Chapter 1

NGX R65 Operational Changes

Solutions in this chapter:

- New SmartPortal Features
- New FireWall-1/VPN-1 Features
- Edge Support for CLM
- Integrity Advanced Server
- New VPN Features
- ClusterXL

- ☑ Summary
- ☑ Solutions Fast Track
- ☑ Frequently Asked Questions

Introduction

Check Point has come a long way since it was formed more than a decade ago. Check Point's latest major release is the NGX R65. This latest version incorporates features such as built-in antivirus, antispam, URL scanning, attack prevention, and route-based virtual private network (VPN) technology. This book will cover the new features introduced in this latest version.

The NGX R65 adds a significant number of features to the Management platform. In addition, a plug-in system was developed, making it easier to add new products to the SmartConsole suite of Management interfaces. This chapter summarizes the new features introduced since NGX R60.

Tools & Traps…

Service Contracts

Always ensure that you download and install an up-to-date Service Contract File for your SmartCenter Server (SCS). Validation of the systems licensing using the User Center helps you to maintain compliance with the Check Point licensing requirements and thus to stay within the law. Installing the Service Contract File on the SCS will allow it to be transmitted to the other gateways as a part of the upgrade procedure. Contract verification is a fundamental component of the Check Point licensing scheme.

See www.checkpoint.com/ngx/upgrade/contract for additional information on Service Contract Files.

New SmartPortal Features

The Check Point SmartConsole GUI clients have long been a significant competitive advantage for Check Point in the firewall space. Using secure internal communication (SIC), these clients provide a common user interface and communicate with the SCS over an encrypted, authenticated, private channel over any Internet Protocol (IP) network, including the Internet.

Before NGX, anyone who wanted access to the SCS needed to install the GUI clients, a possible problem for organizations with strict configuration management policies or for administrators who couldn't always use their own laptops. SmartPortal was introduced in NGX and allowed the firewall administrator to extend read-only browser-based access to the SCS to people outside the security team and to those on PCs without the GUI clients. It's essentially a secure Web interface into your SCS. NGX R65 added the ability to modify the internal user database so that SmartPortal users can create users and add them to existing user groups. The SmartPortal license is included in the SmartCenter Pro license and the UTM-1 appliances; otherwise, you have to purchase it separately.

Eventia Correlation Unit and Eventia Analyzer Server

SmartView Monitor is able to provide status updates from the Correlation Unit and Eventia Analyzer Server. Correlation Unit status checks include:

- Checking whether the Eventia Correlation Unit is active
- Checking whether the Eventia Correlation Unit is connected to the Eventia Analyzer Server
- Checking whether the Eventia Correlation Unit is connected to the log server
- Reporting on Eventia Correlation Unit and log server connection details and availability
- Monitoring offline job status reports
- Monitoring and reporting on low disk space

You can use Eventia Analyzer Server status to:

- Report the last handle event time that was recorded
- Report whether the Eventia Analyzer Server is active
- Report an inventory of correlation units the Eventia Analyzer Server is connected with
- Display the volume of events received in a selected period

The Eventia Correlation Unit's relation to other components will report trouble with the Eventia Correlation Unit's status. The Eventia Analyzer Server maintains

system status to present information about connections to all Eventia Correlation Unit(s) that are currently associated.

SmartView Tracker

SmartView Tracker offers the ability to contact the SmartDefense Advisory information related to an explicit SmartDefense log. This can help an administrator to appraise configuration options to understand why the specific SmartView Tracker log occurred. SmartDefense's Advisory feature does not exhibit log entries that do not have an attack name and/or attack information.

IPv6 Reporting

IPv6 source or destination information will now display in the report. An administrator can define an Eventia Reporter filter using an IPv6 address, source, and destination.

DNS Implementation

Domain name system (DNS) implementation requires fewer resources. Furthermore, it is possible to control the requests for Time Out.

Remote License Management

The Eventia Reporter Server can 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 is able to integrate with multiple versions of SmartCenter Management from NGX R54 and later.

You can install Eventia Reporter as a stand-alone deployment or a distributed deployment. Eventia Reporter recognizes all the network objects in the SmartCenter Management database via an internal process referred to as *dbsync* when it is installed as a distributed deployment. Eventia Reporter can recognize objects from multiple versions (from NGX R54 and later) using dbsync.

Eventia Reporter and Analyzer Integration

Eventia Reporter, Eventia Analyzer Server, and Eventia Correlation Units are situated in the same package, and you can install them on the same server. You can use the high-level *evstop* and *evstart* commands to stop and start the Eventia Reporter and Analyzer.

Three new content inspection express reports are included with the new version of Eventia Reporter. They are the Anti Virus, Web (URL) Filtering, and Anti Spam reports.

New FireWall-1/VPN-1 Features

VPN technology has been an integral part of firewalls since the late 1990s. With the rise of the Internet in the early 1990s, most firms' first concerns were for a firewall that allowed them safe connectivity between their internal networks and the Internet. Once organizations began to use the Internet to connect separate offices, it became obvious that providing VPN functionality was a natural fit for firewall manufacturers. The fact that network address translator (NAT), IPSec, and antispoof checking have complex interactions has further driven the consolidation of these functionalities into a single perimeter device.

Although VPN technology was initially a separate add-on to FireWall-1, it soon became part of the standard package, and now, with version NGX, the firewall product itself has been renamed *VPN-1 Pro*, for reasons that aren't entirely obvious, given the large mindshare and recognition of the name *FireWall-1*.

NGX offers several new updates and upgrades in VPN functionality.

SmartDefense Profiles

SmartDefense/Web Intelligence is Check Point's way of providing an intelligent defense against attacks directed at open ports as well as a defense against other, more sophisticated types of attacks. Though previous versions of FireWall-1/VPN-1 included early versions of SmartDefense/Web Intelligence, these defenses have been upgraded and improved in NGX.

Because your site may have separate networks that each need a special level of protection, SmartDefense Protection Profiles have been updated and you now can tailor the SmartDefense protection configuration using the precise defenses required for each gateway. You can view the SmartDefense Protection Profiles using SmartPortal.

AMT Support

The NGX R65 now supports Intel Active Management Technology (AMT) for Linux and SecurePlatform to isolate endpoint computers that violate the network security policy. In addition, AMT Quarantine installs a special security policy that restricts inbound and outbound traffic on suspect endpoint hosts that protects the larger network from malicious activity.

Aggressive Aging

Aggressive Aging helps to manage the connections table capacity and memory consumption of the firewall to increase durability and stability. This feature introduces a 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 the set user-defined threshold (or high-water 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 unanticipated traffic such as during a denial of service (DoS) attack.

Cooperative Enforcement

Administrators can ensure that users traversing the firewall are protected by the Integrity endpoint shield. When configuring a Check Point gateway, the administrator identifies whether hosts accessing the network from the internal interface have to be authorized by the Integrity Server. A user not authorized by the Integrity Server receives notification (through the Hypertext Transfer Protocol [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 the Integrity Server 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 deployment mode.

Handling an Unauthorized Host

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

Internal URL Web Filtering

In the 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 (e.g., pornography, illegal software, or spyware) can be blocked.

Web (URL) filtering is based on the SurfControl engine which is now built into Check Point software. This provides for filtering rules based on the organization's needs, predefined categories made up of URLs and patterns of URLs, and a Web filtering database provided by Check Point.

Internal Antivirus Scanning

Since R61, antivirus scanning has been included in the NGX. Enabling antivirus scanning using the CA eSafe engine will allow you to scan an assortment of network protocols, trap them in the kernel, and forward them to the security server, which then transmits the captured files or data to the antivirus engine. The antivirus engine will allow or block data, depending on the reply from the antivirus engine. Antivirus scanning will apply to all traffic that has been permitted using the Security Policy.

SmartView Monitor can now provide statuses and counters for gateways with antivirus and Web filtering. The statuses are divided into the following two categories:

- Current status
- Update status (such as when the signature update was last verified)

Antivirus statuses are associated with signature checks and Web filtering statuses are associated with URLs and categories. SmartView Monitor can also run antivirus and Web filtering counters. For instance, the following reports are available:

- Top five attacks in the past hour
- Top 10 attacks since the last reset
- Top 10 HTTP attacks in the past hour
- General information regarding HTTP attacks

Signature Updates

You can schedule virus signatures to automatically update at any preferred period, or you can start manual updates of virus signatures at any time. Check Point provides antivirus and Web filtering updates. Check Point User Center credentials are necessary for the updates.

Continuous Download

The antivirus engine acts as a proxy, and will cache the scanned file prior to sending it to the client. Continuous Download will trickle data while the antivirus scan is taking place. If a virus is found during the scan, the file transfer is concluded. File types for which Continuous Download will not be used are configurable.

Scanning Files

You can scan files "by direction" or by IP address. In either instance, antivirus scanning will be performed only against traffic that has been permitted through the security rulebase.

Layer 2 Firewalling

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 stand-alone gateways.

VoIP Features

New Session Initiation Protocol (SIP) features to enhance Voice over IP (VoIP) include:

- Media Gateway Control Protocol (MGCP) NAT support
- MGCP on dynamic ports
- SIP NAT support in a Back-to-Back User Agent (B2BUA) configuration
- Static NAT for SIP proxies in the internal network
- Extended SIP state machines
- Blocked/allowed SIP commands
- Interoperability with Nortel, Broadsoft, Cisco, NEC, Polycom, Sylantro, Avaya, and others

SYN Cookies

A SYN-cookies mode has been added to SYNDefender to prevent a DoS SYN flood attack. In a SYN flood, external hosts overwhelm a server machine by sending a constant stream of Transmission Control Protocol (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 receive an ACK in return, meaning that the original request for a connection was legitimate. Using SYN cookies, the TCP three-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 host, 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 is 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 SYN-ACK with a cookie set 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.

Edge Support for CLM

The NGX R65 provides Edge support for the customer log module (CLM). This support will allow the administrator to choose the destination for the logs. The target can be the SCS; syslog is also supported.

Management Plug-In System

The NGX R65 introduces an additional infrastructure that enables the use of management plug-ins. The new plug-in architecture introduces the ability to dynamically add new features and support 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 that are necessary for managing new gateway products or specific features, thus avoiding a full upgrade to the next release.

Connectra Management

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

Connectra Tab

SmartDashboard has a new tab for Connectra. All Connectra-related configurations are performed using the objects in this tab. 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 configurations.

Provider-1 Support

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

SmartView Monitor

SmartView Monitor can monitor Connectra gateways, and produce reports concerning statuses and activities.

Integrity Advanced Server

For Integrity 6.6 on the R65 installation CD, the embedded datastore now supports up to 2,000 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 are much simpler now with the embedded datastore.) Customers with more than 2,000 concurrent users should continue to use Integrity 6.5 until Integrity 7.0 is released.

New VPN Features

NGX offers several new updates and upgrades in VPN functionality. We will discuss some of the new features for VPN support with NGX R65 in the following sections.

Understanding the New VPN Options

Rather than creating individual encryption rules to handle the traffic between VPN terminator gateways, the user need only create a VPN community and then specify the gateways and properties. With NGX R65, Check Point has preserved this useful and simple mental model and has added some additional functionality.

Allowing Directional VPN Rules

Enforcement of VPN rules by direction of connection is now possible. By going to the **Policy | Global Properties | VPN | Advanced** dialog box, you can check the box allowing directional specificity in the VPN element in the rulebase. Whereas in NG AI, directionality in VPN communities was an all-or-nothing proposition, the ability to now specify directionality is useful.

Allowing Backup Links and On-Demand Links

A pair of VPN gateways can now have multiple links between them (say, through multiple Internet service providers [ISPs]), allowing more than one communication path between them. This allows the configuration of back-up links and on-demand links.

Allowing Wire Mode VPN Connectivity

You can now enable VPN connections in NGX as wire mode, reflecting the fact that communications over the VPN are inherently trusted. When you label a connection as wire mode, packets traversing this connection are not inspected by stateful inspection, enabling these connections to successfully fail over. In wire mode, dynamic routing protocols are available for VPN traffic.

Allowing Route-Based VPNs

NGX now supports the Open Shortest Path First/Border Gateway Protocol (OSPF/BGP) for VPN traffic routing. Every tunnel is represented as a virtual adapter, allowing OSPF and BGP traffic to be encapsulated.

Allowing Permanent Tunnels

Permanent tunnels are "nailed-up" connections. This permits more advanced monitoring of VPN traffic through these tunnels, and prevents latency problems for applications that are sensitive to link setup delays.

Same Local IP and Cluster IP Address for VTIs

The NGX R65 provides the capability to arrange the same local IP and cluster IP address for virtual tunnel interfaces (VTIs) on the equivalent cluster member, reducing the total number of IP addresses required in a cluster configuration.

Antispoofing for Unnumbered Interfaces on IPSO

The NGX R65 now provides support for antispoofing on unnumbered interfaces on the Nokia IPSO.

Dynamic Routing and VTIs

The R65 provides support for networks that use dynamic routing to deploy a remote IP address of VTIs in clusters.

Configurable Metrics for Dial-up Routes

The R65 provides the capability to separately configure the metric of dial-up routes.

Interoperability between SecurePlatform and IPSO

SecurePlatform gateways using VTIs can use OSPF as of R65. This provides enhanced interoperability between SecurePlatform using numbered VTIs, and the Nokia/IPSO platform using unnumbered VTIs.

Route-Based VPN Improvements

NGX R65 management gateways may be located in the encryption domain without having to filter out its IP address from the dynamic routing protocol distribution for route-based VPN configurations.

Customer-Defined Scripts for VPN Peers

Customer scripts are capable of running on the R65 in cases where a VPN peer has stopped partaking in a community that has RIM enabled.

Route-Based VPN and IP Clustering Support

The R65 supports IP address clustering with route-based VPN on IPSO.

RIM Performance Improvements on IPSO

The R65 features a performance improvement with RIM for the process of injecting routes on Nokia IPSO.

SSL Extender

The SSL Network Extender (SNX) is now fully supported on the Microsoft Windows Vista operating system. With NGX R65 it provides the capability to add:

- An ICS policy per user group with the facility to characterize an integrity Clientless Security (ICS) policy for each individual user group
- An encryption domain per user group allowing the capacity to describe an encryption domain for each individual user group

The NGX R65 also has a considerably improved connection speed associated with the Secure Sockets Layer (SSL) extender.

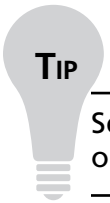
SecureClient Mobile

SecureClient Mobile is a client for mobile devices to add VPN and firewall capabilities. It substitutes for SecureClient for PocketPCs, works on a variety of platforms, facilitates simple deployments, and features an easy upgrade path. SecureClient Mobile's VPN is based on SSL (HTTPS) tunneling and permits handheld systems to connect to resources protected by Check Point gateways in a secure manner. The client can be controlled by third-party applications via a programmable and extensible interface.

SecureClient Mobile operates in the following modes:

- **Centrally managed mode** The client bonds with a gateway configured for SecureClient Mobile, and downloads a set of policies that were sent to the gateway from SCS. The client can then enforce the policies it received.
- **SNX mode** This mode lets a client connect to a gateway configured only for an SNX. The client does not download policies in this mode, but will implement a set of policies that were loaded upon client installation. It can

integrate with any gateway configured to provide SNX network mode. This mode is supported by Check Point VPN-1 Pro R55 HF10 versions and later, and on Connectra 2.0 and later.



TIP

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

ClusterXL

In this section, we'll discuss interface bonding and multicast routing failover support.

Interface Bonding

Interface bonding facilitates the construction of a redundant, fully meshed topology in High Availability mode configurations. A fully meshed topology requires two interfaces on a gateway that attach to two switches (one active and one passive). This bonds the interfaces, letting them operate as a unit, sharing an IP and Media Access Control (MAC) address. If a failure occurs on the active switch connection, the active interface senses the failure and will fail over to the supplementary bonded interface that is connected to the second switch.

Multicast Routing Failover Support

The Multicast group, source address, and incoming and outgoing interface indexes of Multicast traffic are synchronized among all cluster members for cluster deployments in the NGX R65. This synchronization provides the capacity to continue Multicast sessions if a failover condition occurs. The NGX R65 supports PIM-DM and PIM-SM Multicast routing protocols.

Summary

Check Point releases a major upgrade to its core VPN-1 product every two or three years, and version NGX R65 is the latest in this line.

SmartDefense and Web Intelligence have received moderate upgrades in the NGX R65. This is still a fascinating set of tools for the network security administrator to understand and configure against all sorts of higher-level attacks.

Eventia Reporter provides a way to tackle those large and growing log files and provide detailed, informative reports and traffic analysis.

VPN functionality has seen significant improvements and now delivers on the full promise of the enhanced community-based VPNs we saw in the previous version.

SecurePlatform continues to evolve and improve. The product line is now split, with the addition of SecurePlatform Pro, which offers dynamic routing and support for Remote Authentication Dial-in User Service (RADIUS) authentication for firewall administrators. Dynamic routing adds some risk and some complexity, and is now available to those larger organizations that wish to more fully integrate the underlying router in their Check Point firewalls into their existing dynamic routing configuration.

Solutions Fast Track

New SmartPortal Features

- ☑ SmartPortal allows the firewall administrator to extend browser-based access to the SCS to persons outside the security team and to those on PCs without the GUI clients.
- ☑ SmartPortal is essentially a secure Web interface into your SCS for viewing policies and logs.
- ☑ You can install SmartPortal either on a dedicated server or on the SCS itself.
- ☑ With SmartPortal, you can limit access to specific IP addresses.

New FireWall-1/VPN-1 Features

- ☑ The "Hacker versus Firewall" arms race has moved up the stack to a higher level.
- ☑ SmartDefense and Web Intelligence have capabilities in three broad categories: defense against attacks, implicit defenses, and abnormal-behavior analysis.

- ☑ The SmartDefense Service is an annual subscription service that provides ongoing and real-time updates and configuration advisories.

Edge Support for CLM

- ☑ The NGX R65 provides Edge support for the customer log module (CLM). This support will allow the administrator to choose the destination for the logs.
- ☑ The NGX R65 introduces an additional infrastructure that enables the use of management plug-ins.
- ☑ The NGX R65 is the first version to manage Connectra gateways centrally.

Integrity Advanced Server

- ☑ For Integrity 6.6 on the R65 installation CD, the embedded datastore now supports up to 2,000 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.
- ☑ Customers with more than 2,000 concurrent users should continue to use Integrity 6.5 until Integrity 7.0 is released.

New VPN Features

- ☑ Rather than creating individual encryption rules to handle the traffic between VPN terminator gateways, the user need only create a VPN community and then specify the gateways and properties. With NGX R65, Check Point has preserved this useful and simple mental model and has added some additional functionality.
- ☑ Enforcement of VPN rules by direction of connection is now possible.
- ☑ You can now enable VPN connections in NGX as wire mode, reflecting the fact that communications over the VPN are inherently trusted.

ClusterXL

- ☑ Interface bonding facilitates the construction of a redundant, fully meshed topology in High Availability mode configurations.

- ☑ If a failure occurs on the active switch connection, the active interface senses the failure and will fail over to the supplementary bonded interface that is connected to the second switch.
- ☑ The Multicast group, source address, and incoming and outgoing interface indexes of Multicast traffic are synchronized among all cluster members for cluster deployments in the NGX R65.

Frequently Asked Questions

Q: Limiting access to specific IP addresses was always an important part of two-factor security with SmartConsole clients. Can I do that with SmartPortal?

A: Yes, limiting access to specific IP addresses is retained in the new interface. You can configure this by creating or editing the hosts.allowed file on the SmartPortal Server.

Q: Where do I install the SmartPortal Server?

A: You can install SmartPortal either on a dedicated server or on the SCS itself.

Q: Which Web browsers are compatible with SmartPortal?

A: SmartPortal is compatible with these browsers:

- Internet Explorer
- Mozilla
- Firefox
- Netscape

The only other requirements are that you enable JavaScript and disable pop-up blockers.

Q: Is a SmartDefense Services subscription required to use SmartDefense or Web Intelligence?

A: No. SmartDefense and Web Intelligence are built in. You need the subscription only to get real-time updates and configuration advisories.

Q: I don't see where in my rulebase I can select SmartDefense. Where is it?

A: SmartDefense and Web Intelligence are configured on their own tabs within SmartDashboard.

Q: What types of defenses does SmartDefense/Web Intelligence provide?

A: SmartDefense/Web Intelligence provides defenses against attacks, implicit defenses, and abnormal-behavior analysis.

Q: What type of objects can be cloned?

A: Only network and host objects can be cloned, but that's a good start.

Q: Do I need a separate license for SecurePlatform?

A: No. SecurePlatform (the regular version) is free. SecurePlatform Pro requires a separate, additional license.