Nokia IP VPN

Version 1.0

Getting Started Guide

Part Number: N451100001 Rev A

RESTRICTED RIGHTS LEGEND

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

IMPORTANT NOTE TO USERS

This software and hardware is provided by Nokia Inc. as is and any express or implied warranties, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall Nokia, or its affiliates, subsidiaries or suppliers be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Nokia reserves the right to make changes without further notice to any products herein.

TRADEMARKS

Nokia is a registered trademark of Nokia Corporation. Other products mentioned in this document are trademarks or registered trademarks of their respective holders.

Nokia Contact Information

CORPORATE HEADQUARTERS

Web Site	http://www.nokia.com
Telephone	1-888-477-4566 *or* 1-650-625-2000
Fax	1-650-691-2170
Mail Address	Nokia Inc. 313 Fairchild Drive Mountain View, California 94043-2215 USA

REGIONAL CONTACT INFORMATION

Americas	Nokia Internet Communications. 313 Fairchild Drive Mountain View, CA 94043-2215 USA	Tel: 1-877-997-9199 Outside USA and Canada: +1 512-437-7089 email: ipsecurity.na@nokia.com
Europe, Middle East, and Africa	Nokia House, Summit Avenue Southwood, Farnborough Hampshire GU14 ONG UK	Tel: UK: +44 161 601 8908 Tel: France: +33 170 708 166 email: ipsecurity.emea@nokia.com
Asia-Pacific	438B Alexandra Road #07-00 Alexandra Technopark Singapore 119968	Tel: +65 6588 3364 email: ipsecurity.apac@nokia.com

NOKIA CUSTOMER SUPPORT

Web Site:	https://support.nokia.com/		
Email:	tac.support@nokia.com		
Americas		Europe	
Voice:	1-888-361-5030 or 1-613-271-6721	Voice:	+44 (0) 125-286-8900
Fax:	1-613-271-8782	Fax:	+44 (0) 125-286-5666
Asia-Pacific			
Voice:	+65-67232999		
Fax:	+65-67232897		

021216

Contents

About This Document

Welcome to the *Nokia IP VPN Getting Started Guide v1.0*. This guide is written for system administrators and other knowledgeable professionals who are installing Nokia IP VPN gateways to create site-to-site virtual private networks (VPNs). It is assumed that administrators have a basic knowledge of IP networking, routing, and network architecture.

This document provides an overview about how to install and configure your Nokia IP VPN and introduces new features for large-scale VPN infrastructure deployments. It contains the following sections:

- "Introducing the Nokia IP VPN" provides an overview of the Nokia IP VPN, including features and benefits.
- "Evaluating and Planning Your Network" describes what you need when you plan your network and describes the network topologies that the Nokia IP VPN supports.
- "Installing a Central Office Gateway" describes how to physically install your gateway, how to perform the initial gateway configuration, and provides an overview of IPSO v3.7.
- "Routing Overview" describes the types of routing, routing protocols, and the high-availability features offered in the Nokia IP VPN.
- "High Availability" describes the high-availability features offered in the Nokia IP VPN, including IPSO clustering and VRRP.
- "Configuring Your Nokia IP VPN" describes how to configure your Nokia IP VPN gateway by using the Check Point VPN-1/FireWall-1 management software.
- "Adding a Branch Office" describes the process for adding a branch office to your VPN.
- "Using Management Services" describes the types of management services you can use to monitor, debug, and

maintain your VPN, including NTP, syslog, SNMP, upgrading IPSO, backing up and restoring files, and Nokia Horizon Manager.

- "Further Assistance" describes other Nokia documentation that provides detailed information about installing, configuring, and managing your Nokia IP VPN.

Introducing the Nokia IP VPN

Nokia IP VPN delivers features for large-scale IP virtual private network (VPN) infastructure deployments. Nokia delivers a single cohesive set of capabilities for scalable IP VPN end-to-end and provides a new class of availability and scalability in Nokia IP VPN gateways.

Nokia IP VPN delivers the following features:

- Full suite of IPSec VPN protocols
- Integrated routing and security
- Robust high-availability features
- Optimized branch office solutions
- End-to-end management

Three major components comprise the Nokia IP VPN architecture:

- Central office gateways
- Branch office gateways
- Management services

From these basic building blocks, a full range of IP VPN solutions are possible. The following section lists the requirements for IP VPNs including supported hardware, supported software, and licensing. It also includes the types of management services that the Nokia IP VPN supports.

Nokia IP VPN Requirements

This section lists the hardware and software recommended for the Nokia IP VPN.

Nokia IP VPN Gateways

Nokia recommends the following central office and branch office gateways:

Central Office Gateways	Branch Office Gateways
• Nokia IP1260 • Nokia IP350 • Nokia IP380 • Nokia IP130	• Nokia IP40

Software Requirements

Nokia IP VPN requires the following software:

- Nokia IPSO operating system v3.7 or later
- Check Point VPN-1/FireWall-1 NG with Application Intelligence or later

Check Point License

You need an appropriate license to enable all Check Point products. You can obtain licenses at http://www.checkpoint.com/usercenter.

For more information about how to obtain a Check Point license, see the Installing and Configuring VPN-1/FireWall-1 chapter of the *Check Point Getting Started Guide*, or your Nokia solution provider.

Nokia recommends that you start to obtain a Check Point license several days before you install or upgrade your VPN. You cannot complete the installation and configuration without a Check Point license.

Management Systems

The management system for the Nokia IP VPN solution consists of two primary components: system management tools that Nokia provides and policy management tools that Check Point provides. These management systems include:

- **System management**—management of the information technology systems in an enterprise. Management services report, monitor, and analyze the entire infastructure. Network management services include NTP, syslog, SNMP, the IPSO CLI, Nokia Network Voyager, and Nokia Horizon Manager.

  You can upgrade, backup, or restore the IPSO operating system software by using the CLI, Voyager, or Nokia Horizon Manager. In addition, you can manage your system by configuring features such as high availability and routing.

- **Policy management**—enables administrators to centrally manage and deploy a single policy to a large number of VPN-1/FireWall-1 enforcement points. Once a policy is defined, it can be automatically distributed to all locations. This distribution dramatically increases management efficiency and strengthens security because the security policy is always up-to-date at all security enforcement points.

  You can manage policies with Check Point SmartCenter, IPSec policies, and access control lists (ACLs). Examples of policy management include internal or external CAs, key generation, and certificate enrollment and revocation.

Evaluating and Planning Your Network

Before you begin installing and configuring your Nokia IP VPN, Nokia recommends that you first evaluate and plan your network by doing the following:

- Create a comprehensive network and enterprise security plan.
- Obtain an IP address and hostname for the Nokia IP VPN gateways you are installing.
- Make sure you have a physical location with adequate ventilation and power.
- Verify that you have connectivity to your network.

For more information about how to plan your installation, see the site requirements section of the *IPxxx Series Installation Guide* for your Nokia product.

- If you are installing a Check Point product on your system, make sure you have a valid Check Point license available.

  Consult your Nokia solution provider for information about how to obtain the proper Check Point license for your installation.

Supported Topologies

Nokia IP VPN provides the foundation for support of several network topologies; single-hub, star, partial mesh, and full mesh. These topologies are briefly described in the following list.

Single-hub topology— most common type of topology. Represents a many-to-one relationship between branch office gateways and a central office gateway.

Star topology— multiple central office gateways interconnected to provide a single virtual hub for spoke connectivity.

Partial mesh topology— represents a many-to-many relationship among gateways in which any given gateway might have a connection with several others.

Full mesh topology— most complex topology, in which all gateways are interconnected with all other gateways to provide any-to-any communication among trusted peers.

For detailed information about how to plan your network, general recommendations, and detailed topology descriptions, see the *Nokia IP VPN Technology Overview*.

Setting Up Central and Branch Office Gateways

Nokia offers both central and branch office gateways for your Nokia IP VPN. The following sections guide you through the process of setting up a central office gateway, adding a branch office gateway, and describe the services you can use to monitor, debug, and manage your VPN.

Installing a Central Office Gateway

This section describes how to install a Nokia central office gateway for your Nokia IP VPN and includes the following:

- Before You Begin
- Installing the Appliance
- Performing the Initial Configuration
- Overview of IPSO v3.7.

Before You Begin

Before you install your Nokia appliance, perform the following tasks:

- Check the contents of the carton against the packing list to make sure that you received all the items that you ordered.
- Read any *Read Me First* documents and the *Nokia IPSO Getting Started Guide and Release Notes* packed with the appliance, and install the system as you planned. Most Nokia appliances fit into a standard 19-inch equipment rack.
- Determine whether to use the DHCP configuration client for the initial configuration of your appliance. For more information, see the *Release Notes* or *Read Me First*.

Installing the Appliance

For information about how to physically connect your device to the network, refer to the documentation for your specific device. For example, if you are installing an IP1260, IP380, IP350, or IP130, see the installation guide for your appliance.

Performing the Initial Configuration

The first time you turn power on to a Nokia appliance, the initial configuration process begins. This process enables you to configure the network settings and provides access to the *admin* account.

If you are not using the DHCP client, use a terminal or terminal emulation program to establish a connection to the console port of

the IP security platform. For detailed instructions, see “Installing the Appliance” in the *IPXXX Series Installation Guide*.

In the initial configuration process do the following:

- Assign a host name.
  Alphanumeric characters (0 to 9, a to z), hyphens (–), and periods (.) are permitted.
- Assign a case-sensitive password to the *admin* user account.
- Choose a browser type (Web or ASCII) to use to complete your configuration.
- From the list of available physical interfaces, choose one to establish a network connection to the system.
- Configure the initial IP address.

For details about how to make the initial network connection, see the chapter on configuring the appliance in the *IPxxx Series Installation Guide*, and the *Nokia IPSO Getting Started Guide and Release Notes* for the Nokia IPSO release installed on your appliance.

After you complete these steps, you should have network connectivity. If you do not have network connectivity, see the troubleshooting chapter in the *Nokia IPXXX Series Installation Guide*.

When the initial configuration is complete, you can use Nokia Network Voyager to configure the remaining network ports.

Accessing Nokia Network Voyager

Nokia Network Voyager is an intuitive browser-based remote management interface that communicates with the routing software to configure interface hardware, set routing protocols and routing policies, and monitor network traffic and protocol performance.

Nokia Network Voyager provides the ability to manage almost every aspect of your Nokia appliance, including the following:

- Routing protocols
- Interface configuration

- DNS settings
- NTP settings

After you have network connectivity, you can complete the configuration process by using the Web-based Nokia Network Voyager.

To complete the configuration by using Voyager, perform the following tasks:

- Launch your browser on the host you want to use to complete the configuration.
- Enter the IP address you assigned during the initial configuration.
- Log in using the username *admin* and the password you entered when you performed the initial configuration.
- Click Config, then Interfaces.
- Configure the physical and logical network interfaces, including port speed and duplex mode.

After you complete the configuration, your Nokia IP VPN appliance is up and running. For more about how to configure and manage your appliance, see the *Nokia Network Voyager Reference Guide*.

Overview of IPSO v3.7.

IPSO is a UNIX-like system based on FreeBSD. Unnecessary features are removed to minimize the need for UNIX system administration. IPSO is a unique operating system kernel that is optimized, security hardened, IP networking enabled, and clusterable. IPSO is optimized to support the Nokia enhanced routing capabilities and the Check Point FireWall-1 firewall functionality, and to harden network security. IPSO has built-in IP routing functionality, including IPV6 standards compliance, making it ideal for internetworking with customer IP networks.

For additional information about new features in IPSO v3.7, see the *IPSO 3.7 Getting Started Guide and Release Notes*.

Routing Overview

Routing is a set of mechanisms through which the gateway determines where to forward an IP packet so that it can arrive at the destination IP address. If the gateway that sends the packet and the destination gateway are physically connected through a serial line or local area network, the sending gateway can send the packet to the destination directly. If the gateways are not physically connected, the gateway that sends the packet must identify the next hop that can forward the packet until it reaches the destination.

A router can create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet. Typically, a packet might travel through a number of network points with routers before it arrives at its destination.

This section discusses the following:

- Types of Routing
- Supported Routing Protocols

For detailed information about routing, see the *Nokia Network Voyager Reference Guide*.

Types of Routing

This section describes the two IP addressing types. Each type has its own application and practicality:

- **Static routing**—explicitly specifies the next hop for packets destined for a certain subnet. Packets with a destination that does not match any defined static route are routed to the default gateway.
- **Dynamic routing**—uses special routing information protocols to automatically update the routing table with routes known by peer routers. These protocols are grouped according to whether they are Interior Gateway Protocols (IGP), or Exterior Gateway Protocols (EGPs).

When you deploy Nokia IP VPNs, dynamic routing simplifies deployment and maintenance by:

- Treating an IP VPN connection like any other interface
- Eliminating the burden of setting and maintaining static routes
- Automatically rerouting VPN traffic if a system neighboring the VPN gateway fails to provide high availability.

Supported Routing Protocols

You can protect your routing protocols by using VPN over IPSec. Routing over IP VPNs also protects against outsiders learning information about an enterprise network, reduces the complexity of routing in an enterprise network, and enables use of routing despite intervening third-party networks (for instance, the ISP network that might not allow direct exchange of dynamic routing information). Using VPNs between your branch offices can prevent false routing messages, false routing table updates, or spoofing.

Nokia IP VPN provides support for the following routing protocols:

- Border Gateway Protocol (BGP-4)
- Open Shortest Path First (OSPFv2 and v3)
- Routing Information Protocol (RIPv1 and v2)
- Distance Vector Routing Protocol (DVMRP)
- Protocol Independent Multicast (PIM-SM and PIM-DM)
- Static routes

Note

Central office gateways support BGP-4, OSPF, RIP, DVMRP, PIM, and static routes. Branch office gateways (for instance, the Nokia IP40), only supports BGP-4 and static routes. BGP-4 allows branch office gateways to communicate with central office gateways dynamically.

High Availability

Nokia provides two options for configuring your Nokia IP VPN gateway for high availability. Both methods let you set up redundant gateways without configuring dynamic routing or router discovery protocols on every host. The options are:

- IPSO Clustering
- Virtual Redundancy Routing Protocol
- Comparing Clustering and VRRP
- Using IPSO Clustering Instead of VRRP

Note

Nokia recommends that you enable VPN-1/FireWall-1 and activate your security policy before you bring the high-availability configuration on line to use Check Point VPN-1/FireWall-1 with clustering or VRRP.

IPSO Clustering

IP clustering in IPSO allows you to construct scalable, highly available firewall and VPN gateways by using multiple Nokia security appliances. IP clustering lets you set up redundant gateways without configuring dynamic routing or router discovery protocols on every host. Clustering offers an alternative to the IPSO Virtual Router Redundancy Protocol (VRRP) high-availability solution by providing performance scaling in addition to rapid, automatic failover for high availability.

Clustering provides for high availability by eliminating potential single points of failure through redundancy of cluster nodes. Remaining nodes take over the work load of any node that fails or is removed from the cluster. Seamless failover requires application state synchronization (firewall and VPN) among all the cluster nodes. VPN-1/FireWall-1 provides state synchronization.

With clustering, you can easily create load-balanced, fault-tolerant firewalls or VPN gateways. A cluster comprises multiple devices that share a common IP address, and it appears as a single system to the networks on either side of it.

A cluster continues to function if a node fails or is taken out of service for maintenance purposes, and no single point of failure is available if you configure a backup synchronization connection.

Note

To use clustering, you must use Check Point VPN-1/FireWall-1 NG FP2 and later, and all cluster nodes must run the same version of VPN-1/FireWall-1.

The integration of IP routing functionality with support for VRRP and Check Point Firewall-1 make this high-availability configuration an integral part of enterprise networks.

For more information about IP clustering, see the *Nokia IPSO Clustering Configuration Guide* and the *Nokia Network Voyager Reference Guide*.

Virtual Redundancy Routing Protocol

Virtual Redundancy Routing Protocol (VRRP) provides dynamic failover of IP addresses from one Nokia IP security platform to another in the event of a failure. You configure VRRP in one of two ways:

- An active-passive configuration, in which one or more passive Nokia IP security platforms back up one active system and do not forward any traffic unless they become the active system.
- An active-active configuration in which each Nokia IP security platform is active and also is a backup for the other devices in the set. This configuration allows a certain degree of load balancing because you can use static routes to direct traffic at each of the systems.

For more information about how to configure VRRP, see the *Nokia IPSO 3.7 Clustering Configuration Guide* and the *Nokia Network Voyager Reference Guide*.

Comparing Clustering and VRRP

Clusters balance the traffic load among the nodes. VRRP configurations do not do this, although you can use an active-active configuration to achieve some load balancing.

Cluster nodes monitor Check Point VPN-1/FireWall-1 and stop forwarding traffic if the Check Point application stops working. When you run VRRP, an appliance does not stop forwarding traffic if VPN-1/FireWall-1 fails.

Appliances that run VRRP can run dynamic routing protocols and can forward multicast traffic. IPSO clusters do not support dynamic routing, and they cannot forward multicast traffic.

When you use clustering, you can use Cluster Voyager or Cluster CLI to configure and manage all the cluster nodes simultaneously through one browser or CLI session. VRRP does not offer this capability; you must configure and manage each system individually.

Whether you use clustering or VRRP, Nokia recommends that you use a separate network for VPN-1/FireWall-1 synchronization traffic. If you use clustering, you can also configure a backup synchronization network, which eliminates the primary synchronization network as a single point of failure. You cannot create a backup synchronization network with VRRP.

Finally, you can use VRRP in combination with transparent (bridging) mode, but clustering cannot.

Using IPSO Clustering Instead of VRRP

Although VRRP enables some performance scaling through static load sharing, using IPSO clustering for dynamic load balancing is more practical and effective for scaling gateway performance—particularly VPN performance, which is highly scalable.

Use IPSO clustering when:

- You create a new high-availability installation.
- You need VPN performance scaling.

Use VRRP when:

- You already have an existing VRRP pair for high availability and do not need performance scaling.
- You need to assign multiple IP addresses for each logical interface.
- You need to emulate single-system-image dynamic routing.

Configuring Your Nokia IP VPN

This section describes how to configure your Nokia IP VPN gateway by using the Check Point VPN-1/FIreWall-1 management software and includes the following sections:

- Before You Begin
- Installing VPN-1/FireWall-1
- Configuring VPN-1/FireWall-1
- Description of VPN-1/FireWall-1 Components

Before You Begin

Before you configure your Nokia IP VPN, perform the following tasks:

- Make sure you can access the gateway from Voyager and from a console or terminal connection.
- Verify that you are running IPSO v3.7.
- If you did not already, configure the appliance initial interface and the network interfaces. For more information, see the *IPxxx Series Installation Guide* for your gateway.
- To install the VPN-1/FireWall-1 software, make sure that you have at least 60 MB of free disk space in the /opt directory.
- Confirm that you have a static host name associated with the external IP address of the gateway.
- Make sure that your network is properly configured, with special emphasis on routing. Ensure that each of the internal networks and the gateway can see each other. Log on to each of the hosts and PING the other hosts in the internal networks.
- If you plan to install the SmartCenter Server and Enforcement Module on separate appliances, ensure that the SmartCenter Server host can ping the external IP address of the Enforcement Module host, and the reverse.
- In a standalone installation, the SmartCenter Server and the Enforcement Module are on a single node. In a distributed

environment, the SmartCenter Server and the Enforcement Module are separate nodes.

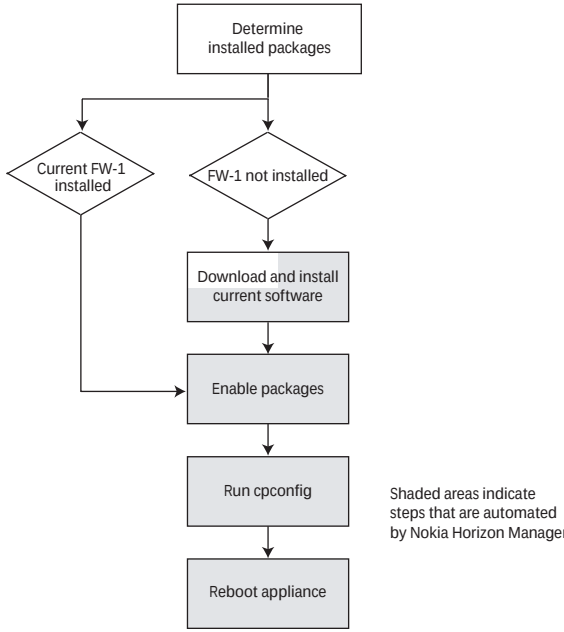
Note

Most Nokia IP VPN deployments use a distributed environment.

Installing VPN-1/FireWall-1

Figure 1 shows the main steps you take to install VPN-1/FireWall-1 on your Nokia appliance.

Figure 1 Firewall Installation and Configuration Steps



For detailed information and steps about the installation process, see the *VPN-1/FireWall-1 for Nokia Getting Started Guide*.

Configuring VPN-1/FireWall-1

After you complete the VPN-1/FireWall-1 installation, you can use the Check Point SmartDashboard application on the SMART Client to define the network objects, users, and security policy. For more information about using SmartDashboard, see the *Check Point Getting Started Guide*.

Description of VPN-1/FireWall-1 Components

This section describes the components that make up the Check Point VPN-1/FireWall-1. VPN-1/FireWall-1 consists of three main components:

Enforcement Module—consists of the VPN-1/FireWall-1 software. The Enforcement Module implements the security policy, logs events, and communicates with the SmartCenter Server.

SmartCenter Server (management server)—maintains the databases of network object definitions, policies, and log files for any number of Enforcement Modules.

SMART Client (management client)—runs the SmartDashboard (Policy Editor), which provides a graphical user interface for the administrator to define network objects, users, and policies.

When installed in a distributed configuration, VPN-1/FireWall-1 implements the client/server model where the SMART Client on a Windows system is running SmartDashboard, and communicates with a management server system that controls an Enforcement Module running on a Nokia configured appliance.

The functionality of VPN-1/FireWall-1 is divided between three workstations. The administrator working on the SMART Client maintains the VPN-1/FireWall-1 security policy and database, which resides on the management server. The management sever installs the policies to the Enforcement Module, which secures the network.

For information about how to install the Enforcement Module and the Smart Center server on a Nokia appliance, see the *VPN-1/FireWall-1 for Nokia Getting Started Guide*. The *VPN-1/FireWall-1 for Nokia Getting Started Guide* also describes how to install the SMART Client on a Microsoft Windows 2000, XP, or NT 4.0 system.

Adding a Branch Office

Nokia IP VPN is designed for enterprises to protect branch offices and delivers the capability for scalable IP VPN end-to-end. With Nokia IP VPN, enterprises can add thousands of sites to their current topology. This section describes the process for adding a branch office gateway to your Nokia IP VPN.

Configuring the Branch Office

After you set up and configure your central office gateways, you are ready to add a branch office. The gateway is configured at the central office except for the IP addresses, which the administrator configures from the branch office by using the CLI or the Web-based interface.

Assume that you are adding a Nokia IP40 as a branch office gateway:

- Configure the Internet connection before you access the Internet through the Nokia IP40. You can configure the Internet connection by using the setup wizard. The setup wizard automatically opens on successful log in.
- The setup wizard allows you to configure your Nokia IP40 for Internet connection quickly and easily through the use of a user friendly interface. The setup wizard guides you through the configuration step-by-step.

  Once your Nokia IP40 is configured, you can access the Internet safely and securely.
- Once you make the connection to the service center, enter the gateway ID for the Nokia IP40. The management station identifies the gateway and retrieves the gateway profile. This profile contains the gateway firewall and VPN policies you need to run your VPN.

For detailed information about how to configure the Internet connection and connect to the service center, see the *Nokia IP40 User's Guide*.

After you set the configuration options for your VPN, you can install each branch office gateway.

To install the Nokia IP40 as a branch office gateway, perform the following tasks:

- Assign the WAN IP address (dynamic or static) to the Nokia IP40.
- Use Check Point SmartDashboard to assign a SmartLSM profile.
- Use SmartLSM to create Nokia IP40 objects.
- Use either the Web interface or CLI to configure the Nokia IP40 to communicate with the Sofaware Management Server, which is part of SmartCenter.
- Return to the SmartDashboard and define VPN communities.
- Using SmartLSM, add dynamic objects to the Nokia IP40 to define an encryption domain.
- Using SmartDashboard, push the policies to the Nokia IP40 SmartLSM profile and the central office gateways.

For more information about the Nokia IP40, see the *Nokia IP40 Getting Started Guide* and the *Nokia IP40 CLI Reference Guide*.

Using Management Services

The Nokia IP VPN solution has a variety of management services to assist you to monitor, debug, and maintain your VPN. Running these services over IPSec VPN establishes secure, end-to-end private network connections over a public networking infrastructure and protects data from unauthorized access, or where vulnerabilities exist. This section describes the type of management services available and how they run over IPSec VPN.

The Nokia IP VPN management services include:

- NTP
- Syslog
- SNMP
- Upgrading IPSO
- Backing Up and Restoring Files
- Nokia Horizon Manager

For detailed information about how to configure and manage these services, see the *Nokia Network Voyager Reference Guide*.

NTP

Network Time Protocol (NTP) is a protocol that allows you to synchronize to UTC time by querying a server with an accurate clock. This protocol can synchronize distributed clocks within milliseconds over long time periods. NTP is ideal for distributed applications that require time synchronization, such as Check Point FireWall-1 Sync, or analyzing event logs from a different computer.

NTP runs as a continuous background client program on the gateway and sends periodic time requests to NTP servers to obtain server time stamps and uses them to adjust the client clock. A time stamp provides evidence that an item existed at a specific time, such as a time-stamped digital certificate that a certificate authority issues for client authentication purposes.

Although NTP is a reliable method to maintain and synchronize times on gateway servers, vulnerabilities exist. If the server times vary with each other or with the correct time, processes can fail, data can be lost, and security is compromised. To prevent hacking or IP spoofing, these time mechanisms need to be secure. NTP over IPSec VPN provides the security and isolation to prevent these types of attacks.

Syslog

The Nokia IP VPN gateway logging system allows you to configure a variety of options for viewing logging information for particular users, resources, authentication methods, and gateway components. These logging messages are stored to the syslog daemon that run on the gateway. The output stored in the file includes information about events such as administrative events, configuration changes, and tunnel events.

Neither the syslog protocol nor the syslog application have mechanisms to provide confidentiality for messages in transit. Because messages are passed in cleartext, an attacker might be able to read the contents of a syslog message or, for example, obtain records of administrative access.

You can secure syslog messages by running syslog over IPSec. VPN provides an encrypted data channel that tunnels the syslog information over the network, protecting all logging information.

SNMP

The Simple Network Management Protocol (SNMP), provides a common framework for managing and monitoring your VPN. This protocol provides a message format for communication between SNMP managers and agents.

The Nokia IP VPN gateway includes support for SNMP traps that alert you when particular events occur during the gateway operation. You must configure the IPSO SNMP agent from Nokia Network Voyager or the CLI to use the SNMP traps. The IPSO SNMP agent is

responsible for performing the SNMP communication to the network management station, based on the Voyager SNMP settings.

Using IPSec, you can define IPSec policies in your monitored systems and management stations so that all SNMP traffic is authenticated and encrypted.

SNMP over IPSec also allows users to configure an SNMP agent to accept SNMP requests from a certain set of VPNs only. With this configuration, providers can provide network management services to their customers, so customers can manage all user VPN devices.

For more information about SNMP, see the *Nokia Network Voyager Reference Guide* or the *Nokia CLI Reference Guide*.

Note

Central office gateways support SNMPv2 and SNMPv3. Branch office gateways (i.e. Nokia IP40) only supports SNMPv2c.

Upgrading IPSO

This section describes how to upgrade IPSO operating system software on your Nokia devices. You can upgrade IPSO by using the CLI, Voyager, or Nokia Horizon Manager.

Depending on the versions of the software you currently have installed, you can use Horizon Manager either to upgrade from an older version of the software to a newer version or to install the new software.

If you use Horizon Manager to manage your appliances, you can upgrade and revert to earlier versions of IPSO on all your appliances simultaneously or in groups of multiple appliances. Horizon Manager employs *Do No Harm* intelligence to prevent incompatible package installations on Nokia appliances.

For more information about how to upgrade IPSO, see the appropriate installation guide for your appliance.

Backing Up and Restoring Files

You can configure your Nokia IP VPN to perform manual or regularly scheduled backups and restore files from locally stored backup files by using the IPSO CLI, Nokia Network Voyager, or Nokia Horizon Manager.

You can back up and restore files quickly by using the command-line interface. If your configuration consists of a single gateway or cluster of gateways, use Voyager. For multiple appliances or large network deployments, you can back up and restore files with Nokia Horizon Manager.

For detailed information about how to back up and restore files, see the *Network Voyager Reference Guide*, the *CLI Reference Guide for IPSO 3.7*, the *Nokia IP40 CLI Reference Guide,* and the *Nokia Horizon Manager User's Guide*.

Nokia Horizon Manager

You can use Nokia Horizon Manager to install and upgrade the Nokia IPSO operating system. Horizon Manager is a network management application built specifically to manage Nokia IP security appliances. Horizon Manager allows you to migrate all of your appliances or groups of your appliances to new versions of Check Point applications, Nokia IPSO versions, and other supported Nokia partner security applications. You can perform backup and restore operations on multiple systems simultaneously regardless of their location on your service provider or enterprise network.

While Nokia Network Voyager provides the administrator access to network configuration tasks (such as interface configuration and routing configuration) and security configuration tasks (such as user configuration and access configuration). Horizon Manager provides users the ability to securely manage software packages, maintain a hardware and software inventory, and provide overall platform management of Nokia IP security platforms and Nokia small office security platforms.

Using Horizon Manager, an administrator can obtain configuration information, upgrade the operating system, revert back to previous

configurations, perform application installations, and distribute necessary licensing to multiple platforms simultaneously, thereby reducing potential human error and improving productivity.

Nokia Horizon Manager also supports initial configuration of Check Point software (cpconfig) and general platform configuration deployment features.

In addition, Horizon Manager offers advanced features that include secure remote access, key maintenance utility, process monitoring, server status and control, and user session management.

For more detailed information about how to manage IP security platforms by using Horizon Manager, see the *Nokia Horizon Manager Getting Started Guide* and the *Nokia Horizon Manager User's Guide*.

Further Assistance

The following documents provide detailed information about how to install, configure, and manage your Nokia IP VPN. In addition to this guide, documentation for this product includes:

- *Nokia IP VPN Technical Overview*—provides information for understanding VPN technologies and information for how to design, implement, and manage a Nokia IP VPN.
- *Nokia IP VPN Gateway Release Notes*—provides important information you should know before you install and configure your Nokia IP VPN.
- *Nokia IPSO 3.7 Clustering Configuration Guide*—provides an overview of IPSO clustering, configuring and managing a cluster, configuring VPN-1/FireWall-1 clustering, and clustering examples.
- *Nokia CLI Reference Guide for IPSO 3.7*—provides information about how to create and implement command-line interface commands that are applicable to IPSO 3.7.
- *Nokia Network Voyager Reference Guide*—provides information about Voyager software used to configure interfaces and routing protocols, manage firewall routing policies, and how to monitor network traffic and protocol performance.
- *Nokia Network Voyager inline help*—inline help is the context-sensitive information source for Voyager. From Voyager, you can click the Help icon to get inline help.
- *Nokia Horizon Manager User's Guide*—provides information about the Nokia Horizon Manager software that allows administrators to perform remote, centralized upgrades and maintenance of multiple IP security appliances simultaneously.
- *Nokia IP40 Quick Start Guide*—provides a quick reference about configuring features for the Nokia IP40.
- *Nokia IP40 Getting Started Guide*—provides information about installing and configuring the Nokia IP40 branch office gateway.

- *Nokia IP40 CLI Reference Guide*—provides information about how to create and implement command-line interface commands for the Nokia IP40.