

## Frequently Asked Questions on the NGX Platform

[General Questions](#)

[Upgrade Questions](#)

[Voice over IP \(VoIP\) Questions](#)

[Advanced Routing Questions](#)

[SMART Management Questions](#)

[NGX Training and Support](#)

### General Questions

#### **What is NGX?**

NGX is the latest security software platform for Check Point firewall, VPN and management solutions. The NGX platform is the only security platform that delivers a unified security architecture for internal, perimeter and Web security. This unified security architecture enables enterprises of all sizes to reduce the cost and complexity of security management and ensure that their security systems can be easily extended to adapt to new and evolving threats.

With the addition of Integrity management functionality to the Check Point unified security architecture, Check Point is the first to deliver unified management across the most critical layers of network security via a single console, increasing the efficiency of enterprise-wide security administration for Check Point customers. Security departments now have total visibility and control of perimeter, internal, Web and endpoint security from a single management system.

#### **What Check Point products are enhanced by the NGX platform release?**

The NGX platform delivers new features and extended functionality to over twenty Check Point products, add-on components and core technologies. This includes VPN-1, VPN-1 UTM (Express/Express CI), VPN-1 Power, SmartCenter (SmartConsole GUI + SmartCenter Server, SmartPortal, SmartView Monitor, Eventia Reporter, SmartLSM), Provider-1, SSL Network Extender, Integrity, SecuRemote, SecureClient, UserAuthority, SecureXL, Application Intelligence and Web Intelligence. In addition, management enhancements in SmartCenter NGX also make management easier for VPN-1 UTM Edge, VSX, FireWall-1 GX and Connectra gateways.

For a complete list of the Check Point products supported on the NGX platform and new features and functionality, see our [NGX Info Center](#) with Release Notes, User Guides, What's New, and more.

#### **What are the key new features of the NGX platform?**

The NGX platform provides hundreds of new features and extended functionality for Check Point perimeter, internal and Web security solutions. Some of the more notable enhancements include:

##### **Unified management for Perimeter, Internal, Web and endpoint security**

SmartCenter NGX is the only centralized management solution for perimeter, internal, Web and endpoint security. Security administrators can now manage VPN-1, VPN-1 UTM Edge, Integrity, Connectra and InterSpect gateways all from a single console.

##### **Expanded intelligent inspection technologies**

The NGX platform delivers significant defenses for SmartDefense, Application Intelligence and Web Intelligence, providing organizations with the most advanced protection from the latest

and most sophisticated threats. This includes comprehensive inspection and security for Voice over IP (VoIP), including the only VoIP security solution to provide Denial of Service (DoS) protection for all the major VoIP protocols (H.323, SIP, MGCP and SCCP (Skinny)). The NGX platform also adds protections for MS RPC, DNS Security, Email Security, and Peer-to-Peer (P2P) (for non-Web traffic) to state of the art Application Intelligence technology.

**Advanced VPN capabilities, including support for dynamic routing protocols**

VPN-1 Power (VPN-1 Pro) now includes advanced capabilities such as dynamic routing via VPN tunnels and Route based VPNs, dramatically simplifying network management in a distributed and dynamically changing network topology.

**Universal, real-time security updates from a single console without interruption**

A unified console for all SmartDefense Services allows businesses to deal with newly discovered security threats quickly and comprehensively, while global SmartDefense updates for Provider-1 enables service providers and large enterprises to easily push policies to end users. SmartDefense profiles, which allow administrators to set different defense settings for different gateways, can be centrally-managed and applied through the SmartDashboard. Administrators also now have a centralized means of updating integrated antivirus functionality found in Check Point's VPN-1 UTM (Express/Express CI) and VPN-1 UTM Edge products, giving them greater control and ensuring cohesive security policies.

For a complete list of features and capabilities of the NGX platform, please visit our [NGX Info Center](#).

**Can I manage the new security features of VPN-1 UTM Edge with SmartCenter?**

Yes, beginning with the NGX R61 release you can centrally manage the antivirus and SmartDefense intrusion prevention features of VPN-1 UTM Edge using SmartCenter NGX.

**On what operating system platforms can the NGX products be installed?**

NGX products are available on the following operating systems: SecurePlatform/SecurePlatform Pro, Windows (2000, 2003, XP) Red Hat Linux (3.0), Sun Solaris 8, 9, and 10, and Nokia IPSO (3.9 and 4.0). For specifics on supported platforms for individual products, please see the compatibility table at our [NGX Info Center](#) or in the "*Check Point NGX Release Notes*".

**What does the "X" stand for in NGX? Is this a totally different product from NG with Application Intelligence? If not, why the new name?**

First, it is important to note that NGX is not a product, but a security software platform that delivers a unified security architecture across Check Point perimeter, internal and Web security solutions. The NGX platform is the successor to the Next Generation (NG) platform.

This new platform is called NGX because it is an "eXtension" to the robust, secure and reliable NG platform that is the basis of the network security defenses for tens of thousands of enterprises. We did not re-architect a new platform – instead we extended an already robust and reliable security platform across our product line, enabling unified management and embedding the most intelligent security technologies across our perimeter, internal and Web security solutions.

With the NGX platform, Check Point customers can enforce security policy with the industry's most intelligent security solutions wherever it is needed in their network in a way that is consistent, cost-effective and easy to manage.

**On what OPSEC platforms is NGX available?**

Check Point hardware partners have released a number of NGX products, including Nokia, Sun, Crossbeam and Nortel. For a complete list of OPSEC partners and products please visit the [OPSEC site](#) and find the solution that's right for you.

### **What NGX releases are available?**

The NGX platform was first announced as the R60 release in May 2005, followed by R60a release which added support for Check Point VPN-1 VSX and Check Point VPN-1 UTM (Express/Express CI) to the NGX platform. The NGX R61 release was announced and published in April 2006. The NGX R62 release was announced and published in October 2006. The NGX R65 release was announced and published in March 2007

### **How has the NGX release been received?**

The NGX release has been an incredible success so far. An informal survey we conducted in November 2005 showed that over 50% of our customers had already upgraded to the NGX platform or were planning their upgrade – an incredible achievement for just six months after NGX was first announced.

### **What's the difference between NGX (R60), NGX (R61), NGX (R62) and NGX (R65)?**

The NGX R61 release extends Check Point's vision for unified security architecture with the integration of endpoint security with Check Point's perimeter, internal and web security gateway solutions, as well as integrated SmartDefense Services with SmartCenter and Provider-1.

Customers can now centrally manage perimeter, internal, Web and end-point security and perform advanced security and network logging, monitoring and reporting—all via a single console – making Check Point the first to deliver unified management across the most critical layers of network security.

The NGX R62 release allows for expanded flexibility and granularity of defenses by introducing SmartDefense profiles. With this release, organizations can define multiple SmartDefense profiles and associate them with different Check Point gateways. This allows each gateway to have different defense settings and SmartDefense attributes. All profiles on all gateways can be centrally-managed through the SmartDashboard.

The NGX R65 release provides for enhanced performance with throughput up to 12 Gbps for VPN-1 Power running on an open server. It also extends the Unified Security Architecture by providing a management plug-in architecture, enabling administrators to quickly add new management functionality without performing a complete upgrade. Customers can now also incorporate their VPN-1 gateways into their network access control strategies, with improved support for Integrity cooperative enforcement and integration with Intel vPro technologies.

### **How do I order the NGX release?**

You can order your NGX Media Kit through your Channel Partner or directly through our "[Get Secure](#)" web site, where you can select the Media Kit you want and even request immediate delivery.

### **Which NGX Media Kit should I order? What's the difference?**

Beginning with the NGX R61 release, the NGX Media Kit is packaged as two different kits containing product installations, guides and tools for use and evaluation.

#### **You should order the "*High End Security Suite*" if you have any of the following:**

- Provider-1
- Security Management Portal (SMP)
- VPN-1 VSX

You should order the "*Internet Security Suite*" if you have any of the following:

**Clients**

- VPN-1 SecureClient
- SSL Network Extender
- SmartConsole
- Integrity Agent
- Integrity Flex
- Integrity Desktop
- Integrity SecureClient
- Integrity Clientless

**Security Solutions**

- FireWall-1
- VPN-1
- VPN-1 Power (VPN-1 Pro)
- VPN-1 UTM (Express/Express CI)
- SmartDefense
- Integrity
- Web Intelligence
- SSL Extender Server
- Provider-1

**Management Solutions**

- SmartCenter
- SmartCenter Pro
- SmartCenter Express
- Eventia Reporter
- SmartView Monitor
- SmartLSM
- SmartPortal

## Upgrade Questions

### Why should I upgrade my Check Point products to NGX versions?

There are several very good reasons why you should upgrade your Check Point products to NGX versions, including any one of our top ten reasons below:

- Simplify management of diverse security solutions using one unified management console
- Implement real-time security updates from a single, unified console without interruption
- Advanced intrusion prevention and antivirus protection for remote sites
- Simple deployment of firewall, VPN, intrusion prevention, and antivirus in less than 5 minutes
- Ensure confidentiality and availability of VoIP communications
- Gain better insights into network and security operational status
- Leverage dynamic routing and multicast protocols in a VPN environment
- Quickly and easily increase remote access for employees
- Increase security against new, evolving attacks
- Protect Web applications against advanced hacking techniques
- Increase security performance
- Simplify VPN deployments with route-based VPNs
- Increase visibility of security policies for non-administrative workers

For more information about upgrading to the NGX platform, please visit the [NGX Upgrade Portal](#).

### Do I have to upgrade my entire Check Point environment to NGX all at once?

No. The NGX platform is backwards compatible with NG versions (FP3 and later) so you can plan your upgrade in phases, depending on specific needs. For example, you could first choose to upgrade your SmartCenter server and upgrade the Enforcement Modules later at your convenience. Whatever your needs you can choose from numerous upgrade scenarios described on our [NGX Upgrade Portal](#) or refer to the "*Check Point NGX Upgrade Guide*" document for detailed step-by-step instructions.

### What is required to upgrade to an NGX version from a previous version (NG - R55, R54, etc.)? Is this upgrade free?

Customers with a valid support contract that includes software upgrades, such as Enterprise Software Subscription, are entitled to upgrade to NGX versions free of charge with only the cost of delivery.

To find out your status and upgrade eligibility, log into your Check Point [User Center account](#) or request status and a quote from your local Check Point partner.

### If I want to upgrade to an NGX version of SmartCenter, can I manage previous versions of Check Point VPN gateways and firewalls (FireWall-1 NG, VPN-1 NG, etc.)?

SmartCenter NGX can manage VPN-1/FireWall-1 NG gateways that have Feature Pack 3 or later (including R55W) installed, VPN-1 UTM Edge, Connectra 2.0, InterSpect 2.0, FireWall-1 GX 2.5, Integrity and VPN-1 VSX gateways.

For a complete list of backwards compatibility and upgradeable products, please visit our [NGX Upgrade Portal](#) or refer to the "*Check Point NGX Upgrade Guide*" document for detailed information.

### What are the requirements for upgrading to the NGX platform? Should I plan to upgrade my hardware before I upgrade?

We recommend that you evaluate your current hardware before any upgrade to ensure optimal performance. To help you evaluate your hardware we've outlined the requirements for each NGX product, based on the operating system, in our [NGX Upgrade Portal](#) and in the "*Check Point NGX Upgrade Guide*".

### **What should I do to upgrade from NG to NGX platform?**

Customers who have version NG FP3 or above installed and would like to upgrade to NGX (R60 and above) will first need to upgrade their NG licenses to NGX licenses. The NGX release will not function with licenses from previous versions.

*Note: You should first complete the license upgrade before you start the actual software upgrade.*

To upgrade your licenses using the "license\_upgrade" utility:

- The "license\_upgrade" utility can be found on each of the NGX CDs, in the **Actions** folder. *Note that this utility is OS dependent.*
- The "license\_upgrade" utility upgrades all relevant licenses and makes them available during the software upgrade. The "license\_upgrade" utility does not upgrade evaluation licenses, temporary licenses, or invalid licenses (licenses that are "old" or that have been "moved" to a new IP address).
- You can simulate the license upgrade process by running the "license\_upgrade" utility on your SmartCenter and selecting the **Simulate** option.

NGX licenses are available for all products that are covered by a valid Support Program or Software Subscription. Log into your Check Point [User Center account](#) to verify your status and upgrade eligibility, or request a quote from your local Check Point partner.

For more details on License Upgrading, see the Upgrade Guide located on the NGX CD and at the [Check Point download site](#).

### **I've already upgraded to NGX R60 and applied Hot Fixes, such as R60 HFA\_02. What is the upgrade path to NGX R65? Will I lose any functionality?**

The NGX R65 release contains all of the features and functionality of the previous releases and subsequent Hot Fixes, so you will not lose any features or functionality by upgrading to NGX R65.

If you're currently on the NGX platform you have a direct upgrade path to NGX R65, regardless of which Hot Fixes you've applied.

### **Does upgrading to the NGX R65 release involve a license upgrade as well?**

A license upgrade is required if you're upgrading from the NG platform to the NGX platform, but not required if you're upgrading from one NGX release to another.

### **What has Check Point done to ensure that upgrading to the NGX platform will be smooth?**

Check Point has developed essential upgrade tools, utilities, and step-by-step instructions to make the NGX upgrade as easy and smooth as possible, including:

[NGX license upgrade tool](#) - New for the NGX platform, this tool can automatically simulate a license upgrade and identify potential issues – and recommended solutions – before upgrading to the NGX platform.

[NGX Upgrade Guide](#) – This provides an overview of the NGX platform with essential step-by-step instructions on upgrading Check Point products to NGX versions on every hardware platform and for most common scenarios.

Check Point has consolidated these tools with important upgrade information into our [NGX Upgrade Center](#) available on the Check Point public Web site, creating a central place to go for all the information needed to plan and implement upgrading to the NGX platform.

### **What tools are available for upgrading to the NGX R65 release?**

You'll find the same tools available for upgrading to NGX R65 platform that were available to upgrade to previous NGX releases, including:

- post\_upgrade\_verifier
- upgrade\_export
- verify\_package
- updates\_download\_helper
- upgrade\_import
- pre\_upgrade\_verifier
- license\_upgrade

You'll find all of these tools as well as detailed instructions, step-by-step guides, and more on the NGX Media Kit and online at our in our [NGX Upgrade Portal](#).

### **What if I want help implementing the NGX release?**

Check Point Professional Services offers an "NGX JumpStart" package specifically designed to accelerate and ensure the success of implementing the NGX release, with dedicated onsite, expert assistance from our Professional Services consultants. Our experts follow proven methodologies to plan, design, implement, review, and tune the NGX release to meet your specific needs and help you maximize benefits ROI of your Check Point solutions. Learn more and request a quote at our [Professional Services Web site](#).

### **How do I obtain more information about purchasing or upgrading to NGX?**

You can find more information about upgrading to NGX versions with our [NGX Upgrade Portal](#), including Release Notes, User Guides, Media Kits, and more.

We also encourage you to contact your local Check Point partner and discuss your goals and needs, and available options and services available to ensure a smooth and successful upgrade. To locate a Check Point solution provider in your area, go to our [Partner Locator](#).

### **Is Real-Time Monitoring included as part of Eventia Reporter?**

Yes, the NGX R61 release adds Real-Time Monitoring capabilities to Eventia Reporter, similar to what was already available for SmartView Reporter & Monitor.

### **Can SmartUpdate NGX upgrade gateways that are at a previous NGX release?**

Yes. For example, SmartUpdate NGX on the R61 release can upgrade gateways using the NGX R60 release, providing backward compatibility and management from a central location.

## **Voice over IP (VoIP) Questions**

### **What are the security issues surrounding VoIP? What kind of deployment challenges are customers facing?**

Since VoIP is an IP based protocol it carries with it the same challenges of securing IP and carries similar risks. Beyond this, VoIP presents some additional challenges due to its varying protocols, multiple communication channels, and varied deployment options. These complexities, if not addressed, can create new opportunities for exploitation.

### **Don't firewalls present challenges in converged voice/data networks? If so, what has Check Point done to address these challenges?**

One of the obstacles to VoIP implementation in the past has been the firewall. Traditional network firewalls were only designed for data applications, so some have had problems handling real-time applications like VoIP, especially in dealing with Network Address Translation (NAT) and VoIP signaling. Since Check Point FireWall-1 is application-aware, understands VoIP protocols and signaling, and supports NAT in VoIP scenarios, Check Point firewalls enable VoIP traffic converged with data traffic while ensuring a high Quality of Service (QoS) for VoIP traffic (real-time delivery, short delay, low jitter and low packet loss across networks).

### **What additional security do I need to ensure the confidentiality, integrity and availability of my VoIP communications?**

Since VoIP traffic is converged with data traffic traveling over IP networks, VoIP is susceptible to many of the same threats as data traffic. To combat this, VPN-1 Power (VPN-1 Pro) secures VoIP networks by protecting against all common threats to VoIP traffic. These threats include call hijacking, where calls intended for the receiver are redirected to someone else, call theft, where the caller pretends to be someone else, and network hacking using ports opened for VoIP connections. Other threats are Denial of Service (DoS) attacks, in which attackers send malformed or fragmented packets.

### **What do the VoIP attacks look like? What is the result?**

Some of the most common attacks include:

- **Denial of Service** -- This attack is targeted at dramatically slowing network performance and can potentially shut down both voice AND data communications. It can also create buffer overflows, in order to compromise systems.
- **Voice Services Theft** -- Hackers use a variety of techniques to obtain free unauthorized telephone calls that many times end up getting billed as company VoIP usage. These attacks can potentially go unnoticed but have direct impact on an organization's bottom line.
- **Voice System Hijacking** -- Malicious users remotely manage devices, change settings, and even eavesdrop on phone conversations. Besides the havoc this attack wreaks on the actual VoIP system and voice communications, it presents a significant security risk for companies in terms of confidential data loss.

### **Are customers currently deploying VoIP or is it still in the pilot phase? What is the hindrance to customers deploying VoIP?**

Actual deployments are happening at a rapid pace. In-Stat/MDR reports that the overall percentage of companies using VoIP communications quadrupled in the past year, growing from 3 percent in 2003 to 12 percent in 2004, and showed substantially higher growth rates among larger enterprises. By the end of 2004, VoIP penetration reached 34 percent among mid-sized businesses, and 43 percent in the large business segment.

### **Will the firewall add noticeable latency to VoIP or introduce increased QoS issues? Is scalability an issue?**

No. From the firewall's perspective, VoIP is simply another set of protocols that must be examined, so there is no abnormal load on the firewall or associated latency when examining VoIP traffic.

Furthermore, in terms of VoIP QoS, since the firewall is focused on call setup and call termination (points of exploitation), the majority of the processing and overhead will occur at these points and not during the actual call when the user would be sensitive to added latency. The net effect of this is a largely transparent experience for the user.

### **Where should firewalls be positioned in a VoIP deployment?**

There are three main ways to position VoIP components. They can be placed on the internal network, placed in the DMZ, or divided between the two. Different scenarios present a trade off between security and ease of deployment. Ideally, it is recommended that external facing equipment be placed in the DMZ with the rest of the equipment placed on the internal network. This solution is the most secure, but can present a challenge in terms of synchronizing the internal and external systems.

#### **Where can I learn more about VoIP security available with Check Point NGX?**

Visit our online resource, "[VoIP Security without the Nightmares](#)", containing everything you need to know about VoIP security available with Check Point NGX, including a security checklist, Whitepapers, featured solutions, and more.

## **Advanced Routing Questions**

### **What are the new advanced routing features delivered with the NGX release? Which products include dynamic routing?**

The NGX platform delivers advanced VPN routing capabilities such as dynamic routing to allow enterprises to manage scalable, fault-tolerant, and secure VPN networks more efficiently with fewer resources. Specifically, the following new advanced VPN features have been added to VPN-1:

**Dynamic routing** -- Check Point now supports Dynamic Routing through VPN tunnels – supporting the most popular protocols for both unicast and multicast traffic -- as an integral part of SecurePlatform Pro.

**Route based VPN** -- VPN-1 enables route-based VPNs, in which the VPN topology is delegated to network routing decisions. Such flexibility gives enterprises a powerful mechanism for providing connectivity in complex and dynamic networks.

**Enhanced VPN Tunnel Management** -- Permanent Tunnels can be established and monitored in real-time via SmartView Monitor NGX, ensuring VPN tunnels are always active. Other VPN enhancements in the NGX release include: Directional VPN Rule Match, Multiple Entry Points, Route Injection Mechanism and Wire Mode.

Dynamic routing is supported on SecurePlatform Pro. Nokia and Crossbeam "Secured by Check Point" appliances also include dynamic routing functionality. For specifics on their offerings please see those vendors' product specifications.

### **Why has Check Point done this – given Check Point's historic positioning that security is a separate discipline from running the network?**

Check Point, unlike its main competition in the firewall/VPN markets, continues to be focused on security. And Check Point is the worldwide leader in the firewall and VPN market.

Check Point has integrated dynamic routing protocols into its VPN-1 suite in order to help its customers ensure uninterrupted VPN connectivity with little to no manual intervention. Integrating dynamic routing with VPNs is an important part of ensuring non-stop connectivity.

Large networks are often managed with dynamic routing protocols that allow automatic propagation of routing information, and make it possible to set up redundant links. Integrating dynamic routing protocols with VPNs reduces the overhead of configuring a large number of routers, and enables the VPN to automatically choose an alternate VPN tunnel in the event a connection goes down.

In addition, integrating support for multicast protocols with VPN gateways will enable enterprises to efficiently and effectively manage multicast traffic.

#### **What routing protocols are supported in SecurePlatform Pro?**

Check Point has embedded routing software in its Secure Platform (SPLAT) Pro— a pre-hardened operating system that is a foundation for its VPN-1 gateways. Protocols supported include RIP (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol), IGMP (Internet Group Management Protocol), PIM-SM (Protocol Independent Multicast-Sparse Mode), and PIM-DM (PIM-Dense Mode) protocols.

The base unicast protocols (RIP and OSPF) will enable simple dynamic routing around network failures with one service provider. BGP will typically be required when a site is connected to two or more different service providers for reliability, redundancy, or high availability purposes. The multicast protocols (IGMP, PIM-SM, PIM-DM) will enable enterprises to efficiently and effectively manage multicast data feeds, such as stock ticker tape or videoconferencing feeds, into their organizations, across the firewalls and de-militarized zones.

#### **Are routing protocols in Check Point products interoperable with router vendors?**

Yes. Dynamic routing protocols embedded in SecurePlatform Pro conform to relevant industry standards and have been tested and are fully interoperable with products from leading routing vendors such as Cisco.

## **SMART Management Questions**

#### **What is SmartPortal?**

SmartPortal is a Web-based management portal that extends browser-based access to SmartCenter and Provider-1. With SmartPortal, the security team can extend browser-based access to outside groups such as technical support staff or auditors, yet maintain centralized control of policy enforcement. SmartPortal users can view security policies and status of Check Point products, as well as administrator audit trails. Advanced users can be given administrator management permissions. This extended functionality facilitates team coordination in mitigating attacks or troubleshooting network and security issues.

#### **Is SmartPortal available for Provider-1?**

Yes. SmartPortal is available with Provider-1 NGX and provides web-based access at the Multi-domain Server (MDS) and Customer Management Add-On (CMA) levels.

#### **What Check Point gateways can be managed via SmartCenter NGX?**

SmartCenter NGX can manage all VPN-1/FireWall-1 NG gateways (including R55W), VPN-1 UTM Edge, Connectra 2.0, Integrity, InterSpect 2.0, FireWall-1 GX 2.5 and VPN-1 VSX gateways. For a complete list of backwards compatibility and upgradeable products, please see our [NGX Info Center](#) or refer to the "*Check Point NGX Release Notes*" for detailed information.

#### **Is SmartPortal only a stand-alone product, or is it included in any other SMART management products?**

SmartPortal is included in SmartCenter Pro and SmartCenter Express Plus, and can also be purchased as an add-on management application for an unlimited number of gateways. Contact your local Check Point reseller for pricing and to request a quote.

### **What centralized management does SmartCenter NGX provide for Connectra gateways?**

In SmartCenter NGX administrators will be able to create objects for Connectra gateways in the SmartDashboard, centrally manage and distribute SmartUpdate and SmartDefense Services updates, and monitor the performance and security state of Connectra traffic via integrated logs.

### **What centralized management does SmartCenter NGX provide for InterSpect gateways?**

Similar to Connectra, from the SmartDashboard, administrators can create InterSpect objects, launch administration sessions for each InterSpect gateway, perform SmartDefense dynamic updates for all or some InterSpect devices, and monitor the performance and security state of InterSpect traffic.

### **Is Integrity management also integrated with SmartCenter NGX?**

With the NGX R61 release SmartCenter NGX can now manage Integrity from same console, on the same server, and by the same administrators who manage other Check Point products including:

- Integrity UI launched from SmartDashboard
- Integrity server can be installed via the same CD.
- SmartCenter and Integrity servers now share the same administrator definitions.
- Endpoint logs are displayed in SmartView Tracker.
- Eventia Reporter introduces special Integrity reports on endpoint entities.
- Integrity status is displayed in SmartView Monitor.

For a complete list of features available for Integrity please see the release notes and “what’s new” documentation online.

### **What are the key benefits of centralized management with SmartCenter NGX?**

The key benefits of SmartCenter NGX are really summarized in two points:

**Lower costs** – Simplified enterprise security management using a single, unified management console lowers IT costs by eliminating the need for separate management log-ins, servers, and reports.

**Accurate, effective security policies** – Using the centralized management and same core technologies to configure and manage security policies means Administrators are already familiar with how to configure and manage policies for endpoint security. This increases the accuracy and effectiveness of security policies to combat the more than 50% of security breaches due to misconfigurations seen by companies today.

### **Can SmartCenter unified management also manage OPSEC partner applications?**

OPSEC devices and applications can be defined as objects within SmartDashboard and can also be used in the rule base.

### **What are the key features in the NGX releases for SmartDefense Services?**

With the NGX R61 release you can easily review, accept and add new defenses (even for new applications and protocols) without going through an OS upgrade or bringing your system offline.

Not only can you extend your enforcement points to adapt to new and evolving threats in real-time, but you’ll see better overall TCO from eliminating the need to buy, implement, and manage separate firewall and IPS solutions for all layers of your network.

The NGX R62 release builds upon the above features and adds SmartDefense profiles, which allow for expanded flexibility and granularity of defenses. SmartDefense profiles allow each gateway to have different defense settings and SmartDefense attributes. All profiles on all gateways can be centrally-managed through the SmartDashboard.

## NGX Training and Support

### **I already have CCSA or CCSE certification. Do I need to get certified on NGX?**

Yes, we recommend that anyone who is planning to implement or upgrade to NGX get trained and certified on Check Point NGX. Training and certification gives you the critical skills, knowledge, and hands-on experience you need to maximize the security, features, and benefits of the NGX platform.

### **What courses are available? Which one should I take?**

If you're CCSE NG certified you should attend our 2-day [Accelerated CCSE NGX](#) course, which covers upgrading to NGX, new features, and essential knowledge to prepare you for the CCSE NGX exam and certification.

If you're not CCSE NG certified you'll need to register for [CCSA NGX or CCSE NGX courses](#), and pass the exams to be certified on NGX. Updating your certification to NGX proves you have the skills and knowledge to maximize the benefits of NGX, increasing your professional standing and worth.

### **Where can I get trained on NGX?**

To learn more about NGX courses and certifications, or find a qualified ATC, visit the [Education Services Web site](#).

### **How long will Check Point continue supporting the NG release?**

Customers with active Enterprise Support contracts will continue to receive unlimited support for all of their Check Point products, no matter what release they are using, well after the announcement of the NGX platform. We encourage customers currently using the NG release to begin planning their upgrades to the NGX platform as soon as possible, to take advantage of all the benefits available and ensure maximum security.