



The NGX Platform

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 perimeter, internal 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.

When will NGX be available?

The NGX versions of 16 Check Point products will be available in May, 2005. NGX Upgrade Packs and Evaluation Kits are available for order on May 16, 2005 from the Check Point public Web site. For a complete list of NGX compatible products, please visit the NGX Upgrade Portal at <http://www.checkpoint.com/ngx/upgrade>.

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

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

For a complete list of the Check Point products supported on the NGX platform, please see the “Getting Started Guide: NGX: R60” or visit the NGX Upgrade Portal at <http://www.checkpoint.com/ngx/upgrade>.

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 and Web security gateways**

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

- **Expanded intelligent inspection technologies**

The NGX platform delivers significant new 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), serving as the only VoIP security solution to provide Denial of Service (DoS) protection for all the major VoIP protocols, including H.323, SIP, MGCP and SCCP (Skinny). The NGX platform also adds to Application Intelligence technology new protections for MS RPC, DNS, Email, and Peer-to-Peer (P2P) (for non-Web traffic) applications.

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

VPN-1 Pro NGX 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.

For a complete list of the hundreds of new features delivered in the NGX platform release, please visit <http://www.checkpoint.com/ngx/upgrade> .

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 (32/64 bit), Solaris 9 (64 bit). NGX will be available on Nokia IPSO (3.9) in June. For specifics on supported platforms for individual products, please see the compatibility table in the “Getting Started Guide: NGX: R60” or the NGX Upgrade Portal at <http://www.checkpoint.com/ngx/upgrade> .

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 will NGX be available, and in what timeframe?

Check Point hardware partners plan to release NGX products in the June-July timeframe. Specifically, Nokia plans to have NGX-based products on IPSO in early June. Sun, Crossbeam and Nortel all plan to offer a NGX-based product by early July.

Upgrade Questions:***Why should I upgrade my Check Point products to NGX versions?***

There are several very good reasons why customers should consider upgrading their Check Point products to NGX versions. The top reasons most customers should consider upgrading is when they want to:

- Simplify management of diverse security solutions
- 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 your Check Point products to the NGX platform, please visit the NGX Upgrade Portal at <http://www.checkpoint.com/ngx/upgrade> .

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

No. The NGX platform is backwards compatible with all NG versions so customers can plan their upgrade in phases, depending on specific needs. For example, customers could first choose to upgrade their SmartCenter server and upgrade the Enforcement Modules later, at their convenience. Customers can choose from numerous scenarios with regards to how they want to upgrade to NGX. These scenarios are described in the “*Upgrade Guide: NGX*” document that can be found in the download section of the Check Point public Web site.

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

The upgrade to the NGX platform is available to all Check Point customers who have a current Enterprise Software Subscription. Customers can check the status of their Support Program in their Check Point User Center account.

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 all VPN-1/FireWall-1 NG gateways (including R55W), VPN-1 Edge, Connectra 2.0, 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 “*The Upgrade*

Guide: NGX (R60)” in the Documentation Download section on the Check Point public Web site.

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

Check Point recommends that customers evaluate their current hardware before proceeding with an upgrade to ensure optimal performance. To assist in this evaluation Check Point has compiled a list of the hardware requirements for each NGX product, based on the operating system, in the “Getting Started Guide: NGX (R60)”.

How do I obtain more information about purchasing/upgrading to NGX?

Customers who are interested in obtaining more information about upgrading their current Check Point products to NGX versions should visit the “NGX Upgrade” section on the Check Point public Web site at <http://www.checkpoint.com/nginx/upgrade> or contact a local Check Point solution provider. To locate a Check Point solution provider in your area, go to our Partner Locator at <http://cgi.us.checkpoint.com/partnerlocator/>.

What has Check Point done to ensure that upgrades to the NGX platform will be smooth for customers?

Check Point has developed essential upgrade tools, utilities, and step-by-step instructions to make the NGX upgrade easy and smooth for customers, specifically:

- NGX license upgrade tool -- New for the NGX platform upgrade, this tool can automatically simulate a license upgrade to the NGX platform and identify potential problems – and how to resolve issues before customers upgrade to NGX.
- 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 – online, offline, distributed environments, and more.

Check Point has consolidated these tools with important upgrade information into a new NGX Upgrade portal available on the Check Point public Web site, giving customers a central place to go for all the information they need to plan and implement their upgrade. The NGX Upgrade portal is located at <http://www.checkpoint.com/nginx/upgrade/>.

Do I need to have Enterprise Software Subscription to upgrade? How can I tell which of my Check Point products are covered by Software Subscription?

Yes. Your Check Point products must be covered by current Check Point Enterprise Software Subscription before you can upgrade products to the NGX platform.

Before you begin the upgrade process you should first ensure that your Check Point products are covered by a current support program (e.g. Enterprise Software Subscription). To see exactly the products and accounts for which you have software subscription, please visit your User Center account at <https://usercenter.checkpoint.com>. In the Accounts page, Enterprise Contract column, and in the Products page, Subscription and Support column, if the account or product is covered, the expiration date is shown. Otherwise, the entry says “Join Now”, with a link to get a quote for purchasing Enterprise Support.

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 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.

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 implemented in Check Point products interoperable with router vendors (Cisco, etc.)?

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, while maintaining 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 Edge, Connectra 2.0, 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 “*The Upgrade Guide: NGX (R60)*” in the Documentation Download section on the Check Point public Web site.

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. SmartPortal can also be purchased as an add-on management application for an unlimited number of gateways for \$5,000.

What centralized management features 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 features 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?

SmartCenter NGX can centralize logs from Integrity servers (Version 6.0) where they can be viewed and analyzed with SmartView Tracker, a visual, real-time application for tracking network traffic and logged activity for Check Point and OPSEC-certified devices.

Will 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.

Training and Certification Questions:

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 certified on Check Point NGX. Training and certification gives you the critical skills and knowledge you need to maximize the security, features, and benefits of NGX and take advantage of new features and technologies.

If you are CCSE NG certified you can attend a 2-day, accelerated “upgrade” course on NGX that will prepare you for the CCSE NGX exam and certification.

If you have a certification other than CCSE NG, you’ll need to register for the full CCSA NGX or CCSE NGX course and pass the exam to be certified on NGX. Updating your certification proves you have the skills and knowledge to maximize the benefits of NGX, increasing your professional standing and worth.

Certifications, just like security, must be kept up-to-date to be effective. To learn more about NGX courses and certifications or find an ATC, visit Education Services Web site at <http://www.checkpoint.com/services/education/>

When will NGX CCSA and CCSE courseware be available?

Final courseware and exams for CCSA NGX and CCSE NGX will be available once we’ve completed our “beta” training and exam period, anticipated to be June 2005. We will be announcing final courseware and exam availability in our ATC and CPO (Certified Professionals Only) newsletters, as well as our Education Services Web site.