Networks running dynamic routing are now able to work with the remote IP address of Virtual Tunnel Interfaces (VTIs) in clusters.

Configurable Metrics for Dialup Routes

Ability to configure the metric of dialup routes.

Interoperability Between SecurePlatform and IPSO

SecurePlatform gateways employing Virtual Tunnel Interfaces (VTIs) now support the OSPF routing protocol. This enables interoperability between SecurePlatform using numbered VTIs, and unnumbered VTIs on the Nokia/IPSO platform.

Route-based VPN Improvements

When configuring a Route Based VPN, the management gateway can now be located in the encryption domain without having to filter out its IP address from the dynamic routing protocol distribution.

Customer Defined Scripts for VPN peers

A customer scripts are capable of running when a VPN peer no longer participates in a community that has RIM enabled.

Route-based VPN and IP Clustering Support

IP address clustering is supported with route-based VPN on IPSO.

RIM Performance Improvements on IPSO

Performance improvement of RIM when injecting routes on IPSO.

SSL Network Extender

SSL Network Extender:

- Is fully supported on the Microsoft Windows Vista operating system
- Includes the ability to add:
 - **An ICS policy per user group.** The ability to define an integrity Clientless Security (ICS) policy for each individual user group
 - **An Encryption Domain per user group.** The ability to define an encryption domain for each individual user group.
- Has significantly improved connection speed.

ClusterXL

Interface Bonding

Interface bonding enables the creation of a fully meshed redundant topology in High Availability (HA) configurations. In a fully meshed topology, two interfaces on a gateway connect to two switches, one in an active manner and one passively. By bonding the interfaces, they operate as a unit, sharing an IP and MAC address. In the event of a failure in the connection to the active switch, the active interface detects the failure and fails-over to the other bonded interface, attached to the second switch.

Multicast Routing Failover Support

In cluster deployments, the multicast group, source address, and incoming and outgoing interface indexes of multicast traffic are now synchronized among all cluster members. This synchronization provides the ability to maintain multicast sessions in the event of failover. Supported multicast routing protocols are PIM-DM and PIM-SM.

NOKIA IPSO

Anti-virus and Web filtering is now supported on IPSO.

SmartUpdate Enhancements

The license Repository window in SmartUpdate now displays contracts as well as regular licenses. Clicking on a specific contract displays the contracts properties, such as contract ID and expiration date as well as which gateways are covered by the contract.

From the License management window, it is possible to see whether a particular license is associated with one or more contracts.

In addition to retrieving licenses from a gateway, SmartUpdate now checks whether the contract file on the gateway is newer than the contract file on SmartCenter Server. If so, a new menu item enables updated contract information to be installed on the management.

SmartView Monitor

Eventia Correlation Unit and Eventia Analyzer Server

SmartView Monitor can now provide statuses from the Correlation Unit and Eventia Analyzer server.

Correlation Unit status examples:

- is the Eventia Correlation Unit active or inactive
- is the Eventia Correlation Unit connected to the Eventia Analyzer server
- is the Eventia Correlation Unit connected to the log server
- Eventia Correlation Unit and log server connection status
- offline job status
- lack of disk space status

Eventia Analyzer Server status examples:

- last handle event time
- is the Eventia Analyzer Server active or inactive
- a list of correlation units the Eventia Analyzer Server is connected to
- how many events arrived in a specific time period.

The Eventia Correlation Unit should be connected to the log server(s) so that it can read logs. It also needs to be connected to the Eventia Analyzer Server so that it can send events to it. If problems occur in the Eventia Correlation Unit's connection to other components (for example, SIC problems) the problems are reported in the Eventia Correlation Unit's status.

For the same reasons, the Eventia Analyzer server contains statuses that provide information about its connect to all the Eventia Correlation Unit(s) that it is currently connected to.

Anti Virus and Web Filtering

SmartView Monitor can now provide statuses and counters for gateways with Anti Virus and web filtering.

The statuses are divided into the following two categories:

- Current Status
- Update Status (for example, when was the signature update last checked)

Anti Virus statuses are associated with signature checks and web filtering statuses are associated with URLs and categories.

In addition, SmartView Monitor can now run Anti Virus and web filtering counters. For example:

- top five attacks in the last hour
- top 10 attacks since last reset
- top 10 http attacks in the last hour
- HTTP attacks general info
- etc.....

Provider-1/SiteManager-1

SmartView Monitor can now be used to monitor MDSs. This information can be viewed in the Gateway Status View. In this view it is now possible to display Provider-1 counter information (for example, CPU, Overall Status, etc...).

SmartView Tracker

SmartView Tracker now offers the ability to access SmartDefense Advisory information associated with a specific SmartDefense log.

This information can help you analyze your configuration choices and better understand why the specific SmartView Tracker log appeared.

This SmartDefense Advisory feature does not appear for logs that do not contain an Attack Name and/or Attack Information.

Eventia Analyzer

Businesses are faced with many challenges in securing their network environments. One of the primary challenges is the scale of information, which, especially in large organizations, becomes nearly impossible to review and manage. Valuable information typically would only be able to be inferred by correlating information from different sources over time and creating events. Eventia Analyzer, now added to the Check Point Suite of products, resolves these issues by:

1. Collecting, correlating, and consolidating these events in a central repository.
2. Enabling the quick identification of previously undetectable harmful activity through event correlation, which also minimizes the amount of data that needs to be reviewed.
3. Deploying resources on the threats that pose the greatest risk to the business environment.

Eventia Reporter

A number of enhancements have been made to Eventia Reporter in the areas of:

IPv6 Reporting

IPv6 source or destination information will now appear in the report. It is now possible to define an Eventia Reporter filter using an IPv6 address, source and destination.

DNS Implementation

DNS implementation requires less resources and it is possible to control the requests Time Out (refer to the *How To* chapter in the *Eventia Reporter User Guide* for additional information).

Remote License Management

The Eventia Reporter server will now search for the Eventia Reporter license on the Eventia Reporter machine if the license is not found on the Management Server.

Eventia Reporter on Multiple Versions of SmartCenter Management

Eventia Reporter in a Distributed installation can work with multiple versions of SmartCenter Management from R54 and up.

Eventia Reporter can be installed on a Standalone deployment or a Distributed deployment (refer to the Getting Started Guide for additional information). When installed on a Distributed deployment, Eventia Reporter recognizes all the Network Objects in the SmartCenter Management database via an internal process referred to as `dbsync`. With `dbsync` Eventia Reporter can recognize objects from multiple versions (that is, from R54 and up).

Eventia Reporter and Analyzer Integration

Eventia Reporter, Eventia Analyzer Server, and Eventia Coorelation Unit, are located in the same package and can be installed on the same machine.

`evstop` and `evstart` are high level commands used to start and stop the Eventia Reporter and Analyzer.

Working with Multiple Eventia Reporters

In a Distributed installation, more than one Eventia Reporter can be associated with the same SmartCenter Management or Provider-1. When more than one log server is used performance is improved by balancing the load among the different Eventia Reporters. Each instance of Eventia Reporter must be installed on a separate machine.

Result Limitation

Eventia Reporter now enables you to prevent large report outputs by limiting the amount of rows generated by the report.

Integrity Advanced Server

For Integrity 6.6 on the R65 installation CD, the Embedded Datastore now supports up to 2000 concurrent users, removing the need for an external database. Logs, which are now stored on the embedded Check Point Log server, integrate with Check Point and third party reporting tools. (The Check Point log server is a high performance log server that scales to the needs of the most intensive customers. Archiving, backup, and restore is much simpler now with the embedded datastore.) Customers with more than 2,000 concurrent users should continue using Integrity 6.5 till Integrity 7.0 is released.

SecureClient Mobile

SecureClient Mobile is a client for mobile devices that includes a VPN and a firewall. It replaces SecureClient for PocketPCs. The client works on various platforms and enables easy deployment and upgrade.

SecureClient Mobile's VPN is based on SSL (HTTPS) tunneling and enables handheld devices to securely access resources behind Check Point gateways.

The client can be triggered/controlled by 3rd party applications by exporting a programmable and extensible interface.

SecureClient Mobile has the following two modes of operation:

- **Centrally Managed Mode:** The client connects to a gateway configured for SecureClient Mobile, and downloads a set of policies that were sent to the gateway from SmartCenter server. The client enforces these policies.
- **SSL Network Extender Mode:** The client connects to a gateway configured only for SSL Network Extender. In this mode, the client does not download policies, but enforces a set of policies predefined upon client installation. The client works with

any gateway configured for SSL Network Extender Network mode (available on Check Point VPN-1 Pro R55 HF10 versions and above, and on Connectra 2.0 and above).

For additional information on how to configure SSL Network Extender mode on a Check Point VPN-1 Pro gateway, refer to the *VPN User Guide*. For additional information on how to configure SSL Network Extender mode on a Connectra gateway, refer to the *Connectra Web Security Gateway* guide.

SecureClient Mobile is supported on the Windows Mobile 2003/SE/5.0 operating system.

Provider-1/SiteManager-1

- **Management Plug-ins View.** This new View indicates whether a plug-in is activated per Customer, and displays a *Needs Attention* notification for any plug-in that has not been activated properly.
- **Install on Dynamic Objects.** Installs a security policy on dynamic objects.
- **Gateway Function Oriented Global Policy.** Global security rules can now be installed on specific gateways or groups of gateways for a Customer CMA, allowing gateways with different functions to receive different global security rules. When installing global policy to a number of similarly configured CMAs, the relevant global rules are installed to all of the relevant gateways on each CMA.

This feature is particularly useful for enterprise deployments of Provider-1, where Customer CMAs typically represent geographic subdivisions of an enterprise. For example, an enterprise deployment may have Customer CMAs for business units in New York, Boston, and London, and each CMA will be similarly configured, with a gateway (or gateways) to protect a DMZ, and others to protect the perimeter. This new capability allows an administrator to configure the global policy so that certain global security rules are installed to DMZ gateways, wherever they exist, and different rules are installed to the perimeter gateways.

- **Global Manager.** Global Manager is a new type of administrator account in the MDG. With access to Global SmartDashboard, a Global Manager is capable of managing global policies and global objects. For a Global Manager to have additional access to CMA policies, read-write or partial access rights must be specifically assigned.

VPN-1 Power VSX

VPN-1 Power VSX provides the ability to:

- Distribute Virtual Systems on different members of a cluster, effectively spreading the Virtual System traffic load within the cluster, with **ClusterXL Virtual System Load Sharing**.
- Manage the processing power of a VSX machine, with **Resource Control**.
- Control the network quality of service in the VSX network environment, with **Check Point Lightweight QoS Enforcement**.

It also initiates support for a range of network interface cards and servers.