NOKIA

IP45 Security Platform

User's Guide

Version 4.0

Part Number: N450000261 Rev. 001

December 2006

COPYRIGHT

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.

060101

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 Inc. 313 Fairchild Drive Mountain View, CA 94043-2215 USA	Tel: 1-877-997-9199 Outside USA and Canada: +1 512-437-7089 email: info.ipnetworking_americas@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: info.ipnetworking_emea@nokia.com
Asia-Pacific	438B Alexandra Road #07-00 Alexandra Technopark Singapore 119968	Tel: +65 6588 3364 email: info.ipnetworking_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		

050602

Contents

About this Guide

This guide provides information and procedures about how to install and configure the Nokia IP45 security platform. This guide provides information about the new features incorporated in the Nokia IP45. This version of the Nokia IP45 uses the SofaWare VPN-1 Embedded NG. For a quick reference on how to configure features in the Nokia IP45, see the *Nokia IP45 Security Platform Quick Start Guide v4.0* and the *Nokia IP45 Security Platform Online Help,* part of the graphical user interface (GUI) in the device.

Installation and maintenance should be performed by experienced technicians or Nokia-approved service providers only.

This preface provides the following information:

- In this Guide
- Conventions this Guide uses
- Related Documentation

In this Guide

This guide is organized into the following chapters and appendixes:

- Chapter 1, "Introduction" provides the information you need to know before installing the Nokia IP45 security platform.
- Chapter 2, "Installing the Nokia IP45 Security Platform" describes how to install the device, lists operating system requirements, protocols and how to establish a network connection.
- Chapter 3, "Getting Started" describes how to start by using the IP45, and provides information on first-time login and connecting to the Internet.
- Chapter 4, "Accessing the Nokia IP45 Security Platform" describes different methods of connecting to your IP45, and methods of configuring the device.
- Chapter 5, "Connecting to the Internet with the Nokia IP45 Security Platform" describes how to configure your IP45 for connecting to the Internet, and viewing and managing your Internet connection.
- Chapter 6, "Managing your Local Area Network," describes how to configure the Nokia IP45 features.
- Chapter 7, "Quality of Service" provides information about Quality of Service (QoS) and how to configure the QoS classes.

- Chapter 8, “Setting Up the Nokia IP45 Security Platform Security Policy”describes methods to define the firewall level, configure virtual servers, and create firewall rules.
- Chapter 9, “Configuring Network Access,” describes the network access procedures and usage of SSH and SSL.
- Chapter 10, “Configuring and Monitoring SNMP,” describes the procedure to configure Simple Network Management Protocol, set community strings, send and enable SNMP traps.
- Chapter 11, “High-Availability,” describes about the High Availability feature.
- Chapter 12, “Configuring Nokia IP45 Through Out-of-Band Management,” describes the method to configure the Nokia IP45 through Out of Band Management.
- Chapter 13, “Configuring Device Functions,” discusses how to configure device functions such as setting date and time, loading factory defaults and performing firmware upgrade.
- Chapter 14, “Viewing Reports,” describes how to view reports such as Event Log, Active Computers, Active Connections, and VPN Tunnels.
- Chapter 15, “Working with VPNs,” describes how to configure a VPN by using the Nokia IP45.
- Chapter 16, “Using Managed Services” describes methods for enabling and using subscription services such as Web filtering, email antivirus, automatic and manual updates.
- Chapter 17, “Troubleshooting,”discusses typical problems users encounter and provides solutions to these problems.
- Appendix A, “Specifications,” describes the Nokia IP45 specifications.
- Appendix B, “Compliance Information,” contains the compliance information of the Nokia IP45 security platform.

Conventions this Guide uses

The following sections describe the conventions this guide uses, including notices, text conventions, and command-line conventions.

Notices

Warning
Warnings advise the user that either bodily injury might occur because of a physical hazard, or that damage to a structure, such as a room or equipment closet, might occur because of equipment damage.

Caution
Cautions indicate potential equipment damage, equipment malfunction, loss of performance, loss of data, or interruption of service.

Note
Notes provide information of special interest or recommendations.

Command-Line Conventions

This section defines the elements of commands that are available in Nokia products. You might encounter one or more of the following elements on a command-line path.

Table 1 Command-Line Conventions

Convention	Description
Command	This required element is usually the product name or other short word that invokes the product or calls the compiler or preprocessor script for a compiled Nokia product. It might appear alone or precede one or more options. You must spell a command exactly as shown and use lowercase letters.

Italics	Indicates a variable in a command that you must supply. For example:
	`delete interface` *`if_name`*
	Supply an interface name in place of the variable. For example:
	`delete interface nic1`

Angle brackets < >	Indicates arguments for which you must supply a value:
	`retry-limit <1-100>`
	Supply a value. For example:
	`retry-limit 60`

Square brackets [ ]	Indicates optional arguments.
	`delete [slot` *`slot_num`*`]`
	For example:
	`delete slot 3`

Vertical bars, also called a *pipe* (|)	Separates alternative, mutually exclusive elements.
	`framing <sonet | sdh>`
	To complete the command, supply the value. For example:
	`framing sonet`
	or
	`framing sdh`

Table 1 Command-Line Conventions (*continued*)

Convention	Description
-flag	A flag is usually an abbreviation for a function, menu, or option name, or for a compiler or preprocessor argument. You must enter a flag exactly as shown, including the preceding hyphen.
.ext	A filename extension, such as .ext, might follow a variable that represents a filename. Type this extension exactly as shown, immediately after the name of the file. The extension might be optional in certain products.
(. , ; + * - /)	Punctuation and mathematical notations are literal symbols that you must enter exactly as shown.
' '	Single quotation marks are literal symbols that you must enter as shown.

Text Conventions

Table 2 describes the text conventions this guide uses.

Table 2 Text Conventions

Convention	Description
`Monospace font`	Indicates command syntax, or represents computer or window output, for example: `Log error 12453`
`Bold monospace font`	Indicates text you enter or type, for example: **`# configure nat`**
Key names	Keys that you press simultaneously are linked by a plus sign (+): Press Ctrl + Alt + Del.
Menu commands	Menu commands are separated by a greater than sign (>): Choose File > Open.
The words enter and type	Enter indicates you type something and then press the Return or Enter key. Do not press the Return or Enter key when an instruction says *type*.
Italics	• Emphasizes a point or denotes new terms at the place where they are defined in the text. • Indicates an external book title reference. • Indicates a variable in a command: `delete interface` *if_name*

Menu Items

The Nokia IP45 menu items in procedures are separated by the greater than sign (>).

For example, Start > Programs > Nokia > Security indicates that you first click Start, then choose the Programs menu command, then choose Nokia, and finally choose Security.

Related Documentation

In addition to this guide, documentation for this product includes the following:

- *Nokia IP45 Security Platform Quick Start Guide Version 4.0*—describes the system features and provides an overview of how to get your appliance up and running.
- *Nokia IP45 Security Platform Getting Started Guide Version 4.0*—describes how to install and configure the Nokia IP45 security platform.
- *Nokia IP45 Security Platform CLI Reference Guide Version 4.0*—describes all the IP45 commands that are used for managing the appliance.
- *Nokia IP45 Security Platform Release Notes Version 4.0*—describes what you should know before you install and configure the IP45.

1 Introduction

This chapter introduces the Nokia IP45 security platform and includes the following topics:

- About the Nokia IP45 Security Platform
- Nokia IP45 Security Platform Features
- Network Requirements
- Nokia IP45 Security Platform Front Panel
- Nokia IP45 Security Platform Rear Panel

About the Nokia IP45 Security Platform

The Nokia IP45 security platform provides dependable Internet access for the remote and branch offices of a distributed enterprise. The Nokia IP45 supports features like dial-up connection, redundant WAN connection to headquarters, and dual homing with BGP to route return traffic securely, over VPN. IP45 appliances are RoHS complaint.

The Nokia IP45 security platform can be integrated with an overall enterprise security policy for maximum security. The IP45 facilitates centralized management and automatic deployment with the security management architecture of Check Point and Nokia Horizon Manager.

The Nokia IP45 security platform is available with the following licenses:

- Nokia IP45 Tele 8
- Nokia IP45 Satellite 16
- Nokia IP45 Satellite 32
- Nokia IP45 Satellite U (Unlimited)

All these versions of the Nokia IP45 provide a Web-based interface that enables you to configure and manage the Nokia IP45.

The Nokia IP45 security platform comes pre-installed with the license of your choice. You can upgrade the IP45 security platform to a more advanced configuration without replacing the hardware. For details about license upgrade, contact your local reseller.

Nokia IP45 Tele 8

Nokia IP45 Tele 8 is for home telecommuters and work extenders who also need VPN client access. The IP45 Tele 8 supports both firewall and VPN client capabilities over an eight-node network. The device supports VPN client capabilities for users to connect to the central office from their home with firewall protection, extending the enterprise network to the employees' home offices.

IP45 Tele 8 can act as a VPN server, which allows a single user to securely access resources protected by the device from home or while travelling.

Note
Computers that actually pass through the firewall are counted. Devices such as network printers connected in LAN that do not normally get connected to the Internet are not counted.

Nokia IP45 Satellite 16, Satellite 32, Satellite Unlimited

Nokia IP45 Satellite 16, IP45 Satellite 32, and IP45 Satellite Unlimited provide full firewall, and VPN connectivity for remote and branch offices or independent, small, and medium enterprises with sixteen, thirty-two, and unlimited node networks, respectively. Using these solutions, remote and branch offices can securely exchange information between them with distributed enterprises and small and medium enterprises at a low price with excellent performance.

Nokia IP45 Security Platform Features

The following section contains a summary of the Nokia IP45 security platform features.

Connectivity

Table 3 provides details about the IP45 v4.0 connectivity.

Table 3 Nokia IP45 Security Platform Connectivity

Feature	Nokia IP45 Tele 8	Nokia IP45 Satellite 16/32/Unlimited
LAN, WAN, and console ports	✓	✓
DMZ Support		✓
Manual Ethernet port settings	✓	✓

Table 3 Nokia IP45 Security Platform Connectivity (*continued*)

Feature	Nokia IP45 Tele 8	Nokia IP45 Satellite 16/32/Unlimited
Dynamic routing by using OSPF		✓
Unnumbered PPP	✓	✓
Users (nodes)	8	16, 32, unlimited
PPPoE client	✓	✓
PPTP client	✓	✓
DHCP client	✓	✓
DHCP server	✓	✓
DHCP relay	✓	✓
Backup DHCP relay	✓	✓
DHCP reservation	✓	✓

Table 3 Nokia IP45 Security Platform Connectivity (*continued*)

Feature	Nokia IP45 Tele 8	Nokia IP45 Satellite 16/32/Unlimited
Customizing DHCP Options (DNS servers, WINS servers, NTP servers, Domain name, VoIP call managers, TFTP server and TFTP boot file name)	✓	✓
Static IP	✓	✓
MAC cloning	✓	✓
MAC Cloning for WAN2	✓	✓
Static NAT, static routes	✓	✓
Dial-up Internet connection		✓
Routing support by using BGP	✓	✓
Source routing	✓	✓
High-Availability (Group ID, enhanced interface tracking, VPN effect, WAN Virtual IP)		✓
Traffic Shaper	✓	✓

Table 3 Nokia IP45 Security Platform Connectivity (*continued*)

Feature	Nokia IP45 Tele 8	Nokia IP45 Satellite 16/32/Unlimited
Traffic Shaper enhancements	✓	✓
Traffic Monitor	✓	✓
Dead Connection Detection	✓	✓

Firewall

Table 4 provides details about the IP45 security platform firewall connectivity.

Table 4 Firewall Connectivity

Feature	Nokia IP45 Tele 8	Nokia IP45 Satellite (16/32/Unlimited)
Firewall Type	Check Point Firewall-1 Embedded NG	Check Point Firewall-1 Embedded NG
Network Address Translation (NAT)	✓	✓
INSPECT policy rules	✓	✓
User defined rules	✓	✓
Three levels of Preset security policies	✓	✓
DoS protection	✓	✓

Table 4 Firewall Connectivity (*continued*)

Feature	Nokia IP45 Tele 8	Nokia IP45 Satellite (16/32/Unlimited)
Anti-spoofing	✓	✓
Attack logging	✓	✓
Voice over IP (H.323) support	✓	✓
Exposed host	✓	✓
DMZ network		✓
VLAN support		✓
SmartDefense and Application Intelligence	✓	✓

VPN Connectivity

Table 5 provides details about the IP45 security platform VPN connectivity.

Table 5 VPN Connectivity

Feature	Nokia IP45 Tele8	Nokia IP45 Satellite 16/32/Unlimited
IPSEC VPN remote access server	✓	✓
IPSEC VPN site-to-site gateway		✓
IPSEC VPN remote access client	✓	✓
Authentication		
X.509 certificates	✓	✓
RSA secure ID	✓	✓
Office Mode Network	✓	✓
VPN pass through	✓	✓
Enhanced MEP support		✓
Advanced VPN configuration	✓	✓
Encryption	AES/3DES/DES	AES/3DES/DES
Authentication	SHA1/MD5	SHA1/MD5
SecuRemote server	✓	✓

Table 5 VPN Connectivity (*continued*)

Feature	Nokia IP45 Tele8	Nokia IP45 Satellite 16/32/Unlimited
L2TP VPN server	✓	✓
RADIUS Client		✓
RADIUS Enhancements		(vendor specific attribute (VSA), Radius Realm support, Radius time-out and retries setting)
DAIP with VPN certificates		✓
Backup VPN gateways		✓
SmartCenter Connector (SSC) NG AI support	✓	✓
Bypass NAT	✓	✓
Bypass Firewall	✓	✓
NAT Traversal		✓
Route all traffic		✓

Table 5 VPN Connectivity (*continued*)

Feature	Nokia IP45 Tele8	Nokia IP45 Satellite 16/32/Unlimited
Route-Based VPN and failover		✓
Multiple PPP connections	✓	✓
Enhanced active tunnels display	✓	✓

Management

Table 6 provides details about the IP45 security platform management.

Table 6 Management

Feature	Nokia IP45 Tele 8	Nokia IP45 Satellite (16/32/Unlimited)
Web-based management	✓	✓
Access to the IP45 through OOB, SSH and SNMP	✓	✓
Telnet access	✓	✓
HTTPS access (local and remote)	✓	✓
Remote firmware upgrades	✓	✓

Table 6 Management (*continued*)

Feature	Nokia IP45 Tele 8	Nokia IP45 Satellite (16/32/Unlimited)
Nokia Horizon Manager support from v1.5 SP1 onwards	✓	✓
Multiple administrators		✓
Users Manager	✓	✓
Guest HotSpot Users		✓
User account expiration	✓	✓
Nokia CLI shell	✓	✓
Management systems (Nokia Horizon Manager, SofaWare SMP, Check Point SmartCenter, Check Point Smart Update)	✓	✓
Check Point Smart LSM Check Point Provider-1		✓
Packet Sniffer	✓	✓
SmartDefense policy wizard	✓	✓

Security Services

Table 7 provides details about the IP45 security platform security services.

Table 7 Security Services

Feature	Nokia IP45 Tele 8	Nokia IP45 Satellite (16/32/Unlimited)
VStream embedded antivirus	✓	✓
Firewall security updates	✓	✓
Software updates	✓	✓
Web filtering	✓	✓
Email antivirus protection	✓	✓
Secure HotSpot		✓
Dynamic DNS service (When managed by SofaWare Management Portal (SMP) and Nokia Horizon Manager (NHM)).	✓	✓
VPN management	✓	✓
Centralized logging	✓	✓

Table 7 Security Services (*continued*)

Feature	Nokia IP45 Tele 8	Nokia IP45 Satellite (16/32/Unlimited)
Customized security policy	✓	✓
Protocol support for TCP/IP, ICMP, GRE, ESP and UDP	✓	✓
Certificate Finger print display	✓	✓

Diagnostics and Maintenance

Table 8 provides details about the IP45 v4.0 diagnostics and maintenance.

Table 8 Diagnostics and Maintenance

Feature	Nokia IP45 Tele 8	Nokia IP45 Satellite (16/32/Unlimited)
Configuration Import or Export	✓	✓
Firmware upgrade	✓	✓
Preset configuration	✓	✓
Known good configuration	✓	✓

Table 8 Diagnostics and Maintenance (*continued*)

Feature	Nokia IP45 Tele 8	Nokia IP45 Satellite (16/32/Unlimited)
OOB management	✓	✓
Diagnostic tools (netstat, traceroute, arp, ping, WHOIS, nslookup, tcpdump)	✓	✓

Network Requirements

To set up the Nokia IP45 security platform to connect to the Internet, you need the following:

- A broadband Internet connection by cable or DSL modem with Ethernet interface (RJ-45) or a dial-up connection with a serial modem (V90 or ISDN T/A)
- 10Base-T or 100Base-T Ethernet switch or hub (optional)
- 10Base-T or 100Base-T network interface card installed on each computer
- TCP/IP network protocol installed on each computer
- CAT5 network cable with RJ-45 connectors for each computer
- Internet Explorer 5.0 or later, or Netscape Navigator 4.5 and later

Note
Nokia recommends that you use either Microsoft Internet Explorer 5.5 or later, or Netscape Navigator 6.2 or later.

Overview

The following sections provide an overview of the Nokia IP45 security platform rear and front panels.

Nokia IP45 Security Platform Rear Panel

All physical connections (network and power) to the IP45 are made through the rear panel.

Table 9 explains the items on the rear panel of the Nokia IP45.

Figure 1 Rear panel of the Nokia IP45

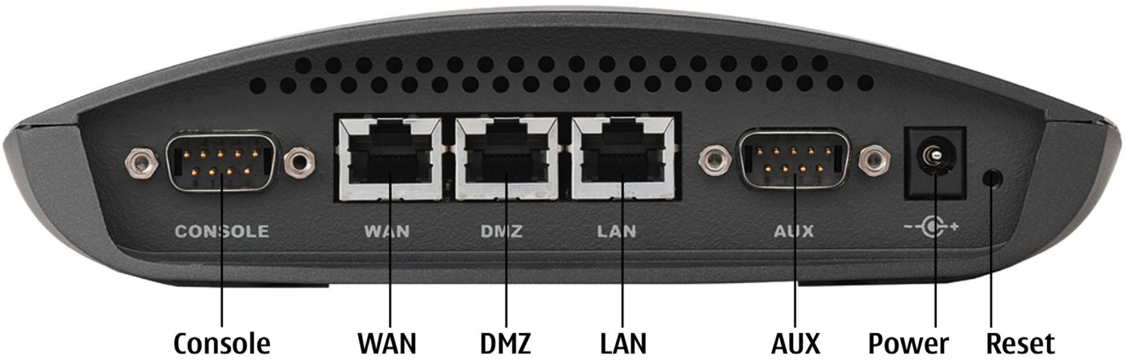


Table 9 Rear Panel of the IP45

Label	Description
Console	The console port is a 9-pin male connector that can be connected to the serial (COM) port of your computer. You can then use the command-line interface (CLI) to communicate with the device.
WAN	Wide area network. An Ethernet port (RJ-45) used to connect your cable or xDSL modem.
DMZ (WAN2)	Demilitarized zone. Ethernet port (RJ-45) used to connect computers or other network devices. Similar to LAN port in operation. This can be used as WAN2, secondary WAN connection.
LAN	Local area network. Ethernet port (RJ-45) used to connect computers or other network devices.
AUX	The auxiliary port or dial-in port is a 9-pin male connector. This port is used to dial in to the IP45 through a modem when the IP45 is unreachable through other ports.

Table 9 Rear Panel of the IP45 (*continued*)

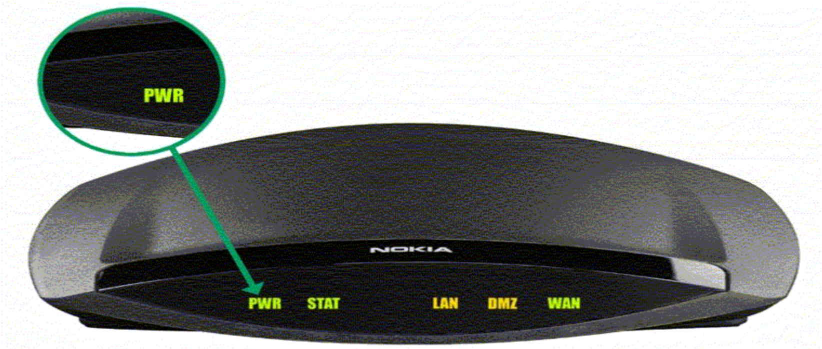
Label	Description
Power	A power jack used to supply power to the device. Connect the power adapter to this jack. The device connects to the power source.
Reset	Used to reboot or reset the IP45 to its factory defaults. Use a large flat-tipped object, such as a thick paper clip, to press the reset button. *Short press* (one second)**:** reboots the Nokia IP45 security platform. *Long press* (seven seconds)**:** resets the IP45 to its factory defaults. This results in loss of all security services and passwords. *Short press during boot up*: boots the IP45 in special deployment mode. See "Resetting the Nokia IP45 Security Platform by Using the Reset Button" on page 248.

Note
Do not use a sharp pin or thin piece of metal to press the Reset button.

Nokia IP45 Security Platform Front Panel

You can monitor the IP45 operations by viewing the LEDs on the front panel.

Figure 2 Front Panel of the Nokia IP45 Security Platform



The items on the front panel of the Nokia IP45 security platform are explained in Table 10 on page 36.

Table 10 Front Panel of the Nokia IP45

Label	Description
PWR	Off: Device not powered on Green Solid: Device is on
STAT	Off: Device off Green solid: Device passed hardware test and finished booting. Red solid: Hardware error Amber solid: Booting Green blinking: Device passed hardware test and is fully booted. Device is at its default state. First-time password is not set. Red blinking: Software error Amber blinking: Device is performing a function such as setting factory defaults, loading firmware or loading an exported configuration.
LAN DMZ WAN	Off: No connection Green solid: Interface connected and auto-negotiated at 10 Mbps Amber solid: Interface connected and auto-negotiated at 100 Mbps Amber/Green blinking: Traffic passing through the interface

2 Installing the Nokia IP45 Security Platform

This chapter describes how to set up and install the Nokia IP45 security platform in a networking environment. The chapter includes the following topics:

- Before you Install the Nokia IP45 Security Platform
- Setting Up the Nokia IP45 Security Platform with Microsoft Windows 98 or Millennium Operating Systems
- Setting Up the Nokia IP45 Security Platform with Microsoft Windows XP and 2000 Operating Systems
- Setting Up the Nokia IP45 Security Platform with an Apple Computer
- Connecting the Nokia IP45 Security Platform to the Network
- Installing your Network

Before you Install the Nokia IP45 Security Platform

Before you connect and set up the Nokia IP45 security platform, you must check the following:

- Whether TCP/IP is installed on your computer.
- The TCP/IP settings of your computer, to ensure that it obtains its IP address automatically.

The following sections guide you through the TCP/IP setup and installation process.

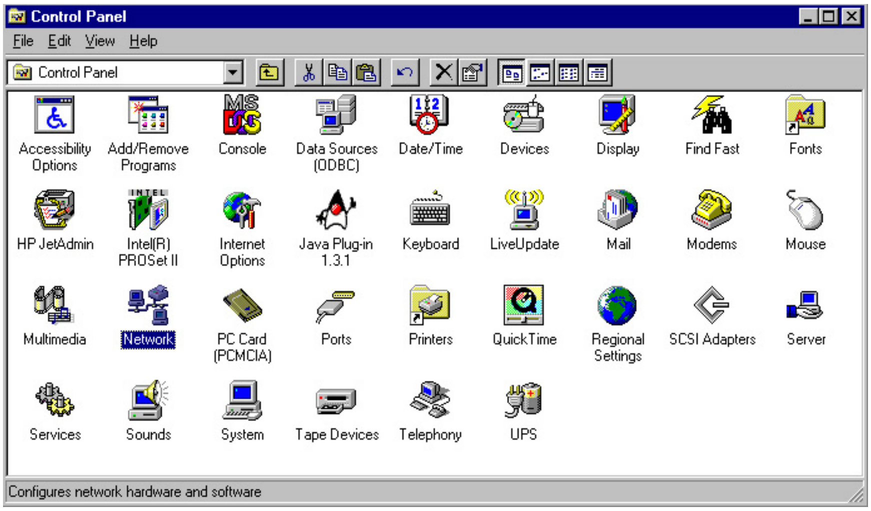
Setting Up the Nokia IP45 Security Platform with Microsoft Windows 98 or Millennium Operating Systems

If you are using Windows 98 or Windows ME, configure TCP/IP as follows.

To check for TCP/IP Installation

1. Choose Start > Settings > Control Panel.

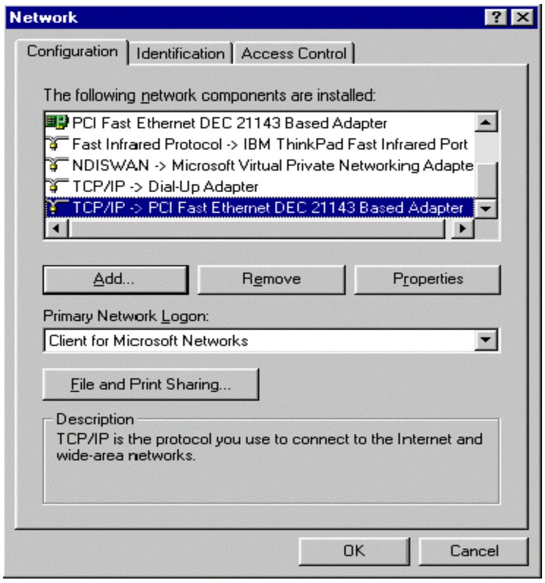
   The Control Panel window opens.



Configures network hardware and software

2. Double-click the Network icon.

   The Network window opens.



The following network components are installed:

- PCI Fast Ethernet DEC 21143 Based Adapter
- Fast Infrared Protocol -> IBM ThinkPad Fast Infrared Port
- NDISWAN -> Microsoft Virtual Private Networking Adapte
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> PCI Fast Ethernet DEC 21143 Based Adapter

Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

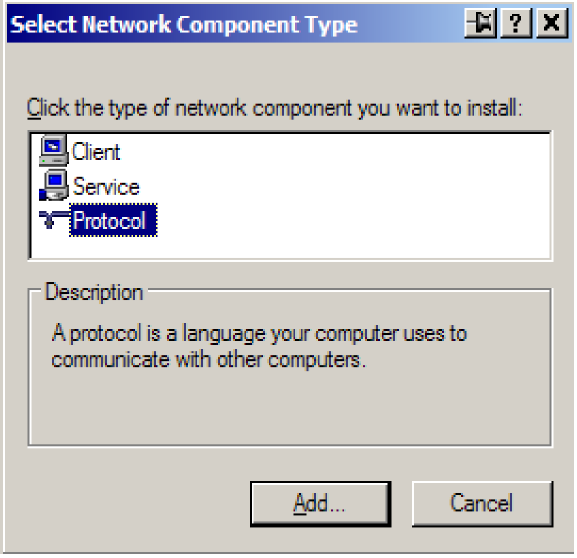
In the Network window, check if TCP/IP appears in the network components list and if it is already configured with the Ethernet card installed on your computer.

If TCP/IP is already installed and configured on your computer, skip the following procedure about how to install TCP/IP.

To install TCP/IP

1. In the Network window, click Add.

   The Select Network Component Type window opens.

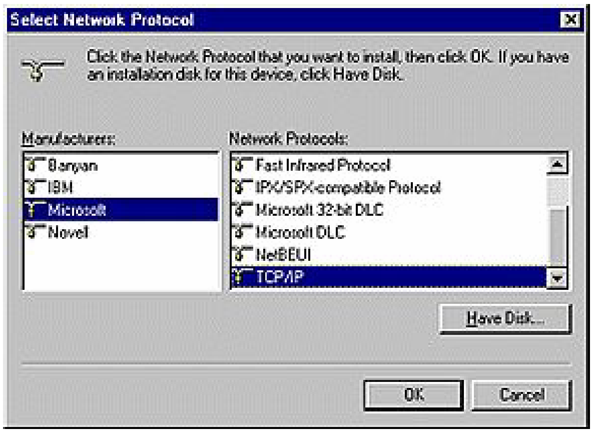


Click the type of network component you want to install:

Description
A protocol is a language your computer uses to communicate with other computers.

2. Choose Protocol and click Add.

The Select Network Protocol window opens.



Select Network Protocol

Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this device, click Have Disk.

Manufacturers: Microsoft

Network Protocols: TCP/IP

3. In the Select Network Protocol window, choose Microsoft in Manufacturers and TCP/IP in Network Protocols.
4. Click OK.

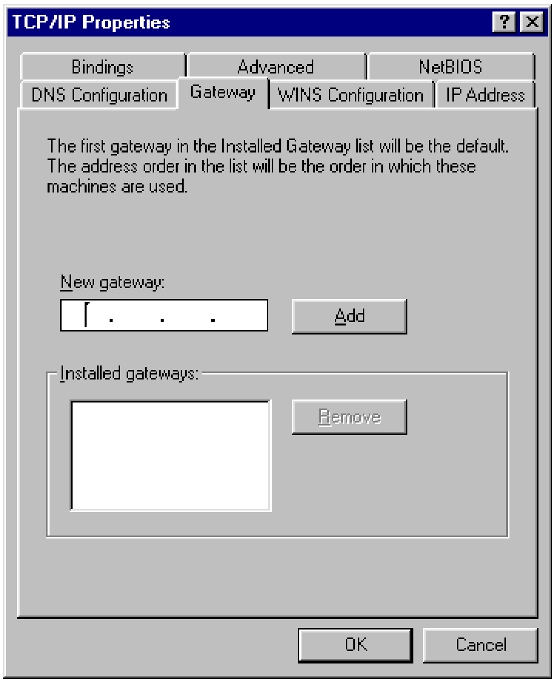
   If you are prompted for original Windows installation files, provide the installation CD and relevant path, D:\win98, D:\win95, and so on.
5. Restart your computer if prompted.

If you are connecting the IP45 to an existing LAN, consult your network manager/system administrator for the correct configuration.

To make TCP/IP settings

1. In the Network window, double-click the TCP/IP Service for the Ethernet card on your computer (TCP/ IP > PCI Fast Ethernet DEC 21143 Based Adapter).

   The TCP/IP Properties window opens.

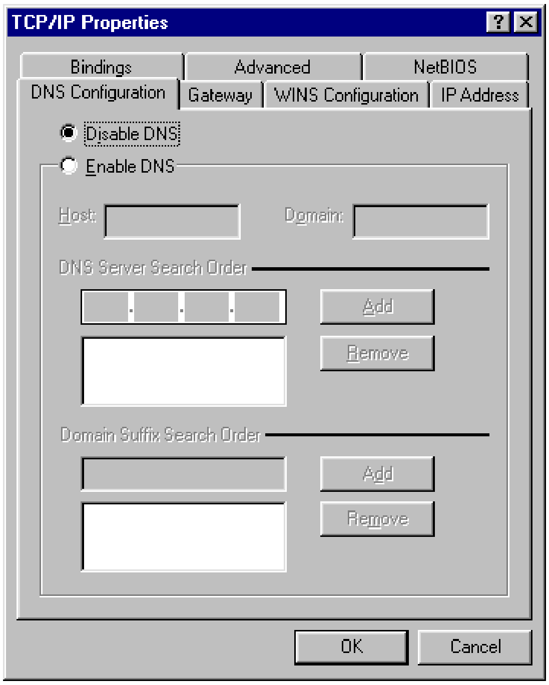


TCP/IP Properties

The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

New gateway: . . .

2. Click the Gateway tab and delete any installed gateways.
3. Click the DNS Configuration tab and click Disable DNS.

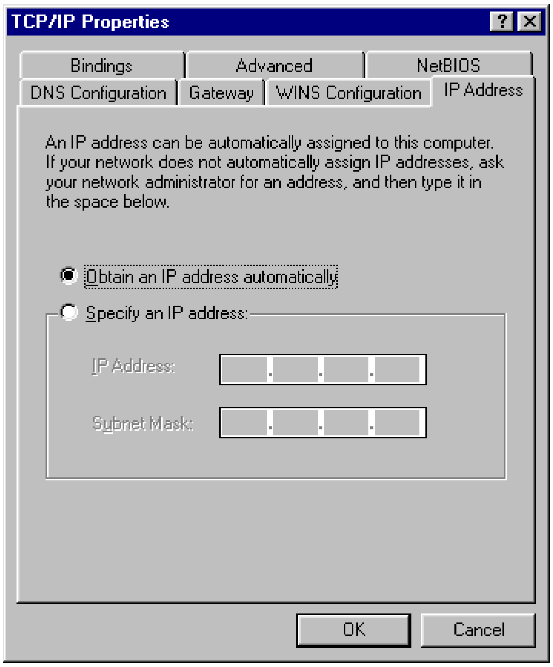


TCP/IP Properties

● Disable DNS

○ Enable DNS

4. Click the IP Address tab, and click Obtain an IP address automatically.



TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

Note
Nokia recommends that you use DHCP to assign IP addresses instead of assigning a static IP address to your computer. To assign a static IP address, click Specify an IP address and enter an IP address in the range of 192.168.10.129 to 254. Enter 255.255.255.0 as the Subnet Mask. Click OK to save the new settings.

5. Click Yes when the *Do you want to restart your computer?* message appears.

   Your computer must restart for the new settings to take effect.

   Your computer is now ready to access the IP45.

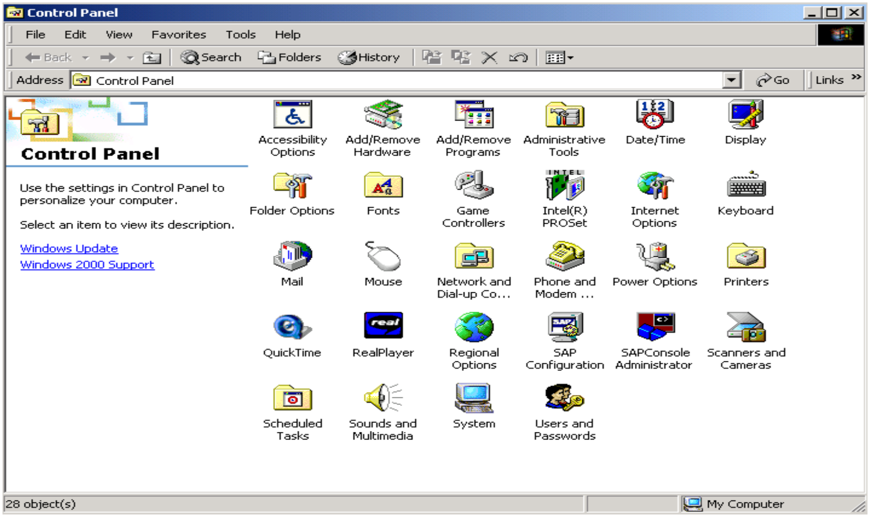
Setting Up the Nokia IP45 Security Platform with Microsoft Windows XP and 2000 Operating Systems

Windows XP has an Internet connection firewall option. Nokia recommends that you disable the firewall option if you are using the Nokia IP45.

To check for TCP/IP installation

1. Choose Start > Settings > Control Panel (in Windows XP Start > Control Panel from.)

   The Control Panel window opens.



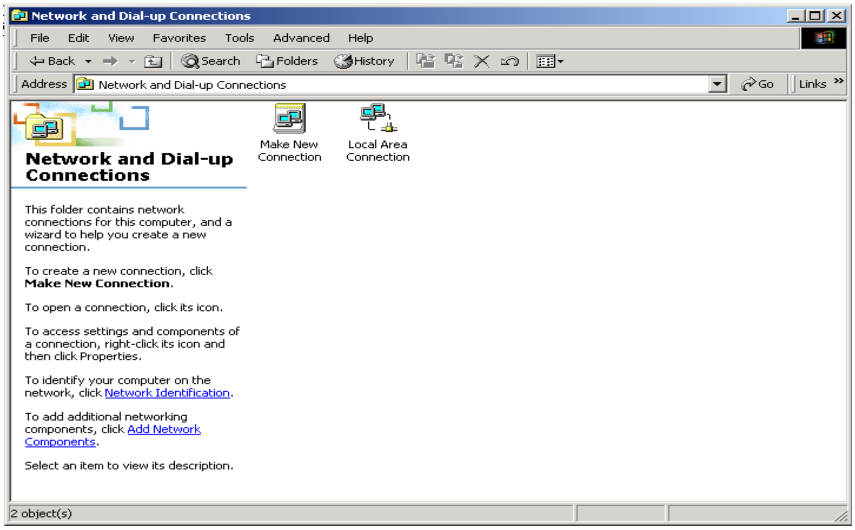
Use the settings in Control Panel to personalize your computer.

Select an item to view its description.

28 object(s)

2. Double-click the Network and Dial-up Connections icon (in Windows XP double-click the *Network Connections* icon).

The Network and Dial-up Connections window opens.


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go Links
Make New Connection
Local Area Connection
2 object(s)

Network and Dial-up Connections

This folder contains network connections for this computer, and a wizard to help you create a new connection.

To create a new connection, click **Make New Connection**.

To open a connection, click its icon.

To access settings and components of a connection, right-click its icon and then click Properties.

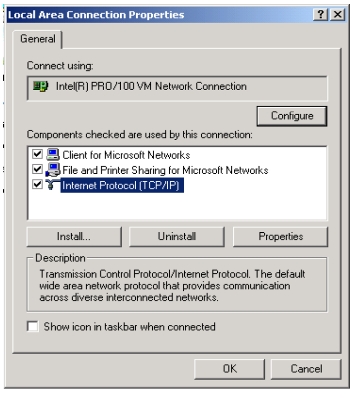
To identify your computer on the network, click Network Identification.

To add additional networking components, click Add Network Components.

Select an item to view its description.

3. Right-click the Local Area Connection icon and select Properties from the drop-down list.

   The Local Area Connection Properties window opens.



Connect using:

Intel(R) PRO/100 VM Network Connection

Components checked are used by this connection:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

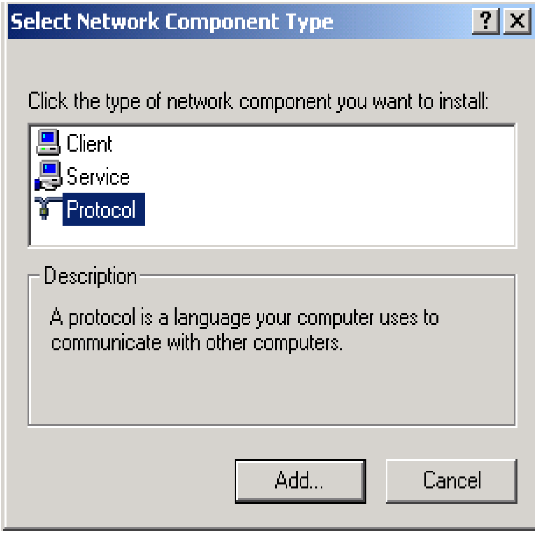
4. Check for TCP/IP in the Component list and whether it is configured with the Ethernet card installed on your computer.

   If TCP/IP does not appear in the Components list, install it as described in the section “To install TCP/IP” on page 39. If TCP/IP is already installed, skip the next section.

To install TCP/IP

1. In the Local Area Connection Properties window, click Install.

   The Select Network Component Type window opens.



Select Network Component Type

Click the type of network component you want to install:

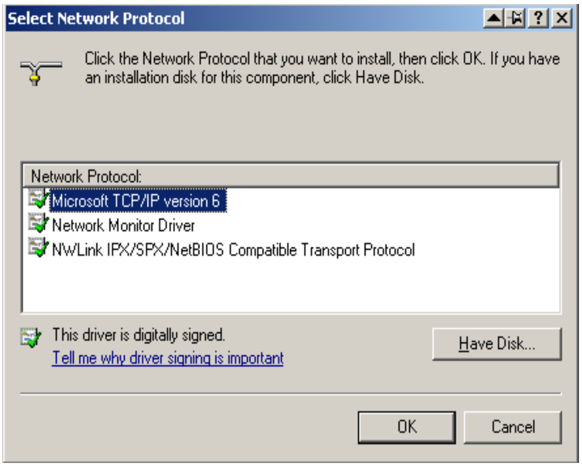
- Client
- Service
- Protocol

Description

A protocol is a language your computer uses to communicate with other computers.

2. Choose Protocol and click Add.

   The Select Network Protocol window opens.



Select Network Protocol

Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.

Network Protocol:

- Microsoft TCP/IP version 6
- Network Monitor Driver
- NWLink IPX/SPX/NetBIOS Compatible Transport Protocol

This driver is digitally signed.

Tell me why driver signing is important

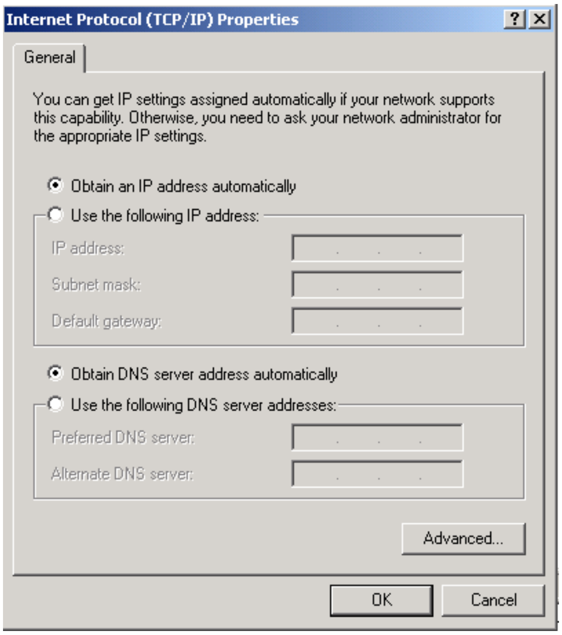
3. In the Select Network Protocol window, choose Internet Protocol (TCP/IP) and click OK.

   The TCP/IP protocol is installed on your computer.

To make TCP/IP settings

1. In the Local Area Connection Properties window, double-click Internet Protocol (TCP/IP) and click Properties.

   The Internet Protocol (TCP/IP) Properties window opens.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

2. Click Obtain an IP address automatically.

Note
Nokia recommends that you use DHCP to assign IP addresses instead of assigning a static IP address to your computer. To assign a static IP address, select Specify an IP address and enter an IP address in the range of 192.168.10.129 to 254. Enter 255.255.255.0 as the subnet mask. Click Ok to save the new settings.

3. Click Obtain DNS server address automatically.
4. Click OK to save the new settings.

   Your computer is now ready to access your IP45.

Setting Up the Nokia IP45 Security Platform with an Apple Computer

Use the following procedure to set up the TCP/IP protocol:

To make TCP/IP settings

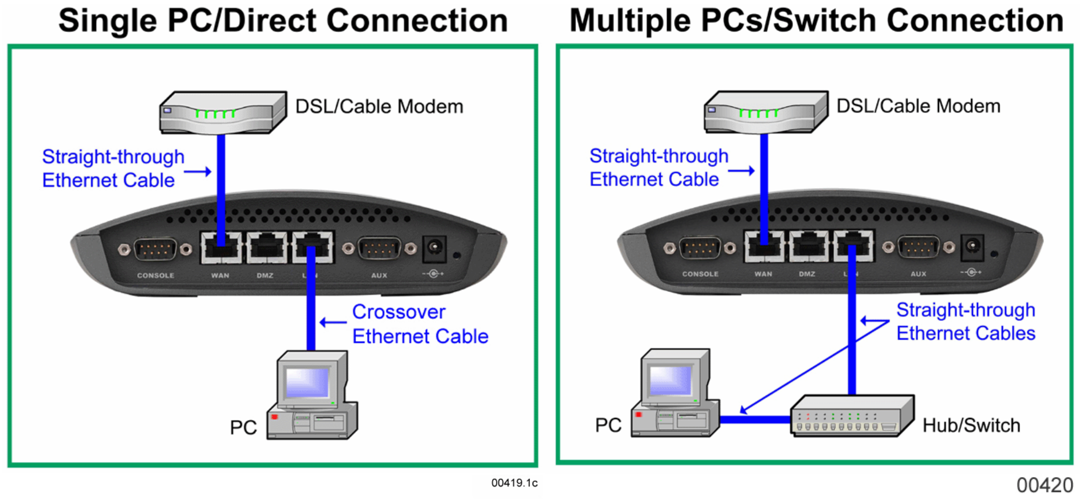
1. Choose Apple Menus > Control Panels > TCP/IP.

   The TCP/IP window opens.
2. Select Ethernet from the Connect drop-down list.
3. Select Using DHCP Server from the Configure drop-down list.
4. Close the window and save the setup.

Connecting the Nokia IP45 Security Platform to the Network

The following examples illustrate proper network cabling of the IP45 topology.

Figure 3 IP45 Topologies


Single PC/Direct Connection
DSL/Cable Modem
Straight-through Ethernet Cable
CONSOLE
WAN
DMZ
AUX
Crossover Ethernet Cable
PC
00419.1c
Multiple PCs/Switch Connection
DSL/Cable Modem
Straight-through Ethernet Cable
CONSOLE
WAN
DMZ
AUX
Straight-through Ethernet Cables
PC
Hub/Switch
00420

Installing your Network

Plan your network and the location of the IP45 to install the network.

To install the network

1. Connect the LAN cable
   - a. Connect one end of the Ethernet cable to the LAN port at the rear end of the device.
   - b. Connect the other end of the Ethernet cable to the computer, hubs, or another network. device.

2. Connect the DMZ cable
    a. Connect one end of the Ethernet cable to the DMZ port at the rear end of the device.
    b. Connect the other end of the Ethernet cable to the computer, hubs, or another network device.
3. Connect the WAN cable:
    a. Connect one end of the Ethernet cable to the WAN port at the rear end of the device.
    b. Connect the other end of the Ethernet cable to a cable modem, xDSL modem, or a corporate network.
4. Connect the power adapter to the power socket at the rear end of the device.
5. Plug in the AC power adapter to the electrical outlet.

3 Getting Started

This chapter describes the basic configurations and settings you need to perform to start using your Nokia IP45 security platform.

This chapter includes the following topics:

- First-Time Login
- Configuring the Nokia IP45 Security Platform for Internet Connection
- Making Initial Nokia IP45 Security Platform Settings
- Logging On to the Nokia IP45 Security Platform
- Accessing Nokia IP45 Securely

First-Time Login

After you connect your IP45 security platform to your network as described in "Connecting the Nokia IP45 Security Platform to the Network" on page 47, wait for the STAT LED to turn green.

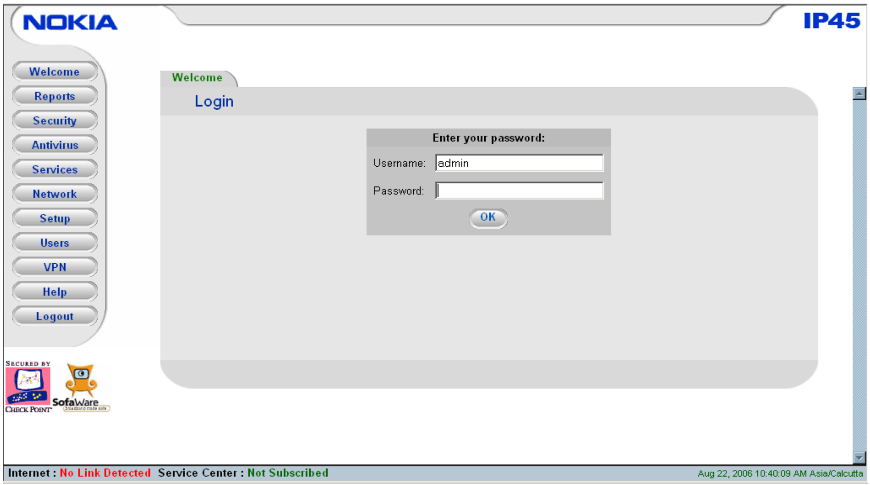
To login for the first time

1. Open your Web browser and type http://my.firewall in the location text box.

   The first time login page opens, prompting for a password.

   If you cannot access the GUI portal, see "Troubleshooting" on page 319 in this document.

Note
The IP45 ships without a password defined. If you are logging in for the first time, you are prompted to define the password by entering it twice. If you logged in before, enter the username and password you previously defined.



Login

Enter your password:

Username: admin

Password:

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 10:40:09 AM Asia/Calcutta

2. Type a password and re-type the password to confirm.
3. Click OK.

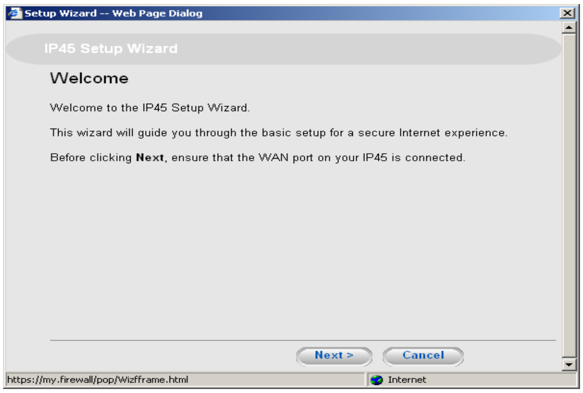
Note
The password must be between five and eleven alphanumeric characters. To change the password, click Setup on the main menu, and click Password. Enter the new password and confirm to update the change.

Configuring the Nokia IP45 Security Platform for Internet Connection

This section describes how to make the initial settings for your Nokia IP45 security platform to connect to the Internet by using the Setup wizard.

To connect to the Internet from the Nokia IP45 security platform

1. After you set the administrator password, you are prompted to make the initial settings from the Setup wizard.



Setup Wizard -- Web Page Dialog
IP45 Setup Wizard
Next >
Cancel
https://my.firewall/pop/Wizfframe.html
Internet

Welcome

Welcome to the IP45 Setup Wizard.

This wizard will guide you through the basic setup for a secure Internet experience.

Before clicking **Next**, ensure that the WAN port on your IP45 is connected.

The wizard guides you through making an Internet connection, setting the device time, registering for support services, and performing other basic configurations.

2. Click OK to continue.

3. The Internet Connection Method dialog box appears.

For more information about how to connect to the Internet, see "To configure an Internet connection by using the setup wizard" on page 74.

Making Initial Nokia IP45 Security Platform Settings

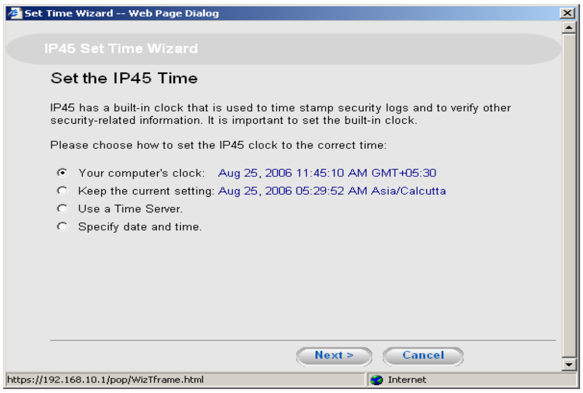
When you exit the Internet Connection Method wizard, you are prompted to set the device time. This section describes how to use the Setup wizard to set the device time, and how to make the initial Nokia IP45 security platform settings.

Setting the Nokia IP45 Security Platform Time

Use the following procedure to set the time of the Nokia IP45 security platform.

To set the time

1. When the IP45 Set Time wizard opens, check the appropriate setting.


Set Time Wizard -- Web Page Dialog
IP45 Set Time Wizard
Next >
Cancel
https://192.168.10.1/pop/WizTframe.html
Internet

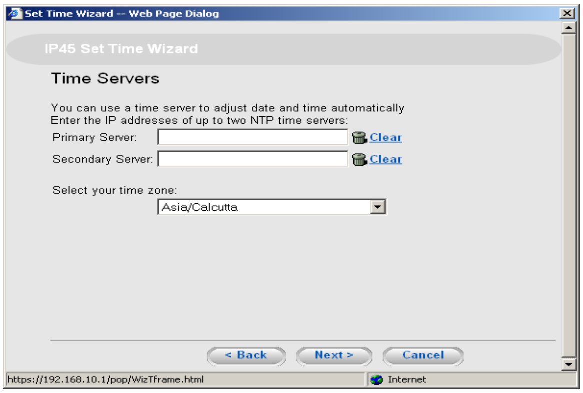
Set the IP45 Time

IP45 has a built-in clock that is used to time stamp security logs and to verify other security-related information. It is important to set the built-in clock.

Please choose how to set the IP45 clock to the correct time:

● Your computer's clock: Aug 25, 2006 11:45:10 AM GMT+05:30
○ Keep the current setting: Aug 25, 2006 05:29:52 AM Asia/Calcutta
○ Use a Time Server.
○ Specify date and time.

- If you check *Your computer's clock*, the IP45 automatically updates with the time settings of your computer.
- If you check *Keep the current time*, the IP45 retains its current time settings. No changes are made.
- If you check *Use a time Server*, the Time Servers window opens


Set Time Wizard -- Web Page Dialog
IP45 Set Time Wizard
Clear
Clear
< Back
Next >
Cancel
https://192.168.10.1/pop/WizTframe.html
Internet

Time Servers

You can use a time server to adjust date and time automatically
Enter the IP addresses of up to two NTP time servers:

Primary Server:

Secondary Server:

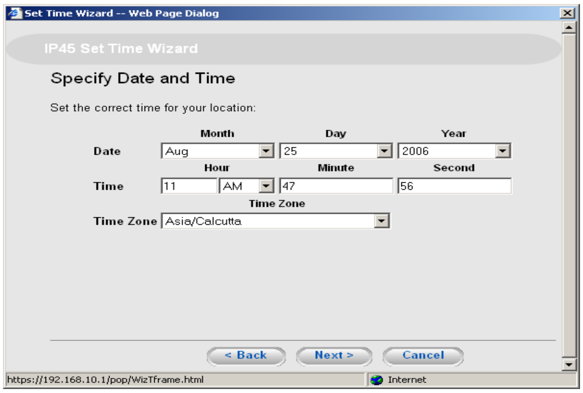
Select your time zone: Asia/Calcutta

  - Enter the IP Addresses for the Primary and Secondary time servers.
  - Select the time zone
  - Click Next
  - Click Finish.

Note
To edit the IP addresses of the time servers, click Clear next to the Primary and Secondary servers, enter the new IP address.

- The IP45 automatically applies the time settings.
- If you check *Specify date and time*, the Specify Date and Time window opens.

You can manually update the IP45 time settings.

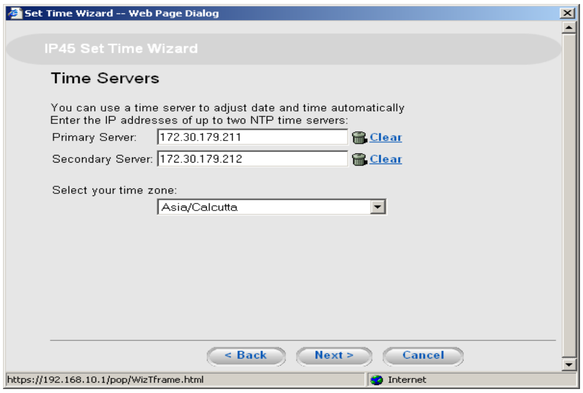

Set Time Wizard -- Web Page Dialog
IP45 Set Time Wizard
< Back
Next >
Cancel
https://192.168.10.1/pop/WizTframe.html
Internet

Specify Date and Time

Set the correct time for your location:

	Month	Day	Year
Date	Aug	25	2006
	Hour	**Minute**	**Second**
Time	11 AM	47	56
	Time Zone		
Time Zone	Asia/Calcutta		

2. Click Next to change your IP45 time settings:
   - If you choose to use a time server by clicking Use a Time Server, the Time Servers window opens.


Set Time Wizard -- Web Page Dialog
IP45 Set Time Wizard
Clear
Clear
< Back
Next >
Cancel
https://192.168.10.1/pop/WizTframe.html
Internet

Time Servers

You can use a time server to adjust date and time automatically
Enter the IP addresses of up to two NTP time servers:

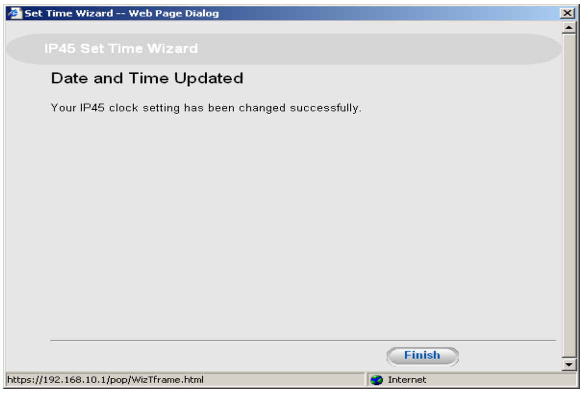
Primary Server: 172.30.179.211

Secondary Server: 172.30.179.212

Select your time zone:
Asia/Calcutta

3. Specify the IP addresses of the Primary and Secondary servers, to use as NTP time servers. Select time zone from the Time Zone drop down list.
4. Click Next.

The IP45 Set Time Wizard Date and Time Updated dialog box appears, indicating that time settings are changed successfully.


Set Time Wizard -- Web Page Dialog
IP45 Set Time Wizard

Date and Time Updated

Your IP45 clock setting has been changed successfully.

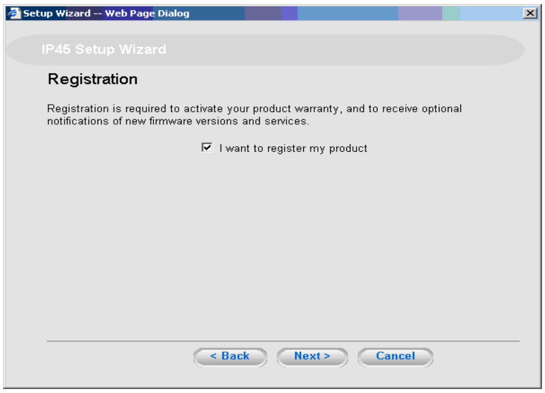
Finish
https://192.168.10.1/pop/WizTframe.html
Internet

5. Click Finish to exit the Set Time wizard.

Registering with the Nokia Support Site

You can register with the Nokia Support Site when you make your time settings.

The IP45 Setup Wizard begins when you exit the Set Time wizard.



Registration

Registration is required to activate your product warranty, and to receive optional notifications of new firmware versions and services.

☑ I want to register my product

Check the I want to register my product check box, and click Next.

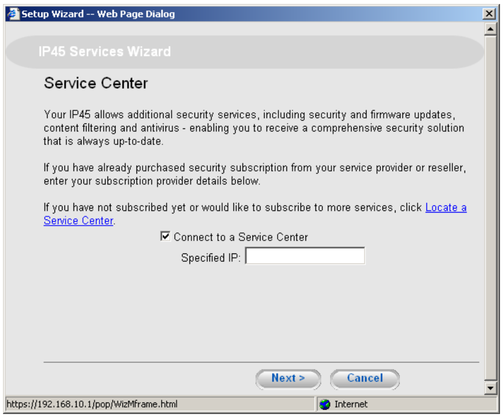
You are automatically taken to Nokia Support Web site:

https://support.nokia.com/agreement/SOHOregister.shtml.

Use the instructions on the Web site to complete the registration process and gain access to support Web resources and software updates.

Connecting to a Central Management Server

When you are registered for support, the Service Center window opens.



Service Center

Your IP45 allows additional security services, including security and firmware updates, content filtering and antivirus - enabling you to receive a comprehensive security solution that is always up-to-date.

If you have already purchased security subscription from your service provider or reseller, enter your subscription provider details below.

If you have not subscribed yet or would like to subscribe to more services, click Locate a Service Center.

☑ Connect to a Service Center

Specified IP:

This window allows you to define the central management server that the IP45 connects to.

The IP45 can connect to a central management server to allow central management of the firewall and VPN policies. Central management can also allow the IP45 to subscribe to additional services such as antivirus and URL filtering. The central server can be either a Check Point Smart Center, Smart Center Pro, or SofaWare Management Portal.

If your IP45 is centrally managed by any of these servers, check *Connect to a service center* and enter the IP address of the central management server in the Specified IP text box, then click Next. You are then prompted to enter the authentication information that allows the IP45 to communicate with the management server where you previously defined the IP45 object.

If your IP45 is not managed by a central management server, check *Connect to a service center*, and click Next.

For information connecting to service centers, see “Managing Large Scale Deployments of Nokia IP45” on page 70. For information about how to use subscription services, see “Using Managed Services” on page 303.

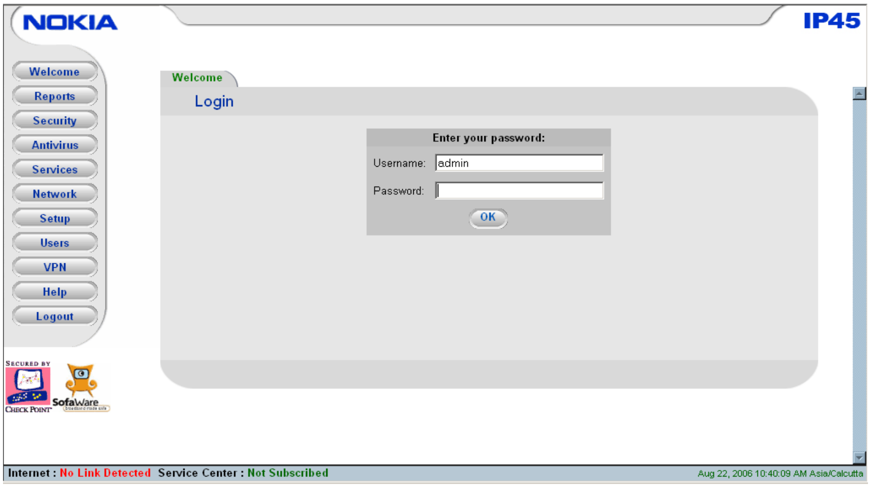
Logging On to the Nokia IP45 Security Platform

When you exit the Setup wizard, the IP45 Welcome page opens.

To access the graphical user interface of the Nokia IP45 security platform

1. Open your Web browser, and enter http://my.firewall in the address bar.

   The Login page opens.



Welcome

Login

Enter your password:

Username: admin

Password:

OK

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 10:40:09 AM Asia/Calcutta

2. Enter the password for the IP45 Tele 8 license.

   For IP45 Satellite X licenses, enter the username and password. If you are logging on for the first time, use *admin* as the username.

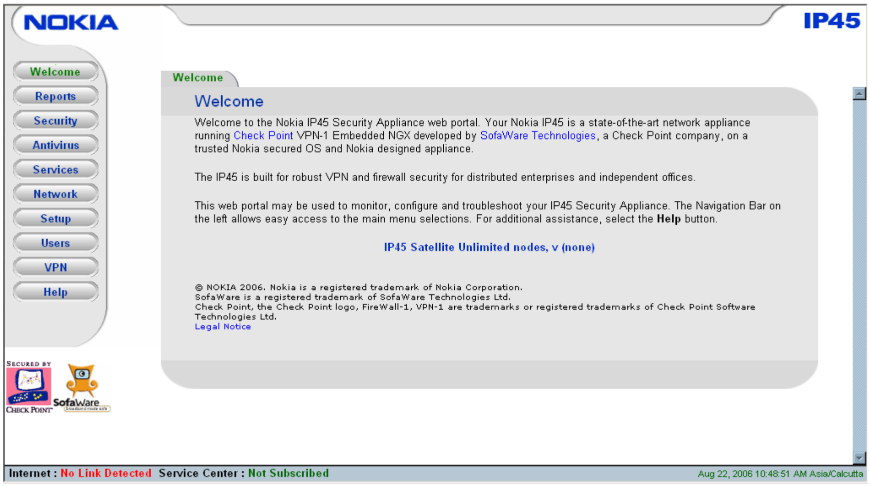
Note

The default user name for all Nokia IP45 licenses is *admin*. For the IP45 Satellite X licenses, you can define additional users. These additional users have separate usernames and passwords. For the IP45 Tele 8 license, you can only log on with the username admin. However, you can change the password. The password in all cases should be five to eleven alphanumeric characters.

You need to define your password in two instances:

- At the initial login
- When you reset the device to defaults

After the initial login, the Welcome page opens.



Welcome

Welcome to the Nokia IP45 Security Appliance web portal. Your Nokia IP45 is a state-of-the-art network appliance running Check Point VPN-1 Embedded NGX developed by SofaWare Technologies, a Check Point company, on a trusted Nokia secured OS and Nokia designed appliance.

The IP45 is built for robust VPN and firewall security for distributed enterprises and independent offices.

This web portal may be used to monitor, configure and troubleshoot your IP45 Security Appliance. The Navigation Bar on the left allows easy access to the main menu selections. For additional assistance, select the **Help** button.

IP45 Satellite Unlimited nodes, v (none)

© NOKIA 2006. Nokia is a registered trademark of Nokia Corporation.
SofaWare is a registered trademark of SofaWare Technologies Ltd.
Check Point, the Check Point logo, FireWall-1, VPN-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.
Legal Notice

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 10:48:51 AM Asia/Calcutta

The Welcome page displays the license type of your device (Tele 8 or Satellite X).

Accessing Nokia IP45 Securely

You can access the IP45 graphical user interface (GUI) through HTTPS either remotely or locally (from your internal network). For information about how to access through HTTPS from a remote location, see "Enabling HTTPS Web Access" on page 206.

Note
First configure HTTPS to access the IP45 GUI from a remote location.

To access the Nokia IP45 security platform through HTTPS from the Internet

1. To access the IP45 locally, enter **https://my.firewall** in the address bar of your browser

    Note
    The URL starts with HTTPS, not HTTP.

    The Welcome page opens.

To access the Nokia IP45 security platform from a remote location

1. Enter **https://<external IP address of IP45>:981** in the address bar of your browser.

    Note
    The URL starts with HTTPS, not HTTP.

If you are accessing the Nokia IP45 security platform for the first time, the security certificate in the IP45 is not yet known to the browser, so a security alert appears.

2. Click Yes to install the security certificate of the IP45 that you are trying to access. If you are using Internet Explorer 5.0 or later, do the following:

   a. Click View Certificate.

      The Certificate information page opens, with the General tab displayed.

   b. Click Install Certificate.

      The Certificate Import Wizard appears.

   c. Click Next.

      The Certificate Store appears.

      Select Automatically select the Certificate Store based on the type of certificate.

   d. Click Next.

      Completing the Certificate Import Wizard message appears.

   e. Click Finish.

      The Root certificate Store message appears.

   f. Click Yes.

      The certificate is installed.

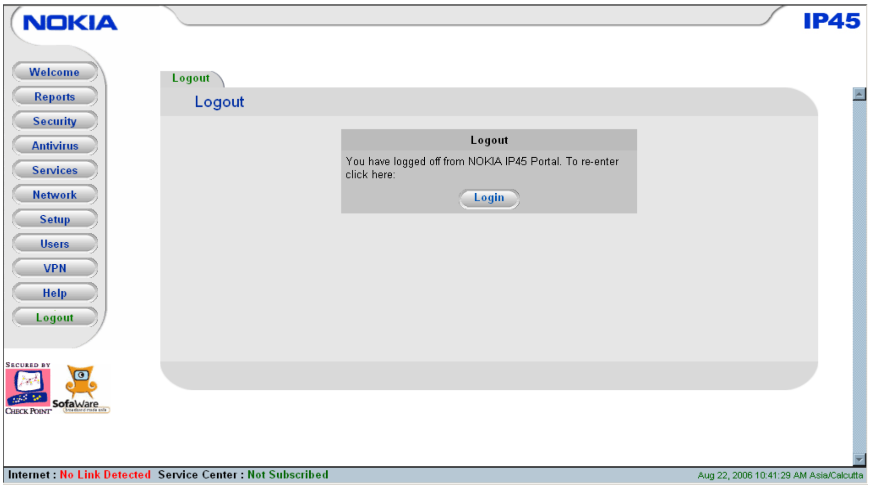
Logging Off from the Nokia IP45 Security Platform

Logging off terminates the Nokia IP45 security platform session. To connect to the IP45 again, enter the password.

To log off from IP45, perform one of the following procedures:

- If you are connected locally, click Logout.

The Logout page opens.



Logout

Logout

You have logged off from NOKIA IP45 Portal. To re-enter click here:

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 10:41:29 AM Asia/Calcutta

- If you are connected through HTTPS, close the browser window.

For information about connecting to your device through HTTPS, see "Accessing Nokia IP45 Securely" on page 57.

Understanding the Nokia IP45 Web GUI

When you log on to the Nokia IP45 security platform by using HTTP or HTTPS, you can configure the device by using the following methods:

- **Quick Setup Wizard**—configures the most common settings required for the IP45 to be up and running. The Web-based graphical user interface (GUI) automatically guides you through this wizard after your initial login.
- **Advanced GUI**—configures the various advanced features of the IP45.

For a configuration to take effect, click Submit.

For a brief description of the main components of the IP45 GUI, see the following sections. When you are familiar with these components, you are ready to make advanced configuration changes to the IP45 security platform.

Using the Nokia IP45 Security Platform Web-based User Interface

Table 11 provides a summary of the web-based GUI.

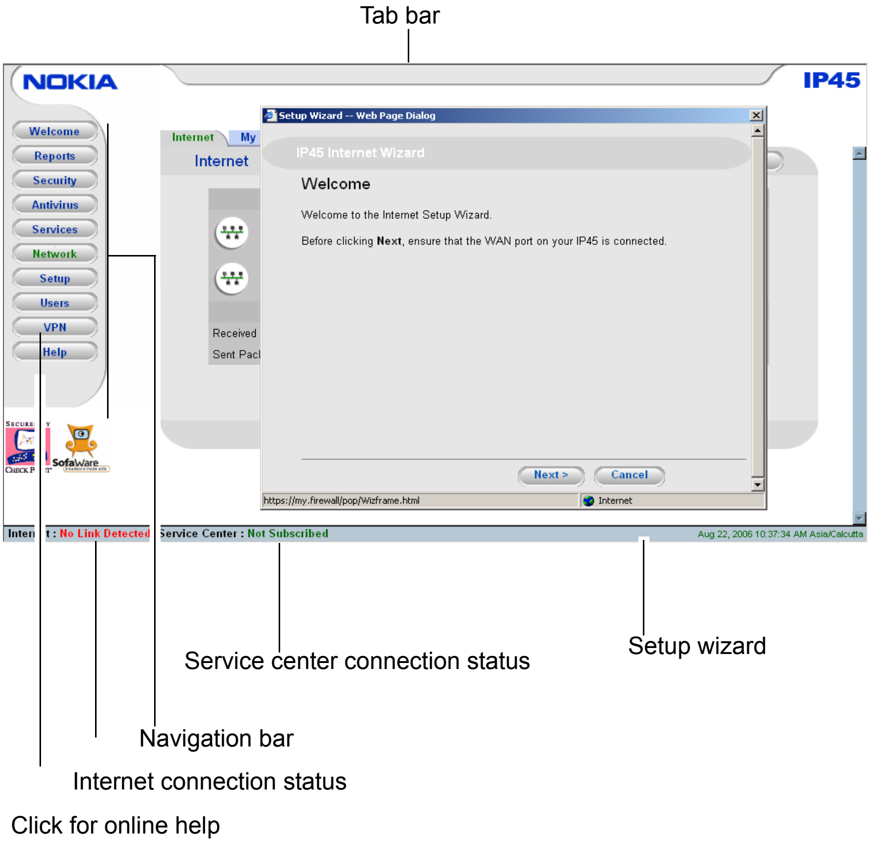
Table 11 Summary of the main components of the Nokia IP45 GUI

Component	Description
Navigation bar	Used to access various feature sets in the IP45 security platform
Tab bar	Used to access and configure all features in the IP45 security platform
Wizard	Used to configure common settings
Status bar	Provides status after a specific configuration
Help	Online help to assist you in configuring the IP45

Graphical User Interface Details

This section provides details about Nokia IP45 v4.0 graphical user interface (GUI).

Figure 4 Main Components of the Nokia IP45 Security Platform GUI



Setup Wizard -- Web Page Dialog

IP45 Internet Wizard

Welcome

Welcome to the Internet Setup Wizard.

Before clicking **Next**, ensure that the WAN port on your IP45 is connected.

https://my.firewall/pop/Wizframe.html

Internet : No Link Detected

Service Center : Not Subscribed

Aug 22, 2006 10:37:34 AM Asia/Calcutta

Note
The Nokia IP45 Tele 8 license does not support all of the features described in Table 12. For information on features supported by the Tele configuration, see "Nokia IP45 Security Platform Features" on page 22.

Table 12 provides information about the name and functionality of each element in the Nokia IP45 GUI.

Table 12 Names and Functions of the Nokia IP45 GUI Elements

Main Tab	Secondary Tabs	Description
Welcome		Displays Welcome and configuration information.
Reports	Event Log	Displays the last 100 events in four different categories: Blue, Red, Orange, and Green.
	Traffic Monitor	Allows you to visualize the network traffic(in graphical representation)
	Active Computers	Allows you to view computers on your network.
	Active Connections	Allows you to view current connections between your network and the external world.
	VPN Tunnels	Displays a list of established VPN tunnels.
Security	Firewall	Allows you to control firewall security level.
	Servers	Allows you to selectively allow incoming traffic from known applications and Internet services.
	Rules	Allows you to customize your security policy.
	SmartDefense	Allows you to deal with application-level attacks.
	HotSpot	Allows you to access the network from a public place on authentication
	Exposed Host	Allows you to define a Demilitarized Zone, i.e. a computer not protected by firewall.
Antivirus	Antivirus	Allows you to enable or disable the antivirus settings
	Policy	Allows you to add new rules and edit existing rules of antivirus policy
	Advanced	Allows you to select the file types to scan and block and also to define various other advanced settings such as archiving files, defining nested levels and compression ratio etc.
Services	Account	Provides information on services available in your service plan, and allows you to manage security services.
Network	Internet	Displays information on network setup and activity.

Table 12 Names and Functions of the Nokia IP45 GUI Elements (*continued*)

Main Tab	Secondary Tabs	Description
	My Network	Allows you to configure network settings.
	Ports	Allows you to manage ports and view ports status.
	Traffic Shaper	Allows you to define QoS classes.
	Network Objects	Allows you to configure network objects.
	Routes	Allows you to configure and edit routes
Setup	Firmware	Displays current firmware version and details
	High Availability	Allows you to configure high availability feature.
	Logging	Enables you to specify syslog server and syslog port.
	Management	Allows you to specify the protocols and accessing information for the IP45.
	Tools	Comprises several tools to effectively manage your IP45.
Users	Internal Users	Allows you to view, add, edit, and delete list of the IP45 users.
	RADIUS	Allows you to change your RADIUS settings.
VPN	VPN Server	Allows you to enable or disable a VPN server.
	VPN Sites	Allows you to view and edit a list of the configured VPN sites.
	VPN Login	Enables you to manually log in to a VPN site.
	Certificate	Allows you to control certificates for site-to-site VPN usage.
Help		Online Help.
Logout		Logs you out of the IP45.

Table 13 provides information about the elements in Status Bar.

Table 13 Status Bar

Field	Description
Internet	Your Internet connection status. You have different fields under Internet status. They are: • *Connected*: your IP45 device is connected to the Internet • *Not Connected*: your IP45 device is not connected to the Internet • *Establishing Connection*: your IP45 device is connecting to the Internet. • *Contacting Gateway*: your IP45 device is trying to contact the Internet default gateway. • *Disabled*: The Internet connection has been disabled, manually. You can configure both primary and secondary Internet connections. When both the connections are configured, the Status bar shows this status.
Service Center	Displays your subscription services status. Your Service Center offer various subscription services like firewall services, and optional services such as Web filtering, and email antivirus. The service center status can be one of the following: • *Not Subscribed*: you are not subscribe to security services • *Connection Failed*: your IP45 device failed to connect to the service center. • *Connecting*: your IP45 device is connecting to the service center • *Connected*: you are connected to the service center, and the security services are active.

Note
You can view help information about a field by pointing to the help icon in the right corner of the IP45 GUI screens. The Help icon is visible only for those fields that have further information available. For information about other fields, please see related sections in the *IP45 Security Platform User’s Guide Version 4.0* or choose Help from the main menu.

4 Accessing the Nokia IP45 Security Platform

This chapter discusses the methods for accessing and configuring the Nokia IP45 security platform. This chapter also provides an introduction to centrally managing large scale deployments of Nokia IP45 by using Nokia Horizon Manager, SmartCenter Large Scale Manager, and the SofaWare Security Management Portal.

The main topics for this chapter include:

- Connection Methods
- Configuration Methods
- Connecting the Nokia IP45 Security Platform to a Computer by Using the Console Port
- Using Telnet to Connect to the Nokia IP45 Security Platform
- Enabling and Disabling Telnet Access to Nokia IP45
- Accessing Nokia IP45 with HTTP and HTTPS
- Managing Large Scale Deployments of Nokia IP45

Connection Methods

You can connect to your Nokia IP45 security platform locally through LAN, WAN, DMZ, or console ports for Inband management. You can also connect from a remote location by using modem dial-in for out-of-band management (OOB).

For information about how to use OOB to configure your device, see "Configuring Nokia IP45 Through Out-of-Band Management" on page 233.

Typically the WAN port for your device is connected to your Internet service provider (ISP), while the LAN port is connected to your computer, or to a hub, if you are using the IP45 between your computer network and the outside world. You can connect your computer to the console port of your IP45 to manage the device by using the command-line interface (CLI).

Configuration Methods

The Nokia IP45 security platform supports the following configuration methods:

- Command-line interface (CLI) by using console, Telnet, Secure Shell (SSH)

- Web-based graphical user interface (GUI) by using HTTP, and HTTPS.

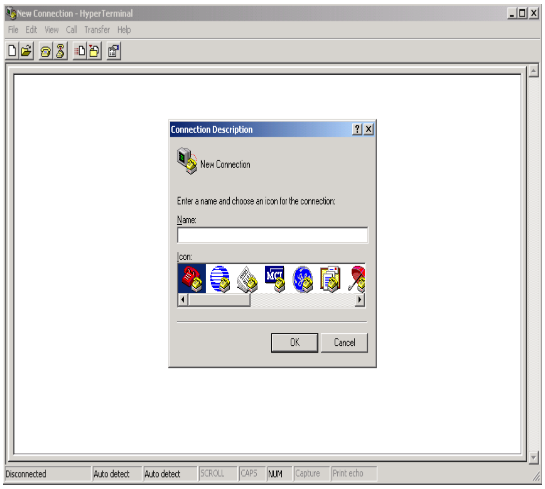
Connecting the Nokia IP45 Security Platform to a Computer by Using the Console Port

Your Nokia IP45 security platform has a console serial port. Connect the RS-232 cable (that is shipped along with the device) from the serial port of your computer to the console port of the IP45. You can then manage the device by using a terminal emulation program such as Hyper Terminal.

To connect to Nokia IP45 with HyperTerminal

1. To start the HyperTerminal program, choose: Start > Programs > Accessories > Communications > HyperTerminal.

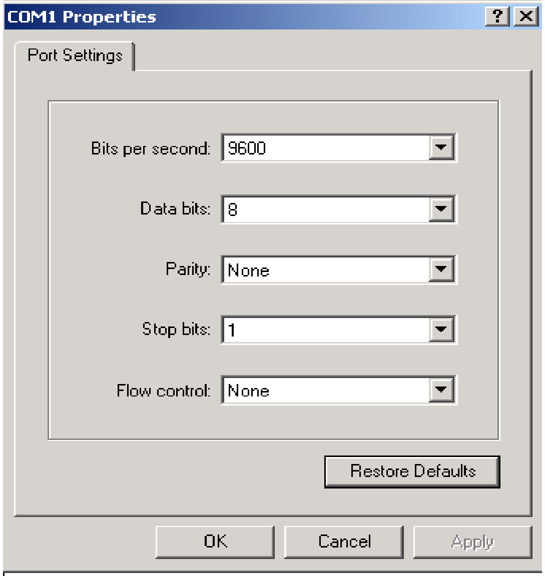
   The Connection Description window opens.



Enter a name and choose an icon for the connection:

2. Assign a name for your connection, such as *IP45,* and click OK.
3. Select the serial port that you will use: COM1 or COM2, and click OK.

4. When you select the serial port, the COM1 (or COM2) Properties window opens.



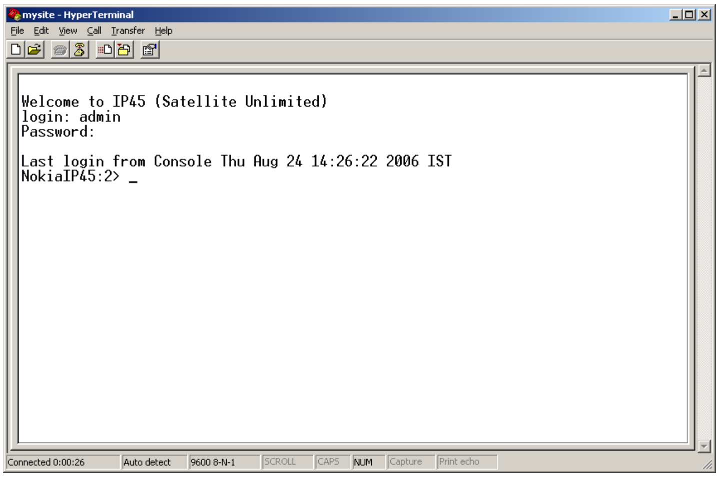
Bits per second: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None

Select the following port settings:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

5. Click Ok to continue.

6. The login prompt is displayed by default.



```
Welcome to IP45 (Satellite Unlimited)
login: admin
Password:

Last login from Console Thu Aug 24 14:26:22 2006 IST
NokiaIP45:2> _
```

The IP45 ships without a password defined. If you are logging in for the first time, you are prompted to define the password by entering it twice. If you logged in before, enter the username and password you previously defined.

For more information about CLI commands, see the *Nokia IP45 Security Platform CLI Reference Guid*e, *Version 4.0*.

Using Telnet to Connect to the Nokia IP45 Security Platform

You can access the command-line interface through a Telnet session.

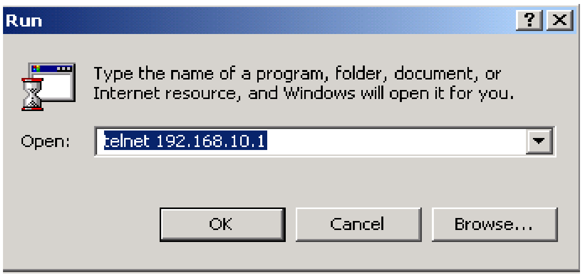
Telnet access is disabled by default. You can allow Telnet access from the LAN, and WAN by configuring separate user rules. (No LAN or WAN access is available until it is configured)

Note
Before you start Telnet, ensure that the Telnet program is installed on your computer, and that you can access the IP45 by using Telnet. The method for starting Telnet differs between operating systems. You can use the method given here to start a Telnet session from Windows 2000.

To connect to the IP45 security platform by using Telnet

1. Choose Start > Run
2. In the command window that opens, type *telnet* followed by the IP address of your IP45 security platform.

   If your device IP address is 192.168.10.1, the run window opens as follows:

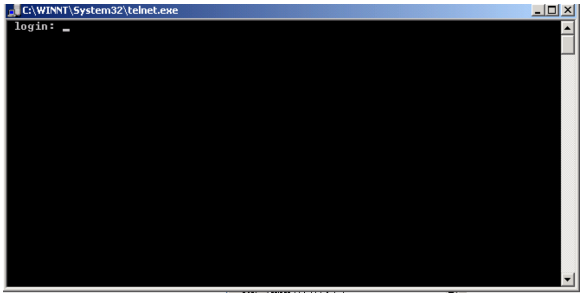


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: telnet 192.168.10.1

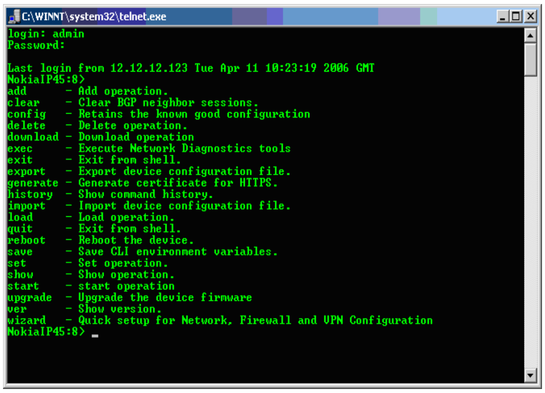
3. Click OK.

The Telnet command window opens with a login prompt.



```
login: _
```

4. Enter your username and password.You can now manage your IP45 security platform by using simple commands.
5. Press the tab key to view a list of useful, simple commands to start managing your IP45. For more information, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0*.



```
login: admin
Password:

Last login from 12.12.12.123 Tue Apr 11 10:23:19 2006 GMT
NokiaIP45:8>
add      - Add operation.
clear    - Clear BGP neighbor sessions.
config   - Retains the known good configuration
delete   - Delete operation.
download - Download operation
exec     - Execute Network Diagnostics tools
exit     - Exit from shell.
export   - Export device configuration file.
generate - Generate certificate for HTTPS.
history  - Show command history.
import   - Import device configuration file.
load     - Load operation.
quit     - Exit from shell.
reboot   - Reboot the device.
save     - Save CLI environment variables.
set      - Set operation.
show     - Show operation.
start    - start operation
upgrade  - Upgrade the device firmware
ver      - Show version.
wizard   - Quick setup for Network, Firewall and VPN Configuration
NokiaIP45:8> _
```

Enabling and Disabling Telnet Access to Nokia IP45

Telnet access is disabled by default.

Use the following command from the IP45 CLI to enable Telnet access to the device:

```
set acl service telnet enable
```

Use the following command to disable Telnet:

```
set acl service telnet disable
```

This command disables Telnet access from the WAN, LAN, and DMZ ports.

Using Secure Shell to Connect to the Nokia IP45 Security Platform

You can use Secure Shell (SSH) to access your IP45 security platform, securely. SSH is an application protocol and software suite that allows secure network services over an insecure network such as the Internet.

Note
By default, SSH access is allowed from LAN, and DMZ.

To access your Nokia IP45 security platform with SSH

1. Install an SSH client that allows you to make SSH connections to your IP45.
2. Provide the following information to connect to the device:
   - IP Address of the device
   - username
   - Authentication method, whether Password or Public Key

For more information about SSH, see “Configuring Network Access” on page 191.

Accessing Nokia IP45 with HTTP and HTTPS

You can access and manage your IP45 through a user-friendly GUI. For more information, see Logging On to the Nokia IP45 Security Platform on page 55.

Managing Large Scale Deployments of Nokia IP45

You can centrally manage the Nokia IP45 security platform by using the following applications:

- Nokia Horizon Manager
- Check Point SmartCenter LSM
- SofaWare Management Portal

These centralized management applications allow you to manage large-scale deployments.

For an overview of how to manage your device, see “Using Managed Services” on page 303.

Deploying the Nokia IP45 Security Platform with the Nokia Horizon Manager

You can manage the Nokia IP45 security platform by using the Nokia Horizon Manager.

Nokia Horizon Manager is a software application designed to manage, and configure a large number of Nokia IP security platforms (devices) that reside on a corporate enterprise, managed service provider (MSP), or hosted applications service provider network (ASP).

You can use Nokia Horizon Manager to perform software inventory, configuration, and image management operations.

Deploying the Nokia IP45 Security Platform with the Check Point SmartCenter Large Scale Manager

The Check Point SmartCenter Large Scale Manager (LSM) allows you to manage many Check Point Remote Office/Branch Office (ROBO) gateways from a single SmartCenter Server.

For additional information on installing and configuring LSM, see Check Point SmartCenter LSM documentation.

Deploying Nokia IP45 with SofaWare Management Portal

The SofaWare Security Management Portal (SMP) is a security platform that enables centralized management of a large number of firewalls embedded in broadband access devices or gateways.

You can use the SofaWare SMP for both policy and configuration management.

Note
Configure the management servers by using SofaWare Management Portal before you can use subscription services such as Web filtering, email antivirus, and software updates by Nokia IP45.

Using the Sofaware Management Portal, you can:

- Update security policies and user interface files.
- Configure and fine-tune SofaWare management services like Web filtering, email antivirus, and software updates.

5 Connecting to the Internet with the Nokia IP45 Security Platform

This chapter explains how to configure the Internet to make a secure connection by using the Nokia IP45 security platform.

This chapter includes the following topics:

Configuring an Internet Connection

You can configure an Internet connection by using one of the following setup tools:

- **Setup Wizard**—guides you through the configuration process, step by step.
- **Advanced Setup**—provides advanced setup options.

Note
You must configure the Internet connection on initial operation, and reset to defaults operations.

Using the Setup Wizard

You can use the Setup Wizard to configure the Internet connection for the Nokia IP45 security platform through the graphical user interface (GUI). The Setup Wizard guides you through the configuration process, step by step.

You can connect to the Internet using any of the following broadband connection methods:

- PPPoE (PPP over Ethernet)
- PPTP

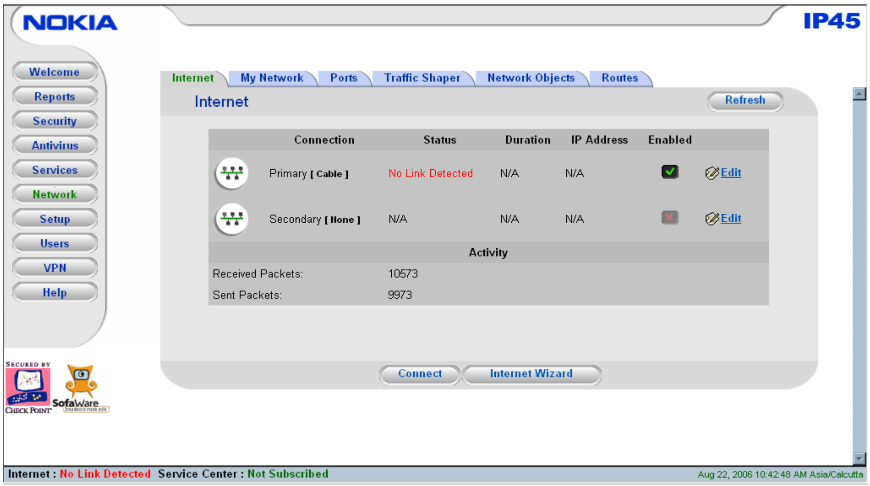
- Cable Modem
- Static IP
- DHCP (Dynamic IP)

Note
The IP45 Setup wizard, which you can use for basic configuration of the device, is always accessible from Setup > Firmware.

To configure an Internet connection by using the setup wizard

1. Choose Network from the main menu.

   The Internet page opens.



Connection	Status	Duration	IP Address	Enabled	
Primary [Cable]	No Link Detected	N/A	N/A	✓	Edit
Secondary [None]	N/A	N/A	N/A	✗	Edit

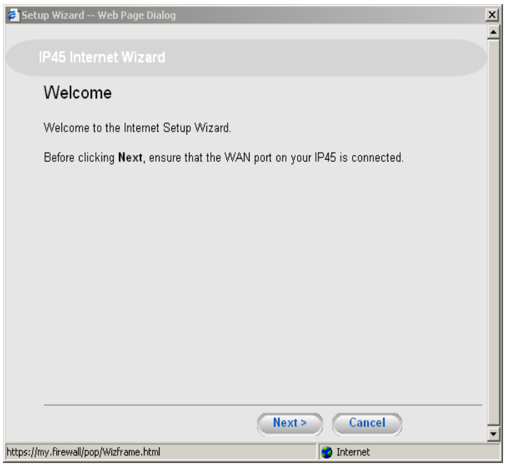
Activity

Received Packets:	10573
Sent Packets:	9973

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 10:42:48 AM Asia/Calcutta

2. Click Internet Wizard at the bottom of the page.

   The IP45 Internet Wizard appears.

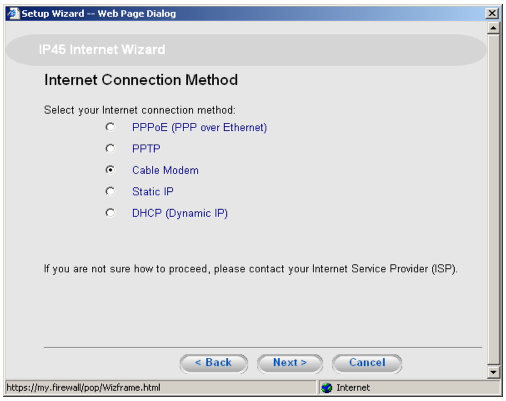

Setup Wizard -- Web Page Dialog
IP45 Internet Wizard
Next >
Cancel
https://my.firewall/pop/Wizframe.html
Internet

Welcome

Welcome to the Internet Setup Wizard.

Before clicking **Next**, ensure that the WAN port on your IP45 is connected.

3. Click Next to proceed.
4. The Internet Connection Method window opens.


Setup Wizard -- Web Page Dialog
IP45 Internet Wizard
< Back
Next >
Cancel
https://my.firewall/pop/Wizframe.html
Internet

Internet Connection Method

Select your Internet connection method:

○ PPPoE (PPP over Ethernet)
○ PPTP
● Cable Modem
○ Static IP
○ DHCP (Dynamic IP)

If you are not sure how to proceed, please contact your Internet Service Provider (ISP).

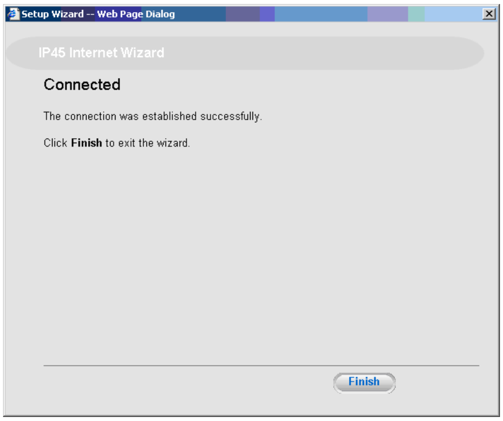
5. Select the Internet connection method, and click Next.

   You can choose between the following modes of broadband connection:

   - PPPoE (PPP over Ethernet)
   - PPTP
   - Cable Modem
   - Static IP
   - DHCP (Dynamic IP)

Note
If you select to connect by PPTP or PPPoE dialer, do not use dial-up software to connect to the Internet. The IP45 does the PPPoE negotiation.

6. Follow the wizard instructions until the Connected message appears.



Connected

The connection was established successfully.

Click **Finish** to exit the wizard.

7. Click Finish.

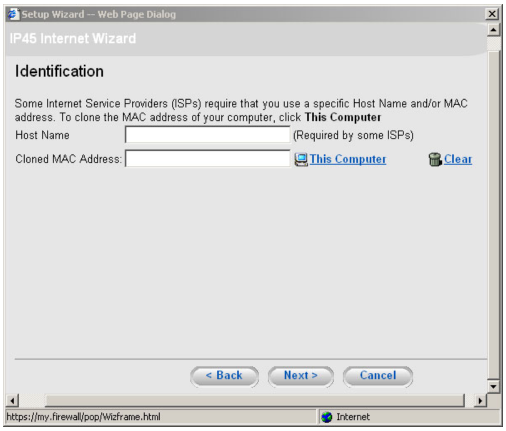
   You are now connected to the Internet.

   The wizard prompts you to register and set up your subscription options, which vary from product to product.

   For information about configuring device time, registering with Nokia Support Center and subscribing to additional services with the Setup wizard, see "Getting Started" on page 49.

Cable Modem Connection Settings

If you select cable modem connection through the procedure "To configure an Internet connection by using the setup wizard" on page 74, the Identification window opens.


Setup Wizard -- Web Page Dialog
IP45 Internet Wizard

Identification

Some Internet Service Providers (ISPs) require that you use a specific Host Name and/or MAC address. To clone the MAC address of your computer, click **This Computer**

Host Name (Required by some ISPs)

Cloned MAC Address:

This Computer
Clear
< Back
Next >
Cancel
https://my.firewall/pop/Wizframe.html
Internet

Type the Host name and MAC Clone address if they are required by the ISP. For more details on cloning MAC address, see "To configure for cable modem connection" on page 77.

To configure for cable modem connection

1. Type the Host name in the Identification window.

   This field is optional. It might be required by your ISP and if so the ISP provides it.

2. Click Next.

   The Confirmation message appears.

3. Click Next.

   The device attempts to connect to the Internet.

   At the end of the connection process, the Connected message appears. When you are connected, the wizard prompts you to register your details and set up your subscription options, which vary from product to product.

4. Follow the instructions until the wizard is done, and then click Finish.

MAC Cloning

Some ISPs require that you register any MAC addresses of the computer behind the cable modem before you establish an Internet connection.

Nokia IP45 takes the place of the computer behind the cable modem and you can use MAC cloning to enter the original computer MAC address without contacting the ISP to change that information.

Cloning a MAC Address

A MAC address is a 12-digit identifier assigned to every network device. If your ISP restricts connections to specific, recognized MAC addresses, you must clone a MAC address.

IP45 v4.0 supports MAC cloning for WAN2 (DMZ).

To clone a MAC address

1. Choose Network from the main menu.

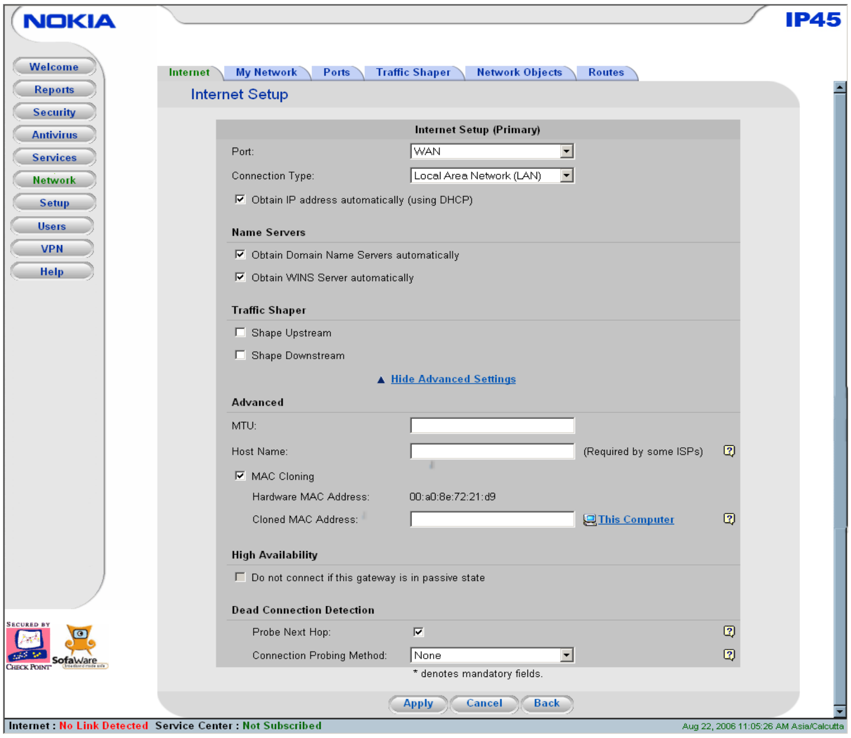
   The Internet page opens.

2. To clone the MAC address, click the Edit next to the interface.

   The Internet Setup page opens.

3. Click *Show Advanced Settings*.

The Internet Setup page now displays the MAC cloning option.



Internet Setup

Internet Setup (Primary)

Port: WAN

Connection Type: Local Area Network (LAN)

☑ Obtain IP address automatically (using DHCP)

Name Servers

☑ Obtain Domain Name Servers automatically

☑ Obtain WINS Server automatically

Traffic Shaper

□ Shape Upstream

□ Shape Downstream

▲ Hide Advanced Settings

Advanced

MTU:

Host Name: (Required by some ISPs)

☑ MAC Cloning

Hardware MAC Address: 00:a0:8e:72:21:d9

Cloned MAC Address: This Computer

High Availability

□ Do not connect if this gateway is in passive state

Dead Connection Detection

Probe Next Hop: ☑

Connection Probing Method: None

* denotes mandatory fields.

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 11:05:26 AM Asia/Calcutta

4. Select MAC Cloning. Do one of the following:

a. Click This Computer to automatically clone the MAC address of your computer to the IP45.

or

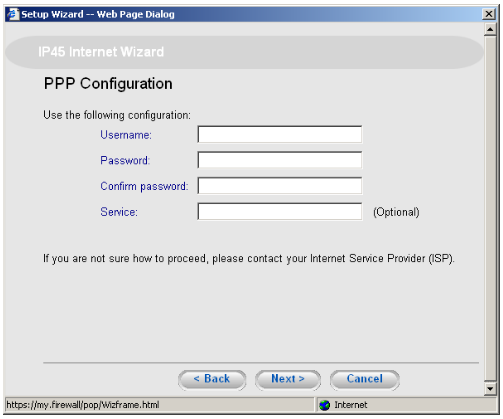
b. If the ISP requires authentication by using the MAC address of a different computer, type the MAC address in the Cloned MAC Address field.

5. Click Apply.

To connect by using a PPPoE connection

1. Select PPPoE from the Internet Connection Method window.

   The PPP Configuration window opens.



Setup Wizard -- Web Page Dialog

IP45 Internet Wizard

PPP Configuration

Use the following configuration:

Username:

Password:

Confirm password:

Service: (Optional)

If you are not sure how to proceed, please contact your Internet Service Provider (ISP).

https://my.firewall/pop/Wizframe.html

2. Type the following:

   a. Your username, and password and confirm the password.

   b. The service name. This field is optional.

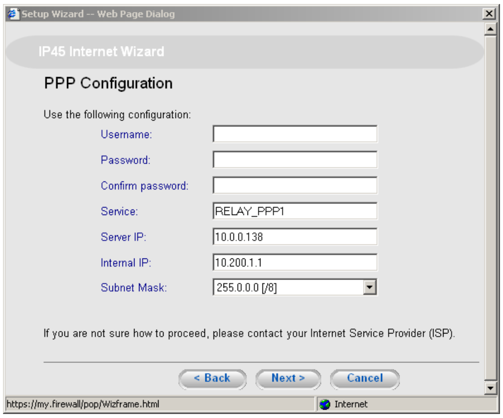
3. Click Next.

   The system attempts to connect to the Internet through the PPPoE connection. At the end of the connection process, the Connected message appears.

To connect by using the PPTP connection

1. Select PPTP from the Internet Connection Method window.

   The PPP Configuration window opens.



Setup Wizard -- Web Page Dialog

IP45 Internet Wizard

PPP Configuration

Use the following configuration:

Username:

Password:

Confirm password:

Service: RELAY_PPP1

Server IP: 10.0.0.138

Internal IP: 10.200.1.1

Subnet Mask: 255.0.0.0 [/8]

If you are not sure how to proceed, please contact your Internet Service Provider (ISP).

https://my.firewall/pop/Wizframe.html

2. Type the following information:

   - Username and Password, and confirm the password.

- Service name.
- IP address of the PPTP modem in the Server IP text box.
- Local IP address required for accessing the PPTP modem in the Internal IP text box.
- Subnet Mask of the PPTP modem.

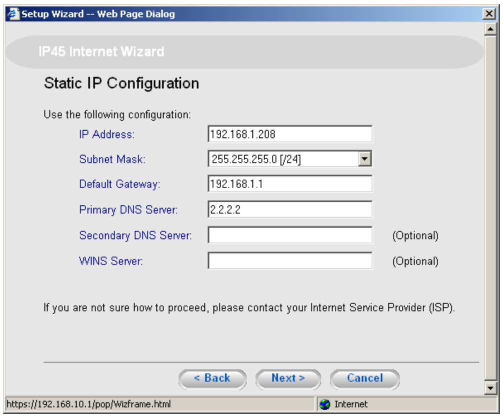
3. Click Next.

   The Connecting message appears while the system attempts to connect to the Internet through the PPTP connection. At the end of the connection process, the Connected message appears.

To connect by using a static IP connection

1. Select Static IP from the Internet Connection Method window.

   The Static IP Configuration window opens.


Setup Wizard -- Web Page Dialog

IP45 Internet Wizard

Static IP Configuration

Use the following configuration:

IP Address: 192.168.1.208

Subnet Mask: 255.255.255.0 [/24]

Default Gateway: 192.168.1.1

Primary DNS Server: 2.2.2.2

Secondary DNS Server: (Optional)

WINS Server: (Optional)

If you are not sure how to proceed, please contact your Internet Service Provider (ISP).

https://192.168.10.1/pop/Wizframe.html

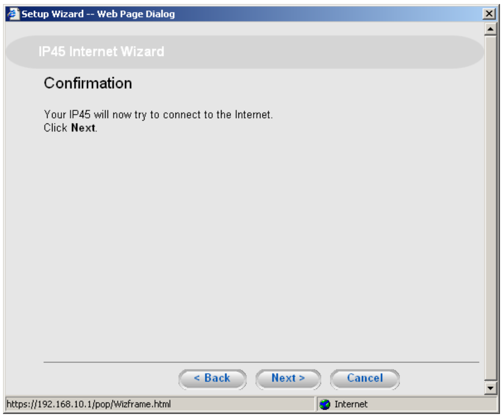
2. Type the following information:
   - Static IP address of the Nokia IP45 appliance.
   - Subnet Mask that applies to the static IP address.
   - IP address of the Default Gateway of your Internet service provider.
   - IP address of the Primary DNS Server
   - IP address of the Secondary DNS Server. This field is optional.
   - IP address of the WINS Server. This field is optional.
3. Click Next.

   The Connecting message appears while the system attempts to connect to the Internet through the static IP connection. At the end of the connection process, the Connected message appears.

To connect using a DHCP connection

1. Select DHCP (Dynamic IP) from the Internet Connection Method window.
2. Click Next.

   The Confirmation message appears.


Setup Wizard -- Web Page Dialog
IP45 Internet Wizard
< Back
Next >
Cancel
https://192.168.10.1/pop/Wizframe.html
Internet

Confirmation

Your IP45 will now try to connect to the Internet.
Click **Next**.

3. Click Next.

   The Connecting message appears while the system attempts to connect to the Internet through the DHCP connection. At the end of the connection process, the Connected message appears.

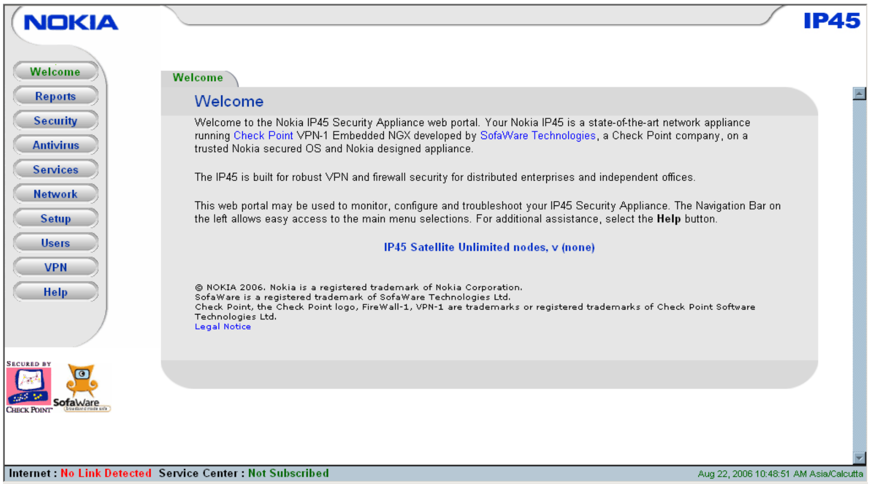
Manually Configuring the Internet Setting

You can configure the Internet settings for your IP45 manually.

To configure the Internet connection

1. Proceed as per steps 1 and 2 in "Using the Setup Wizard" on page 73 to connect using PPTP and PPPoE.
2. Click Cancel on the Internet Setup wizard.

The Welcome page is displayed.



Welcome

Welcome to the Nokia IP45 Security Appliance web portal. Your Nokia IP45 is a state-of-the-art network appliance running Check Point VPN-1 Embedded NGX developed by SofaWare Technologies, a Check Point company, on a trusted Nokia secured OS and Nokia designed appliance.

The IP45 is built for robust VPN and firewall security for distributed enterprises and independent offices.

This web portal may be used to monitor, configure and troubleshoot your IP45 Security Appliance. The Navigation Bar on the left allows easy access to the main menu selections. For additional assistance, select the **Help** button.

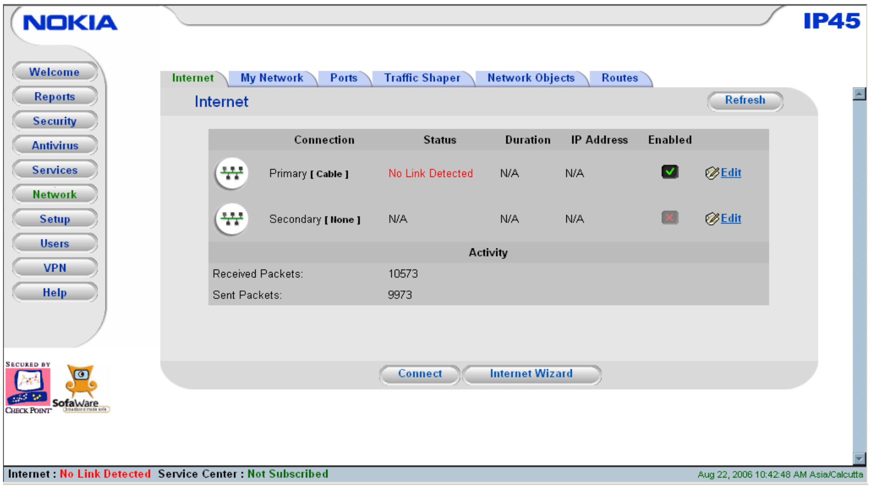
IP45 Satellite Unlimited nodes, v (none)

© NOKIA 2006. Nokia is a registered trademark of Nokia Corporation.
SofaWare is a registered trademark of SofaWare Technologies Ltd.
Check Point, the Check Point logo, FireWall-1, VPN-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.
Legal Notice

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 10:48:51 AM Asia/Calcutta

3. Choose Network from the main menu.

   The Internet page opens.



Internet

Connection	Status	Duration	IP Address	Enabled	
Primary [Cable]	No Link Detected	N/A	N/A	✓	Edit
Secondary [None]	N/A	N/A	N/A	☒	Edit

Activity

Received Packets:	10573
Sent Packets:	9973

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 10:42:48 AM Asia/Calcutta

4. Click Edit next to Primary.

   The Internet Setup page with a list of connection type options appears.

5. Select the Connection Type.

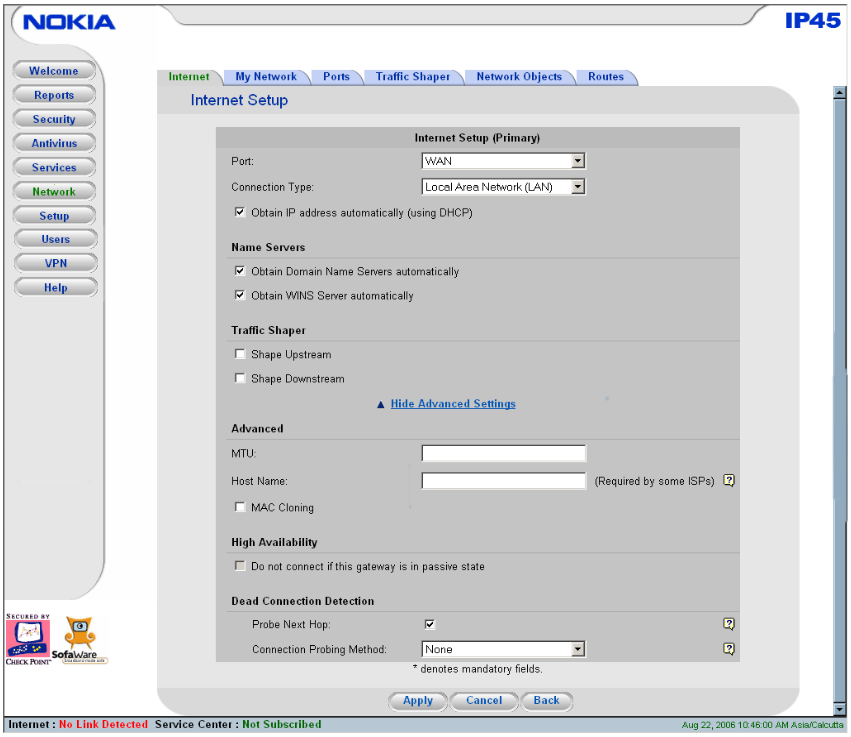
   The display changes according to the connection type you select. Perform the following procedures in accordance with the connection type you choose.

To use a LAN connection

The following steps provide details about the LAN connection.

1. Select LAN connection from the Internet Setup page at Connection Type.
2. Click *Show Advanced Settings*.

The following page opens.



Internet Setup

Internet Setup (Primary)

Port: WAN

Connection Type: Local Area Network (LAN)

☑ Obtain IP address automatically (using DHCP)

Name Servers

☑ Obtain Domain Name Servers automatically

☑ Obtain WINS Server automatically

Traffic Shaper

☐ Shape Upstream

☐ Shape Downstream

▲ Hide Advanced Settings

Advanced

MTU:

Host Name: (Required by some ISPs)

☐ MAC Cloning

High Availability

☐ Do not connect if this gateway is in passive state

Dead Connection Detection

Probe Next Hop: ☑

Connection Probing Method: None

* denotes mandatory fields.

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 10:46:00 AM Asia/Calcutta

3. Select the Port: WAN, WAN2, Serial, None.
4. If you do not want the IP45 to obtain an IP address automatically by using DHCP, do the following:
    a. Uncheck the Obtain IP address automatically (using DHCP) check box.
    b. Type the IP address that your service provider provides.
    c. Select the subnet mask from the drop-down list that applies to the IP address you Typed.
    d. Type the IP address of the default gateway of your service provider.
5. To assign an IP address automatically by using DHCP, but not configure DNS servers automatically, do the following:
    a. Uncheck the Obtain DNS Servers automatically check box.
    b. Type the Primary DNS server IP address.
    c. Type the Secondary DNS server IP address.
    d. Type the WINS Server IP address.
6. Select the Shape Upstream and Shape Downstream to enable traffic shaper.
7. Type the Upstream Link Rate value in kbps.
8. Type the Downstream Link Rate value in kbps, slightly lower than the Upstream Link Rate value.

9. Click *Show Advanced Settings*.

10. Type the maximum transmission unit (MTU-1500)

11. Type the Host Name.

    This field is optional: some ISPs might require it, and they provide the host name.

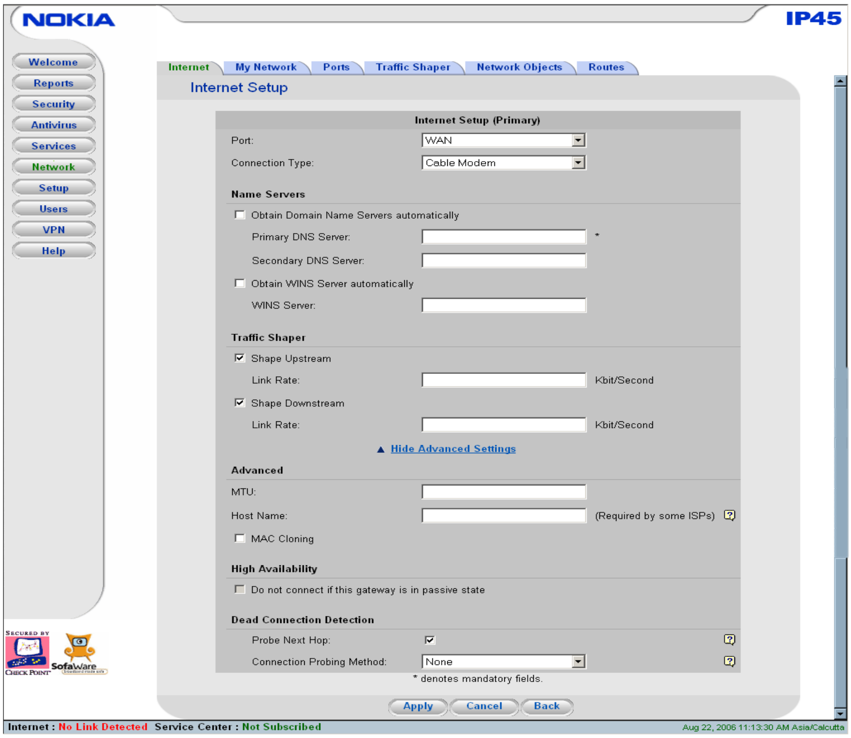
12. Click Apply.

To use a cable modem connection

1. Select Cable Modem type from the Internet Setup page at Connection Type.

2. Click *Show Advanced Settings*.

   The Internet Setup page opens.



Internet Setup

Internet Setup (Primary)

Port: WAN

Connection Type: Cable Modem

Name Servers

□ Obtain Domain Name Servers automatically

Primary DNS Server: *

Secondary DNS Server:

□ Obtain WINS Server automatically

WINS Server:

Traffic Shaper

☑ Shape Upstream

Link Rate: Kbit/Second

☑ Shape Downstream

Link Rate: Kbit/Second

▲ Hide Advanced Settings

Advanced

MTU:

Host Name: (Required by some ISPs)

□ MAC Cloning

High Availability

□ Do not connect if this gateway is in passive state

Dead Connection Detection

Probe Next Hop: ☑

Connection Probing Method: None

* denotes mandatory fields.

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 11:13:30 AM Asia/Calcutta

3. Enter the Host Name.

   This field is optional: some ISPs might require it, and they provide the host name.

4. Complete the remaining fields as per the information provided in the procedure “To use a LAN connection” on page 82.

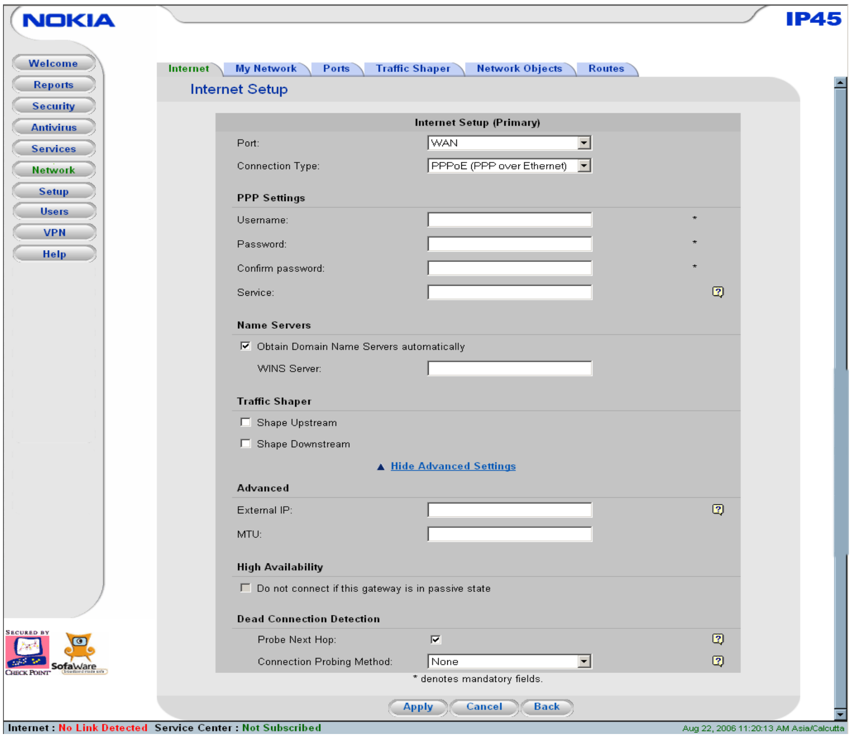
5. Click Apply.

To use a PPPoE connection

1. Choose PPPoE from the Internet Setup page at Connection Type.

2. Click *Show Advanced Settings*.

The following page opens:



Internet Setup

Internet Setup (Primary)

Port:	WAN
Connection Type:	PPPoE (PPP over Ethernet)

PPP Settings

Username:	*
Password:	*
Confirm password:	*
Service:	

Name Servers

☑ Obtain Domain Name Servers automatically

WINS Server:

Traffic Shaper

☐ Shape Upstream

☐ Shape Downstream

▲ Hide Advanced Settings

Advanced

External IP:

MTU:

High Availability

☐ Do not connect if this gateway is in passive state

Dead Connection Detection

Probe Next Hop:	☑
Connection Probing Method:	None

* denotes mandatory fields.

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 11:20:13 AM Asia/Calcutta

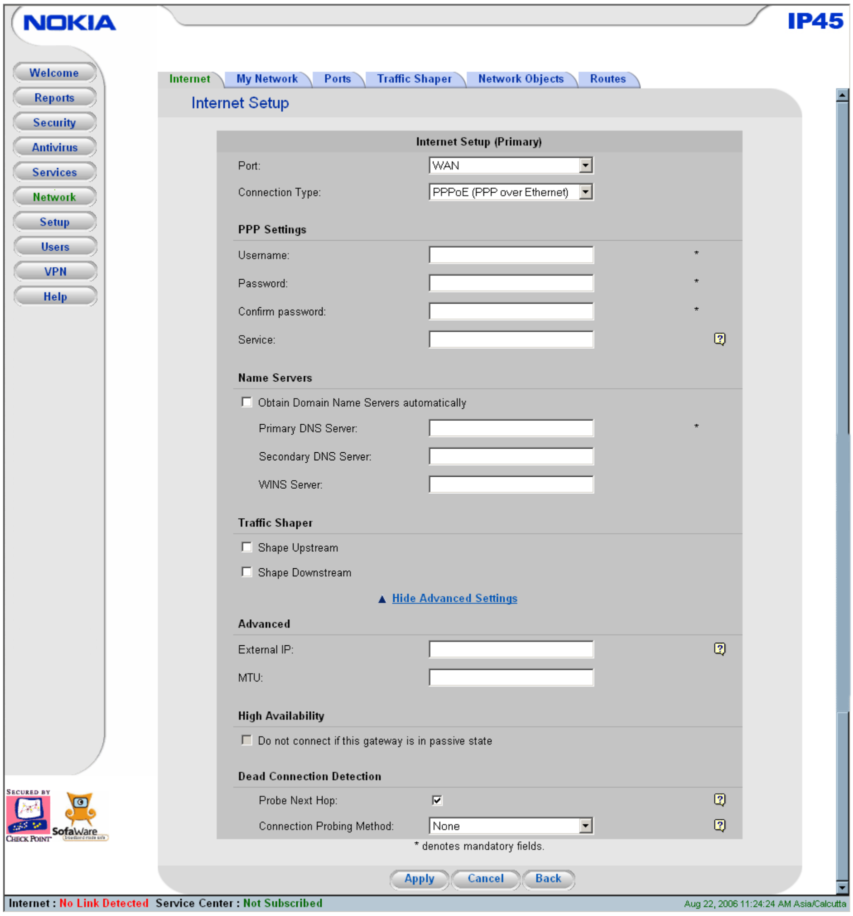
3. Enter the following information:
   - Enter your Username and Password, and confirm the Password.
   - Enter the service name as given by your service center

Note
If your service center did not provide you with a service name, leave this text box empty.

You can set the maximum transmission unit size (MTU). Nokia recommends that you leave this field empty. However, to modify the default MTU, consult with your service provider.

4. If you are not using automatic configuration of DNS servers, do the following:
   - Uncheck the Obtain Domain Name Servers automatically check box
   - Enter the Primary DNS server IP address.
   - Enter the Secondary DNS server IP address.
   - Enter the WINS Server IP address.

The following page opens:



Internet Setup

Internet Setup (Primary)

Port: WAN

Connection Type: PPPoE (PPP over Ethernet)

PPP Settings

Username: *

Password: *

Confirm password: *

Service:

Name Servers

☐ Obtain Domain Name Servers automatically

Primary DNS Server: *

Secondary DNS Server:

WINS Server:

Traffic Shaper

☐ Shape Upstream

☐ Shape Downstream

▲ Hide Advanced Settings

Advanced

External IP:

MTU:

High Availability

☐ Do not connect if this gateway is in passive state

Dead Connection Detection

Probe Next Hop: ☑

Connection Probing Method: None

* denotes mandatory fields.

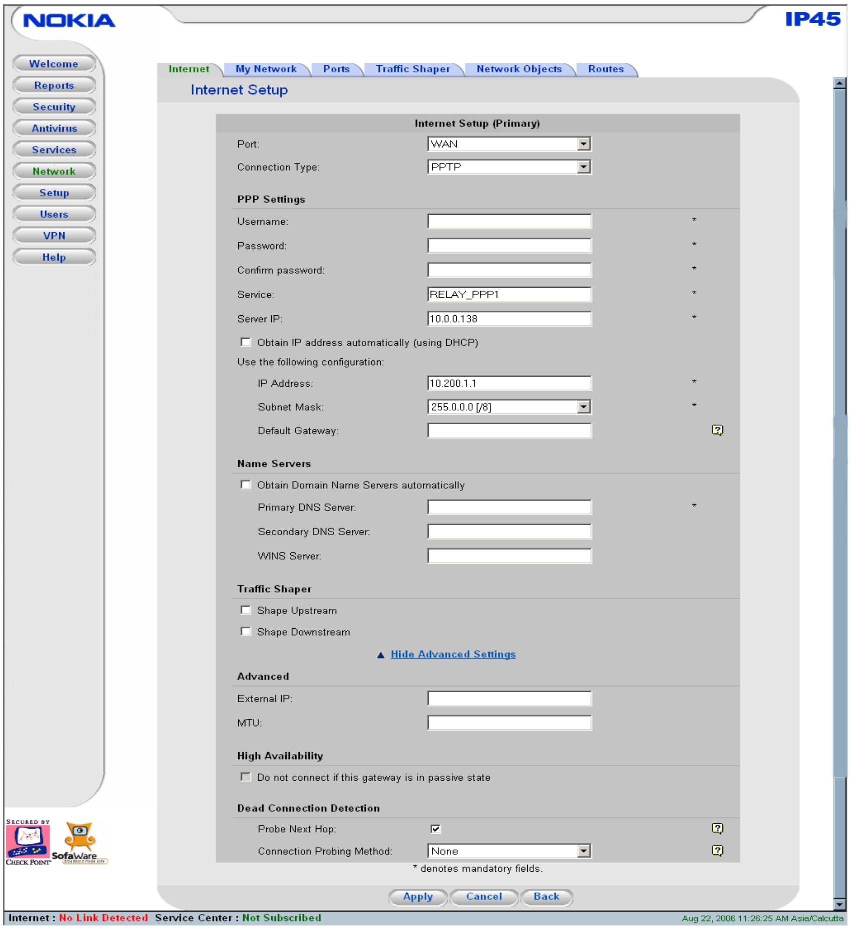
Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 11:24:24 AM Asia/Calcutta

5. Click Apply.

To use a PPTP connection

1. Choose PPTP Internet Setup page at Connection Type.
2. Click *Show Advanced Settings*.

The following page opens:



Internet Setup

Internet Setup (Primary)

Port: WAN

Connection Type: PPTP

PPP Settings

Username: *

Password: *

Confirm password: *

Service: RELAY_PPP1 *

Server IP: 10.0.0.138 *

□ Obtain IP address automatically (using DHCP)

Use the following configuration:

IP Address: 10.200.1.1 *

Subnet Mask: 255.0.0.0 (/8) *

Default Gateway:

Name Servers

□ Obtain Domain Name Servers automatically

Primary DNS Server: *

Secondary DNS Server:

WINS Server:

Traffic Shaper

□ Shape Upstream

□ Shape Downstream

▲ Hide Advanced Settings

Advanced

External IP:

MTU:

High Availability

□ Do not connect if this gateway is in passive state

Dead Connection Detection

Probe Next Hop: ☑

Connection Probing Method: None

* denotes mandatory fields.

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 11:26:25 AM Asia/Calcutta

3. Enter the following information:

a. Your username and password, and confirm the password.

b. The service name as given by your service provider.

c. The IP address of the PPTP server as given by your service provider.

d. The IP address of the PPTP client as given by your service provider.

e. Select the PPTP client subnet as given by your service provider.

You can configure the MTU size. Nokia recommends that you leave this field empty. Consult your service provider to modify the default MTU.

4. If you are not using automatic configuration of DNS servers, do the following:

a. Clear the Obtain DNS servers automatically check box.

The Internet page with DNS server options appears.

b. Enter the Primary DNS server IP address.

c. Enter the Secondary DNS server IP address.

5. Click Apply.

Table 14 Internet Connection Fields

Field	Action
Host Name	Type the hostname for authentication. If your ISP has not provided you with a host name, leave this field blank. Most ISPs do not require a specific hostname.
Port	Type of port you want to use for connecting to the Internet. Options: • WAN: configuring an ethernet-based connection through WAN port. • WAN2: configuring an ethernet-based connection through DMZ/ WAN2 port. • Serial: to configure a dial-up connection. • None: To configure none.
Username	Type your user name.
Password	Type your password.
Confirm password	Re type your password to confirm.
Service	Type your service name. If your ISP has not provided you with a service name, leave this field empty.
Server IP	IP address of the server. If you selected PPTP, type the IP address of the PPTP server as given by your ISP.
Internal IP	Local IP address. If you selected PPTP, type the local IP address required for accessing the PPTP modem.
Obtain IP address automatically (Using DHCP)	Clear this option if you do not want the Nokia IP45 device to obtain an IP address automatically.
Obtain Domain Name Servers automatically	Clear this option if you do not want the Nokia IP45 device to obtain an IP address automatically.
IP Address	Type the static IP address of your IP45 device.
Subnet Mask	Select the subnet mask that applies to the static IP address of your device.

Table 14 Internet Connection Fields (*continued*)

Field	Action
Default Gateway.	Type the IP address of your ISP's default gateway.
Primary DNS Server	Type the primary DNS server IP address.
Secondary DNS Server	Type the secondary DNS server IP address.
WINS Server	Type the WINS server IP address.
Shape Upstream Link Rate	Select this option to enable traffic shaper for outgoing traffic. Type a rate (in kilobits/second) slightly lower than lower than the maximum measured upstream speed of your Internet connection, in the field provided. Try different rates in order to determine which one provides the best results. For information on using traffic shaper, see "Using Traffic Shaper" on page 127.
Shape Downstream Link Rate	Select this option to enable Traffic Shaper for incoming traffic. Then type a rate (in kilobits/second) slightly lower than lower than the maximum measured downstream speed of your Internet connection. You may try different rates in order to determine which one provides the best results. **Note** Traffic Shaper cannot control the number or type of packets it receives from the Internet; it can only affect the rate of incoming traffic by dropping inbound traffic less accurate than the shaping of outbound traffic. It is therefore recommended to enable traffic shaping for incoming traffic only if necessary. For information on using Traffic Shaper, see"Using Traffic Shaper" on page 127.
Do not connect if this gateway is in passive state	If you are using High Availability, select this option to configure WAN high availability. The gateway connects to the Internet only if it is the active gateway in the high availability cluster. This field is only enabled if high availability is configured. For information on high availability, see "High-Availability" on page 213.

Table 14 Internet Connection Fields (*continued*)

Field	Action
External IP	If you selected PPTP, type the IP address of the PPTP client as given by your ISP. If you selected PPPoE, this field is optional, and you need not enter this value unless specified by your ISP.
MTU	This field allows you to control the maximum transmission unit size. As a general recommendation you should leave this field empty. To modify the default MTU value, it is recommended that you consult with your ISP first and use MTU values between 1300 and 1500.

Dial-Up PPP

You can connect the Nokia IP45 security platform to the Internet by using a dial-up connection. The device can establish a PPP connection to an ISP by using an external modem connected to an auxiliary port. The modem can be an analog modem or an ISDN terminal adapter.

You can use the following modems:

- Analog modem 56 Kbps (DTE speed: up to 115200)
- ISDN TA (using PPP) 64 Kbps (DTE speed: up to 230400)
- ISDN TA (using MLPPP) 128 Kbps (DTE speed: up to 460800)

Configuring Dial-Up

You can configure the dial-up option using either the GUI or the command-line interface (CLI).

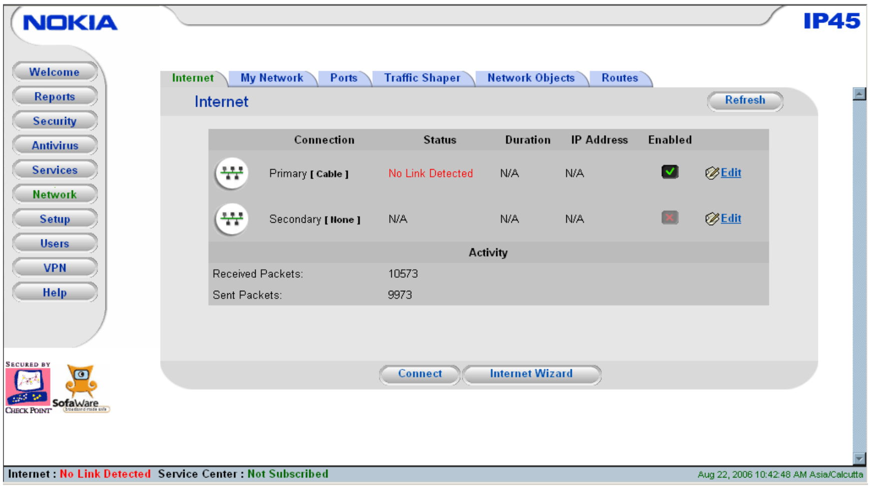
Using the GUI

The following sections provide details about how to configure dial-up connections on the Nokia IP45 security platform by using the GUI:

To configure dial-up settings using the GUI

1. Choose Network from the main menu.

   The Internet page opens.



Internet

Connection	Status	Duration	IP Address	Enabled	
Primary [Cable]	No Link Detected	N/A	N/A	✓	Edit
Secondary [None]	N/A	N/A	N/A	☒	Edit

Activity

Received Packets:	10573
Sent Packets:	9973

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 10:42:48 AM Asia/Calcutta

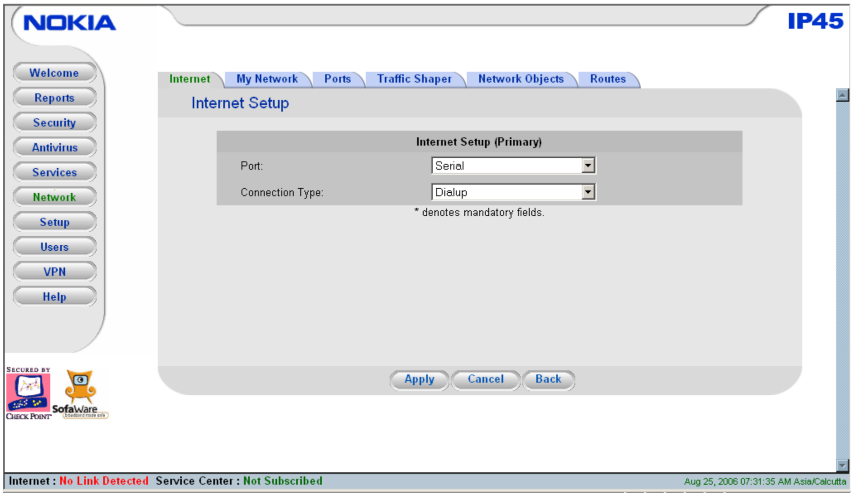
2. Click Edit next to the Primary Internet connection.

   The Internet Setup page opens.

3. Select Serial from the drop-down list next to Port.

4. Select Dialup from the drop-down list next to Connection Type.

   The following page opens.



Internet Setup

Internet Setup (Primary)

Port:	Serial
Connection Type:	Dialup

* denotes mandatory fields.

Internet : No Link Detected Service Center : Not Subscribed Aug 25, 2006 07:31:35 AM Asia/Calcutta

5. Click Apply.

   Dialup is configured.

Configuring Dial-up Setting by Using the CLI

To configure the dial-up by using the command line interface, log in through the console port.

Dial-up mode can be enabled by using the following options available in the CLI:

- **Disable**—WAN connection is established regardless of any interesting traffic.
- **Immediate**—WAN connection is established only when no other higher priority connection (primary) exists, regardless of any interesting traffic. This connection becomes inactive when primary becomes active.

Note
Any traffic that goes to the Internet through LAN is called interesting traffic.

- **Activity**—WAN connection is established only when interesting traffic is initiated from internal network to WAN and when no other higher priority connection (primary) exists. The dialup connection terminates if another higher priority connection becomes active or if there is no traffic for 1 minute.

Note
Dial-up connection option (always on, demand dialing) and other parameters (number, username, password, and so on) can be configured by using CLI.

Use the following commands to configure the dialup profile:

```
set interface wan mode dialup connectondemand <disable |immediate |
activity>

set interface wan2 mode dialup connectondemand <disable |immediate |
activity>
```

For more information about dial-up commands, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

CLI Wizard

Use the following command to configure dial-up by using the CLI wizard:

```
wizard dialup
```

For more information about how to use other dialup commands, see the *Nokia IP45 Security Platform CLI Reference Guide, Version 4.0.*

Multiple Dial-up Profiles

The Nokia IP45 security platform supports 10 dial-up profiles. A round-robin mechanism is used to choose the profiles for connecting to the Internet. By default, the first dial-up profile is used. On failure of the first dial-up, the device attempts to use the successive profiles for successful Internet connection.

Either dial-up or an out-of-band management (OOB) instance alone can exist on the device at any given time.

Note
You can configure ten dial-up profiles. Only one profile will be active at a time.You cannot configure dial-up for both primary and secondary Internet connections.

Enabling or Disabling the Internet Connection

You can enable or disable the Internet connection by using the following procedure.

To enable or disable the Internet connection

1. Choose Network from the main menu.

   The Internet page opens.

2. Next to the Internet connection, do one of the following:

   a. To enable the connection, click the adjacent sign (x) mark

      The button changes to a check mark, and the connection is enabled.

   b. To disable the connection, click the adjacent check mark.

      The button changes to sign (x) mark, and the connection is disabled.

Using Quick Internet Connect or Disconnect

By using connect or disconnect (depending on the connection status) on the Internet page, you can establish a quick Internet connection by using the currently selected connection type. In the same manner, you can terminate the active connection.

The Internet connection retains its connected or not connected status until the Nokia IP45 is rebooted. The IP45 then connects to the Internet if the connection is enabled. For information on how to enable the Internet connection, see “Enabling or Disabling the Internet Connection” on page 93.

Configuring a Backup Internet Connection

You can configure both a primary and a secondary Internet connection for the Nokia IP45 security platform. The secondary connection acts as a backup, so that even if the primary connection fails, the IP45 remains connected to the Internet.

You can configure different DNS servers for the two connections. The IP45 device acts as a DNS relay and routes requests from computers within the network to the appropriate DNS server for the active Internet connection.

The two connections can be of different types. But they both cannot be LAN, and DHCP connections.

To set up backup Internet connection

1. Choose Networks from the main menu.

   The Internet page opens.

2. Click Edit next to Primary, and Secondary connection types to configure a backup Internet connection.

For basic topology illustrations, see "Connecting the Nokia IP45 Security Platform to the Network" on page 47.

Note
To physically connect multiple WAN devices to Nokia IP45, you must have a switch, connected to the WAN port.

Viewing Internet Information

To view the status, duration, and activity information, choose Network from the main menu. The Internet page opens.

Table 15 displays the Internet connection information.

Table 15 Internet Connection Information

Field	Description
Status	Indicates the connection status.

Duration	Indicates the connection duration, if active. The duration is given in the format hh:mm:ss, where:
	hh = hours
	mm = minutes
	ss = seconds

IP Address	Your IP address
Enabled	Indicates whether or not the connection is enabled.
WAN MAC Address	MAC address of IP45.
Cloned MAC Address	Cloned MAC address.

Table 15 Internet Connection Information (*continued*)

Field	Description
Received Packets	Number of data packets received in the active connection.
Sent Packets	Number of data packets sent in the active connection.

Detecting Dead Connections

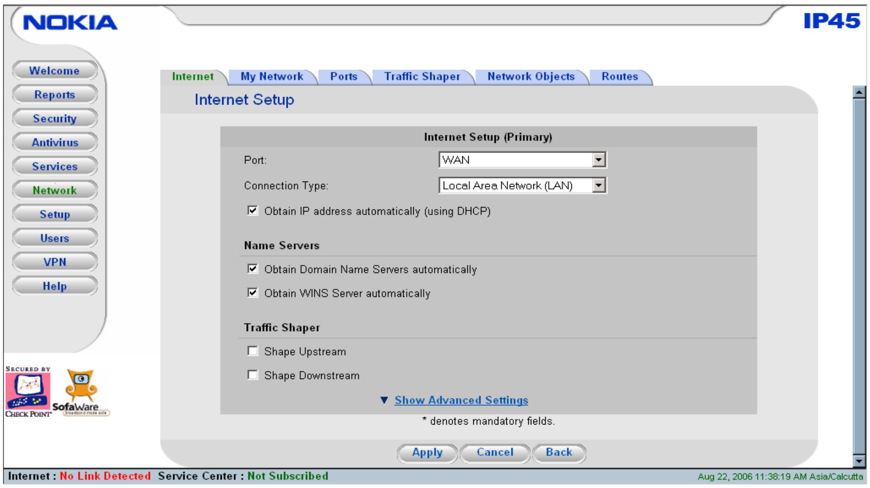
The Nokia IP45 security platform v4.0 supports dead internet connection detection. If the Internet connection is identified to be inactive, a failover is performed to the secondary Internet connection to insure continuous connectivity.

You can detect dead connection by using the methods as described in the following procedure.

To configure dead connection detection

1. Choose Internet from the main menu.
2. Click Edit next to the type of connection to choose. For example Primary LAN.

   The following page opens.



Internet Setup

Internet Setup (Primary)

Port: WAN

Connection Type: Local Area Network (LAN)

☑ Obtain IP address automatically (using DHCP)

Name Servers

☑ Obtain Domain Name Servers automatically

☑ Obtain WINS Server automatically

Traffic Shaper

☐ Shape Upstream

☐ Shape Downstream

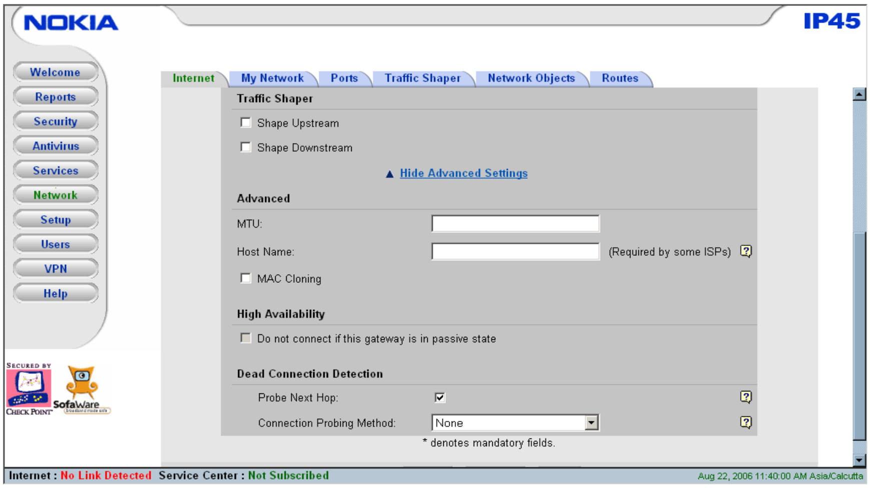
* denotes mandatory fields.

Internet : No Link Detected Service Center : Not Subscribed

Aug 22, 2006 11:38:19 AM Asia/Calcutta

3. Click *Show Advanced Settings*.

   The following page opens displaying the dead connection configuration details.



Traffic Shaper

☐ Shape Upstream

☐ Shape Downstream

Advanced

MTU:

Host Name: (Required by some ISPs)

☐ MAC Cloning

High Availability

☐ Do not connect if this gateway is in passive state

Dead Connection Detection

Probe Next Hop: ☑

Connection Probing Method: None

* denotes mandatory fields.

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 11:40:00 AM Asia/Calcutta

4. To automatically detect the loss of connectivity to the default gateway, select Probe Next Hop.
5. Select probing method from the options provided in Connection Probing Method drop-down list.
6. Choose the values for the option selected by using the information provided in Table 16.
7. Click Apply.

Table 16 Dead Connection Detection

Field	Description
Probe Next Hop	Select this option to automatically detect loss of connectivity to the default gateway. If the default gateway does not respond and the Internet connection is considered to be down, a failover is performed to the second Internet connection, (if configured) to ensure continuous Internet connectivity. By default, this option is selected.
Connection Probing Method	Select the method for probing by using this option. The probing methods available are: • None (default value)—does not perform Internet connection probing. Next hop probing is still used, if the Probe Next Hop check box is selected. This is the default value • Ping Addresses—ping anywhere from one to three servers specified by IP address or DNS name in the 1, 2, and 3 fields. If no response is received for 45 seconds from the defined servers, the Internet connection is considered to be inactive. Use this method if you have reliable servers that can be pinged. • Probe DNS Servers—probes the primary and secondary DNS servers. If no response is received for 45 seconds from any of the gateways, the Internet connection is considered to be inactive. • Probe VPN Gateway (RDP)—sends RDP echo requests to up to three Check Point VPN gateways specified by IP address or DNS name in the 1, 2, and 3 fields. If no response is received for 45 seconds from any of the defined gateways, the Internet connection is considered to be inactive.

For information about how to configure dead connection detection by using the CLI, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

6 Managing your Local Area Network

This chapter provides detailed information to manage your local area network by using the Nokia IP45 security platform.

You can manage and configure your network connection and settings, and view the connections information on the connection in terms of status, connection duration, and activity.

This chapter includes the following topics:

- Configuring Network Settings
- Enabling and Disabling the DHCP Server
- Changing IP Addresses
- Configuring Network Objects
- Configuring DHCP Reservation
- OSPF
- Viewing Ports Status
- Configuring Source Routes
- Defining the Port Link Speed

Configuring Network Settings

⚠ **Caution**
Network settings are advanced settings. Nokia recommends that these settings not be changed unless it is necessary and you are qualified to do so. Changing network settings might result in losing the connection to the device.

If you change the network settings to incorrect values, and you are unable to correct the error, reset the IP45 to its factory settings.

To reset the Nokia IP45 security platform to its factory default settings, choose Setup > Firmware > Tools > Factory Settings. You can also press the *Reset* button at the rear panel of the device.

Note
To set the device to factory defaults by using the Reset button, press the Reset button for a minimum of seven seconds.

Enabling and Disabling the DHCP Server

The Nokia IP45 security platform has a built-in Dynamic Host Configuration Protocol (DHCP) server that is enabled by default. This allows the IP45 to configure all the devices on your network automatically.

If you have another DHCP server configured in your network, you must disable the DHCP server in your IP45 before you connect the IP45 to the network.

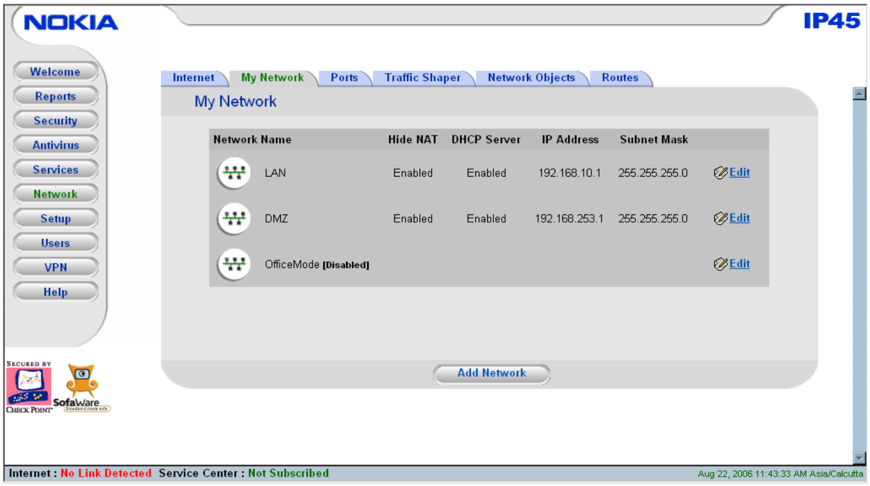
To enable or disable the DHCP server

1. Choose Network from the main menu.

   The Internet page opens.

2. Click My Network.

   The My Network page opens.



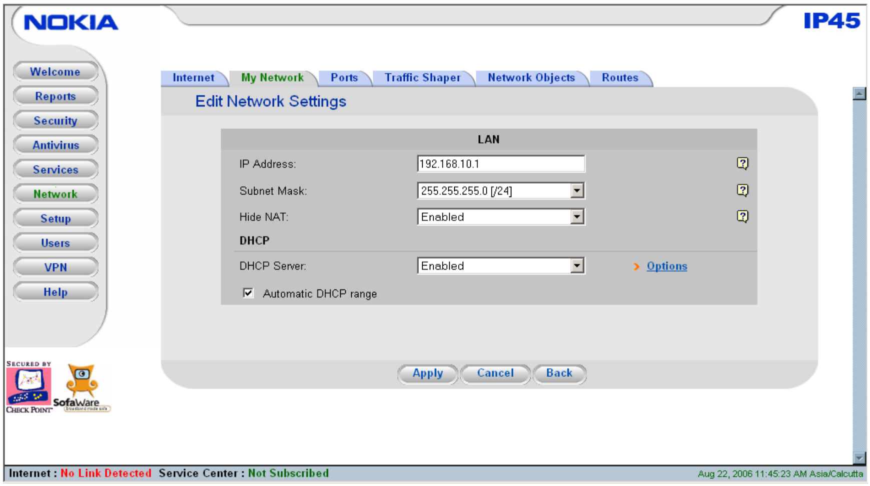
My Network

Network Name	Hide NAT	DHCP Server	IP Address	Subnet Mask	
LAN	Enabled	Enabled	192.168.10.1	255.255.255.0	Edit
DMZ	Enabled	Enabled	192.168.253.1	255.255.255.0	Edit
OfficeMode **[Disabled]**					Edit

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 11:43:33 AM Asia/Calcutta

3. To configure the DHCP server for LAN/DMZ settings, click Edit next to LAN/DMZ.

The Edit Network Settings page opens.



Edit Network Settings

LAN

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0 [/24]

Hide NAT: Enabled

DHCP

DHCP Server: Enabled

☑ Automatic DHCP range

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 11:45:23 AM Asia/Calcutta

4. From the DHCP Server drop-down list, select Enabled or Disabled.
5. Click Apply.

   Table 17 provides information about the DHCP server configuration fields.

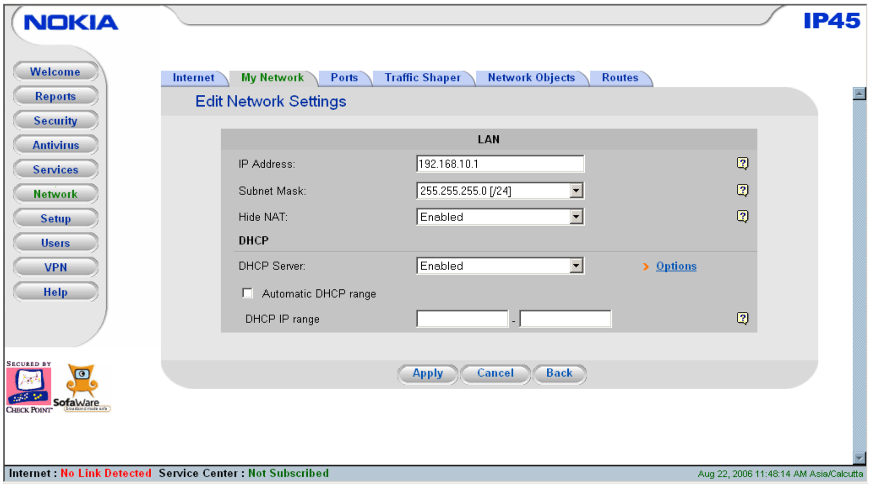
Table 17 DHCP Server Configuration Fields

Field	Action
IP Address	IP address of the LAN interface of the device, which acts as DHCP server.
Subnet Mask	Subnet mask of the DHCP server.
Hide NAT	Options: Enabled: enables hide NAT Disabled: disables hide NAT
DHCP Server	Options: Enabled: enables DHCP server Disabled: disables DHCP server Relay: forwards DHCP requests to a specified DHCP server, relays responses back to the DHCP clients.

To configure DHCP ranges

1. Configure the DHCP server as explained in "To enable or disable the DHCP server" on page 100.
2. To configure the DHCP range manually, uncheck the Automatic DHCP range check box.

The Edit Network Settings page opens.



Edit Network Settings

LAN

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0 (/24)

Hide NAT: Enabled

DHCP

DHCP Server: Enabled

□ Automatic DHCP range

DHCP IP range -

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 11:48:14 AM Asia/Calcutta

3. Enter the DHCP IP addresses in the DHCP IP range text box.
4. Click Apply.

Customizing DHCP Server Options

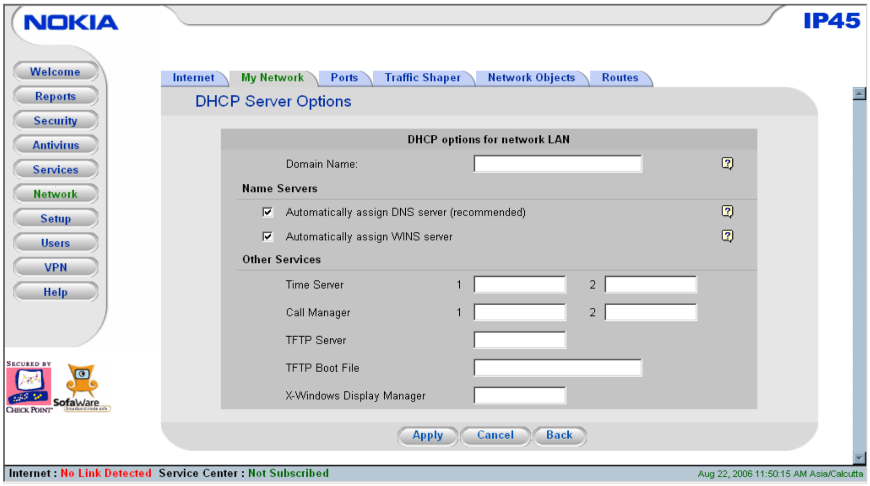
The Nokia IP45 v4.0 supports customizing DHCP server options such as Name Servers, Time Server, Call Manager, TFTP server and boot name, domain name, DNS servers, display manager.Use the following procedure to customize the DHCP options through GUI.

To customize DHCP server options

1. Choose Network from the main menu and select My network.
2. To customize, click Edit next to the interface.

   The Edit Network Settings page opens.
3. Click Options next to the DHCP Server.

   The DHCP Server Options page opens.



DHCP Server Options

DHCP options for network LAN

Domain Name:

Name Servers

☑ Automatically assign DNS server (recommended)

☑ Automatically assign WINS server

Other Services

Time Server 1 2

Call Manager 1 2

TFTP Server

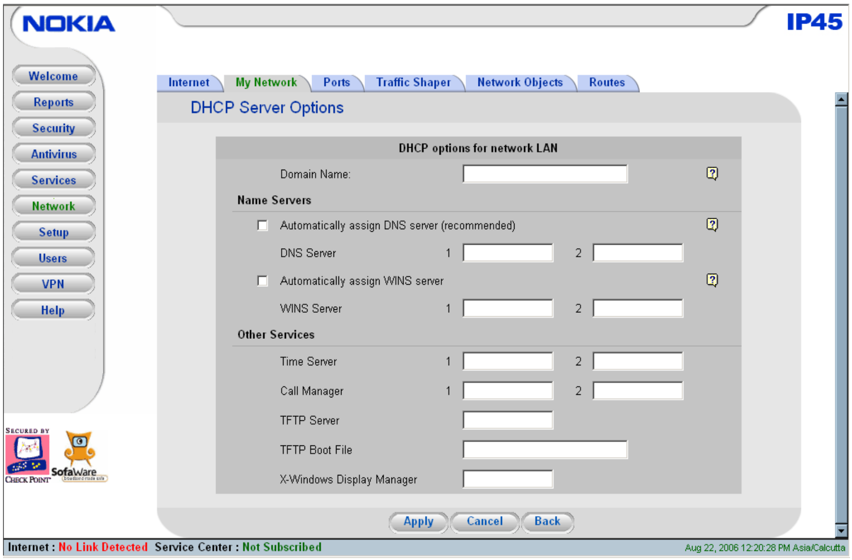
TFTP Boot File

X-Windows Display Manager

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 11:50:15 AM Asia/Calcutta

4. Type the domain name.
5. To automatically assign the DNS and WINS server, select the respective check boxes.
6. To enter the DNS Servers manually, clear these options.

   The DNS Server and WINS server 1 and 2 text boxes appear.



DHCP Server Options

DHCP options for network LAN

Domain Name:

Name Servers

□ Automatically assign DNS server (recommended)

DNS Server 1 2

□ Automatically assign WINS server

WINS Server 1 2

Other Services

Time Server 1 2

Call Manager 1 2

TFTP Server

TFTP Boot File

X-Windows Display Manager

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 12:20:28 PM Asia/Calcutta

7. Type the values using the information provided in Table 18.
8. Type the values in the Other Services fields by using the description provided in Table 18.
9. Click Apply.

Table 18 DHCP Options

Field	Action
Domain Name	Enter a domain name that should be passed to the DHCP clients
Automatically assign DNS server (recommended)	Clear this option if you do not want the gateway to act as a DNS relay server and pass its own IP address to DHCP clients.
DNS Server 1, 2	Type the IP addresses of the primary and secondary DNS servers to pass to DHCP clients instead of the gateway.
Automatically assign WINS server	Clear this option if you do not want DHCP clients to be assigned the same WINS servers as specified by the Internet connection configuration (in the Internet setup page).
WINS Server 1, 2	Type the IP addresses of the primary and secondary WINS servers to be used instead of the gateway.
Time Server	Type the IP address of the primary and secondary NTP servers.
Call Manager	Type the IP address of the primary and secondary VoIP servers.
TFTP Server	Type the IP address of the TFTP server.
TFTP Boot File	Type the boot file to use for booting DHCP clients through TFTP.
X-Windows Display Manager	IP address of the X-Windows server

Configuring a DMZ Network

In addition to the LAN network, the Nokia IP45 security platform allows you to define a second internal network called a demilitarized zone (DMZ).

By default, all traffic is allowed from the LAN network to the DMZ network, and no traffic is allowed from the DMZ network to the LAN network. You can customize this behavior by creating firewall user rules.

For example, you can assign your company accounting department to the LAN network and the rest of the company to the DMZ network. The accounting department would be able to connect to all company computers, while the rest of the employees cannot access any sensitive information on the accounting department computers. You can then create firewall rules that allow specific computers (such as a manager’s computer) to connect to the LAN network and the accounting department.

Nokia IP45 v4.0 supports DMZ as WAN2. That is, the DMZ port can serve as a secondary WAN port. When the DMZ port is assigned to WAN2, the primary Internet connection uses the WAN port, and the secondary uses the DMZ port. For more information about configuring ports, see "Managing Ports" on page 124.

When this option is not in use, you can configure two Internet connections that share the same WAN port.

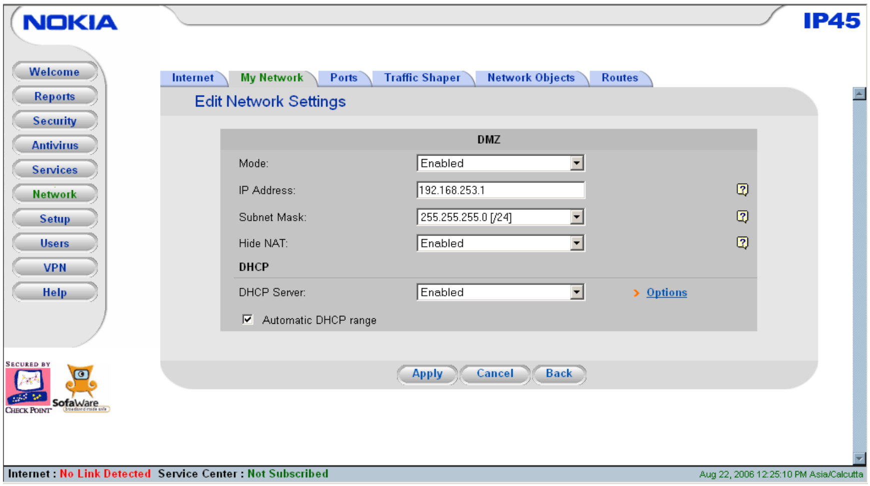
Note
The DHCP server is supported on a DMZ network.

The following procedure describes about how to configure and edit DMZ networks by using the Nokia IP45 graphical user interface:

To configure or edit DMZ network

1. Choose Network > My Network page, and click Edit next to DMZ.

   The Edit Network Settings page opens.



Edit Network Settings

DMZ

Mode: Enabled

IP Address: 192.168.253.1

Subnet Mask: 255.255.255.0 [/24]

Hide NAT: Enabled

DHCP

DHCP Server: Enabled

☑ Automatic DHCP range

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 12:25:10 PM Asia/Calcutta

2. From the Mode drop-down list, select Enabled.
3. In the IP Address text box, enter the IP address of the DMZ network default gateway.

Note
The DMZ network must not overlap the LAN network.

---

4. Enter the value of the subnet mask.
5. From the Hide NAT drop-down list, select Enabled or Disabled.
6. To enter the DHCP range manually, uncheck the Automatic DHCP Range check box.
7. Enter the DHCP range in the provided text boxes.

8. Click Apply.

   The DMZ network values are successfully saved. Enter the new values as required to edit the configured values.

Note
You can disable the DMZ network in the Nokia IP45 v4.0 security platform.

Configuring OfficeMode Network

Typically, when remote access is implemented, the client connects using an Internet IP address locally assigned by an ISP. This can cause the following issues:

- When two clients on the same network (for example: WLAN) use the internal VPN server, they will not be able to communicate with each other over the secure VPN link. This is because their IP addresses are on the same subnet and so they attempt to communicate directly over the local network.
- Some networking protocols or resources might require the IP address of the client to be an internal one.

The IP45 v4.0 supports OfficeMode network that enables to assign a unique IP address to a remote client, thus resolving the above mentioned issues. This unique IP address from the predefined OfficeMode network is assigned when the user connects and authenticates.

Note
OfficeMode requires SecureClient installed on the VPN clients. Secure Remote OfficeMode is not supported.

Note
Customizing DHCP options is not supported in OfficeMode.

You can configure OfficeMode by using the GUI or command-line interface.

To configure the OfficeMode settings

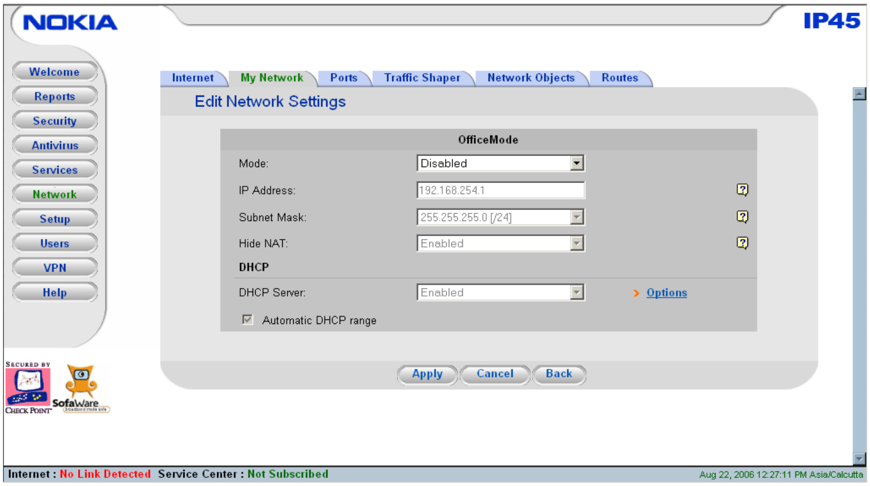
1. Choose Network from the main menu and select My Network.

   The My Network page opens with information about the OfficeMode configuration.

   Note
   By default, OfficeMode is disabled.

2. Click Edit next to the OfficeMode.

   The Edit Network Settings page opens with configurable information for OfficeMode.



Edit Network Settings

OfficeMode

Mode: Disabled

IP Address: 192.168.254.1

Subnet Mask: 255.255.255.0 [/24]

Hide NAT: Enabled

DHCP

DHCP Server: Enabled › Options

☑ Automatic DHCP range

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 12:27:11 PM Asia/Calcutta

3. To enable, select Enabled from the Mode drop-down list.
4. Type the values for IP Address, Subnet Mask and Hide NAT
5. To enter the DHCP range manually, uncheck the Automatic DHCP Range check box.
6. Enter the DHCP range in the provided text boxes.
7. Click Apply.

For information about the commands, see the *Nokia IP45 CLI Reference Guide Version 4.0.*

VLAN Support

A VLAN is a logical network behind your Nokia IP45. Computers in the same VLAN behave like computers that are on the same physical network. Any traffic flows freely between these without the intervention of the firewalls. Traffic between a VLAN and other networks flows as per the security policy set by the user.

By configuring a VLAN, you can assign each division within your organization to different VLANs regardless of their physical location. You can partition your network into several virtual networks.

By default, traffic from VLAN to any other internal network is blocked. Hence, VLANs increase security and reduce network congestion.

Nokia IP45 v4.0 supports tag-based Virtual LANs (VLANs).

Tag-Based VLANs

In a tag-based VLAN you use ports of one of the gateways as a 802.1Q VLAN trunk, connecting Nokia IP45 to a VLAN switch. Each VLAN behind this trunk is assigned an identifying number called VLAN ID or VLAN tag. Tagging ensures that traffic is directed to the correct VLAN.

All outgoing traffic from a tag-based VLAN contains the VLAN tag in the packet headers. Incoming traffic to the VLAN must contain the VLAN tag as well, with out which, the packets are dropped.

Configuring a VLAN

You can configure VLAN by using GUI and command-line interface.

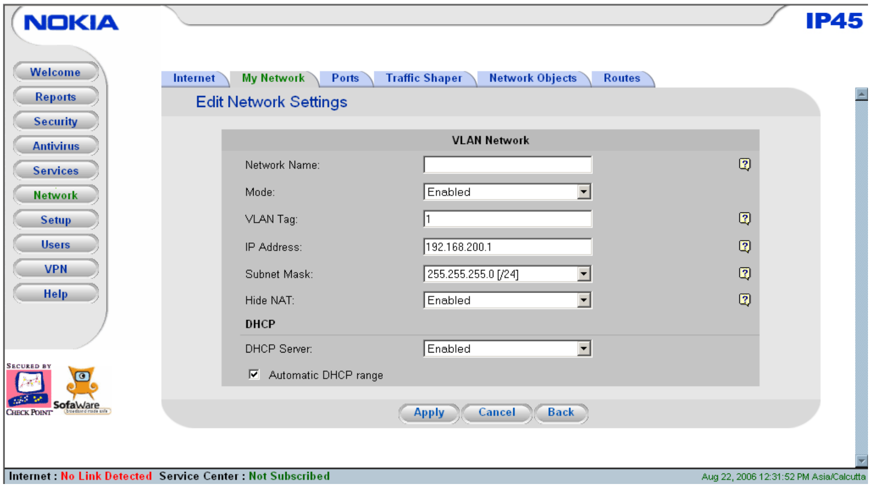
The following sections provide information about how to configure a VLAN by using IP45 Web portal (GUI).

To configure a VLAN

1. Choose Network from the main menu.
2. Click My Network.

   The My Network page opens with an Add Network tab at the bottom.
3. Click Add Network.

   The Edit Network Settings page opens.



Edit Network Settings

VLAN Network

Network Name:	
Mode:	Enabled
VLAN Tag:	1
IP Address:	192.168.200.1
Subnet Mask:	255.255.255.0 [/24]
Hide NAT:	Enabled

DHCP

DHCP Server:	Enabled

☑ Automatic DHCP range

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 12:31:52 PM Asia/Calcutta

4. In the Network Name text box, type a name for the VLAN network.
5. From the Mode drop-down list, select Enabled.
6. Enter the VLAN Tag value.
7. In the IP Address text box, type the IP address of the default gateway for a VLAN network gateway.

Note
The VLAN network must not overlap other networks.

8. In the Subnet Mask field, type the internal network range.

9. Enable or Disable Hide NAT.

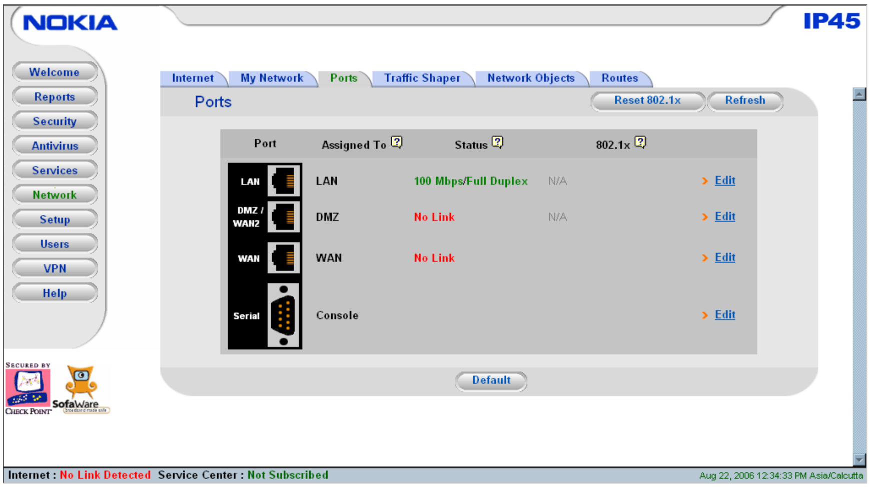
10. Select for Automatic DHCP range. To configure manually, see "Configuring a DMZ Network" on page 104.

11. Click Apply.

12. Choose Network from the main menu.

13. Click the Ports tab.

The Ports page opens.



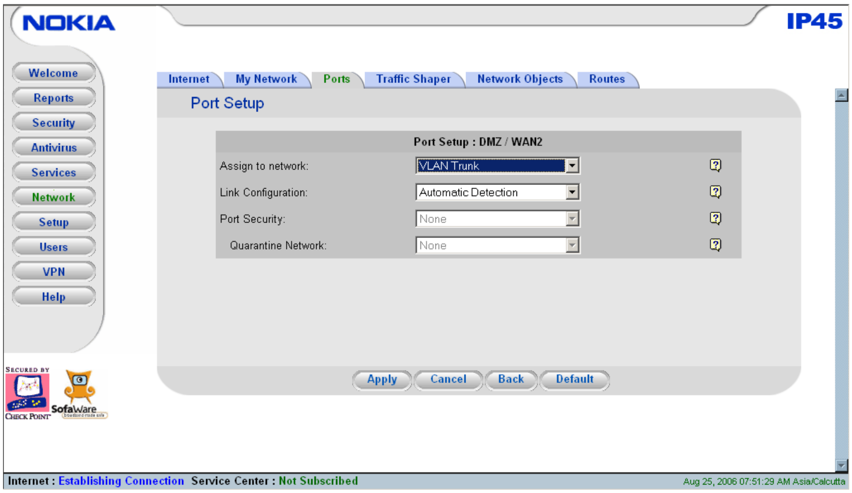
Ports

Port		Assigned To	Status	802.1x	
LAN		LAN	100 Mbps/Full Duplex	N/A	Edit
DMZ / WAN2		DMZ	No Link	N/A	Edit
WAN		WAN	No Link		Edit
Serial		Console			Edit

Internet : No Link Detected Service Center : Not Subscribed
Aug 22, 2006 12:34:33 PM Asia/Calcutta

14. Click Edit at the DMZ/WAN2 option.

The Port Setup window opens.



Port Setup

Port Setup : DMZ / WAN2

Assign to network: VLAN Trunk
Link Configuration: Automatic Detection
Port Security: None
Quarantine Network: None

Internet : Establishing Connection Service Center : Not Subscribed
Aug 25, 2006 07:51:29 AM Asia/Calcutta

15. Select VLAN Trunk from the Assign to network drop-down list.

16. Select the speed from the Link Configuration drop-down list.

17. Click Apply.

    The DMZ/WAN2 ports will no longer allow untagged packets.

18. Configure a VLAN trunk (802.1Q) port on the VLAN-aware switch according to the vendor instructions using the same VLAN IDs.

19. Connect the DMZ port of your device to the VLAN trunk port of the VLAN aware switch.

Note
The DMZ/WAN2 port is indicated as DMZ port on your device.

Table 19 VLAN Configuration Fields

Field	Description
Network Name	A name for the VLAN network. Example: myvlan
Mode	Enabled/Disabled
VLAN Tag	VLAN tag. Value: 1-4095
IP Address	IP address of the default gateway for VLAN network.
Subnet Mask	The internal network range.
Automatic DHCP Range	Select this option to obtain the DHCP range automatically.

Deleting a VLAN

The following procedure provides information about deleting a VLAN.

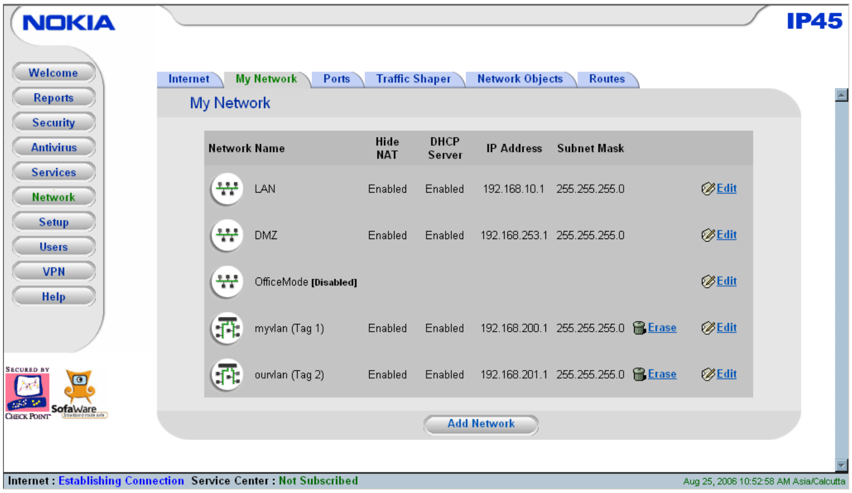
To delete a VLAN

1. Choose Network from the main menu.

   The Internet page opens.

2. Click My Network.

3. The My Network page opens with the list of VLANs, configured.



My Network

Network Name	Hide NAT	DHCP Server	IP Address	Subnet Mask		
LAN	Enabled	Enabled	192.168.10.1	255.255.255.0		Edit
DMZ	Enabled	Enabled	192.168.253.1	255.255.255.0		Edit
OfficeMode **[Disabled]**						Edit
myvlan (Tag 1)	Enabled	Enabled	192.168.200.1	255.255.255.0	Erase	Edit
ourvlan (Tag 2)	Enabled	Enabled	192.168.201.1	255.255.255.0	Erase	Edit

Internet : Establishing Connection Service Center : Not Subscribed Aug 25, 2006 10:52:58 AM Asia/Calcutta

4. To delete, click Erase next to the VLAN.

   A confirmation message appears

5. Click OK.

   The VLAN is deleted.

6. Click Ports.

   The Ports page opens.

7. From the DMZ/WAN2 menu option, select DMZ.
8. Click Apply.

Configuring DHCP Relay

Nokia IP45 v4.0 supports the DHCP relay feature. By using this feature, DHCP requests are forwarded to a specified DHCP server, which is located in a different subnet. This server relays the responses back to the DHCP clients.

This feature allows central management of IP address allocations across an enterprise network. You can also perform DHCP over a VPN tunnel.

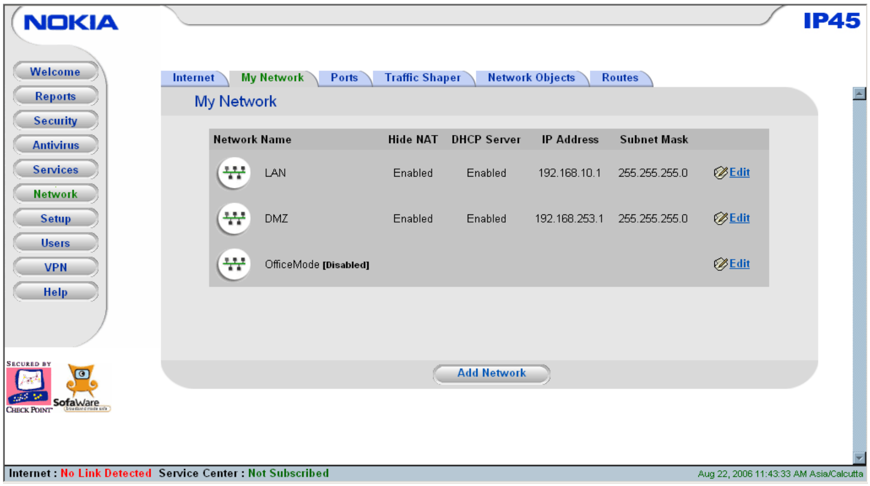
To configure DHCP relay

1. Choose Network from the main menu.

   The Internet page opens.

2. Click My Network.

The My Network page opens.



My Network

Network Name	Hide NAT	DHCP Server	IP Address	Subnet Mask	
LAN	Enabled	Enabled	192.168.10.1	255.255.255.0	Edit
DMZ	Enabled	Enabled	192.168.253.1	255.255.255.0	Edit
OfficeMode [Disabled]					Edit

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 11:43:33 AM Asia/Calcutta

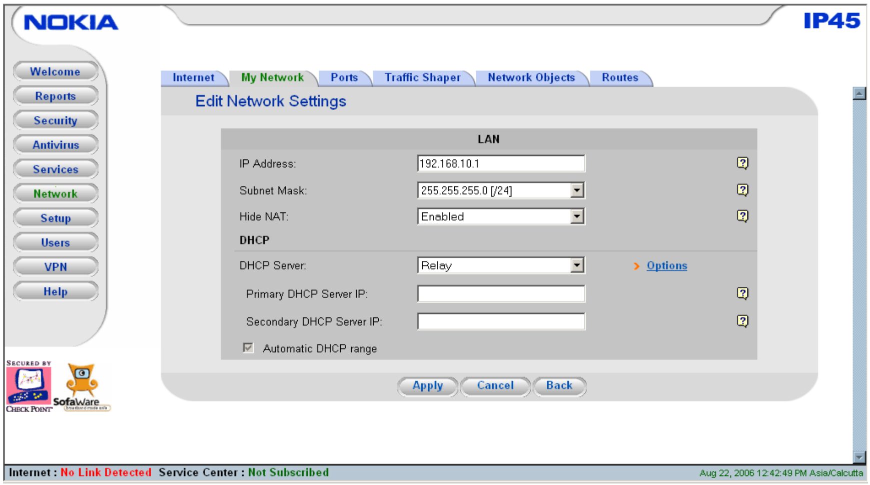
You can configure the DHCP relay IP address for both LAN and DMZ from this page.

3. Click Edit next to LAN/DMZ

   The Edit Network Settings page opens.

4. Select Relay from the DHCP Server drop-down list.

   The Edit Network Settings page opens (example window for LAN).



Edit Network Settings

LAN

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0 (/24)

Hide NAT: Enabled

DHCP

DHCP Server: Relay

Primary DHCP Server IP:

Secondary DHCP Server IP:

☑ Automatic DHCP range

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 12:42:49 PM Asia/Calcutta

5. Select Relay from DHCP Server drop-down list.
6. Enter the IP address of the Primary DHCP Server
7. Enter the IP address of the Secondary DHCP Server
8. Click Apply.

   The DHCP relay IP address for LAN/DMZ is configured.

Backing Up DHCP Relay

A DHCP Relay is used when DHCP clients are located on a different subnet than the DHCP server. When in DHCP relay mode, the IP45 appliance becomes a DHCP relay agent, which relays DHCP messages between clients and servers on different subnets, and even across VPN tunnels.

The IP45 appliance allows to configure a secondary DHCP relay that acts as a backup. When the primary DHCP relay fails to respond, the IP45 DHCP relay agent automatically relays DHCP requests to the secondary server, ensuring continuous availability of this critical network resource.

Backing Up DHCP Relay by Using CLI

The following are the commands to set the DHCP relay backup on LAN and DMZ interfaces:

```
set interface lan [dhcprelayip1 dhcprelayip1] [dhcprelayip2
dhcprelayip2]

set interface dmz [dhcprelayip1 dhcprelayip1] [dhcprelayip2
dhcprelayip2]
```

The following are the commands to show the LAN and DMZ interfaces that are configured for DHCP relay backup:

```
show interface lan [dhcprelayip1 dhcprelayip1] [dhcprelayip2
dhcprelayip2]

show interface dmz [dhcprelayip1 dhcprelayip1] [dhcprelayip2
dhcprelayip2]
```

For more information about DHCP relay backup commands, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

Changing IP Addresses

You can change the IP address of your Nokia IP45 security platform. You can also change the entire range of IP addresses in your network by using the IP45 Satellite X licenses. You might want to do this if, for example, you are adding the IP45 to a large existing network and do not want the network IP address range to change, or if you are using a DHCP server other than the IP45, that assigns addresses within a different range.

If you change the IP address of your IP45, you might have to manually change the network interface TCP/IP setting when you use static IP, or renew the DHCP lease when you use dynamic IP.

To change the IP addresses in your network

1. Choose Network from the main menu, and click My Network.
2. Enter new values in the Internal Network Range fields.

3. To reset the network to its default settings with the DHCP server enabled and the internal network range is 192.168.10.1, click Default.
4. Click Apply.

   You can see the following changes:

   - If you changed the internal network range to X.X.X.X, the IP address of the IP45 is changed to X.X.X.1.
   - If you chose to reset the network to its default settings, the settings are reset.
5. Do one of the following:
   - If your computer is configured to obtain its IP address automatically (by using DHCP), and the DHCP server in your IP45 is enabled, restart your computer. Your computer obtains an IP address in the new range.
   - Otherwise, manually reconfigure your computer to use the new address range by using the TCP/IP settings.

Configuring Network Objects

The IP45 v4.0 supports defining network objects for single computers, and networks. You can configure static NAT, and DHCP reservation by using this feature.

Note
NAT is enabled by default. NAT can only be disabled in IP45 Satellite X licenses. If NAT is disabled, you need to buy an IP address range.

Configuring Static NAT

Static NAT allows mapping of Internet IP addresses and address ranges to hosts inside a network. You can assign separate public IP addresses to both server and client residing on the same network. To allow incoming traffic to a host for which static NAT is defined, You must create an Allow rule.

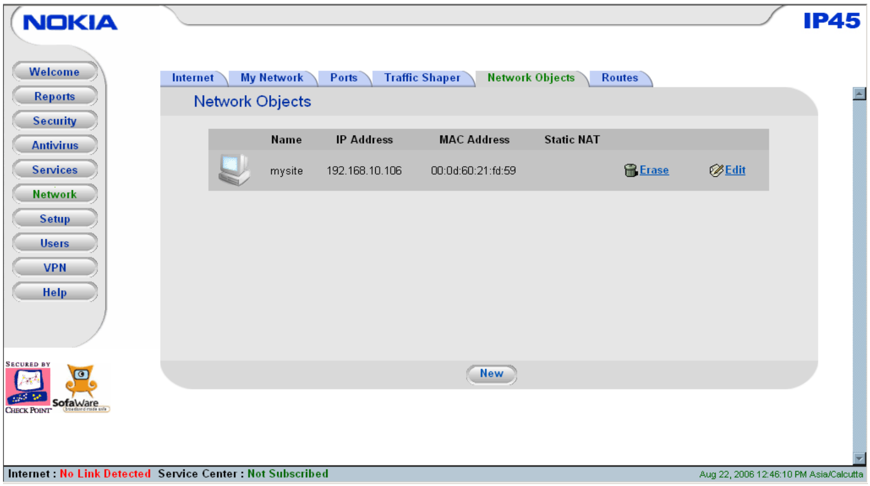
Note
While specifying firewall rules to such hosts, use the internal IP address of the host. Do not use the Internet IP address to which the host IP address is mapped.

To configure static NAT for a single computer

1. Choose Network from the IP45 main menu.

   The Internet page opens.
2. Click Network Objects.

The Network Objects page opens.



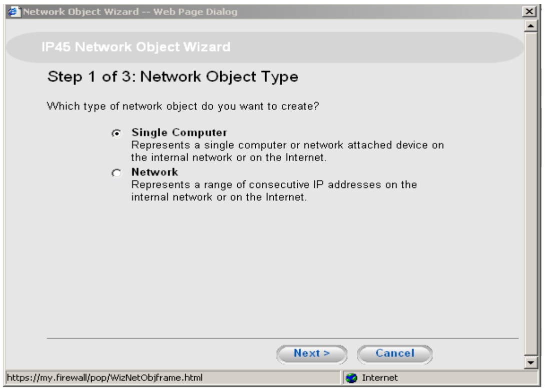
Network Objects

Name	IP Address	MAC Address	Static NAT		
mysite	192.168.10.106	00:0d:60:21:fd:59		Erase	Edit

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 12:46:10 PM Asia/Calcutta

3. Click New.

   The Network Object wizard with Network Object Type window opens.


Network Object Wizard -- Web Page Dialog
IP45 Network Object Wizard
Next >
Cancel
https://my.firewall/pop/WizNetObjframe.html
Internet

Step 1 of 3: Network Object Type

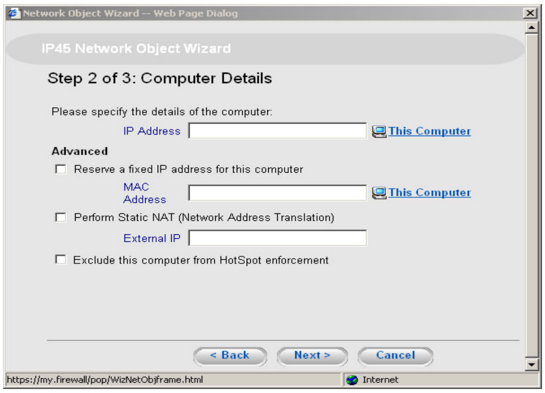
Which type of network object do you want to create?

● Single Computer
Represents a single computer or network attached device on the internal network or on the Internet.

○ Network
Represents a range of consecutive IP addresses on the internal network or on the Internet.

4. To configure static NAT for single computer, select Single Computer.
5. Click Next

The following window opens:


Network Object Wizard -- Web Page Dialog
IP45 Network Object Wizard
This Computer
This Computer
< Back
Next >
Cancel
https://my.firewall/pop/WizNetObjFrame.html
Internet

Step 2 of 3: Computer Details

Please specify the details of the computer:

IP Address

Advanced

□ Reserve a fixed IP address for this computer

MAC Address

□ Perform Static NAT (Network Address Translation)

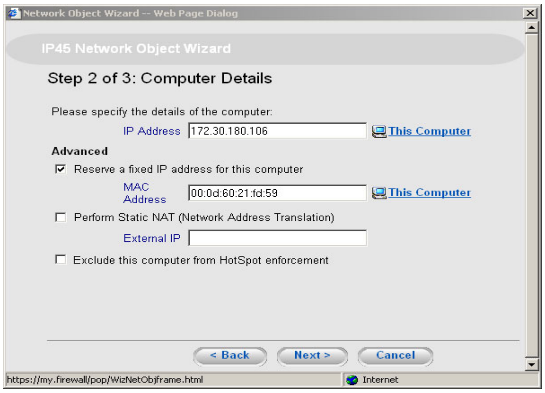
External IP

□ Exclude this computer from HotSpot enforcement

6. Enter the values in the IP Address and MAC Address text boxes. To enter the IP address and MAC address of your computer, click *This Computer* icon.

Note

The VLAN network must not overlap other networks.


Network Object Wizard -- Web Page Dialog
IP45 Network Object Wizard
This Computer
This Computer
< Back
Next >
Cancel
https://my.firewall/pop/WizNetObjFrame.html
Internet

Step 2 of 3: Computer Details

Please specify the details of the computer:

IP Address 172.30.180.106

Advanced

☑ Reserve a fixed IP address for this computer

MAC Address 00:0d:60:21:fd:59

□ Perform Static NAT (Network Address Translation)

External IP

□ Exclude this computer from HotSpot enforcement

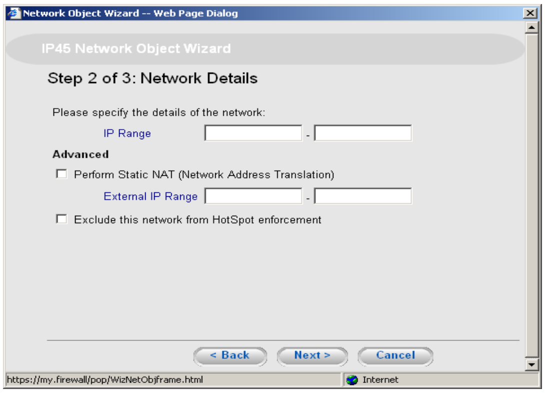
7. Enable the Perform Static NAT check box. Proceed as per the wizard.

   Static NAT is configured for the specified single computer.

To configure static NAT to a network

1. Select Network on the Network Objects window.
2. Click Next.

The Network Details window opens.



Network Object Wizard -- Web Page Dialog

IP45 Network Object Wizard

Step 2 of 3: Network Details

Please specify the details of the network:

IP Range [ ] - [ ]

Advanced

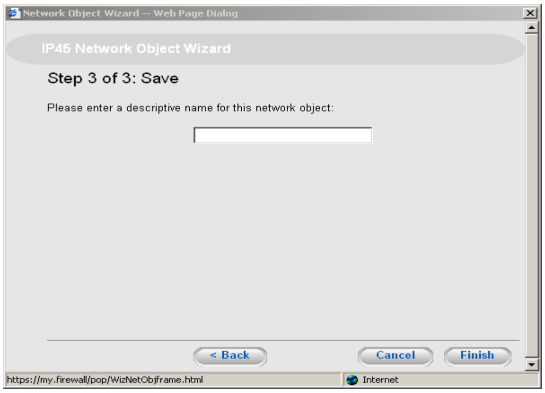
☐ Perform Static NAT (Network Address Translation)

External IP Range [ ] - [ ]

☐ Exclude this network from HotSpot enforcement

3. Specify the IP range for your network in the IP Range text box.
4. To enable static NAT, check the Perform Static NAT check box.
5. Enter the external IP range in the External IP Range text box.
6. Click Next.

   The Save window opens prompting for a descriptive name for the defined network object.



Network Object Wizard -- Web Page Dialog

IP45 Network Object Wizard

Step 3 of 3: Save

Please enter a descriptive name for this network object:

[ ]

7. Enter the name. Example: mynob1.
8. Click Finish.

   Static NAT is configured.

Editing Static NAT

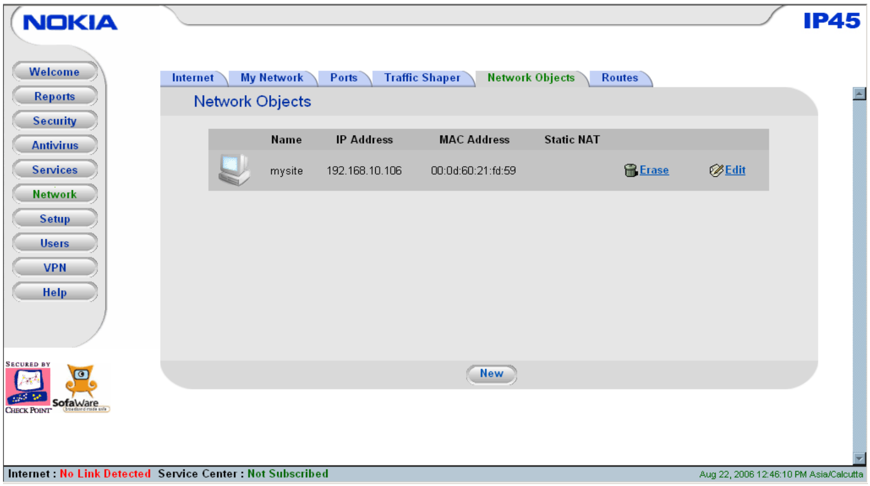
The following procedure describes how to edit the configured static NAT.

To edit static NAT

1. Choose Network from the IP45 main menu.

   The Internet page opens.
2. Click Network Objects.

The Network Objects page opens with the list of configured network objects.



Network Objects

Name	IP Address	MAC Address	Static NAT		
mysite	192.168.10.106	00:0d:60:21:fd:59		Erase	Edit

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 12:46:10 PM Asia/Calcutta

3. Click Edit next to the network object, whose static NAT is to be edited.

The Network Objects wizard appears.

4. Follow the wizard instructions to edit the configured static NAT.

For more information about the wizard screens, see “To configure static NAT for a single computer” on page 114.

Note
You can enable both static NAT and hide NAT for a network object.

Note
The IP45 supports proxy Address Resolution Protocol (ARP). When an external source attempts to communicate with a computer for which static NAT is enabled, the IP45 automatically replies to ARP queries with its own MAC address, thereby enabling communication. As a result, the static NAT Internet IP addresses appear to external sources to be real computers connected to the WAN interface.

Viewing Static NAT

You can view the configured and edited static NAT by using the following procedure:

To view static NAT

1. Choose Network from the IP45 main menu.

The Internet page opens.

2. Click Network Objects.

The Network Objects page opens with the list of configured network objects and static NAT.

Deleting Static NAT

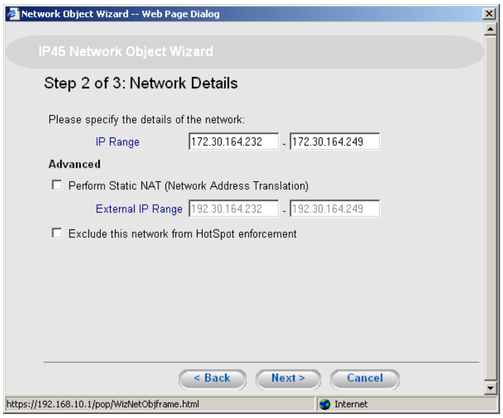
You can delete the configured static NAT by using the following procedure:

To delete static NAT

1. Choose Network > Network Objects.
2. Click Edit next to the network object, to delete the static NAT.

   The Network Object Type window opens.
3. Click Next.

   The Network Details window opens.



Network Object Wizard -- Web Page Dialog
IP45 Network Object Wizard

Step 2 of 3: Network Details

Please specify the details of the network:

IP Range 172.30.164.232 - 172.30.164.249

Advanced

□ Perform Static NAT (Network Address Translation)

External IP Range 192.30.164.232 - 192.30.164.249

□ Exclude this network from HotSpot enforcement

< Back
Next >
Cancel
https://192.168.10.1/pop/WizNetObjframe.html
Internet

4. Uncheck the Perform Static NAT check box.
5. Click Next.
6. Click Finish.

   The static NAT is deleted.

Configuring DHCP Reservation

Nokia IP45 v4.0 supports DHCP reservation. By using this feature, you can ensure that the IP address that the DHCP server assigns to a particular computer is always constant.

Normally a DHCP server assigns the same IP address to the computers. But when the DHCP server runs out of IP addresses and if any computer is inactive, then the IP address of the inactive computer is assigned to another computer.

By using DHCP reservation, you can reserve IP addresses that cannot be assigned to any computers other than the reserved ones. reservation can be done by using the MAC address.

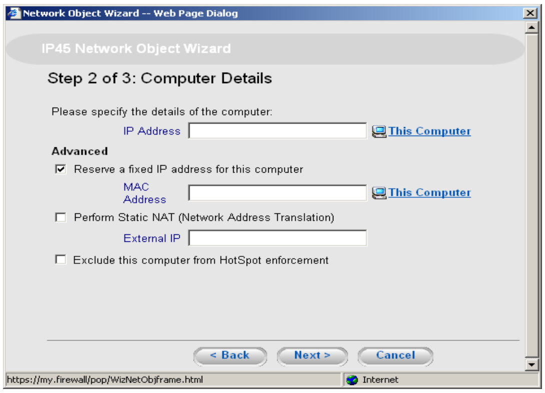
To reserve DHCP

1. Choose Network from the main menu, and click Network Objects.
2. Click New on the Network Objects page.

   The Network Object Type page opens.

3. Select Single Computer, and click Next.

   The Computer Details window opens.



Network Object Wizard -- Web Page Dialog

IP45 Network Object Wizard

Step 2 of 3: Computer Details

Please specify the details of the computer:

IP Address

Advanced

☑ Reserve a fixed IP address for this computer

MAC Address

☐ Perform Static NAT (Network Address Translation)

External IP

☐ Exclude this computer from HotSpot enforcement

4. Enter the value in IP Address text box to reserve.
5. Check Reserve a fixed IP for this computer check box.
6. Click Next.

   The Save window opens.
7. Enter the descriptive name for this network object in the text box provided.
8. Click Finish.

Deleting Network Objects

The following procedure describes how to delete a network object.

To delete a network object

1. Choose Network from the main menu.

   The Internet page opens.
2. Click the Network Objects tab.

   The Network Objects page opens with the list of network objects configured.
3. Click Erase next to the network object, to delete.

   A confirmation message appears.
4. Click OK.

   The network object is deleted.

Configuring Static Routes

Note
You can define static routes only if it is required.

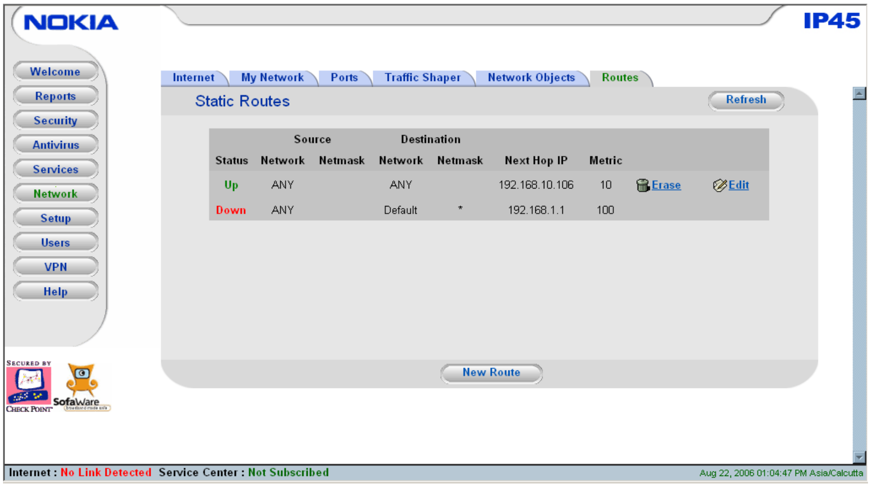
A static route is a setting that explicitly specifies the route for packets destined for a certain subnet. Packets with a destination that does not match any defined static route is routed to the default gateway.

The Static Routes page lists all existing routes, including the default, and indicates whether each route is currently connected, or reachable, or not reachable.

To add a static route

1. Choose Network from the main menu, and click the Routes tab.

   The Static Routes page opens, with a listing of existing static routes.



Static Routes

	Source		Destination					
Status	Network	Netmask	Network	Netmask	Next Hop IP	Metric		
Up	ANY		ANY		192.168.10.106	10	Erase	Edit
Down	ANY		Default	*	192.168.1.1	100		

Internet : No Link Detected Service Center : Not Subscribed

Aug 22, 2006 01:04:47 PM Asia/Calcutta

2. Click New Route.

3. Complete the fields in the wizard by using the information given in Table 20 on page 121.

4. Click Apply.

   The new static route is saved.

Table 20 Edit Route Page Fields

Field	Action
Destination Network	Type the network address of the destination network.
Subnet Mask	Select the subnet mask.

Table 20 Edit Route Page Fields (*continued*)

Field	Action
Next Hop IP	Type the IP address of the gateway (next hop router) to which to route the packets destined for this network.
Metric	Enter the metric value. Route with a lower metric value is preferred.

To edit a static route

1. Choose Network from the main menu, and click Routes tab.

   The Static Routes page opens displaying the list of existing static routes.

2. To edit the route details, do the following:

   a. Click the Edit tab at the row of your preferred route.

   b. Edit the fields by using the information inTable 20 on page 121.

   c. Click Finish.

   The changes are saved.

To delete a static route

1. Choose Network from the main menu, and click the Routes tab.

   The Static Routes page opens displaying a list of existing static routes.

2. In the preferred route row, click the Erase tab.

   A confirmation message appears.

3. Click OK.

   The route is deleted.

Configuring Source Routes

The Nokia IP45 security platform v4.0 supports source routing. In source routing, the next hop route is selected based on both source and destination IP addresses, unlike in traditional routing where only destination IP address is considered. All source routes takes priority over regular routes.

Source routing allows the LAN network to use the primary Internet connection while the DMZ network uses the secondary, thus balancing the load between the two networks.

Use the following procedure to configure source routes using GUI:

To configure source routes

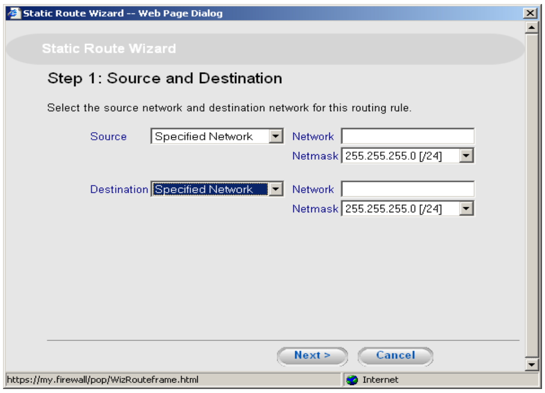
1. Choose Network from the main menu and select Routes.
2. The Routes page opens.

3. Click New Route.

   The Source and Destination window opens.

4. Select the Source and Destination options.

5. If you select Specify Network, enter the values in Network and Netmask fields.


Static Route Wizard -- Web Page Dialog
Static Route Wizard
Next >
Cancel
https://my.firewall/pop/WizRouteFrame.html
Internet

Step 1: Source and Destination

Select the source network and destination network for this routing rule.

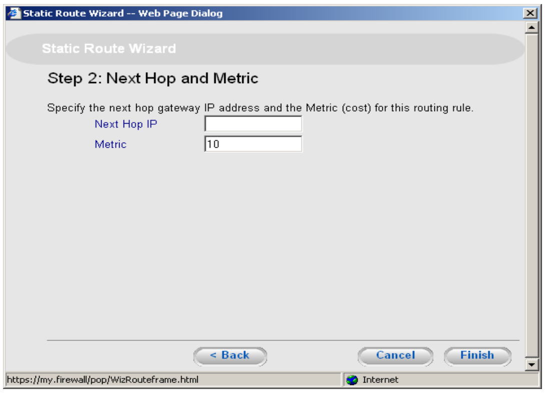
Source: Specified Network
Network:
Netmask: 255.255.255.0 [/24]

Destination: Specified Network
Network:
Netmask: 255.255.255.0 [/24]

6. Click Next.

7. The Next Hop and Metric window opens. Enter the Next Hop IP and Metric Value.

   The default value is 10.


Static Route Wizard -- Web Page Dialog
Static Route Wizard
< Back
Cancel
Finish
https://my.firewall/pop/WizRouteFrame.html
Internet

Step 2: Next Hop and Metric

Specify the next hop gateway IP address and the Metric (cost) for this routing rule.

Next Hop IP:
Metric: 10

8. Click Finish.

For information about the command line interface, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

OSPF

Open Shortest Path First (OSPF) is a link state protocol. This widely used interior gateway protocol distributes routing information between routers in a single autonomous system (AS). OSPF chooses the least-cost path as the best path. It is suitable for complex networks with a large number of routers because it provides equal-cost, multi-path routing, where packets to a single destination can be sent through more than one interface simultaneously.

In a link-state protocol, each participating router maintains a database describing the entire AS topology, which it builds out of the collected link state advertisements of all routers. Each router distributes its local state throughout the AS by flooding.

Each multi-access network with atleast two attached routers has a designated router and a backup designated router. The designated router floods a link state advertisement for the multi-access network and has other special responsibilities. Using a designated router reduces the number of adjacencies required on a multi-access network.

The great advantages of using dynamic routing are automatic distribution of routing tables across the enterprise and automatic rerouting of traffic around failures for high resiliency.

The IP45 OSPF implementation is fully interoperable with the Check Point Advanced Routing Suite, as well as with any other RFC compliant OSPF implementation.

The IP45 OSPF capabilities can be configured through the gateway’s command line interface.

For more information about configuring OSPF by using the command-line interface, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

Managing Ports

By using the web GUI, you can manage the ports of your Nokia IP45 appliance. You can now configure, edit and view the ports status by using GUI.

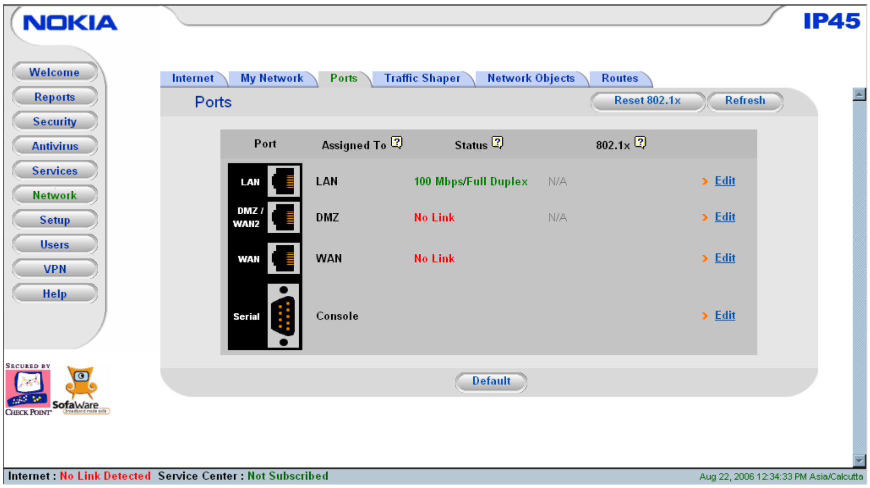
To assign ports

1. Choose Network from the main menu.

The Network page opens.

2. Click Ports.

The Ports page opens.



Port	Assigned To	Status	802.1x	
LAN	LAN	100 Mbps/Full Duplex	N/A	> Edit
DMZ / WAN2	DMZ	No Link	N/A	> Edit
WAN	WAN	No Link		> Edit
Serial	Console			> Edit

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 12:34:33 PM Asia/Calcutta

3. To assign a port, click Edit at the corresponding port.

The Port Setup page opens.

4. Select the values from the drop-down list by using the Table 21.
5. Click Apply.

Table 21 Port Setup page fields

Field	Description
Assign to network	Specifies the network that is assigned to the selected port
Link Configuration	Specifies the link configuration of the port. You can choose automatic detection to set the best configuration. Options: • Automatic Detection • 10 Mbps/Half Duplex • 10 Mbps/Full Duplex • 100 Mbps/Half Duplex • 100 Mbps/Full Duplex
Port Security	Specifies the port security. It is recommended to use 802.1x authentication standard for the security. Options: • None • 802.1x
Quarantine Network	Specifies the quarantine network. Clients that failed to authenticate will be moved to this network.

To edit and reset ports

1. To edit a port, click Edit at the corresponding port.

   The Port Setup page opens.
2. Select the values from the drop-down list by using the Table 21.
3. Click Apply.
4. To reset ports to their default values, click Default at the bottom of the page.

Defining the Port Link Speed

The Nokia IP45 security platform v4.0 supports defining the Ethernet port link speed by using GUI. In earlier releases this option could be set only by using the command-line interface.

By default, the link speed is automatically detected.

To set the link speed for the ports by using GUI

1. Choose Network from the main menu and select Ports.

   The Ports page opens.

2. Click Edit at the corresponding port to define the port link speed.

   The Port Setup page opens.

3. Select the link speed from the Link Configuration drop-down list for each interface.The options available are:

   - Automatic Detection
   - 10Mbps/Half Duplex
   - 10Mbps/Full Duplex
   - 100Mbps/Half Duplex
   - 100Mbps/full Duplex

4. Click Apply.

Viewing Ports Status

The following section provides information about how to view the ports status of your Nokia IP45.

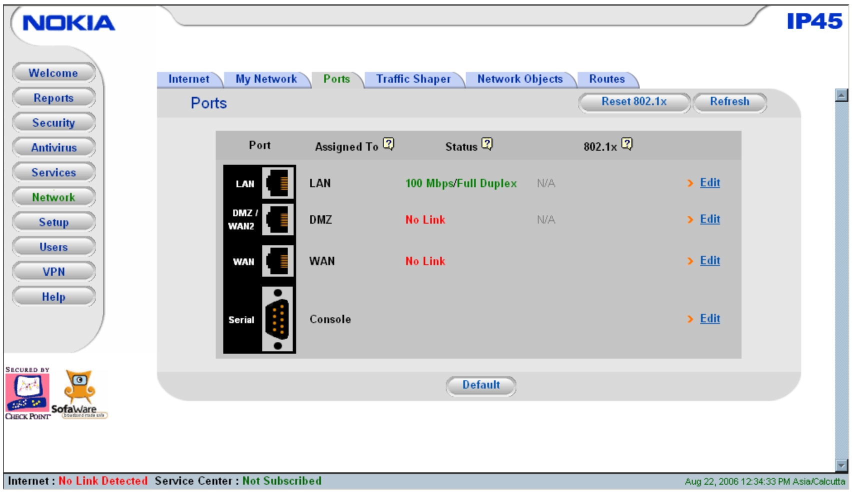
To view ports status

1. Choose Network from the main menu.

   The Network page opens.

2. Click Ports.

   The Ports page opens with information about the ports and their link status.



Ports

Port		Assigned To	Status	802.1x	
LAN		LAN	100 Mbps/Full Duplex	N/A	> Edit
DMZ / WAN2		DMZ	No Link	N/A	> Edit
WAN		WAN	No Link		> Edit
Serial		Console			> Edit

Internet : No Link Detected Service Center : Not Subscribed Aug 22, 2006 12:34:33 PM Asia/Calcutta

7 Quality of Service

This chapter provides information about Quality of Service (QoS), advantages of enabling QoS classes and how to configure QoS parameters. This chapter includes the following sections:

About QoS

A communications network plays a prominent role in the success of an organization. These networks transport a multitude of applications and data including high quality video and real time voice. Bandwidth-intensive applications stretch network capabilities and resources, complement, add value and enhance every business process. Networks must provide secure, predictable, measurable and guaranteed services.

Quality of Service can be achieved by managing delay, delay variation, bandwidth, and packet loss parameters on a network. QoS provides successful end-to-end solutions by using a set of techniques that manage the network resources.

The following sections discuss QoS techniques, and how to configure them.

Using Traffic Shaper

Traffic shaper is a bandwidth management solution that ensures the precedence of important traffic over less important traffic. This allows you to continue your business with less disruption even during network congestion. Traffic shaper uses stateful inspection technology to access and analyze data derived from all communication layers. This data is used to classify traffic in eight user-defined quality of service classes. Traffic shaper divides the available bandwidth among the classes according to the weight. Considering the importance of the traffic, you may assign weight to each class.

You can set bandwidth policies and control the flow of communication by using traffic shaper.

For example:

Web traffic is deemed three times important as FTP traffic and the weight assigned is 30.

FTP traffic is assigned a weight of 10.

When the network is congested, traffic shaper maintains the ratio of bandwidth allocation among web traffic and FTP traffic as 3:1.

Traffic shaper divides the remaining bandwidth among the other classes based on the weight assigned to them. If only Web traffic and FTP are active and competing in the entire network, then the remaining available bandwidth allocated will be 75% and 25% respectively. If Web traffic closes, FTP traffic receives 100% of the bandwidth. Traffic shaper supports Differentiated Services (DiffServ) packet marking. Packets are marked according to the QoS class they belong to. These packets are then granted priority on the public network according to their class.

Note
To enable traffic shaper, see "Configuring an Internet Connection" on page 73.

IP45 v4.0 traffic shaper supports shaping of inbound traffic when multiple internal networks are defined. The earlier releases supported only for a single network.

QoS Classes

You can define different QoS classes based on your requirement. You can assign a bandwidth limit to each class. This limit acts as the maximum bandwidth limit for all the connections under this class. Once a class reaches this set limit, no connections of this class will be allocated any bandwidth, even if unused bandwidth is available. You can also set delay sensitivity, which indicates whether connections belonging to one class should be allowed to precede the connections belonging to other classes.

Nokia IP45 supports four default QoS classes and support a maximum of eight user-defined QoS classes.

Note
To assign traffic to the QoS classes, define an Allow or Allow and Forward firewall rule.

Default QoS Classes

Nokia IP45 supports the following four predefined (default) QoS classes.

Table 22 Default QoS Classes

Class	Weight	Delay Sensitivity	Suitable for
Default	10	Medium (normal traffic)	By default, all traffic is assigned to this class.
Urgent	15	High (interactive traffic)	Traffic that is highly sensitive to delay. For example: IP telephony, videoconferencing, and interactive protocols such as Telnet that require quick user response.
Important	20	Medium (normal traffic)	Normal traffic
Low Priority	5	Low (bulk traffic)	Traffic that is not sensitive to long delays. for example: SMTP traffic.

Enabling QoS Classes

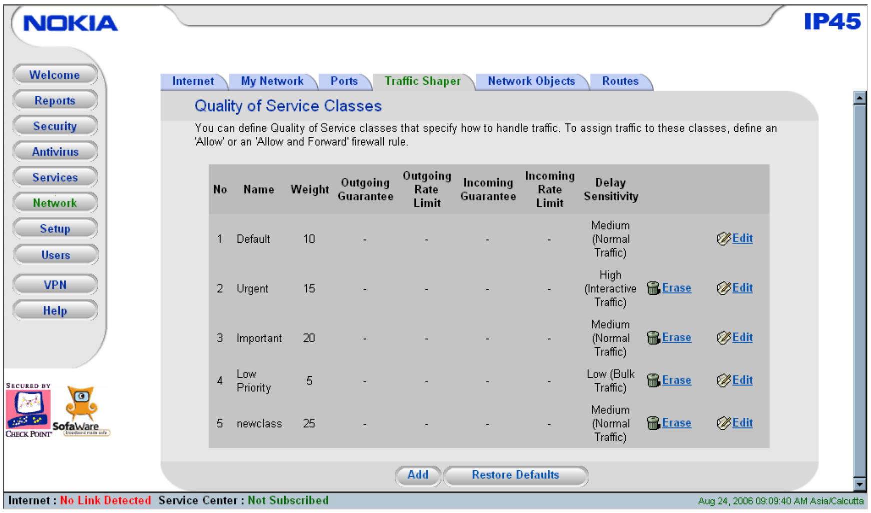
By default the QoS classes are disabled in your IP45 device. You must enable the QoS classes before adding them. You can do this by enabling the traffic shaper while configuring your Internet connections. For more information about enabling the traffic shaper, see “Configuring an Internet Connection” on page 73.

Adding QoS Classes

You can define QoS classes to fit your administrative needs. To add QoS classes

1. Choose Network from the main menu, and click Traffic Shaper.

   The Quality of Service Classes page opens.



Quality of Service Classes

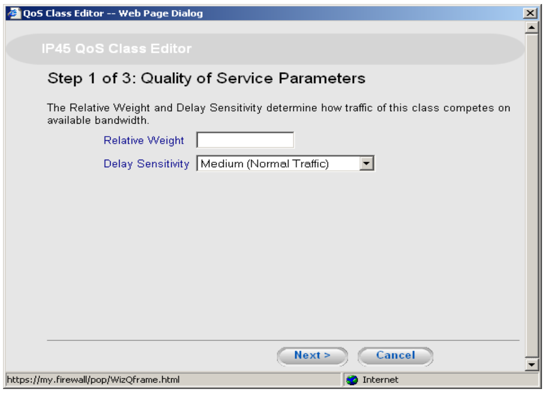
You can define Quality of Service classes that specify how to handle traffic. To assign traffic to these classes, define an 'Allow' or an 'Allow and Forward' firewall rule.

No	Name	Weight	Outgoing Guarantee	Outgoing Rate Limit	Incoming Guarantee	Incoming Rate Limit	Delay Sensitivity		
1	Default	10	-	-	-	-	Medium (Normal Traffic)		Edit
2	Urgent	15	-	-	-	-	High (Interactive Traffic)	Erase	Edit
3	Important	20	-	-	-	-	Medium (Normal Traffic)	Erase	Edit
4	Low Priority	5	-	-	-	-	Low (Bulk Traffic)	Erase	Edit
5	newclass	25	-	-	-	-	Medium (Normal Traffic)	Erase	Edit

Internet : No Link Detected Service Center : Not Subscribed Aug 24, 2006 09:09:40 AM Asia/Calcutta

2. Click Add at the bottom of the page.

   Quality of Services Parameters window opens.


QoS Class Editor -- Web Page Dialog
IP45 QoS Class Editor
Next >
Cancel
https://my.firewall/pop/WizQframe.html
Internet

Step 1 of 3: Quality of Service Parameters

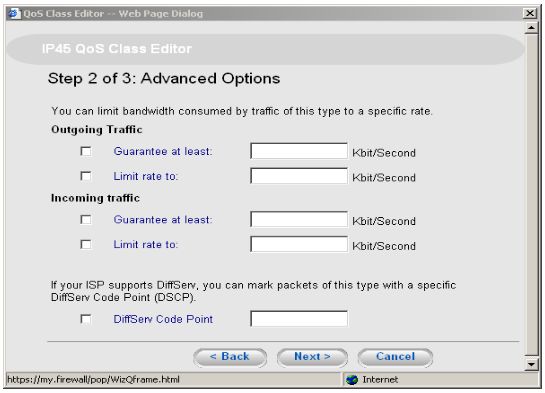
The Relative Weight and Delay Sensitivity determine how traffic of this class competes on available bandwidth.

Relative Weight

Delay Sensitivity: Medium (Normal Traffic)

3. Enter the value for Weight.
4. Select a value from the Delay Sensitivity drop-down list.
5. Click Next.

The Advanced Options window opens.


QoS Class Editor -- Web Page Dialog
IP45 QoS Class Editor
< Back
Next >
Cancel
https://my.firewall/pop/WizQframe.html
Internet

Step 2 of 3: Advanced Options

You can limit bandwidth consumed by traffic of this type to a specific rate.

Outgoing Traffic

- □ Guarantee at least: Kbit/Second
- □ Limit rate to: Kbit/Second

Incoming traffic

- □ Guarantee at least: Kbit/Second
- □ Limit rate to: Kbit/Second

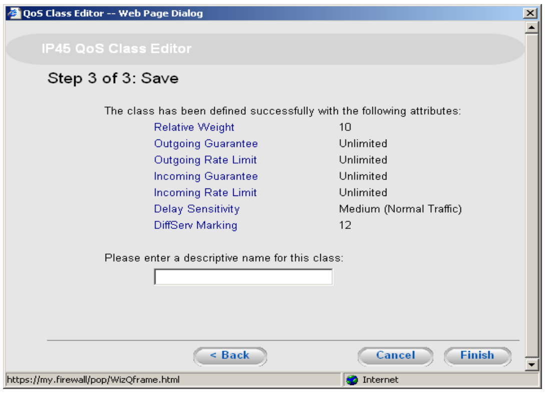
If your ISP supports DiffServ, you can mark packets of this type with a specific DiffServ Code Point (DSCP).

- □ DiffServ Code Point

6. Enter the values as per the information provided in Table 22 on page 129.

7. Click Next.

The Save window opens with the list of values that you configured for the class.


QoS Class Editor -- Web Page Dialog
IP45 QoS Class Editor
< Back
Cancel
Finish
https://my.firewall/pop/WizQframe.html
Internet

Step 3 of 3: Save

The class has been defined successfully with the following attributes:

Relative Weight	10
Outgoing Guarantee	Unlimited
Outgoing Rate Limit	Unlimited
Incoming Guarantee	Unlimited
Incoming Rate Limit	Unlimited
Delay Sensitivity	Medium (Normal Traffic)
DiffServ Marking	12

Please enter a descriptive name for this class:

8. Enter a descriptive name for this class. example: very important

9. Click Finish.

Table 23 QoS Class Parameters

Field	Action
Relative Weight	Type a value indicating the importance of this class, relative to the other defined classes. For example, if you assign one class a weight of 50, and you assign another class a weight of 25, the first class will be allocated twice the amount of bandwidth as the second when the lines are congested.
Delay Sensitivity	The degree of precedence of this class in the transmission queue. Options: Low (bulk traffic)—traffic that is not sensitive to long delays. For example: SMTP traffic (outgoing email). Medium (normal traffic)—normal traffic High (interactive traffic)—traffic that is highly sensitive to delay. For example: IP telephony, video conferencing, and interactive protocols that require quick user response, such as Telnet. **Note** Traffic shaper serves delay-sensitive traffic with a lower latency. That is, traffic shaper attempts to send packets with high level interactive traffic) before packets with a medium (normal traffic) or low (bulk traffic) level.
Outgoing Traffic	
Guarantee at least	Select this option to guarantee a minimum bandwidth for outgoing traffic belonging to this class. Enter the value in kilobits/second in the field provided.
Limit rate to	Select this option to limit the rate of outgoing traffic belonging to this class. Enter the maximum rate in kilobits/second in the field provided.

Table 23 QoS Class Parameters (*continued*)

Field	Action
Incoming Traffic	
Guarantee at least	Select this option to guarantee a minimum bandwidth for the incoming traffic belonging to this class. Enter the value in kilobits/second in the field provided.
Limit rate to	Select this option to limit the rate of incoming traffic belonging to this class. Enter the maximum rate in kilobits/second in the field provided.
DiffServ Code Point	Select this option to mark packets belonging to this class with a DiffServ Code Point (DSCP). Type the DSCP value in the field provided. Value: 0–63 **Note** The marked packets gain priority on the public network according to their DSCP. To use this option, your ISP or private WAN must support DiffServ. You can obtain the correct DSCP value from your ISP or private WAN administrator.

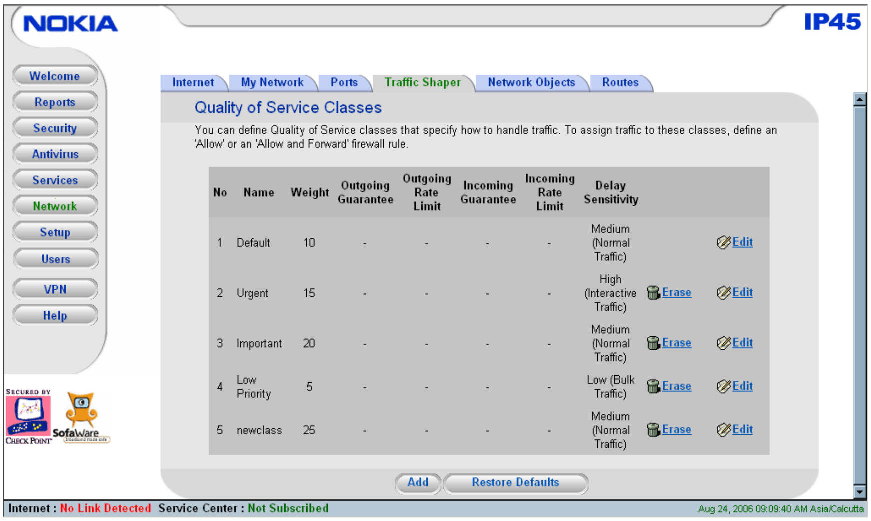
Editing and Deleting QoS Classes

The following procedures describe how to edit and delete the QoS classes.

To edit QoS classes

1. Choose Network >Traffic Shaper.

   The Quality of Service Classes page opens.



Quality of Service Classes

You can define Quality of Service classes that specify how to handle traffic. To assign traffic to these classes, define an 'Allow' or an 'Allow and Forward' firewall rule.

No	Name	Weight	Outgoing Guarantee	Outgoing Rate Limit	Incoming Guarantee	Incoming Rate Limit	Delay Sensitivity		
1	Default	10	-	-	-	-	Medium (Normal Traffic)		Edit
2	Urgent	15	-	-	-	-	High (Interactive Traffic)	Erase	Edit
3	Important	20	-	-	-	-	Medium (Normal Traffic)	Erase	Edit
4	Low Priority	5	-	-	-	-	Low (Bulk Traffic)	Erase	Edit
5	newclass	25	-	-	-	-	Medium (Normal Traffic)	Erase	Edit

Internet : No Link Detected Service Center : Not Subscribed Aug 24, 2006 09:09:40 AM Asia/Calcutta

2. Click Edit next to the QoS class to edit.

   The IP45 QoS Class Editor wizard appears.

3. Enter the new values for Weight and Relative Sensitivity.

4. Click Next.

   The Advanced Options window opens.

5. Enter the new values as per the description provided in Table 22 on page 129.

6. Click Next.

7. The Save window opens displaying the edited information.

8. Click Finish.

   The QoS class values are edited.

To delete a QoS class

1. Choose Network >Traffic Shaper.

   The Quality of Service Classes page opens.

2. Click Erase next to the QoS class to delete.

   The QoS class is deleted.

Note
To restore default QoS classes, click Restore Defaults tab at the bottom of the Quality of Service Classes window.

8 Setting Up the Nokia IP45 Security Platform Security Policy

This chapter describes how to set up the Nokia IP45 security policy and includes the following topics:

VStream Embedded Antivirus

IP45 v4.0 includes a new, embedded, stream-based antivirus engine, VStream, that supports efficient antivirus scanning at the kernel level.

This section includes the following topics:

Features Overview

VStream offers several advantages over traditional proxy-based network antivirus solutions based on Check Point Stateful Inspection and Application Intelligence technologies:

- **Lightweight Streaming**—scans files for malicious content on the fly, without downloading them into intermediate storage, resulting in minimal added latency and support for unlimited file sizes. Able to scan thousands of concurrent connections by storing only minimal state information per connection.
- **Comprehensive Protocol Support**—offers comprehensive protocol support, including HTTP, FTP, NBT, file sharing, POP3, SMTP and IMAP, as well as arbitrary, user-defined TCP and UDP ports.
- **Granular Scanning Policy**—a customizable scanning policy allows specifying with very fine granularity exactly which connections should be scanned for viruses.
- **On-the-fly Decompression**—supports on-the-fly, real-time decompression and scanning of ZIP, TAR, and GZ archive files. Archive files can be scanned with no file size limitation and with support for nested archive files.

In addition to blocking computer viruses and Trojan Horses, VStream also includes Anti-Phishing, blocking fraudulent emails that try to entice users to fake Web sites in attempt to steal sensitive data, such as passwords or credit card details.

You can use VStream as a second layer of antivirus to complement the capabilities and address the weaknesses of desktop antivirus software.

By offering a gateway-based antivirus solution, IP45 blocks security threats before they reach your network. The antivirus signatures are automatically updated, keeping the security up-to-date with no need for user or network administrator intervention.

VStream Antivirus Actions

When it detects malicious content, VStream Antivirus takes action based on the protocol in which the virus was found. For more information, see Table 24.

Table 24 VStream Antivirus Actions

Protocol in which the virus was found	Protocol is detected on this port	Antivirus Action
HTTP	• Port 80 • All ports on which VStream is enabled by the policy	• Terminates the connection
FTP	Port 21	• Terminates the data connection • Sends a *Virus detected* message to the FTP client
POP3	Port 110	• Terminates the connection • Deletes the virus-infected email from the server

Table 24 VStream Antivirus Actions (*continued*)

Protocol in which the virus was found	Protocol is detected on this port	Antivirus Action
SMTP	Port 25	• Rejects the virus-infected email with 554 error code • Sends a *Virus detected* message to the sender
IMAP	Port 143	• Terminates the connection • Replaces the virus-infected email with a *virus found* message
TCP and UDP	Generic TCP and UDP ports other than the ones listed above.	• Terminates the connection

Note
VStream uses a *best effort* approach to detect viruses for all other protocols that are not listed in the table. In such cases, detection of viruses depends on the specific encoding used by the protocol.

In each case, VStream Antivirus blocks the file and writes a log to the Event Log.

Enabling and Disabling VStream Antivirus

VStream Antivirus differs from the Email Antivirus subscription service (part of the Email Filtering service) in the following ways:

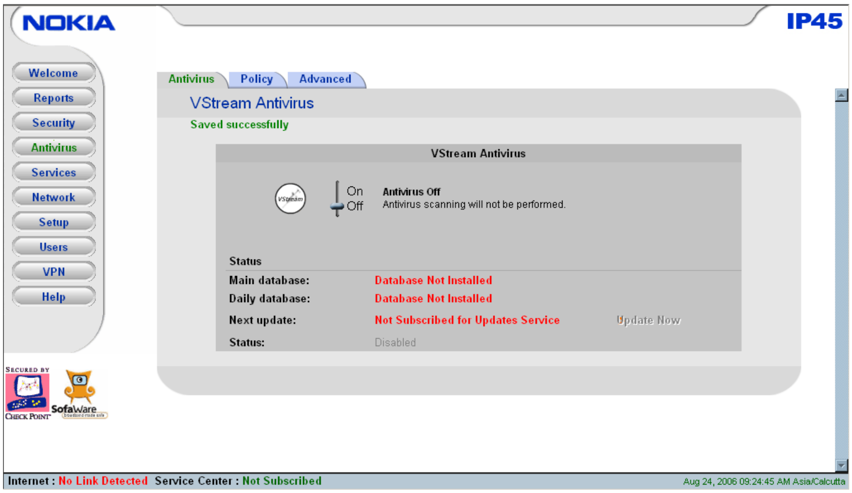
- VStream Antivirus scans for viruses in the IP45 gateway itself while Email Antivirus is centralized, redirecting traffic through the Service Center for scanning.
- VStream Antivirus supports additional protocols while Email Antivirus is specific to email, scanning incoming POP3 and outgoing SMTP connections only.

You can use either antivirus solution or both in conjunction.

To enable and disable VStream antivirus

1. From the main menu, choose Antivirus.

   The VStream Antivirus page opens.



VStream Antivirus

Saved successfully

VStream Antivirus

On
Off

Antivirus Off
Antivirus scanning will not be performed.

Status

Main database:	Database Not Installed	
Daily database:	Database Not Installed	
Next update:	Not Subscribed for Updates Service	Update Now
Status:	Disabled	

Internet : No Link Detected Service Center : Not Subscribed Aug 24, 2006 09:24:45 AM Asia/Calcutta

2. To set the antivirus, move the On-Off lever.

Viewing VStream Signature Database Information

VStream Antivirus maintains two databases: a daily database and a main database. The daily database is updated frequently with the newest virus signatures. Periodically, the contents of the daily database are moved to the main database, leaving the daily database empty. This system of incremental updates to the main database allows for quicker updates and saves on network bandwidth.

You can view information about the VStream signature databases currently in use, in the VStream Antivirus page.

Table 25 VStream Antivirus page fields

Field	Description
Main Database	Displays the date and time at which the main database was last updated, followed by the version number.
Daily Database	Displays the date and time at which the daily database was last updated, followed by the version number.
Next Update	Displays the next date and time at which the IP45 appliance will check for updates.
Status	Displays the current status of the database. Options: • Database Not Installed • OK

Configuring VStream Antivirus

You can configure the VStream Antivirus in the following ways:

- Configuring the antivirus policy
- Configuring the advanced settings

Configuring the antivirus policy

VStream Antivirus policy:

- Allows you to define exactly which traffic should be scanned, by specifying the protocol, ports, and source and destination IP addresses.
- Enables you to define exceptions to rules by processing the rules in the order they appear in the Antivirus Policy table.

To scan all outgoing SMTP traffic, except traffic from a specific IP address

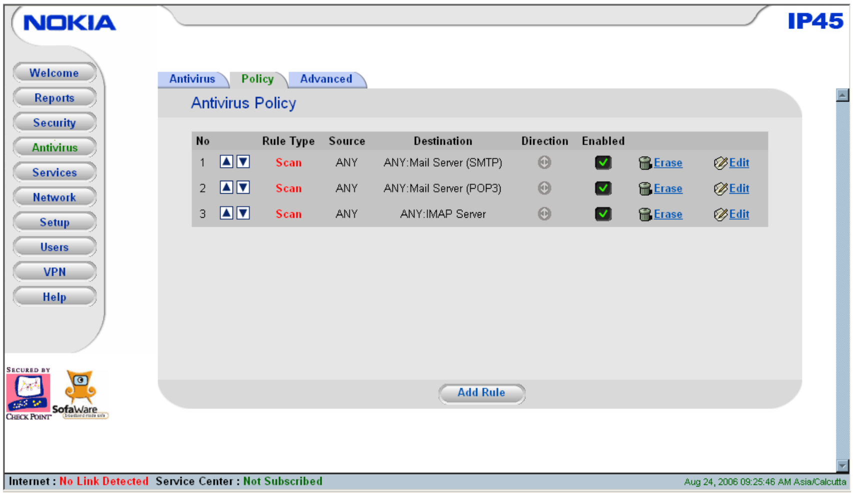
1. Create a rule scanning all outgoing SMTP traffic
2. Move the rule Configuring VStream Antivirus down in the Antivirus Policy table.
3. Create another rule passing SMTP traffic from the desired IP address
4. Move this rule to a higher location in the Antivirus Policy table than the first rule.

The IP45 appliance will process rule 1 first, passing outgoing SMTP traffic from the specified IP address and then it will process rule 2, scanning all outgoing SMTP traffic.

To set antivirus policy

1. From the main menu, choose Antivirus.

   The VStream Antivirus page opens.



Antivirus Policy

No		Rule Type	Source	Destination	Direction	Enabled		
1	▲▼	Scan	ANY	ANY:Mail Server (SMTP)	⊕	☑	Erase	Edit
2	▲▼	Scan	ANY	ANY:Mail Server (POP3)	⊕	☑	Erase	Edit
3	▲▼	Scan	ANY	ANY:IMAP Server	⊕	☑	Erase	Edit

Internet : No Link Detected Service Center : Not Subscribed Aug 24, 2006 09:25:46 AM Asia/Calcutta

2. You can view a list of antivirus rules that are set.

3. For details on the options of this page, see Table 26.

Table 26 Fields of Antivirus policy page

Field	Description
Rule Type	Defines the policy whether to scan, block the viruses or to pass the messages without scanning. Options: • Scan: scans the email messages and files matching the rule • Pass: does not scan the email messages and files
Source	The source of the messages from which they are sent
Destination	The destination to which the messages are sent
Direction	Specifies the direction of data. Options: • Download and Upload • Download • Upload Default value: Download and Upload
Enabled	Specifies whether the rule is enabled or not.

To add a new rule

1. From the main menu, choose AntiVirus.

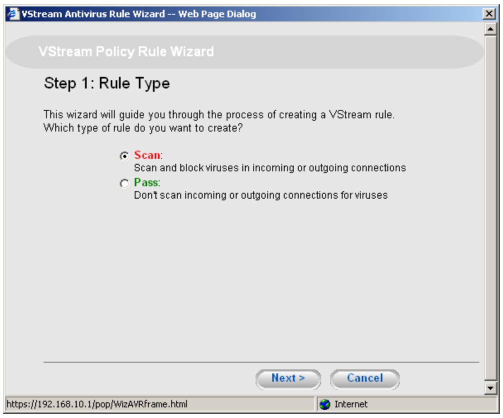
   The VStream Antivirus page opens.

2. Select Policy.

   The Antivirus Policy page opens.

3. Click Add Rule.

   The VStream Policy Wizard opens.



VStream Antivirus Rule Wizard -- Web Page Dialog

VStream Policy Rule Wizard

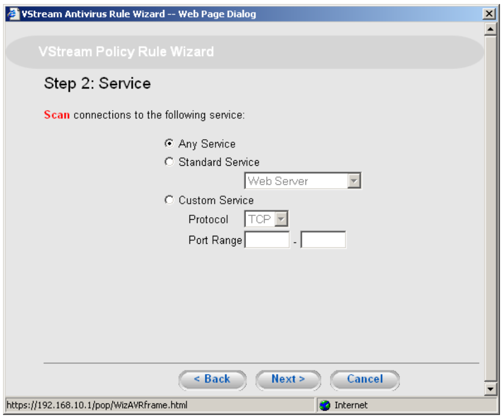
Step 1: Rule Type

This wizard will guide you through the process of creating a VStream rule.
Which type of rule do you want to create?

● Scan:
Scan and block viruses in incoming or outgoing connections

○ Pass:
Don't scan incoming or outgoing connections for viruses

4. If you select scan, Service window opens.



VStream Antivirus Rule Wizard -- Web Page Dialog

VStream Policy Rule Wizard

Step 2: Service

Scan connections to the following service:

● Any Service

○ Standard Service

Web Server

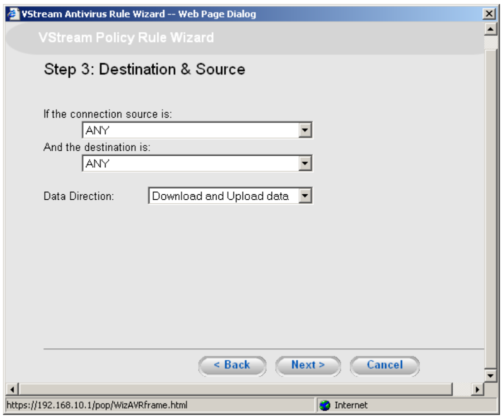
○ Custom Service

Protocol TCP

Port Range -

5. Select the service to scan connections - any service, standard service or custom service.

6. After you select one of the services, the Destination & Source window opens.


VStream Antivirus Rule Wizard -- Web Page Dialog
VStream Policy Rule Wizard
< Back
Next >
Cancel
https://192.168.10.1/pop/WizAVRframe.html
Internet

Step 3: Destination & Source

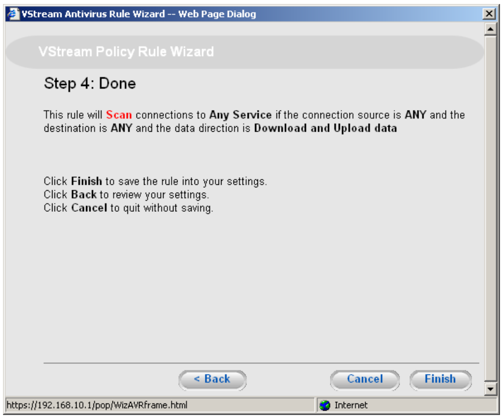
If the connection source is: ANY

And the destination is: ANY

Data Direction: Download and Upload data

7. Select the source of connection and the destination.
8. Select the data direction from the drop-down list.
9. Click Next.

   Done window opens.


VStream Antivirus Rule Wizard -- Web Page Dialog
VStream Policy Rule Wizard
< Back
Cancel
Finish
https://192.168.10.1/pop/WizAVRframe.html
Internet

Step 4: Done

This rule will **Scan** connections to **Any Service** if the connection source is **ANY** and the destination is **ANY** and the data direction is **Download and Upload data**

Click **Finish** to save the rule into your settings.
Click **Back** to review your settings.
Click **Cancel** to quit without saving.

10. Click Finish.

    The new scan rule is added.

Similarly you can select the option *pass* and follow the instructions in the wizard to add new rule of pass type.

For more information on the options of the Antivirus policy wizard, see Table 27.

Table 27 Antivirus Policy fields

Field	Description
Any Service	Specifies that the rule should be applied to any service
Standard Service	Specifies that the rule should be applied to a specific standard service. You can select the standard services from the drop-down list. Options: • Web Server • FTP Server • Mail Server(POP3) • Mail server(SMTP) • IMAP server
Custom Service	Specifies that the rule should be applied to a specific non-standard service. If you select this service, Protocol and Port Range fields are enabled.
Protocol	Specifies the protocol for which the rule should apply. Options: • TCP • UDP • Any
Port Range	Specifies the port range for which the rule should apply. **Note** If you do not enter any number for the range, the rule will apply to all ports. If you enter only one port number, the range will include only that port.
If the connection source is	Specifies the source of the connections you want to allow or block. To specify an IP address, select Specified IP and type the desired IP address in the filed provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided.

Table 27 Antivirus Policy fields (*continued*)

Field	Description
And the destination is	Specifies the destination of the connections you want to allow or block. To specify an IP address, select *Specified IP* and type the desired IP address in the filed provided. To specify an IP address range, select *Specified Range* and type the desired IP address range in the fields provided. To specify the IP45 Portal and network printers, select *This Gateway*. To specify any destination except the IP45 Portal and network printers, select *ANY*. **Note** *Specified Range* and *This Gateway* options are not available in Allow and Forward rules.
Data Direction	Specifies the direction of connections to which the rule should apply. Options: • Download and Upload data: applies to downloaded and uploaded data. • Download data: applies to downloaded data, that is, data flowing from the destination of the connection to the source of the connection. • Upload data: applies to uploaded data, that is, data flowing from the source of the connection to the destination of the connection. Default value: Download and Upload data

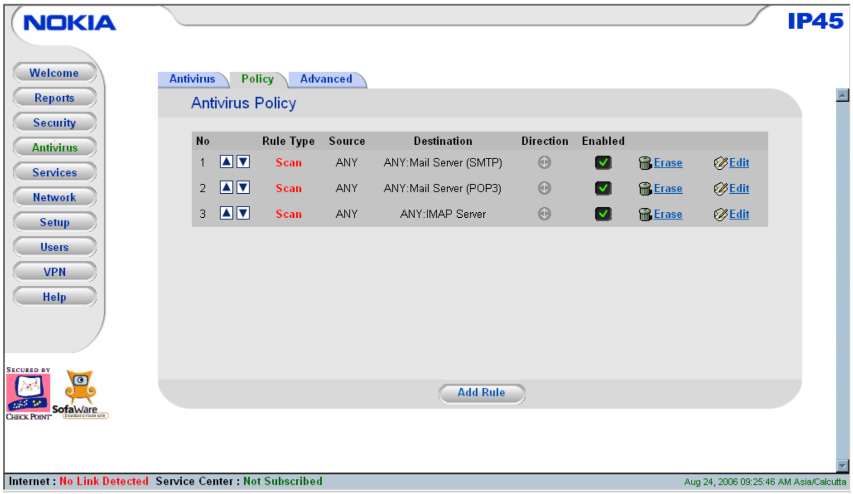
To edit rules

1. From the main menu, choose Antivirus.

   The VStream Antivirus page opens.

2. Select Policy.

   The Antivirus Policy page opens.



Antivirus Policy

No		Rule Type	Source	Destination	Direction	Enabled		
1	▲ ▼	Scan	ANY	ANY:Mail Server (SMTP)	⊕	☑	Erase	Edit
2	▲ ▼	Scan	ANY	ANY:Mail Server (POP3)	⊕	☑	Erase	Edit
3	▲ ▼	Scan	ANY	ANY:IMAP Server	⊕	☑	Erase	Edit

Internet : No Link Detected Service Center : Not Subscribed Aug 24, 2006 09:25:46 AM Asia/Calcutta

3. Click Edit next to the rule type you want to edit.

   The VStream Policy Rule wizard opens.

4. Proceed with the wizard and follow the instructions to edit the existing values.

To delete rules

1. From the main menu, choose Antivirus.

   The VStream Antivirus page opens.

2. Select Policy.

   The Antivirus Policy page opens.

3. Click Erase next to the rule type you want to erase.

   A confirmation message appears.

4. Click OK.

   The selected rule is deleted.

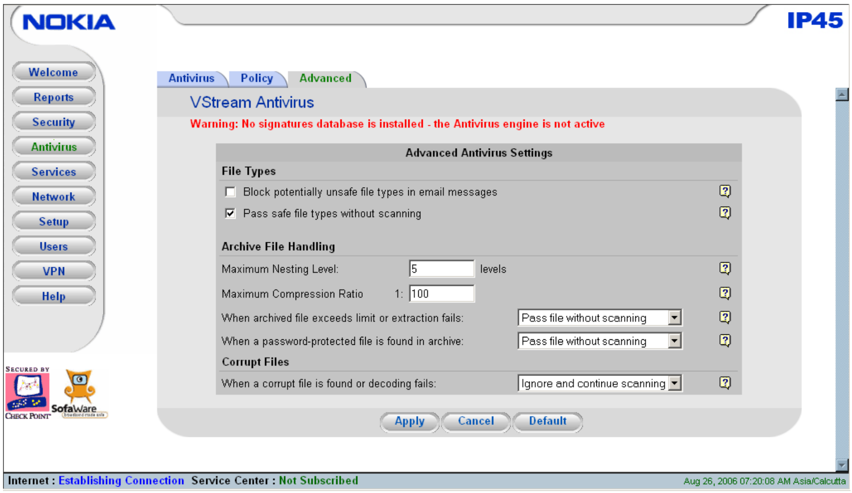
Configuring the advanced settings

You can configure advanced settings for the existing VStream Antivirus policy rules.

To configure advanced antivirus settings

1. From the main menu, choose Antivirus.

   The VStream Antivirus page opens.



VStream Antivirus

Warning: No signatures database is installed - the Antivirus engine is not active

Advanced Antivirus Settings

File Types

☐ Block potentially unsafe file types in email messages

☑ Pass safe file types without scanning

Archive File Handling

Maximum Nesting Level: 5 levels

Maximum Compression Ratio 1: 100

When archived file exceeds limit or extraction fails: Pass file without scanning

When a password-protected file is found in archive: Pass file without scanning

Corrupt Files

When a corrupt file is found or decoding fails: Ignore and continue scanning

Internet : Establishing Connection Service Center : Not Subscribed Aug 26, 2006 07:20:08 AM Asia/Calcutta

2. You can view advanced antivirus settings. Selecting them will enable you to define the advanced options.
3. Select the options using the information provided in the Table 28.
4. Click Apply.

   The new settings will be saved.
5. Click Default to restore default values.

Table 28 Advanced Antivirus Settings page fields

Field	Description
Block potentially unsafe file types in email messages	When enabled blocks all email messages that contain potentially unsafe attachments such as executable files.
Pass safe file types without scanning	When enabled skips scanning of some common file types that are known to be safe. This option when enabled improves performance.
Maximum Nesting Level	Limits the number of nested content levels that will be scanned by the antivirus to prevent a potential attacker from overloading the gateway by sending the extremely nested archive files.
Maximum Compression Ratio	Limits the maximum compression ratio of the files that Vstream can scan.

Table 28 Advanced Antivirus Settings page fields (*continued*)

Field	Description
When archived file exceeds limit or extraction fails	A scan failure may be due to a corrupt file that cannot be read, a file that exceeds the maximum nesting level, or a file that exceeds the maximum compression ratio. Options: • Pass file without scanning • Block file
When a password-protected file is found in archive	VStream cannot extract and scan password-protected files inside archives. You can choose to pass such files without scanning, or to block all password-protected files. Options: • Pass file without scanning • Block file
When a corrupt file is found or decoding fails	Sometimes VStream detects files or encodings that are corrupt or truncated, and cannot be scanned completely. You can choose to ignore and continue scanning or can block these files completely. Options: • Ignore and continue scanning • Block file

Updating VStream Antivirus

If you are subscribed to the VStream Antivirus updates service, virus signatures are updated automatically, keeping security up-to-date, without requesting for your intervention. You can also check for updates manually, if required.

To update VStream antivirus

1. From the main menu, choose Antivirus.

   The VStream Antivirus page opens.

2. Click Update Now.

   The VStream Antivirus is updated with the latest antivirus signatures.

You can configure VStream Antivirus settings by using the command-line interface. For more information about VStream Antivirus commands, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

Setting the Firewall Security Level

You can define the firewall security level on the Firewall page. This level can be adjusted to three states:

- **Low-level security**—enforces basic control on incoming connections, while permitting all outgoing connections.

  At this level, all inbound traffic is blocked to the external IP address except for ICMP echoes. All outbound connections are allowed.

- **Medium-level security**—enforces strict control on all incoming connections, while permitting safe outgoing connections.

  When this level is selected, all inbound traffic is blocked. All outbound traffic is allowed to the Internet except for windows file sharing.

- **High level-security—**enforces strict control on all incoming and outgoing connections.All inbound traffic is blocked. Restricts all outbound traffic except for the following:

  Web traffic (HTTP, HTTPS), email (IMAP, POP3, SMTP), FTP, news groups, Telnet, DNS, IPSec IKE, and VPN traffic.

  The default security level is medium.

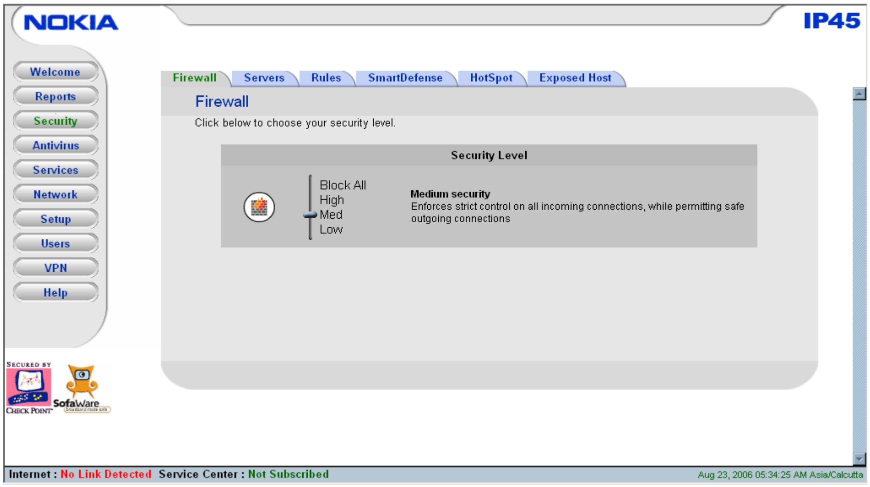
- **Block All**—blocks all traffic.

For information on customizing your security policy, see “Customizing the Nokia IP45 Security Platform Security Policy” on page 150.

To change the firewall security level

1. Choose Security from the main menu.

   The Firewall page opens.



Firewall

Click below to choose your security level.

Security Level

Block All
High
Med
Low

Medium security
Enforces strict control on all incoming connections, while permitting safe outgoing connections

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 05:34:25 AM Asia/Calcutta

2. To set the security level, move the slider or click on the security level.

   The IP45 security level changes accordingly.

Note
While setting the security levels, you might experience a temporary break in the service.

Configuring Virtual Servers

Note
If you do not intend to host any public Internet servers (Web server, email server and so on) in your network, you can skip this section. Configuring servers allows you to create simple Allow and Forward rules for common services. This is equivalent to creating Firewall rules.

You can selectively allow incoming network connections into your network. For example, you can set up your own Web server, email server, Telnet server, or an FTP server.

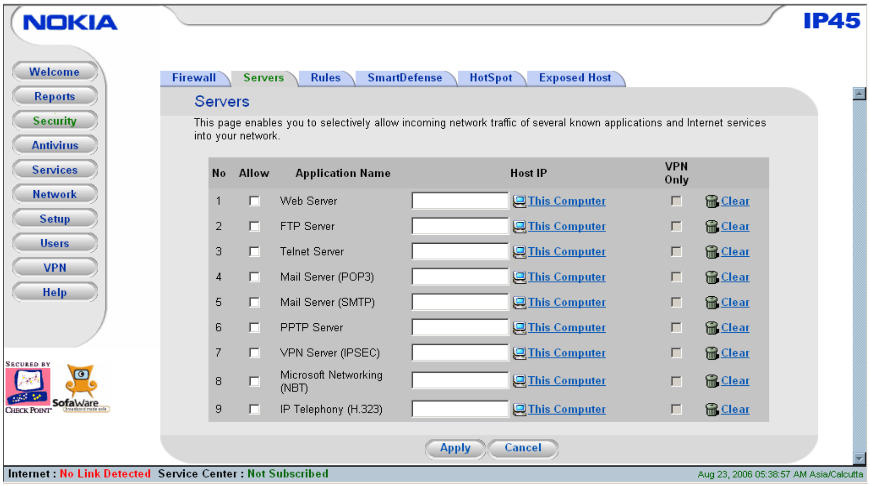
To run a service on a host

1. Choose Security from the main menu.

   The Firewall page opens.

2. Click Servers.

   The Servers page opens, displaying a list of services and a host IP address for each allowed service.



Servers

This page enables you to selectively allow incoming network traffic of several known applications and Internet services into your network.

No	Allow	Application Name	Host IP		VPN Only	
1	□	Web Server		This Computer	□	Clear
2	□	FTP Server		This Computer	□	Clear
3	□	Telnet Server		This Computer	□	Clear
4	□	Mail Server (POP3)		This Computer	□	Clear
5	□	Mail Server (SMTP)		This Computer	□	Clear
6	□	PPTP Server		This Computer	□	Clear
7	□	VPN Server (IPSEC)		This Computer	□	Clear
8	□	Microsoft Networking (NBT)		This Computer	□	Clear
9	□	IP Telephony (H.323)		This Computer	□	Clear

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 05:38:57 AM Asia/Calcutta

3. In the Allow column, check the check box of the desired service or application.

   If you are using IP45 Satellite X, check the feature for Satellite X in the VPN Only column.

4. To allow connections made through a VPN only, select the VPN Only check box.

5. In the Host IP text box of the selected service or application, type the IP address of the computer that runs the service (one of your network computers) or click *This Computer* to allow your computer to host the service.
6. Click Apply.

A success message appears, and the selected computer is allowed to run the desired service or application.

Table 29 Server Fields

Field	Description
Allow	Select the desired service or application.
VPN Only	Select this option to allow only connections made through a VPN.
Host IP	Type the IP address of the computer that will run the service (one of your network computers) or click the corresponding This Computer button to allow your computer to host the service.

To restrict access from external network

1. Click Security on the main menu, and choose Servers.

   The Virtual Servers page opens, displaying a list of services and a host IP address for each allowed service.
2. In the desired service or application row, click Clear.

   The Host IP text box of the desired service is cleared.
3. Click Apply.

   The service or application for the specific host is not allowed.

Customizing the Nokia IP45 Security Platform Security Policy

The following sections describe how to customize your security policy.

Creating Firewall Rules

The Nokia IP45 Security Platform checks the protocol used, the ports range, and destination IP address when deciding whether to allow or block traffic.

By default, in the medium security level, the IP45 blocks all connection attempts from the Internet (WAN) to the LAN, and allows all outgoing connection attempts from the LAN to the Internet (WAN).

Note
User defined rules have priority over default rules.

The IP45 device processes user defined rules in the order they appear in the rules table, such that rule 1 is applied before rule 2 and so on.

Allow and Block Rules

The allow and block rules provide you with greater flexibility in defining and customizing your security policy. You can allow additional inbound services that are not on the virtual servers list, or block outbound communications for specific port ranges and protocols.

To permit incoming access from the Internet to your internal network for specific port ranges and protocols, you must create a new allow rule. To block outgoing access from your internal network to the Internet for specific port ranges and protocols, create a new block rule.

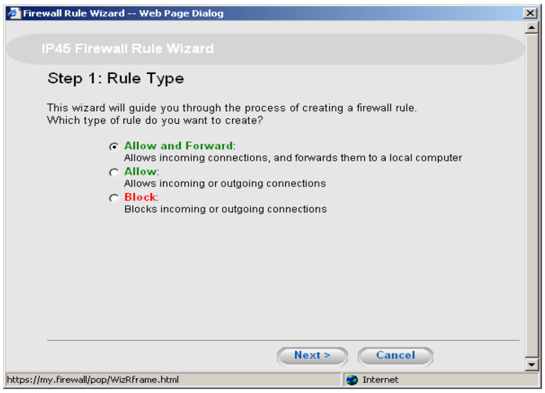
Note
You can specify the IP address range for the source and destination fields in Allow and Block rule.

To create a new rule

1. Choose Security from the main menu.

   The Firewall page opens.

2. Click the Rules tab.
3. The Rules page opens.
4. Click Add Rule on the Rules page to select the type of rule, to add.
5. Select the type of rule, and click Next.



Firewall Rule Wizard -- Web Page Dialog

IP45 Firewall Rule Wizard

Step 1: Rule Type

This wizard will guide you through the process of creating a firewall rule.
Which type of rule do you want to create?

● Allow and Forward:
Allows incoming connections, and forwards them to a local computer

○ Allow:
Allows incoming or outgoing connections

○ Block:
Blocks incoming or outgoing connections

Firewall Rules

This section provides information about the firewall rules that you create.

Note
In IP45 Tele 8, the Allow Rules page does not contain a *VPN Only* column, and the Block Rules page does not contain an *Also VPN* column.

Allow and Forward Rule

These rules enable you to:

- Permit incoming access from the Internet to a specific service in your internal network.
- Forward all such connections to a specific computer in your network.
- Redirect the specified connections to a specific port. This option is called Port Address Translation (PAT).
- Assign traffic to a QoS class.

If traffic shaper is enabled for incoming traffic, then traffic shaper handles relevant connections as specified in the bandwidth policy for the selected QoS class.

For example, if traffic shaper is enabled for incoming traffic, and you create an allow and forward rule associating all incoming Web traffic with the Urgent QoS class, then traffic shaper handles incoming Web traffic as specified in the bandwidth policy for the Urgent class. For information on Traffic Shaper and QoS classes, see “Using Traffic Shaper” on page 127.

This option is only available in IP45 Satellite licenses only. Creating an Allow and Forward rule is equivalent to defining a server in the Servers page.

Note
You must use an Allow and Forward rule to allow incoming connections if your network uses hide NAT.

Note
You cannot specify two allow and forward rules that forward the same service to two different destinations.

Creating an Allow and Forward rule is equivalent to defining a server in the servers page.

Note
You can specify the IP address range for the source only.

Allow Rule

This rule enables you to:

- Permit outgoing access from your internal network to a specific service on the Internet.
- Permit incoming access from the Internet to a specific service in your internal network.
- You can specify the IP address range for source and destination fields.
- Assign traffic to a QoS class.

  If traffic shaper is enabled for the direction of traffic specified in the rule (incoming or outgoing), then traffic shaper handles relevant connections as specified in the bandwidth policy for the selected QoS class.

  For example, if traffic shaper is enabled for outgoing traffic, and you create an allow rule associating all outgoing Web traffic with the Urgent QoS class, then traffic shaper handles outgoing Web traffic as specified in the bandwidth policy for the Urgent class.

  For information on Traffic Shaper and QoS classes, see "Using Traffic Shaper" on page 127.

  This feature is available in Satellite licenses only.

Note
You cannot use an Allow rule to permit incoming traffic, if the network or VPN uses Hide NAT. However, you can use Allow rules for static NAT IP addresses.

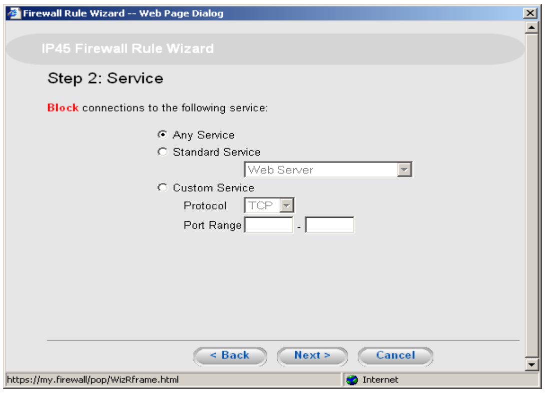
You can allow outgoing connections for services that are not permitted by the default security policy.

You cannot use an allow rule to permit incoming traffic if the network or VPN uses hide NAT. You can use allow rules for static NAT IP addresses.

Block Rule

This rule enables you to:

- Block outgoing access from your internal network to a specific service on the Internet.
- Block incoming access from the Internet to a specific service in your internal network.
- You can specify the IP address range for source and destination fields.



Firewall Rule Wizard -- Web Page Dialog

IP45 Firewall Rule Wizard

Step 2: Service

Block connections to the following service:

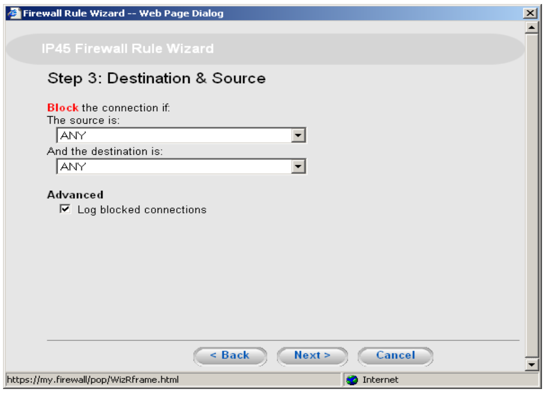
● Any Service
○ Standard Service
Web Server
○ Custom Service
Protocol TCP
Port Range -

https://my.firewall/pop/WizRframe.html

6. Complete the fields using the information in Table 30 on page 155.

7. Click Next.

   The Destination & Source window opens.



Firewall Rule Wizard -- Web Page Dialog

IP45 Firewall Rule Wizard

Step 3: Destination & Source

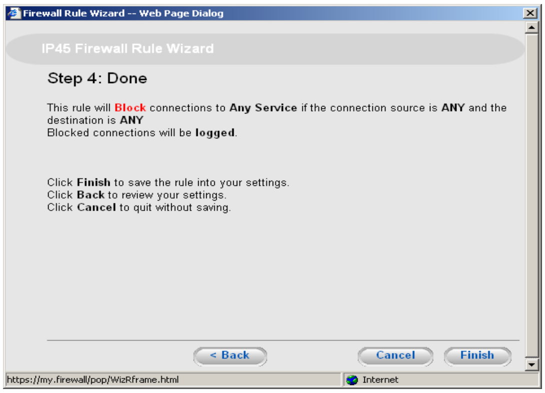
Block the connection if:
The source is:
ANY
And the destination is:
ANY

Advanced
☑ Log blocked connections

8. Complete the fields using information provided in Table 30.

   The Done window opens.

   Table 30 on page 155 gives more information about the firewall rule fields.



Firewall Rule Wizard -- Web Page Dialog

IP45 Firewall Rule Wizard

Step 4: Done

This rule will **Block** connections to **Any Service** if the connection source is **ANY** and the destination is **ANY**
Blocked connections will be **logged**.

Click **Finish** to save the rule into your settings.
Click **Back** to review your settings.
Click **Cancel** to quit without saving.

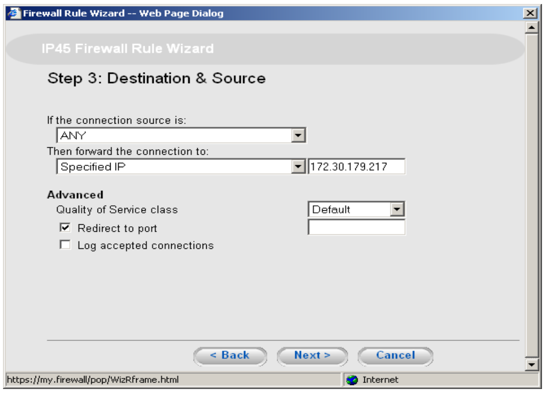
9. Click Finish.

   The new rule appears in the Firewall Rules page.

10. If you selected rule type as Allow and Forward, to redirect the connections to a specific port, select Standard Service or Custom Service from Service window. See step 4.

11. Enter the values as per the information provided in Table 30.

The following window opens:



Firewall Rule Wizard -- Web Page Dialog

IP45 Firewall Rule Wizard

Step 3: Destination & Source

If the connection source is: ANY

Then forward the connection to: Specified IP 172.30.179.217

Advanced

Quality of Service class: Default

☑ Redirect to port

□ Log accepted connections

12. Type the values in connection source and forward to text boxes.
13. Check the Redirect to port check box.
14. Type the value of the port to redirect.
15. Click Next.

    The Done window opens.

16. Click Finish.

    The new firewall rule is configured.

Table 30 Firewall Rule Fields

Field	Action
Any Service	Specifies that the rule should apply to any service.
Standard Service	Specifies that the rule should apply to a specific standard service. You must then select the desired service from the drop-down list.
Custom Service	Specifies that the rule should apply to a specific nonstandard service. The Protocol and Port Range fields are enabled. You must fill them in.
Protocol	Select the protocol (ESP, GRE, TCP, UDP or ANY) for which the rule should apply.
Ports	To specify the port range to which the rule applies, type the start port number in the left text box, and the end port number in the right text box. **Note** If you do not enter a port range, the rule applies to all ports. If you enter only one port number, the range includes only that port.

Table 30 Firewall Rule Fields (*continued*)

Field	Action
Source	Select the source of the connections to allow or block. To specify an IP address, select Specified IP and type the desired IP address in the text box. To specify a range of IP addresses, select Specified Range.
Destination	Select the destination of the connections to allow or block. To specify an IP address, select Specified IP and type the desired IP address in the text box. To specify a range of IP addresses, select Specified Range. **Note** You cannot specify destination range for allow and forward rule.
Quality of Service Class	Select the QoS class to assign specified connections. If Traffic Shaper is enabled, Traffic Shaper handles these connections as specified in the bandwidth policy for the selected QoS class. If Traffic Shaper is not enabled, this setting is ignored. For information on Traffic Shaper and QoS classes, see "Using Traffic Shaper" on page 127 **Note** This drop-down list appears only when you define an Allow rule or an Allow and Forward rule.
Redirect to port	Select this option to redirect the connections to a specific port. Type the port number in the field provided. This option is called Port Address Translation (PAT), and is only available for Allow and Forward rule. Value: 1-65535
Log accepted connections	Select this option to view the log for allowed connections. By default, accepted connections are not logged, and blocked connections are logged.

Deleting and Editing Firewall Rules

This section provides information about how to edit and delete existing firewall rules.

To delete or edit an existing rule

1. Choose Security from the main menu.

   The Firewall page opens.

2. Click the Rules tab and click the Erase icon next to the rule, to delete.

   A confirmation message appears.

3. Click OK.

   The rule is deleted.

4. To Edit an existing rule, click Edit next to the rule

   The Firewall Wizard opens.

5. Proceed as per the wizard to add new values. For more information on adding values, see "Creating Firewall Rules" on page 150.

Viewing the Rules Log for Accepted Connections

You can now view the log for firewall accepted traffic in your IP45 v4.0 security platform. In earlier releases, you could only view blocked traffic information based on your firewall rules. To view this, follow the procedure below:

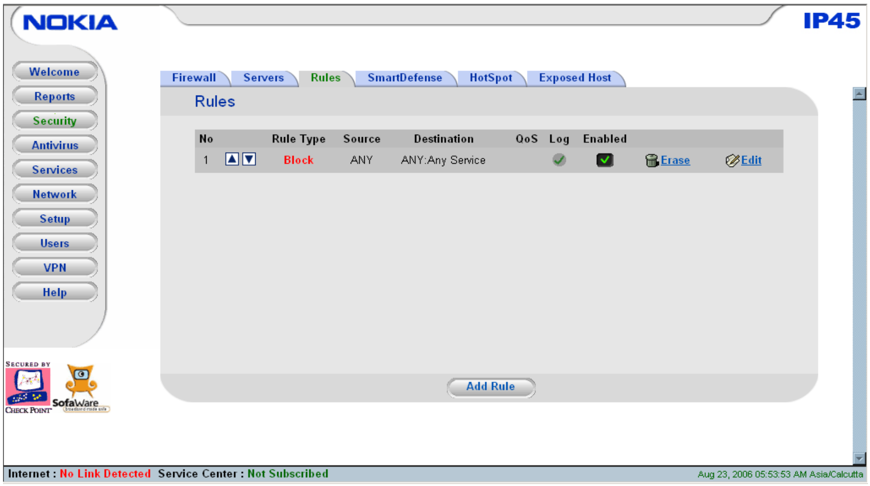
To view the firewall rules log

1. Choose Security from the main menu.

   The Firewall page opens.

2. Click Rules tab.

The Rules page opens with the list of rules added.



Rules

No		Rule Type	Source	Destination	QoS	Log	Enabled		
1	▲▼	Block	ANY	ANY:Any Service		✓	☑	Erase	Edit

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 05:53:53 AM Asia/Calcutta

3. Click the Enabled option, next to log, to view the log of accepted traffic.
4. To disable the log view, click the Enabled tag to turn to a + sign.

Defining an Exposed Host

The Nokia IP45 Security Platform allows you to define an exposed host, which is a computer that is not protected by the firewall. This allows unlimited incoming and outgoing connections between the Internet and the exposed host computer.

This process is useful for setting up a public server.

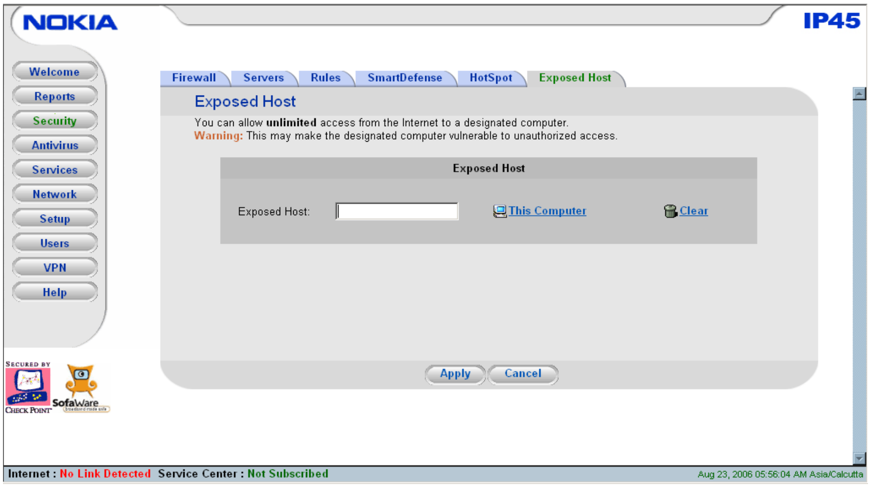
⚠ **Caution**
Entering an IP address can make the designated computer vulnerable to external attacks. Nokia recommends that you not define an exposed host unless you are fully aware of the security risks.

To define a computer as an exposed host

The exposed host receives all traffic that is not forwarded to another computer by using Allow and Forward rules.

1. Choose Security from the main menu, and click the Exposed Host tab.

   The Exposed Host page opens.



Exposed Host

You can allow **unlimited** access from the Internet to a designated computer.
Warning: This may make the designated computer vulnerable to unauthorized access.

Exposed Host

Exposed Host:

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 05:56:04 AM Asia/Calcutta

2. In the Exposed Host text box, type the IP address of the computer to define as an exposed host. Alternatively, you can click This Computer to define your computer as the exposed host.
3. Click Apply.

   The selected computer is now defined as an exposed host.

Editing or Deleting an Exposed Host

This section describes how to edit or delete a define exposed host.

To edit or delete an exposed host

1. Choose Security > Exposed Host.
2. To edit a defined host, click Clear.

   The defined value is deleted.
3. Enter the new value in the Exposed Host field.
4. Click Apply.
5. To delete an exposed host, click Clear.

SmartDefense

The Nokia IP45 Security Platform v4.0 supports the CheckPoint SmartDefense services, which helps the administrators to deal with application-level attacks. SmartDefense uses application intelligence.

Application intelligence provides a combination of attack safeguards and attack blocking tools by:

- Validating the compliance to standards
- Validating expected usage of protocols
- Limiting application ability to carry malicious data
- Controlling application-layer operations

SmartDefense aids proper usage of Internet resources such as FTP, instant messaging, peer-to-peer(P2P) file sharing, FTP uploading.

The SmartDefense page is organized in a tree view, you can configure the nodes by expanding the categories.

IP45 v4.0 supports the SmartDefense Wizard, a simplified method for locally configuring the SmartDefense and Applications Intelligence security policy. The wizard resets all SmartDefense settings to their defaults, and then creates a SmartDefense security policy according to your network and security preferences.

SmartDefense Wizard

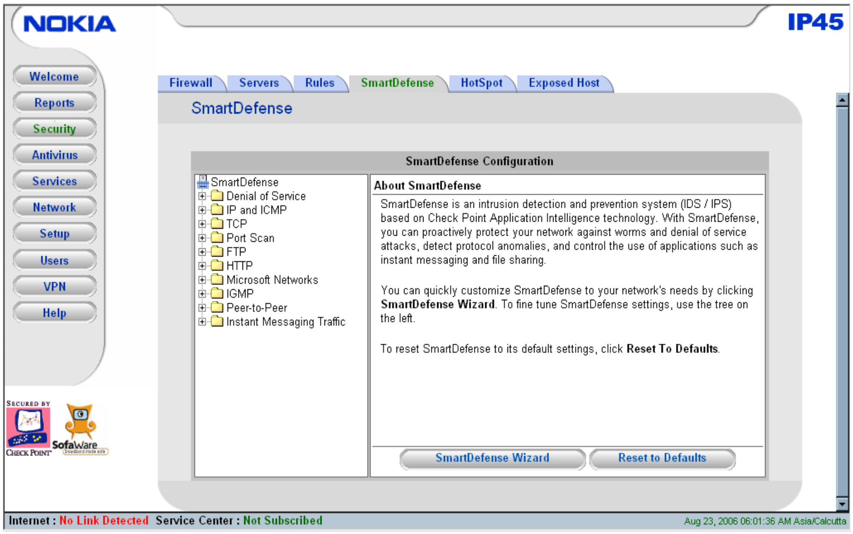
The SmartDefense Wizard allows you to configure your SmartDefense security policy quickly and easily through a user-friendly interface.

After using the wizard, you can fine tune the policy settings by configuring the SmartDefense options in the left pane of the tree. For more information, see “Configuring SmartDefense” on page 163.

To set SmartDefense

1. From the main menu, choose Security > SmartDefense.

   The SmartDefense page is displayed.



SmartDefense

SmartDefense Configuration

About SmartDefense

SmartDefense is an intrusion detection and prevention system (IDS / IPS) based on Check Point Application Intelligence technology. With SmartDefense, you can proactively protect your network against worms and denial of service attacks, detect protocol anomalies, and control the use of applications such as instant messaging and file sharing.

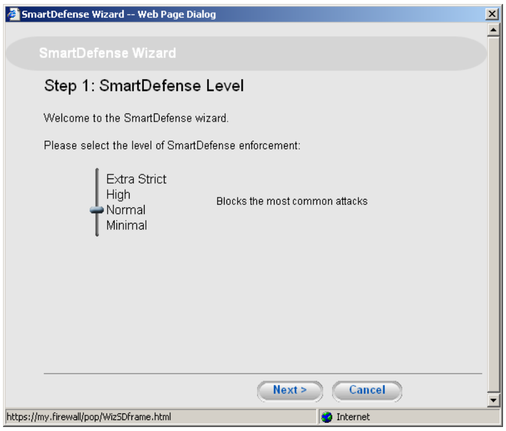
You can quickly customize SmartDefense to your network's needs by clicking **SmartDefense Wizard**. To fine tune SmartDefense settings, use the tree on the left.

To reset SmartDefense to its default settings, click **Reset To Defaults**.

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 06:01:36 AM Asia/Calcutta

2. Click SmartDefense Wizard.

   The SmartDefense wizard appears.



Step 1: SmartDefense Level

Welcome to the SmartDefense wizard.

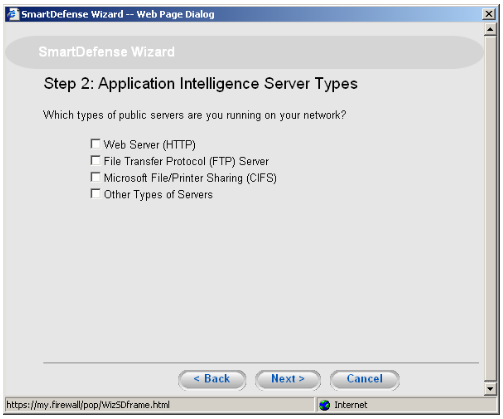
Please select the level of SmartDefense enforcement:

Normal — Blocks the most common attacks

https://my.firewall/pop/WizSDframe.html

3. Select the level of SmartDefense. Options are extra strict, high, normal and minimal.
4. Click Next.

   Application Intelligence Server Types window opens.



SmartDefense Wizard -- Web Page Dialog

SmartDefense Wizard

Step 2: Application Intelligence Server Types

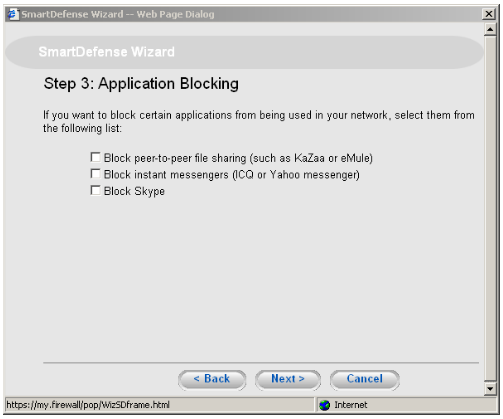
Which types of public servers are you running on your network?

□ Web Server (HTTP)
□ File Transfer Protocol (FTP) Server
□ Microsoft File/Printer Sharing (CIFS)
□ Other Types of Servers

5. Select the type of public servers you run/use on the network. Options are HTTP, FTP, CIFS and other type of servers.

6. Click Next.

   The Application Blocking window opens.



SmartDefense Wizard -- Web Page Dialog

SmartDefense Wizard

Step 3: Application Blocking

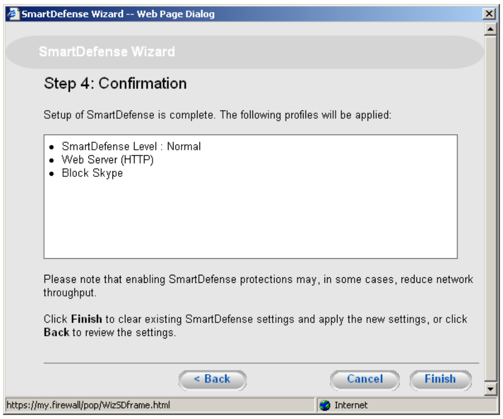
If you want to block certain applications from being used in your network, select them from the following list:

□ Block peer-to-peer file sharing (such as KaZaa or eMule)
□ Block instant messengers (ICQ or Yahoo messenger)
□ Block Skype

7. Select the type of applications that should be blocked in your network: peer-to-peer file sharing, instant messengers and skype.

8. Click Next.

   The Confirmation window opens.



Step 4: Confirmation

Setup of SmartDefense is complete. The following profiles will be applied:

- SmartDefense Level : Normal
- Web Server (HTTP)
- Block Skype

Please note that enabling SmartDefense protections may, in some cases, reduce network throughput.

Click **Finish** to clear existing SmartDefense settings and apply the new settings, or click **Back** to review the settings.

9. SmartDefense rules are set and you can view a list of profiles that you selected.

10. Click Finish to clear the existing settings and to apply the new settings.

Restoring Default Settings

You can also restore the default settings of SmartDefense.

To restore default settings

1. From the main menu, choose Security > SmartDefense.

The SmartDefense page is displayed.

2. Click Reset to Defaults.

The default settings are restored.

Configuring SmartDefense

You can handle the following by using SmartDefense.

- Denial of Service
- IP and ICMP
- TCP
- Port Scan
- FTP
- HTTP
- Microsoft Networks
- IGMP
- Peer to Peer
- Instant Messaging Traffic

Denial of Service

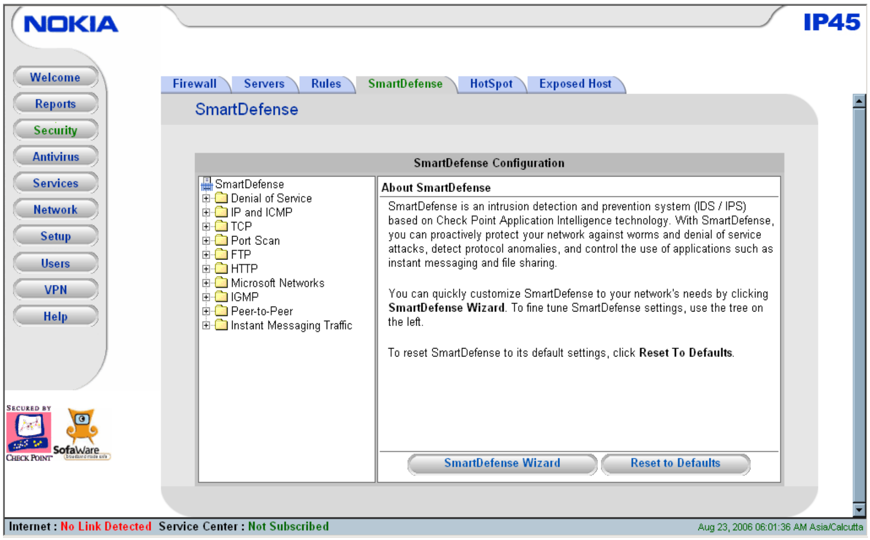
Denial of Service includes the following attacks:

- **TearDrop**—the attacker sends two IP fragments, the latter entirely contained within the former. This causes some computers to allocate too much memory and crash.
- **Ping of Death**—in a Ping of Death Attack, the attacker sends a fragmented PING request that exceeds the maximum IP packet size (64 KB). Some operating systems are unable to handle such requests and crash.
- **LAND**— the attacker sends a SYN packet, in which the source address and port are the same as the destination (the victim computer). The victim computer then tries to reply to itself and either reboots or crashes.
- **Non-TCP Flooding**—advanced Firewalls maintain state information about connections in a State table. In non-TCP Flooding attacks, the attacker sends high volumes of non-TCP traffic. Since such traffic is connectionless, the related state information cannot be cleared or reset, and the firewall State table is quickly filled up. This prevents the firewall from accepting new connections and results in a Denial of Service (DoS).
- **DDoS Attack**—in a distributed denial-of-service attack (DDoS attack), the attacker directs multiple hosts in a coordinated attack on a victim computer or network. The attacking hosts send large amounts of spurious data to the victim, so that the victim is no longer able to respond to legitimate service requests.

To handle teardrop attack

1. From the main menu, choose Security > SmartDefense.

   SmartDefense page is displayed.



SmartDefense is an intrusion detection and prevention system (IDS / IPS) based on Check Point Application Intelligence technology. With SmartDefense, you can proactively protect your network against worms and denial of service attacks, detect protocol anomalies, and control the use of applications such as instant messaging and file sharing.

You can quickly customize SmartDefense to your network's needs by clicking **SmartDefense Wizard**. To fine tune SmartDefense settings, use the tree on the left.

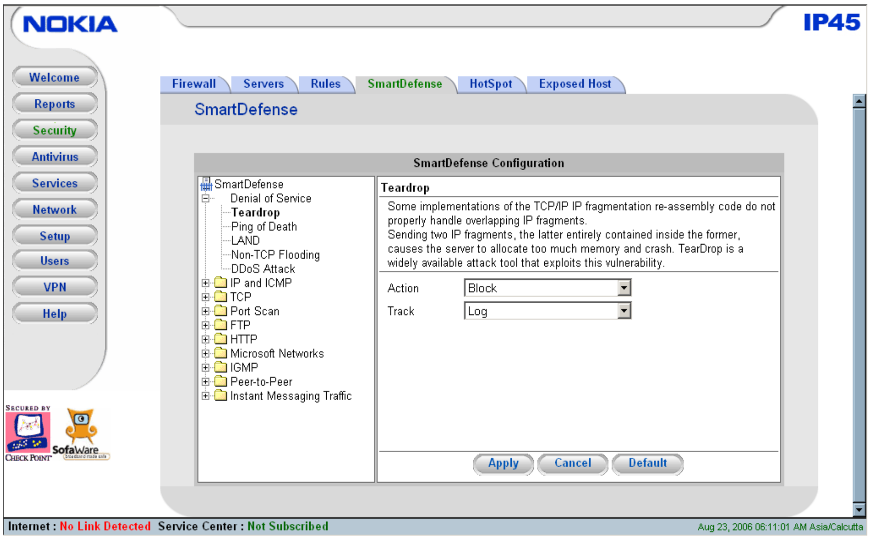
To reset SmartDefense to its default settings, click **Reset To Defaults**.

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 06:01:36 AM Asia/Calcutta

SmartDefense GUI is organized as a tree structure in which each branch represents a category of setting.

2. Select Denial of Service to expand the tree view.
3. Select Teardrop.

   The teardrop configuration information appears in the SmartDefense configuration pane.



Teardrop

Some implementations of the TCP/IP IP fragmentation re-assembly code do not properly handle overlapping IP fragments.
Sending two IP fragments, the latter entirely contained inside the former, causes the server to allocate too much memory and crash. TearDrop is a widely available attack tool that exploits this vulnerability.

Action: Block

Track: Log

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 06:11:01 AM Asia/Calcutta

4. Select the field values by using the information provided in Table 31.
5. Click Apply.

   The settings are saved.
6. To store the default setting, click Default.

   A confirmation message appears.

   Click OK.

Table 31 Denial Of Service - fields for Teardrop, Ping of Death, LAND and DDoS

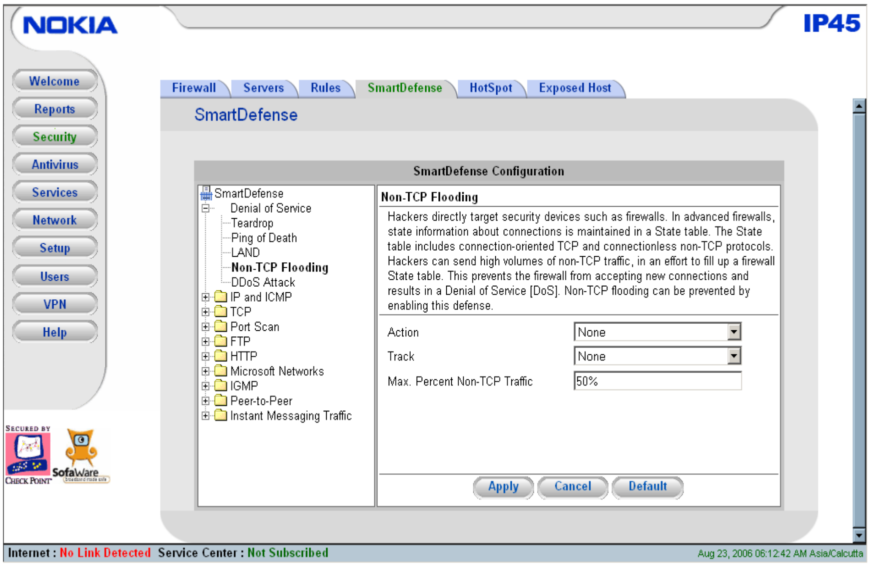
Field	Action
Action	Choose the action to be taken against the Denial of Service attacks. Options: • Block: blocks the attack • None: no action is required Default value: Block
Track	Specify whether to log the attacks. Options: • Log: logs the attack • None: does not log the attack Default value: Log

Note
For handling the Denial of Service attacks like Ping of Death, LAND and DDoS attacks, follow the procedure “To handle teardrop attack” on page 164.

To protect against non TCP Floodings

1. Select Non TCP Floodings from the Denial of Service tree view.

   The Non TCP Flooding configuration information appears.



Non-TCP Flooding

Hackers directly target security devices such as firewalls. In advanced firewalls, state information about connections is maintained in a State table. The State table includes connection-oriented TCP and connectionless non-TCP protocols. Hackers can send high volumes of non-TCP traffic, in an effort to fill up a firewall State table. This prevents the firewall from accepting new connections and results in a Denial of Service [DoS]. Non-TCP flooding can be prevented by enabling this defense.

Action: None
Track: None
Max. Percent Non-TCP Traffic: 50%

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 06:12:42 AM Asia/Calcutta

2. Select the field values by using Table 32.

Table 32 Fields for Non TCP Flooding

Field	Action
Action	Choose the action to be taken when the percentage of state table capacity used for non-TCP connections reaches the maximum percent non TCP traffic threshold. Options: • Block: blocks any additional non-TCP connections • None: no action is required Default value: None
Track	Specify whether to log the non-TCP connections that exceed the maximum percent non TCP traffic threshold. Options: • Log: logs the connections • None: does not log the connections Default value: None
Max. Percent Non-TCP Traffic	Type the maximum percentage of state table capacity allowed for non TCP connections. Default value: 0%.

3. Click Apply.

IP and ICMP

This option allows you to enable various IP and ICMP protocol tests and configure various protection against IP and ICMP related attacks. It includes:

- **Packet Sanity**— performs several Layer 3 and Layer 4 sanity checks. These include verifying packet size, UDP and TCP header lengths, dropping IP options, and verifying the TCP flags.

Note
To select values for Packet Sanity, expand the IP and ICMP tree, click Packet Sanity and select the values from the drop-down list by using the information provided in Table 33.

Table 33 Fields for Packet Sanity

Field	Action
Action	Choose the action to be taken when a packet fails a sanity test. Options: • Block: blocks the failed packets • None: no action is required Default value: Block
Track	Specify whether to issue logs for packets that fail the sanity tests. Options: • Log: logs the failed packets • None: does not log the failed packets Default value: Log
Disable relaxed UDP length verification	The UDP length verification sanity check compares the UDP header length of the packet with the UDP length mentioned in the UDP header field of the packet. The packet is supposed to be corrupted if the values are not equal. IP45v4.0 does not discard the offending packets though the sanity check is performed. Options: • True: disable relaxed UDP length verification. The packets that fail the UDP length verification check are not discarded. • False: does not disable relaxed UDP length verification. The packets that fail the UDP length verification check are discarded. Default value: False

- **Max Ping Size**— uses ICMP protocol to check whether a remote machine is active. A request is sent by the client, and the server responds with a reply echoing the client's data. An attacker can echo the client with a large amount of data, causing a buffer overflow. You can protect against such attacks by limiting the allowed size for ICMP echo requests.

Note
To select values for Max. Ping Size, expand the IP and ICMP tree, click Max Ping Size and select the values from the drop-down list by using the information provided in Table 34.

Table 34 Fields for Max. Ping Size

Field	Action
Action	Choose the action to be taken when an ICMP echo response exceeds the Max Ping Size threshold. Options: • Block: blocks the request • None: no action is required Default value: Block
Track	Specify whether to log ICMP echo responses that exceed the Max Ping Size threshold. Options: • Log: logs the responses • None: does not log the responses Default value: Log
Max Ping Size	Specify the maximum data size for ICMP echo response. Default value: 1500

- **IP Fragments**—when an IP packet is too big to be transported by a network link, it is split into several smaller IP packets and transmitted in fragments. To conceal a known attack or exploit, an attacker might imitate this common behaviour and break the data section of a single packet into several fragmented packets. Without reassembling the fragments, it is not always possible to detect such an attack. Therefore the IP45v4.0 always reassembles all the fragments of a given IP packet before inspecting it to make sure there are no attacks or exploits in the packet.

Note
To select values for IP Fragments, expand the IP and ICMP tree, click IP Fragments and select the values from the drop-down list by using the information provided in Table 35.

Table 35 Fields for IP Fragments

Field	Action
Forbid IP Fragments	Specify whether all fragmented packets should be dropped. Options: • True: drops all fragmented packets. • False: no action is required. Default value: False In general, it is recommended to leave the field set to False. Setting this field to True may disrupt Internet connectivity because it does not allow any fragmented packets.
Max Number of Incomplete Packets	Type the maximum number of fragmented packets allowed. Packets exceeding this threshold will be dropped. Default value: 300
Timeout for Discarding Incomplete Packets	When the IP45 receives packet fragments, it waits for additional fragments to arrive so that it can reassemble the packet. Type the number of seconds to wait before discarding incomplete packets. Default value: 10 seconds
Track	Specify whether to log the fragmented packets. Options: • Log: logs all the fragmented packets. • None: does not log the fragmented packets Default value: None

- **Network Quota**—an attacker may try to overload a server in your network by establishing a very large number of connections per second. To protect against Denial of Service (DoS) attacks, Network Quota enforces a limit upon the number of connections per second that are allowed from the same source IP address.

Note
To select values for Network Quota, expand the IP and ICMP tree, click Network Quota and select the values from the drop-down list by using the information provided in Table 36.

Table 36 Fields for Network Quota

Field	Action
Action	Choose the action to be taken when the number of network connections from the same source reaches the Max. Connections/ Second per Source IP threshold. Options: • Block: blocks all new connections from the source. Existing connections will not be blocked • None: no action is required Default value: Block
Track	Specify whether to log the connections from a specific source that exceed the Max. Connections/Second per Source IP threshold. Options: • Log: logs the connections • None: does not log the connections Default value: Log
Max. Connections/ Second from Same Source IP	Type the maximum number of network connections allowed per second from source IP address. Default value: 100 Set a lower threshold for stronger protection against DoS attacks. **Note** Setting this value too low can lead to false alarms.

- **Welchia**—the Welchia worm uses the MS DCOM vulnerability or a WebDAV vulnerability. After infecting a computer, the worm begins searching for other live computers to infect. It does so by sending a specific ping packet to a target and waiting for the reply that signals that the target is alive. This flood of pings may disrupt network connectivity.

Note
To select values for Welchia, expand the IP and ICMP tree, click Welchia and select the values from the drop-down list by using the information provided in Table 37.

Table 37 Fields for Welchia

Field	Action
Action	Choose the action to be taken when a Welchia worm is detected. Options: • Block: blocks the attack • None: no action is required Default value: Block
Track	Specify whether to log Welchia worm attacks. Options: • Log: logs the attack • None: does not log the attack Default value: Log

- **Cisco IOS DOS**—Cisco routers are configured to process and accept Internet Protocol version 4 (IPv4) packets by default. When a Cisco IOS device is sent, a specially crafted sequence of IPv4 packets (with protocol 53 - SWIPE, 55 - IP Mobility, 77- Sun ND, or 103-Protocol Independent Multicast - PIM), the router will stop processing inbound traffic on that interface.

Note
To select values for Cisco IOS DOS, expand the IP and ICMP tree, click Cisco IOS DOS and select the values from the drop-down list by using the information provided in Table 38.

Table 38 Fields for Cisco IOS DOS

Field	Action
Action	Choose the action to be taken against a Cisco IOS DOS attack. Options: • Block: blocks the attack • None: no action is required Default value: Block
Track	Specify whether to log the Cisco IOS DOS attacks. Options: • Log: logs the attack • None: does not log the attack Default value: Log

Table 38 Fields for Cisco IOS DOS (*continued*)

Field	Action
Number of Hops to Protect	Type the number of hops from the enforcement module that Cisco routers should be protected. Default value: 10
Action Protection for SWIPE - Protocol 53/ Action Protection for IP Mobility - Protocol 55/ Action Protection for SUN-ND - Protocol 77/ Action Protection for PIM - Protocol 103	Choose the action to be taken when an IPv4 packet of the specific protocol type is received. Options: • Block: drops the packet • None: no action is required Default value: Block

- **Null Payload**—some worms, such as Sasser, use ICMP echo request packets with null payload to detect potentially vulnerable hosts.

Note
To select values for Null Payload, expand the IP and ICMP tree, click Null Payload and select the values from the drop-down list by using the information provided in Table 39.

Table 39 Fields for Null Payload

Field	Action
Action	Choose the action to be taken when null payload ping packets are detected. Options: • Block: blocks the packets • None: no action is required Default value: Block
Track	Specify whether to log the null payload ping packets. Options: • Log: logs the packets • None: does not log the packets Default value: Log

TCP

This option allows you to configure various protections related to the TCP protocol.

It includes the following:

- **Strict TCP**—out-of-state TCP packets are SYN-ACK or data packets that arrive out of order, before the TCP SYN packet.

Note
To select values for Strict TCP, expand the TCP tree, click Strict TCP and select the values from the drop-down list by using the information provided in Table 40.

Table 40 Fields for Strict TCP

Field	Action
Action	Choose the action to be taken when an out-of-state TCP packet arrives. Options: • Block: blocks the packets • None: no action is required Default value: None
Track	Specify whether to log the out-of-state TCP packets. Options: • Log: logs the packets • None: does not log the packets Default value: Log

- **Small PMTU**—Small PMTU (Packet MTU) is a bandwidth attack in which the client fools the server into sending large amounts of data using small packets. Each packet has a large overhead that creates a bottleneck on the server. You can protect from this attack by specifying a minimum packet size for data sent over the Internet.

Note
To select values for Small PMTU, expand the TCP tree, click Small PMTU and select the values from the drop-down list by using the information provided in Table 41.

Table 41 TCP - fields for Small PMTU

Field	Action
Action	Choose the action to be taken when a packet is smaller than the Minimal MTU Size threshold. Options: • Block: blocks the packet • None: no action is required Default value: None
Track	Specify whether to issue logs for packets that are smaller than the Minimal MTU Size threshold. Options: • Log: issues logs • None: does not issue logs Default value: Log
Minimal MTU Size	Type the minimum value allowed for the MTU field in IP packets sent by a client. An overtly small value will not prevent an attack, while an overtly large value might degrade performance and cause legitimate requests to be dropped. Default value: 300

- **SynDefender**—protects against SYN Flooding denial of service attacks. IP45 v4.0 enables fine tuning SynDefender to avoid false alarms.

Note
To select values for SynDefender, expand the TCP tree, click SynDefender and select the values from the drop-down list by using the information provided in Table 42.

Table 42 TCP - fields for SynDefender

Field	Action
Action	Choose the action to be taken when a packet is smaller than the Minimal MTU Size threshold. Options: • Block: blocks the packet • None: no action is required Default value: None
Track	Specify whether to issue logs for packets that are smaller than the Minimal MTU Size threshold. Options: • Log: issues logs • None: does not issue logs Default value: Log
Log Mode	When more than 5 incomplete TCP handshakes are detected within 10 seconds, an attack is made. We can set the mode whether to log per attack or for each unfinished handshake. Options: • Log per attack: logs every attack • Log each unfinished handshakes: logs each unfinished handshake • None:does not log
Maximum Time for Completing the Handshake	Allows to fine tune the amount of time (in seconds) after which a TCP handshake is considered incomplete.
Protect external interfaces only	Specifies whether SynDefender should be enabled for all the firewall interfaces, or for external (WAN) interfaces only.

You can set the SynDefender by using the command-line interface. For more information about SynDefender commands, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

Port Scan

An attacker can perform a port scan to determine whether ports are open and vulnerable to an attack. This is most commonly done by attempting to access a port and waiting for a response. The response indicates whether or not the port is open.

This option includes the following types of port scans:

- **Host Port Scan**—the attacker scans ports of specific host to determine which of the ports are open.
- **Sweep Scan**—the attacker scans various hosts to determine where a specific port is open.

The following table depicts the fields of Port Scan.

Table 43 Fields for Port Scan

Field	Action
Number of ports accessed	SmartDefense detects ports scans by measuring the number of ports accessed over a period of time. The number of ports accessed must exceed the Number of ports accessed value, within the number of seconds specified by the In a period of [seconds] value, in order for SmartDefense to consider the activity a scan. Type the minimum number of ports that must be accessed within the In a period of [seconds] value, in order for SmartDefense to consider the activity a scan. For example, if this value is 30, and 40 ports are accessed within a specified period of time. SmartDefense will detect the activity as a port scan. For Host Port Scan, the default value is 30. For Sweep Scan, the default value is 50.
In a period of [seconds]	SmartDefense detects ports scans by measuring the number of ports accessed over a period of time. The number of ports accessed must exceed the Number of ports accessed value, within the number of seconds specified by the In a period of [seconds] value, in order for SmartDefense to consider the activity a scan. Type the maximum number of seconds that can elapse, during which the Number of ports accessed threshold is exceeded, in order for SmartDefense to detect the activity as a port scan. For example, if this value is 20, and the Number of ports accessed threshold is exceeded for 15 seconds, SmartDefense will detect the activity as a port scan. If the threshold is exceeded for 30 seconds, SmartDefense will not detect the activity as a port scan. Default value: 20 seconds

Table 43 Fields for Port Scan

Field	Action
Track	Specify whether to issue logs for scans. • Log: issues logs • None: does not issue logs Default value: Log
Detect scans from Internet only	Specify whether to detect scans originating only from Internet. • True: detects only scans from the Internet • False: does not detect only scans from the Internet

FTP

This option allows you to configure various protections related to the FTP protocol.

It includes the following protections:

- **FTP Bounce**—when connecting to an FTP server, the client sends a PORT command specifying the IP address and port to which the FTP server should connect and send data. An FTP Bounce attack is when an attacker sends a PORT command specifying the IP address of a third party instead of attacker's own IP address. The FTP server then sends the data to the victim machine.

Note
To select values for FTP Bounce, expand the FTP, click FTP Bounce and select the values from the drop-down list by using the information provided in Table 44.

Table 44 Fields for FTP Bounce

Field	Action
Action	Choose the action to be taken against the FTP Bounce attacks. Options: • Block: blocks the attack • None: no action is required Default value: Block
Track	Specify whether to log the FTP Bounce attacks. Options: • Log: logs the attack • None: does not log the attack Default value: Log

- **Block Known Ports**—you can choose to block the FTP server from connecting to well-known ports. This provides a second layer of protection against FTP bounce attacks, by preventing such attacks from reaching well-known ports.

Note
To select values for Block Known Ports, expand the FTP, click Block Known Ports and select the values from the drop-down list by using the information provided in Table 45.

Table 45 Fields for Block Known Ports

Field	Action
Action	Choose the action to be taken when the FTP server attempts to connect to a well-known port. Options: • Block: blocks the connection • None: no action is required Default value: None

- **Block Port Overflow**—FTP clients send PORT commands when connecting to the FTP server. A PORT command consists of a series of numbers between 0 and 255, separated by commas. To enforce compliance to the FTP standard and prevent potential attacks against the FTP server, you can block PORT commands that contain a number greater than 255.

Note
To select values for Block Port Overflow, expand the FTP tree, click Block Port Overflow and select the values from the drop-down list by using the information provided in Table 46.

Table 46 Fields for Block Port Overflow

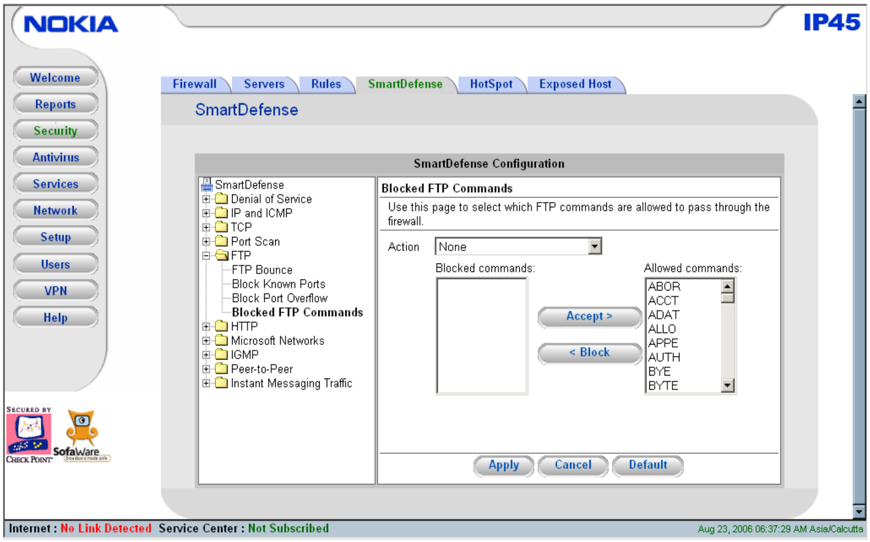
Field	Action
Action	Choose the action to be taken against the PORT commands containing a number greater than 255. Options: • Block: blocks the PORT command • None: no action is required Default value: Block

- **Blocked FTP Commands**—some seldom-used FTP commands may compromise FTP server security and integrity. You can specify which FTP commands should be allowed to pass through the security server, and which should be blocked.

To manage FTP commands

1. Choose Security > SmartDefense > FTP > Blocked FTP Commands.

   The following page opens.



SmartDefense Configuration

Blocked FTP Commands

Use this page to select which FTP commands are allowed to pass through the firewall.

Action: None

Blocked commands:

Allowed commands: ABOR, ACCT, ADAT, ALLO, APPE, AUTH, BYE, BYTE

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 06:37:29 AM Asia/Calcutta

2. From the Action drop-down list, select any one of the following options:

   - **Block**—to enable FTP command blocking

     The FTP commands listed in the Blocked Commands list box will be blocked.

Note
FTP command blocking is enabled by default.

   - **None**—to disable FTP command blocking

     configuring smartdefense: All FTP commands are allowed including those in the Blocked Commands list box.

3. To block particular FTP command, select the command from the Allowed Commands list box and do the following:

   a. Click Block.

   The FTP command appears in the Blocked Commands list box.

   b. Click Apply.

   When FTP command blocking is enabled, the FTP command will be blocked.

4. To allow a specific FTP command, select the command from the Blocked Commands list box and do the following:

   a. Click Accept.

      The FTP command appears in the Allowed Commands list box.

   b. Click Apply.

      The FTP command will be allowed, regardless of whether the FTP command blocking is enabled or disabled.

HTTP

This option provides various protection mechanisms to stop the exploits of HTTP headers and to block the worms that take advantage of the vulnerabilities of the HTTP protocol. It includes:

- **Header Rejection**—some exploits use the HTTP headers to cause damage. The exploit can be carried in standard headers with custom values or in custom headers. This protection allows you to reject HTTP requests that contain specific headers and header values.

Note
To select values for Header Rejection, expand the HTTP tree, click Header Rejection and select the values from the drop-down list by using the information provided in Table 47.

Table 47 Fields for Header Rejection

Field	Description
Action	Choose the action to be taken when particular HTTP requests that contain specific headers and header values are made. Options: • Block: blocks such requests • None: no action is required Default value: None

Table 47 Fields for Header Rejection

Field	Description
Track	Specify whether to issue logs for the malicious HTTP requests. Options: • Log: logs the malicious HTTP requests • None: does not log the malicious HTTP requests Default value: None You can also see a list. 180 Solutions AltNet Peer Point Manager Atwola BearShare Gator Google Desktop Search Grokster Ads QuickTime Plugin QuickTime RealOne Player Shoutcast Target Saver and few more.

- **Worm Catcher**—a worm is a self-replicating malware that propogates by actively sending itself to new machines. Some worms propogate by using security vulnerabilities in the HTTP protocol. This protection allows you to detect and block worms based pre-defined patterns.

Note

To select values for Worm Catcher, expand the HTTP tree, click Worm Catcher and select the values from the drop-down list by using the information provided in Table 48.

Table 48 Fields for Worm Catcher

Field	Description
Action	Choose the action to be taken when worms are detected. Options: • Block: blocks the worms • None: no action required Default value: None
Track	Specify whether to issue logs for the worms that are detected. Options: • Log: logs the detection of worms • None: does not log the detection of worms Default value: None
	You can also see a list of worms. Check or uncheck the worms to be detected. Apache Tomcat Malicious Request Apache Tomcat RealPath Apache Tomcat path disclosure 1 Apache Tomcat path disclosure 2 Apache Tomcat path disclosure 3 Apache Tomcat sample code BizTalk Buffer Overrun CodeRed Frontpage Extensions Buffer Overrun Htr Overflow MDAC Overflow Nimda Sanity.A Worm

Microsoft Networks

This category includes File and Print Sharing.

- **File and Print Sharing**—Microsoft operating systems and Samba clients rely on Common Internet File System (CIFS), a protocol for sharing files and printers. However, this protocol is also widely used by worms as a means of propagation.

The following table depicts the fields of Microsoft Networks.

Table 49 Fields for Microsoft Networks

Field	Action
Action	Choose the action to be taken when the CIFS worm attacks are detected. • Block: blocks the attack • None: no action is required Default value: None
Track	Specify whether to log the CIFS worm attacks. • Log: logs the attack • None: does not log the attack Default value: None
	Select the worm patterns to detect from the CIFS worm patterns lists. Patterns are matched against file names (including file paths but excluding the disk share name) that the client is trying to read or write from the server.

IGMP

This category includes the IGMP protocol.

- **IGMP**—IGMP is used by hosts and routers to dynamically register and discover multicast group membership. Attacks on the IGMP protocol usually target a vulnerability in the multicast routing software/hardware used, by sending specially crafted IGMP packets.

Note
To select values for IGMP, expand the IGMP tree, click IGMP and select the values from the drop-down list by using the information provided in Table 50.

Table 50 Fields for IGMP

Field	Action
Action	Choose the action to be taken against the IGMP attacks. Options: • Block: blocks the attack • None: no action is required Default value: Block
Track	Specify whether to log the IGMP attacks. Options: • Log: logs the attack • None: does not log the attack Default value: Log
Enforce IGMP to multicast addresses	According to the IGMP specification, IGMP packets must be sent to multicast addresses. Sending IGMP packets to a unicast or broadcast address might constitute an attack. So IP45v4.0 blocks such packets. Specify whether to allow or block the IGMP packets that are sent to non-multicast addresses. Options: • Block: blocks the IGMP packets that are sent to non-multicast addresses. • None: no action is required Default value: Block

Peer to Peer

SmartDefense can block peer-to-peer traffic by identifying the proprietary protocols and preventing the initial connection to the peer-to-peer networks. This prevents the search operations too in addition to downloads.

This category includes the following connection types:

- **Kazaa**—a distributed peer-to-peer file sharing service that runs on the port 1214.

Note
To select values for Kazaa, expand the Peer to Peer tree, click Kazaa and select the values from the drop-down list by using the information provided in Table 51.

Table 51 Peer to Peer - fields for Kazaa, Gnutella, eMule and BitTorrent

Field	Action
Action	Specify the action to be taken when a connection is attempted. Options: • Block: blocks the connection • None: no action is required Default value: None
Track	Specify whether to log peer-to-peer connections. Options: • Log: logs the connection • None: does not log the connection Default value: None
Block proprietary protocols on all ports	Specify whether the proprietary protocols should be blocked on all ports. Options: • Block: blocks the proprietary protocol on all ports. This prevents all communication using this peer-to-peer application. • None: does not block the proprietary protocols on all ports. Default value: Block
Block masquerading over HTTP protocol	Specify whether the masquerading over HTTP protocol should be blocked. Options: • Block: blocks the masquerading over HTTP protocol. • None: does not block the masquerading over HTTP protocol.

- **Gnutella**—a protocol designed for sharing files on a distributed network.
- **eMule**—a file sharing client based on the eDonkey2000 protocol.
- **BitTorrent**—a peer-to-peer file distribution tool.

Note
To select values for the Gnutella, eMule and BitTorrent connection types, expand the Peer to Peer tree, click corresponding node and select the values from the drop-down list by using the information provided in Table 51.

Instant Messaging Traffic

SmartDefense can block instant messaging applications that use VoIP protocols by identifying the fingerprints and HTTP headers of messaging application.

This category includes the following instant messengers:

- **Skype**
- **Yahoo**
- **ICQ**

Note
To select values for instant messages, expand the Peer to Peer tree, click appropriate nodes and select the values from the drop-down list by using the information provided in Table 52.

Table 52 Instant Messaging Traffic - fields for Skype, Yahoo and ICQ

Field	Action
Action	Choose the action to be taken when a connection is attempted. Options: • Block: blocks the connection • None: no action is required Default value: None
Track	Specify whether to log the Instant Messenger connections. Options: • Log: logs the connection • None: does not log the connection Default value: None
Block proprietary protocols on all ports	Specify whether the proprietary protocols should be blocked on all ports. Options: • Block: blocks the proprietary protocol on all ports. This prevents all communication using this peer-to-peer applicaton. • None: does not block the proprietary protocols on all ports Default value: Block
Block masquerading over HTTP protocol	Specify whether the masquerading over HTTP protocol should be blocked. Options: • Block: blocks the masquerading over HTTP protocol. • None: does not block the masquerading over HTTP protocol.

For information about SmartDefense command-line interface, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

Secure HotSpot

Nokia IP45 v4.0 supports secure HotSpot Internet access to its networks. Users need to have access information to the HotSpot access, which can be obtained by visiting http://my.hotspot page. On acceptance of terms and conditions, the user is provided with the access information. The user is prompted for authentication (username and password) on every login to these HotSpot networks.

SecuRemote VPN users, who are authenticated by the Internal VPN server are not prompted for the authentication.

My HotSpot provides support for quick guest access, as provided by the administrator. For more information on adding guest HotSpot users, see “Adding Guest HotSpot Users” on page 194.

Enabling Secure HotSpot

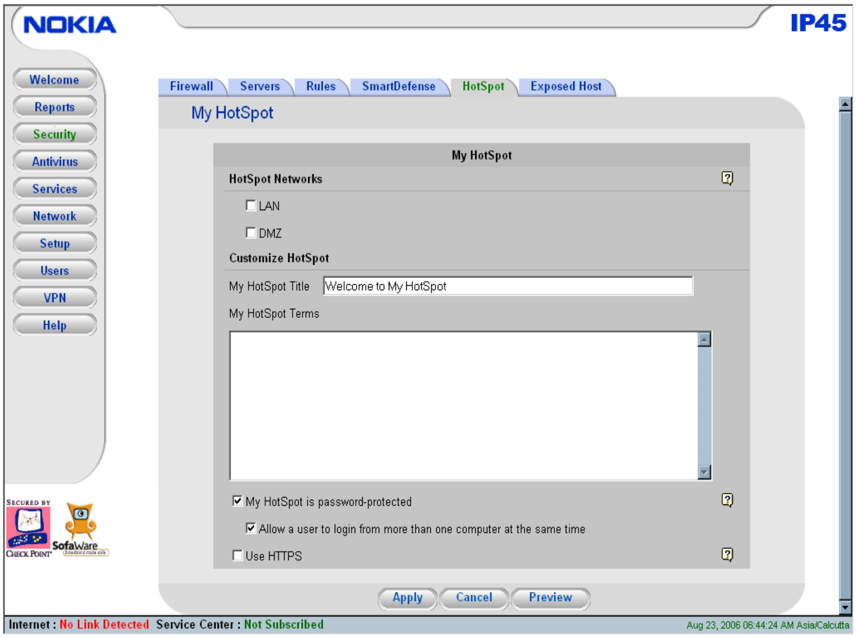
You can enable the secure HotSpot feature by using the GUI and command-line interface.

Use the following procedure to enable Hot Spot feature using the GUI.

To configure secure HotSpot

1. Choose Security from the main menu and select HotSpot.

   My HotSpot page opens.



My HotSpot

My HotSpot

HotSpot Networks

☐ LAN

☐ DMZ

Customize HotSpot

My HotSpot Title: Welcome to My HotSpot

My HotSpot Terms

☑ My HotSpot is password-protected

☑ Allow a user to login from more than one computer at the same time

☐ Use HTTPS

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 06:44:24 AM Asia/Calcutta

2. Select the HotSpot network by checking against the respective check box. You can select multiple networks.
3. Enter the information in the fields by using Table 53.
4. Click Apply.
5. To preview the HotSpot page, click Preview.

Table 53 HotSpot

Field	Action
My HotSpot Title	Type a name that should appear on your HotSpot page Default value: Welcome to My HotSpot
My HotSpot Terms	Type the terms and conditions that the user must agree to, before accessing the HotSpot network. You might use HTML tags as required.
My HotSpot is password protected	Select this option to prompt for user authentication to access the HotSpot network. The Allow a user to login from more than one computer at the same time check box appears. Check this to allow the user to access from multiple computers. If you Does not select this option, any user who accepts the terms as provided in My HotSpot terms will be able to access the HotSpot network.

For information about configuring HotSpot with the CLI, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

9 Configuring Network Access

This chapter describes how to create and manage the Nokia IP45 security platform users. Network access procedures, Secure Shell (SSH) and Secure Socket Layer (SSL) are discussed in this chapter.

The chapter includes the following sections:

Changing your Password

You can change the password of your Nokia IP45 security platform, any time. The method for changing the password varies depending on the IP45 configuration you are using.

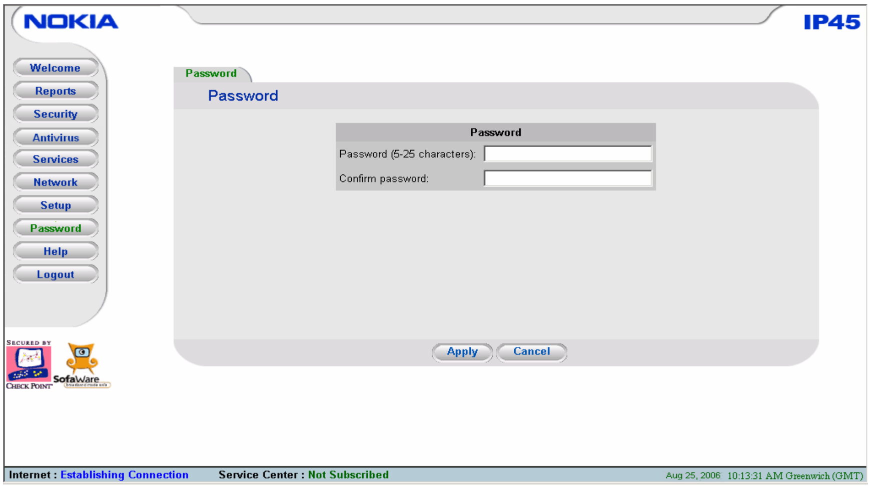
The default username and password for Nokia IP45 Tele 8 Configuration is *admin.*You can change the password for this user.

Note
After the initial login, You can change the username also.

To change the password for IP45 Tele 8

1. Choose Password from the main menu.

   The Password page opens.



Password

Password

Password (5-25 characters):

Confirm password:

Internet : Establishing Connection Service Center : Not Subscribed Aug 25, 2006 10:13:31 AM Greenwich (GMT)

2. Edit the Password and Confirm password fields.

Note
Use five to twenty five alphanumeric characters for the new password.

3. Click Apply.

   Your changes are saved.

   In Nokia IP45 Satellite X, you can define multiple users and perform the following tasks:

   - Change your password
   - Add users
   - View and edit users
   - Delete users
   - Set up remote VPN access for users

To change the password for IP45 Satellite X

1. Choose Users from the main menu.

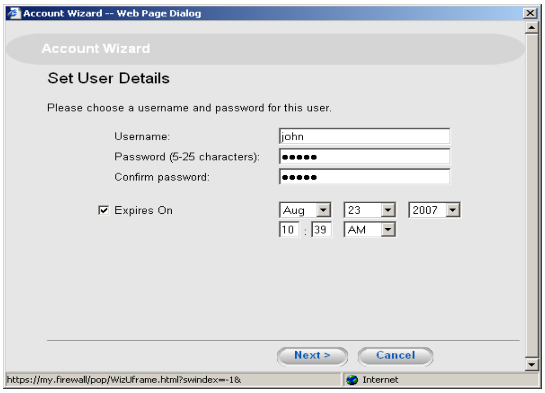
   The Users page opens.

2. In the username row, click Edit.

   The Set User Details window opens.

3. Edit the Password and Confirm password fields.

4. Enter the expiry date.



Account Wizard -- Web Page Dialog
Account Wizard

Set User Details

Please choose a username and password for this user.

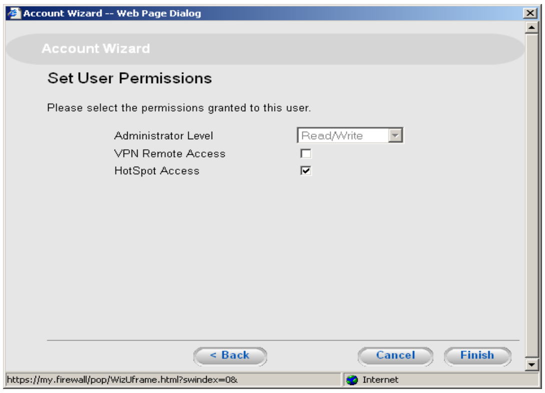
Username:	john
Password (5-25 characters):	●●●●●
Confirm password:	●●●●●
☑ Expires On	Aug 23 2007 10 : 39 AM

Next >
Cancel
https://my.firewall/pop/WizUframe.html?swindex=-1&
Internet

Note
Use five to twenty five alphanumeric characters for the new password.

5. Click Next.

The Set User Permissions window opens.



Account Wizard -- Web Page Dialog
Account Wizard

Set User Permissions

Please select the permissions granted to this user.

Administrator Level	Read/Write
VPN Remote Access	□
HotSpot Access	☑

< Back
Cancel
Finish
https://my.firewall/pop/WizUframe.html?swindex=0&
Internet

Adding Users

You can add users with IP45 Satellite X only. The number of IP45 users you can add is limited according to your software.

IP45v4.0 includes a new administrative role, the Users Manager. A Users Manager is an administrator who can create new users with HotSpot or VPN access permissions, while preventing the user from accidentally modifying other aspects of the appliance configuration.

To add a user

1. Choose Users from the main menu.

   The Internal Users page opens.

2. Click New User.

   The Set User Details wizard opens. The options that appear on the page depend on the software and services you are using.

3. Complete the fields by using the information in Table 54 on page 196.
4. Click Apply.

   The new user is saved.

You can also add users by using command-line interface. For more information, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

Adding Guest HotSpot Users

Nokia IP45 v4.0 supports quick HotSpot guests, by providing temporary network access. You can also print the details of the guest user.

By default, the quick guest user has the following characteristics:

- Username is in the format guest<number>, where <number> is a unique three-digit number.

  For example: guest123.

- Password is randomly generated
- Expires in 24 hours
- No administration level access
- HotSpot access permission

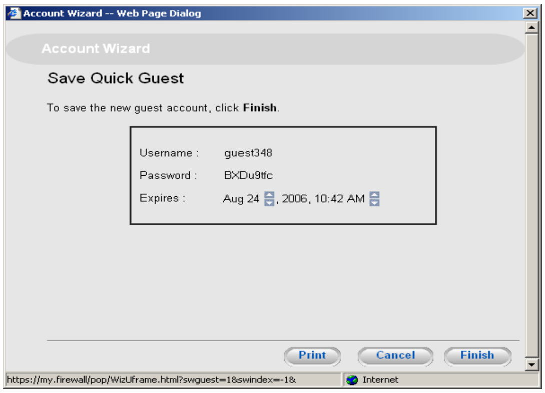
To add a Quick Guest

1. Choose Users from the main menu and select Internal Users.

   The Internal Users page opens.

2. Click Quick Guest at the bottom of the page.

   The Save Quick Guest wizard appears.



Account Wizard -- Web Page Dialog
Account Wizard

Save Quick Guest

To save the new guest account, click **Finish**.

Username :	guest348
Password :	BXDu9tfc
Expires :	Aug 24, 2006, 10:42 AM

Print
Cancel
Finish
https://my.firewall/pop/WizUframe.html?swguest=1&swindex=-1&
Internet

3. User name and password information for the quick guest is displayed along with the expiry period.
4. In the Expires field, specify the expiry period by clicking on the arrows at date and time.
5. Click Print to print the guest user details.
6. Click Finish.

   The guest user is saved.

Viewing and Editing Users

You can view and edit users with IP45 Satellite X license only.

To view or edit users

1. Choose Users from the main menu.

   The Users page opens.

2. Click Edit against the user to edit.

   The Set User Details window opens with the user's details. The options that appear on the page depend on the software and services you are using.

3. To edit the user's details, do the following:

   a. Edit the fields with the help of Table 54 on page 196.

   b. Click Apply.

   The changes are saved.

4. To return to the Users page without making any changes, click Cancel.

   Table 54 gives details about the Edit User fields.

Table 54 Edit User Page Fields

Field	Action
Username	Enter a username for the user.
Expires on	Select the expiry date and time.
Hotspot Access	Allows the user to access hotspot. Uncheck to deny access to hotspot.
Password	Enter a password for the user. Use five to twenty-five alphanumeric characters (letters or numbers) for the new password.
Confirm Password	Re-enter the user's password.
Administrator Level	Select the user's level of access to the Nokia IP45 portal. The levels are: • No Access—the user cannot access the IP45. • Read/Write—the user can log on to the IP45 and modify system settings. • Read Only—the user can log on to the IP45, but cannot modify system settings. For example, you could assign this administrator level to technical support personnel who need to view the event log. Default value: No Access.
VPN Remote Access	Allows the user to connect to this IP45 by using their VPN client. For further information about setting up VPN remote access, see Chapter 15, "Working with VPNs." This option is available in IP45 Satellite X configuration only.

Deleting Users

You can delete users with IP45 Satellite X only.

Note
The *admin* user cannot be deleted.

To delete a user

1. Choose Users from the main menu.

   The Internal Users page opens.

2. Click the Erase icon next to the user, to delete.

   A confirmation message appears.

3. Click OK.

   The user is deleted.

Setting Up Remote VPN Access for Users

You can set up VPN access for users with IP45 Satellite X only.

If you are using the IP45 as a VPN server, you can allow users to access it remotely through their VPN clients (a Check Point SecureClient, Check Point SecuRemote, IP45 Tele 8, or another IP45 Satellite X).

To set up remote VPN access for a user

1. Enable your VPN server by using the procedure in "To set up the IP45 device as a SecuRemote VPN server" on page 259.

2. Add the user to the system by using the procedure in "Adding Users" on page 194.

   You must select the VPN Remote Access option.

Using RADIUS Authentication

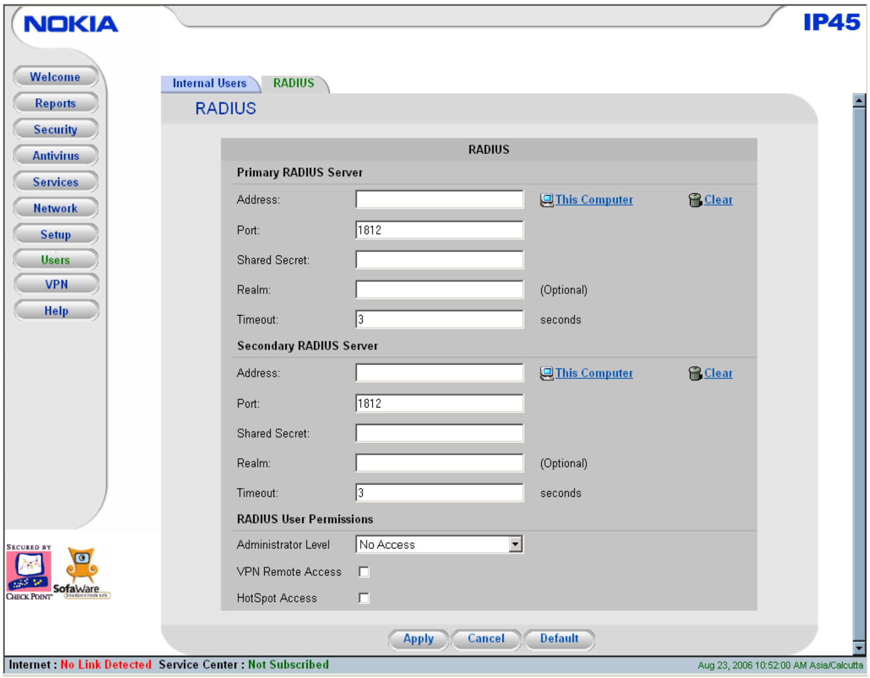
You can use RADIUS to authenticate both the Nokia IP45 security platform users, and the VPN clients, trying to connect to the device.

When a user accesses the IP45 GUI and tries to log on, the IP45 sends the entered username and password to the RADIUS server. The server then checks whether the RADIUS database contains a matching username and password pair. If so, the user is logged on.

To use RADIUS authentication

1. Choose Users from the main menu, and click the RADIUS tab.

   The RADIUS page opens.



RADIUS

RADIUS

Primary RADIUS Server

Address:		This Computer	Clear
Port:	1812		
Shared Secret:			
Realm:		(Optional)	
Timeout:	3	seconds	

Secondary RADIUS Server

Address:		This Computer	Clear
Port:	1812		
Shared Secret:			
Realm:		(Optional)	
Timeout:	3	seconds	

RADIUS User Permissions

Administrator Level	No Access
VPN Remote Access	□
HotSpot Access	□

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 10:52:00 AM Asia/Calcutta

2. Complete the fields by using the information provided in Table 55.

   Check the VPN Remote access check box to enable VPN remote access. This is optional.

3. Click Apply.

Table 55 gives more information about the fields in RADIUS page.

Table 55 RADIUS Page Fields

Fields	Action
Address	Type the IP address of the computer that run the RADIUS service (one of your network computers) or click the corresponding This Computer button to allow your computer to host the service. To clear the text box, click Clear.
Port	Type the port number on the RADIUS server's host computer. To reset this field to the default port (1812), click Default.
Shared Secret	Type the shared secret to use for secure communication with the RADIUS server.

Table 55 RADIUS Page Fields (*continued*)

Fields	Action
Administrator Level	Select the level of access to the IP45 portal to assign to all users that the RADIUS server authenticates. The levels are: • No Access: the user cannot access the IP45. • Read/Write: the user can log on to the IP45 and modify system settings. • Read Only: the user can log on to the IP45, but cannot modify system settings. Default value: No Access
Realm	Type the realm to append to RADIUS requests. The realm will be appended to the username as <username>@<realm>
Time-out	Type the interval of time in seconds between attempts to communicate with the RADIUS server. Default value: 3 seconds **Note** You can configure *retries* value by using the command-line interface. For more information about the command-line interface, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0*.

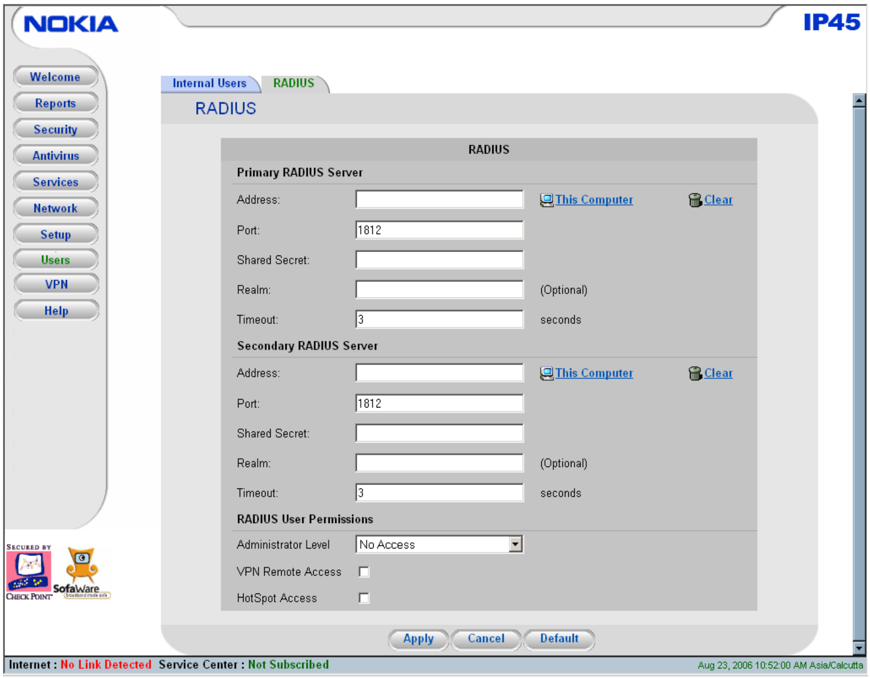
RADIUS Vendor Specific Attributes

Nokia IP45 v4.0 supports RADIUS vendor specific attributes (VSA). The RADIUS can use the VSA to allocate specific set of permissions to the authenticated user. Multiple permissions can be specified in a single response. Any permission, provided by the RADIUS overrides the permission that is configured locally.

To configure vendor specific attributes

1. Choose Users from the main menu and select RADIUS.

   The RADIUS page opens with the list of available options.



RADIUS

RADIUS

Primary RADIUS Server

Address:

Port: 1812

Shared Secret:

Realm: (Optional)

Timeout: 3 seconds

Secondary RADIUS Server

Address:

Port: 1812

Shared Secret:

Realm: (Optional)

Timeout: 3 seconds

RADIUS User Permissions

Administrator Level: No Access

VPN Remote Access ☐

HotSpot Access ☐

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 10:52:00 AM Asia/Calcutta

2. Scroll down to RADIUS User Permissions.
3. Select the administrator level of access from the drop-down list. The following are the options available.
   - **Read/Write**—user can log on to the my.firewall portal and modify system settings.
   - **Users Manager**—an administrator who can create new users with *none* as administrator level and who is a read-only user.
   - **Read Only**—user can log on to the my.firewall portal, but cannot modify system settings.
   - **No Access**—user cannot access the my.firewall portal.
4. If the user can access the network from a remote access VPN client, select the VPN Remote Access check box.
5. If the user can log on using the My hotspot page, Select the HotSpot Access check box.
6. Click Apply.

Access Control

You can set access control to your Nokia IP45 security platform.

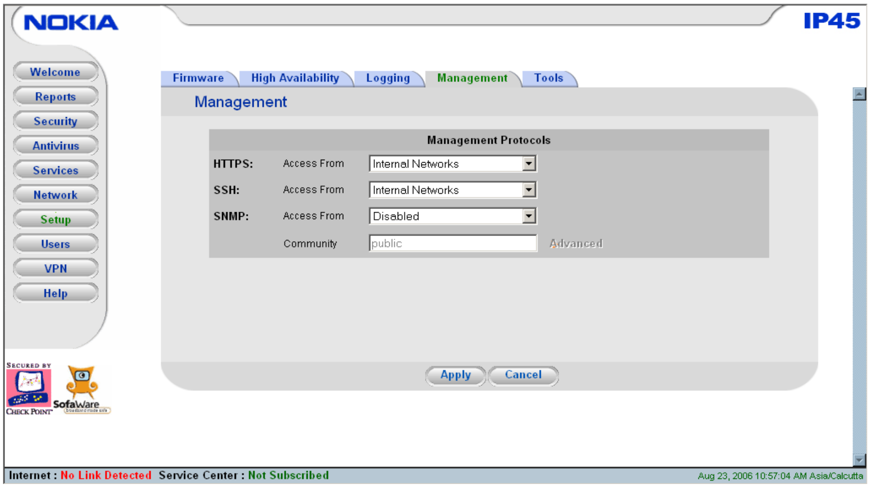
To set the access control

1. Choose Setup from the main menu.

   The Firmware page opens.

2. Click Management.

   The Management page opens.



Management

Management Protocols

HTTPS:	Access From	Internal Networks
SSH:	Access From	Internal Networks
SNMP:	Access From	Disabled
	Community	public

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 10:57:04 AM Asia/Calcutta

3. Select (Access from) from the drop-drown list for HTTPS, SSH, and SNMP Access control.

   You can select one of the following:

   - **Internal Networks**—you can access the device only when you are within a LAN.
   - **Internal Networks +VPN**—you can access the device when you are in a LAN or connected through VPN.
   - **Internal Networks +IP Range**—only specified computers with a given IP address range can access the device.
   - **ANY**—you can access the appliance from any location.

Telnet Access

Note
Telnet access is disabled by default. To allow Telnet access from the LAN, WAN, and DMZ, configure separate user rules.

For more information about Telnet access, see "Using Telnet to Connect to the Nokia IP45 Security Platform" on page 68.

Secure Shell

The Nokia IP45 supports SSH 2.0. The SSH feature in the IP45 provides secure remote access to the device. In addition, SCP is supported to enable secure upgrade of the device, downloading of public keys, HTTPS certificates, import and export features.

Configuring SSH

To start using SSH remotely, first set IP45 to accept requests from SSH clients.

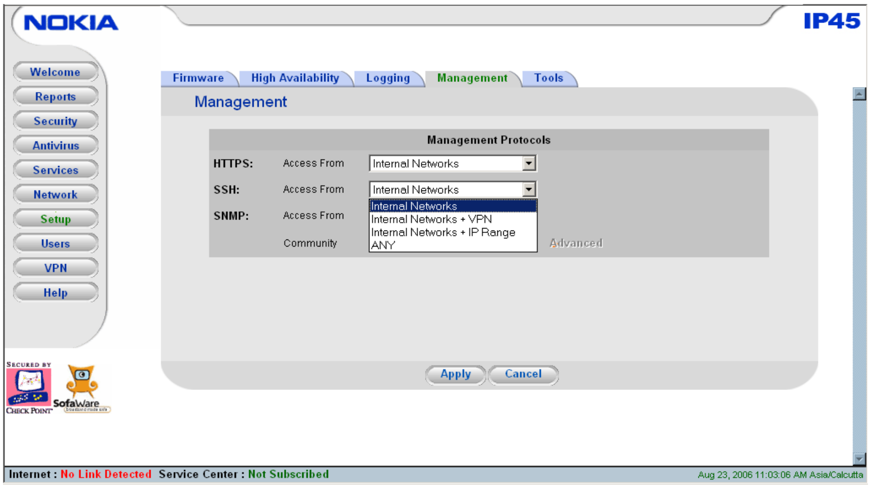
To enable IP45 to accept SSH requests

1. Choose Setup from the main menu.

   The Setup page opens.

2. Click the Management tab.

   The Management page opens.



Management

Management Protocols

HTTPS:	Access From	Internal Networks
SSH:	Access From	Internal Networks
SNMP:	Access From	
	Community	

Internal Networks
Internal Networks + VPN
Internal Networks + IP Range
ANY

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 11:03:06 AM Asia/Calcutta

Note

Secure Shell access is enabled by default from the LAN and DMZ interfaces. Setting of management rules, which is described in this section, is applicable only for allowing SSH access from the WAN side.

3. From the SSH drop-down list, choose one of the following:

   - Internal Network
   - Internal Network + VPN
   - IP Address Range
   - ANY

   Click Internal Network to enable only computers from your internal network to access your IP45 through SSH. Similarly, click ANY to enable any host (with any IP address) to connect to IP45 through SSH, and so on.

Enabling or Disabling SSH Service

Note
Secure Shell (SSH) options cannot be configured from the Nokia IP45 GUI. Use the command-line options from a command shell (such as HyperTerminal) to configure these options. A brief list of important command-line options for configuring Secure Shell (SSH) is included in the user guide for the purpose of introduction. For additional and detailed information, see the Nokia *IP45 Security Platform CLI Reference Guide Version 4.0*.

Use the following commands to enable, disable, and view the status of SSH service:

To enable the SSH service, use the following command:

```
set ssh server
          enable <0 | 1>
```

To view the SSH service, use the following command:

```
show ssh server
          enable
```

Arguments

```
enable <0 / 1>
```

The value of 0 disables SSH and the value of 1 enables SSH. The default value is 1 since SSH is enabled by default.

SSH Authentication Methods

You can perform the SSH authentication in the following ways:

- **Password authentication**—set up by default. In this method, you can connect to the SSH server running on the IP45 from the SSH client installed on your computer, after entering your password.
- **Public-key authentication—**one of the most secure ways to authenticate by using SSH. The basic principle in public-key authentication is the use of a pair of computer-generated keys: private key and public key. A public key is not useful unless you have the corresponding private key.

Using SSH Client

You need an SSH client to connect to the SSH server running on the IP45. Install an SSH client if you do not have one already.

You can use the SSH client to connect to the IP45 by using password authentication or public key authentication. For additional information, see *User Manual* of the SSH client you are using.

Configuring Advanced Secure Shell Server Options

For additional information on using the command line options, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

Configuring Server Authentication of Users

Use the following commands to configure the type of authentication the server uses to authenticate users:

```
set ssh server
          password-authentication <0 | 1>
          publickey-authentication <0 | 1>
```

Use the following commands to show user authentication configurations:

```
show ssh server
          password-authentication
          publickey-authentication
```

Configuring Server Protocol Details

Use the following commands to configure SSH protocols:

```
set ssh server
          ciphers name
          keepalives <on / off>
          listen-addr address
          listen-addr2 address
          maxconnections Number
          port <1-65535>
```

Use the following commands to show SSH protocol configurations:

```
show ssh server
          ciphers
          keepalives
          listen-addr
          listen-addr2
          maxconnections
          port
```

Configuring Service Details

Use the following commands to configure the service details:

```
set ssh server
          login-grace-time integer
```

Use the following commands to show the service details:

```
show ssh server
          login-grace-time
```

Configuring Server Implementation

Use the following commands to configure the type of authentication the server will use to authenticate users.

```
set ssh server
          log-level name
```

Use the following commands to show service detail configurations:

```
show ssh server
          log-level
```

Configuring and Managing SSH Key Pairs

This section provides details about how to configure and manage your SSH key pairs.

Managing New Host Keys

Use the following commands to generate new host keys:

```
set ssh hostkey
     dsa size <768 | 1024 | 2048 |4096>
     rsa size <768 | 1024 | 2048 |4096>
```

Use the following commands to view host keys:

```
show ssh hostkey
     dsa
     rsa
```

Managing Authorized Keys

Use the following commands to add authorized keys:

```
add ssh authkeys
     <dsa | rsa> user admin <openssh-format | ssh2-format> file
```

Use the following commands to delete authorized keys:

```
delete ssh authkeys
     <dsa | rsa> user admin id
```

Use the following commands to view keys configured for various user accounts:

```
show ssh authkeys
      <dsa | rsa> user admin id identifier
      <dsa | rsa> user admin list
```

Secure Socket Layer

Secure Socket Layer (SSL) enables secured communication over insecure networks. This protocol uses a private key to encrypt data that is passed through an SSL connection and ensures a secure connection between the client and the server.

Enabling HTTPS Web Access

You can enable HTTPS remote access, so that the IP45 users can securely access the IP45 portal from the Internet, by accessing the URL https://X.X.X.X:981, where X.X.X.X is the IP45 Internet IP address.

Note
The URL https://my.firewall is accessible from the Internal network by default.

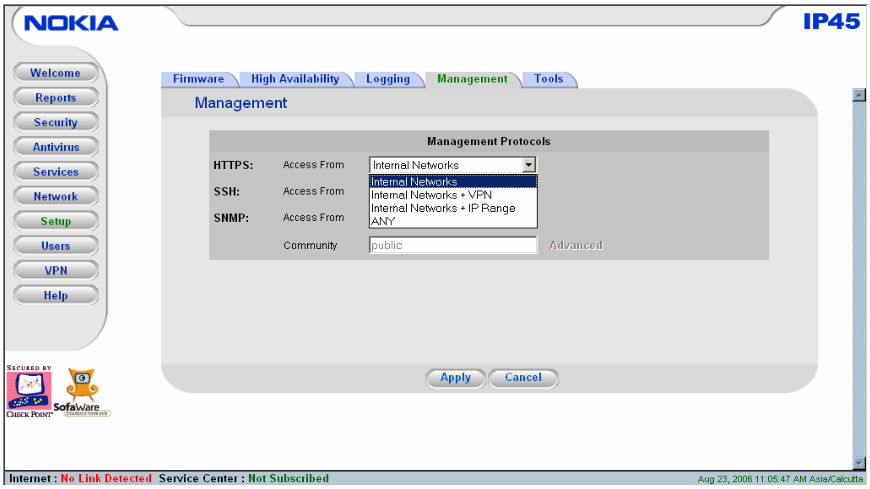
To enable HTTPS Web access

1. Choose Setup from the main menu.

   The Setup page opens.

2. Click the Management tab.

   The Management page opens.



Management

Management Protocols

HTTPS: Access From Internal Networks

SSH: Access From

SNMP: Access From

Community public

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 11:05:47 AM Asia/Calcutta

3. From the HTTPS drop down list, click:

   - **Internal Network**—to enable only users of your internal network to access your IP45 through HTTPS.

- **Internal Network + VPN**—to enable users of your internal network and users connected to your IP45 through a VPN tunnel to access your IP45 through HTTPS.
- **IP Address Range**—to give a range of IP addresses. Traffic from these IP addresses only can access your IP45 through HTTPS.
- **ANY—**to enable traffic generated from any IP address to access your IP45 through HTTPS.

4. Click Apply when you finish making the settings.

   The Saved Successfully message appears.

Generating a Self-Signed Certificate and Private Key by Using the CLI

Use the following command to generate a certificate and its associated private key. To better ensure your security, generate the certificate and private key over a trusted connection.

```
generate https ssl-certificate key-bits <512 | 768 | 1024> <passphrase
name | prompt-passphrase> country name state-or-province name locality
name organization name organizational-unit name common-name name e-mail
address name <cert-file path | cert-request-file path> key-file path
```

For more information, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0*.

Installing a Certificate and Private Key

Use the following commands to copy a certificate and its associated private key in the /var/etc/https_ssl_cert_server.crt and /var/etc/https_ssl_server.key files. Copying the certificate and private key to these files makes them available to establish SSL-secure Web connections.

```
set https ssl-certificate
     cert-file path key-file path <passphrase name | prompt-
      passphrase>
```

For more information, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

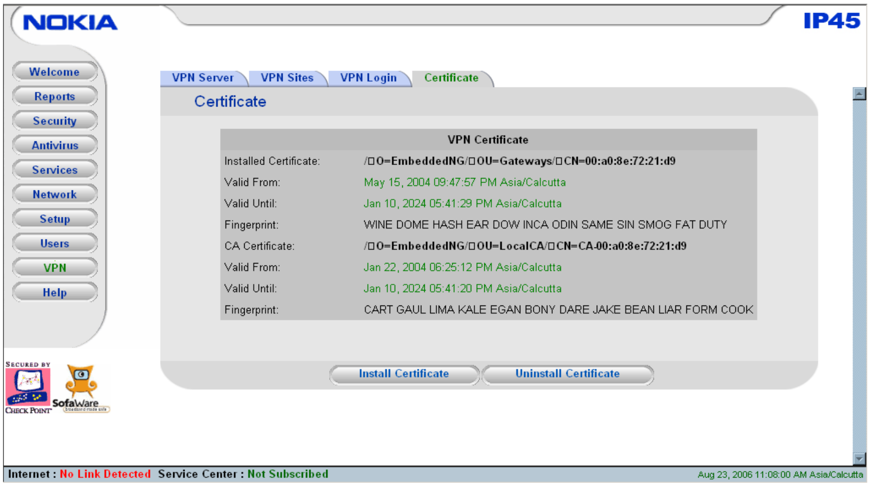
Viewing Certificate Fingerprint Display

The Nokia IP45 v4.0 supports certificate fingerprint display, a unique text used to identify the certificate. This fingerprint will match the fingerprint displayed in the SecuRemote VPN clients, upon connection to the appliance.

If the administrator provides a fingerprint to a SecuRemote user, the user should verify that the root CA fingerprint that is displayed matches with the one provided by the administrator.You can view the certificate fingerprint information by using the IP45 GUI.

To view a certificate fingerprint, choose VPN from the main menu and select Certificate.

The VPN certificate information is displayed with the fingerprint text, as shown below:



Certificate

VPN Certificate	
Installed Certificate:	/□O=EmbeddedNG/□OU=Gateways/□CN=00:a0:8e:72:21:d9
Valid From:	May 15, 2004 09:47:57 PM Asia/Calcutta
Valid Until:	Jan 10, 2024 05:41:29 PM Asia/Calcutta
Fingerprint:	WINE DOME HASH EAR DOW INCA ODIN SAME SIN SMOG FAT DUTY
CA Certificate:	/□O=EmbeddedNG/□OU=LocalCA/□CN=CA-00:a0:8e:72:21:d9
Valid From:	Jan 22, 2004 06:25:12 PM Asia/Calcutta
Valid Until:	Jan 10, 2024 05:41:20 PM Asia/Calcutta
Fingerprint:	CART GAUL LIMA KALE EGAN BONY DARE JAKE BEAN LIAR FORM COOK

Internet : No Link Detected Service Center : Not Subscribed

Aug 23, 2006 11:08:00 AM Asia/Calcutta

10 Configuring and Monitoring SNMP

This chapter provides information about how to configure the Simple Network Management Protocol (SNMP) and how to use SNMP to manage the Nokia IP45 security platform.

This chapter covers the following topics:

SNMP Description

SNMP is the industry standard for monitoring and managing devices on data communication and telecommunication devices or systems. SNMP helps in centrally monitoring and diagnosing such devices.

The Nokia IP45 security platform supports the following MIBs:

- MIB-II (for more information, see RFC 1213)
- Host Resource MIB (for more information, see RFC 1514)

SNMP Configuration from the Nokia IP45 Security Platform

You can use the Nokia IP45 GUI portal and the command-line interface (CLI) to set, change, and view parameters for SNMP.

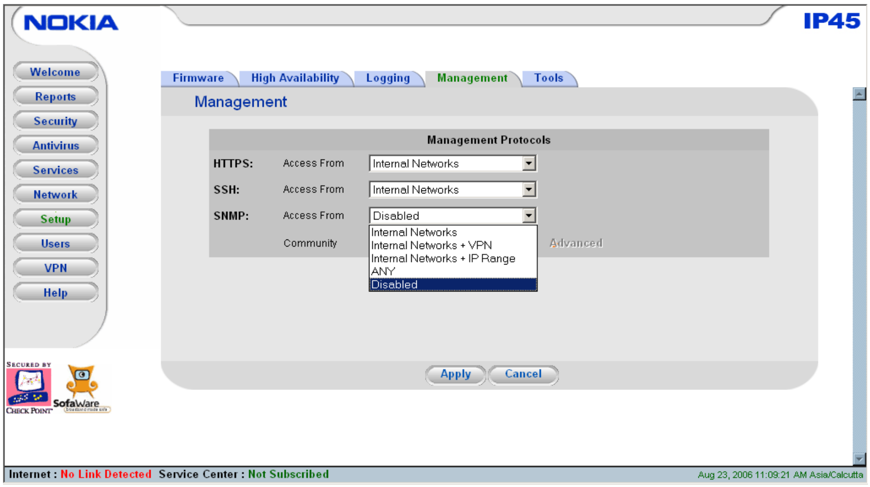
Setting Up SNMP Access to the Nokia IP45 Security Platform

Allow or disallow SNMP manager software running outside your network to monitor the Nokia IP45 security platform.

To enable SNMP access

1. Click Setup in the main menu, and click the Management tab.

   The Management page opens.



Management

Management Protocols

HTTPS: Access From Internal Networks

SSH: Access From Internal Networks

SNMP: Access From Disabled

Community

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 11:09:21 AM Asia/Calcutta

2. Select one of the following from the SNMP drop-down list list.

   - Internal Network
   - Internal Network + VPN
   - IP Address Range
   - ANY
   - Disabled

   If you select Internal Network, SNMP access to the IP45 is allowed from computers in your internal network or LAN only; if you select IP Address Range, you can specify a range of IP addresses from which SNMP access is allowed to your IP45.

Configuring the SNMP Parameters

When you set the SNMP access rules, you can configure the SNMP parameters from the Nokia IP45 security platform GUI.

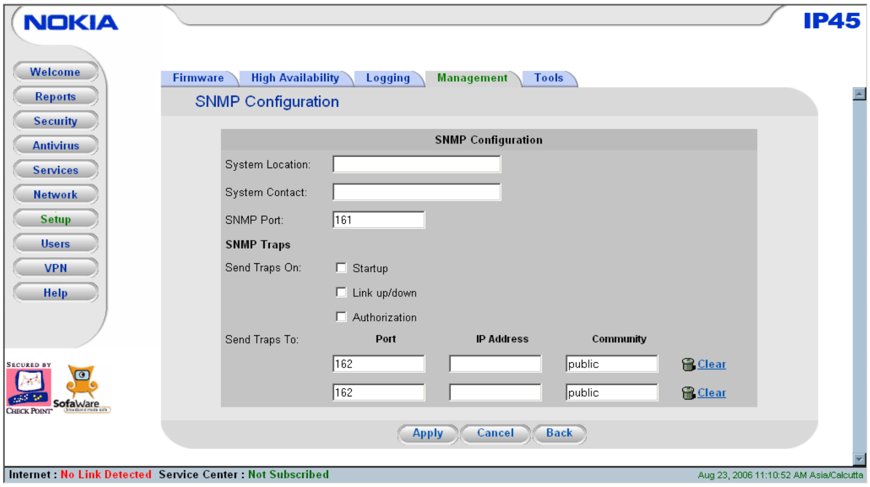
To configure the SNMP parameters

1. Define the SNMP community name in the Management page. See “To enable SNMP access” on page 210.

   A community name must be specified to monitor your device by using SNMP.

2. Click the Advanced tab.

The SNMP Configuration page opens.



SNMP Configuration

SNMP Configuration

System Location:

System Contact:

SNMP Port: 161

SNMP Traps

Send Traps On: □ Startup □ Link up/down □ Authorization

Send Traps To:	Port	IP Address	Community
	162		public
	162		public

Internet : No Link Detected Service Center : Not Subscribed

Aug 23, 2006 11:10:52 AM Asia/Calcutta

3. Specify the System Location. Example: California.
4. Specify the System Contact. Example: phone number.
5. Specify the SNMP port.This number defines the port where the SNMP daemon will run.
6. Define the SNMP traps to be generated:
   - **Startup**—this trap is generated and reported to the SNMP Manager when the SNMP daemon re-initializes.
   - **Link up/down**—this trap is generated and reported to the SNMP Manager when the connection to WAN or LAN is temporarily unavailable or becomes available.
   - **Authorization**—this trap is generated and reported to the SNMP manager when SNMP access is attempted with an incorrect community name.
7. Specify the port number. The default port number is 162
8. Specify the IP address where the SNMP manager is running, so that traps that are generated can be sent to the correct IP address.
9. Enter the name of the SNMP community string in the Community text box. Default: public.

   It is recommended to change this as the SNMP agents use this as password while connecting to the device.

Note

Set the trapPduAgent to a specified IP address from the command prompt so as to view the IP address of the device from where a trap is generated. Use the command *set snmp trappduAgent ip_address* from the IP45 CLI for setting the trapPduAgent. You cannot set the trapPduAgent from the IP45 GUI portal. For more information, see *the Nokia IP45 Security Platform CLI Reference Guide Version 4.0*.

Configuring SNMP Parameters from the Command-Line Interface

You can use set and view parameters for SNMP.

Setting SNMP Parameters

Nokia IP45 supports SNMPv2c and SNMP v1 and v2 traps.

Use the following commands to set the SNMP parameters:

```
set snmp
     contact      - SNMP Contact
     enable       - Enables SNMP Daemon
     location     - SNMP Location
     port         - SNMP Port
     trapPduAgent - snmp trappduagent
     trapreceiver - snmp Trapreceiver
     traps        - SNMP Traps
```

Viewing SNMP Parameters

Use the following commands to view the SNMP parameters:

```
show snmp
     community    - SNMP Community
     contact      - SNMP Contact
     enable       - Displays SNMP Daemon
     location     - SNMP Location
     port         - SNMP Port
     trapPduAgent - snmp trappduagent
     trapreceiver - snmp Trapreceiver
     traps        - SNMP Traps
```

For additional and detailed information on how to use the set and show commands, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

11 High-Availability

High-availability (HA) provides reliable, dependable and business-class secure access. HA caters to device failures, connects to multiple ISP supporting demand dialing, allows Internet link selection to cater to ISP link failures, and provides seamless routing of encrypted traffic across multiple WAN links.

This chapter includes the following sections:

- High-Availability Sample Scenario
- Configuring Multiple HA Clusters
- Configuring High-Availability
- High-Availability over VPN

High-Availability Sample Scenario

You can create a High-Availability cluster consisting of two or more IP45 security platforms. Each gateway in the HA cluster has a separate IP address within the local network. The gateways also share a single virtual IP address, which is the default gateway address for the local network.

Control of the virtual IP address is passed as follows:

The role of the gateway is determined by the priority assigned to it.

1. The gateway with the highest priority acts as the active gateway and uses the virtual IP address. Other gateways in the network are passive gateways.
2. The active gateway sends periodic signals, or heartbeats, to the network though a synchronization interface. Any internal network existing on both the gateways can be a synchronization interface.
3. If the heartbeat from the active gateway stops, indicating that the active gateway has failed, the gateway with the highest priority becomes the new active gateway and takes over the virtual IP Address.
4. When a gateway that was inactive becomes active again, or if there is a change in its priority, the gateway sends a heartbeat notifying the status to the other gateways in the cluster.

The IP45 security platform supports Internet connection tracking. Each IP45 can track the status of its Internet connection and can reduce its own priority by a user-specified amount, if the connection goes down.

Note
If the priority of the Active Gateway drops below the priority of another gateway, then the other gateway becomes the Active Gateway.

Note
You can force a fail-over to a passive IP45 security platform. A fail-over is required to verify whether HA is working properly, or if the active IP45 security platform needs any repairs. To force a fail-over, switch off the primary or disconnect it from the LAN network.

Configuring Multiple HA Clusters

The IP45 security platform supports configuring multiple HA clusters on the same network. To configure multiple HA clusters, each cluster must be assigned a unique identification.

While configuring HA, you can specify that only the active gateway in the cluster should connect to the Internet. This is called WAN HA, and is useful in the following scenarios:

- Your Internet subscription cost is based on the connection time. Having the passive appliance needlessly connected to the Internet costs you more.
- To enable multiple appliances share the same static IP address without creating an IP address conflict.

Note
To avoid multiple appliances with same WAN IP address acting as primary, select *Do not connect if this gateway is in passive state* option under High-Availability, while configuring the Internet.

WAN HA avoids an IP address change, and thereby ensures virtually uninterrupted access from the Internet to internal servers at your network.

Ensure the following requirements are met before you configure the HA:

- At least two identical IP45 security platforms with same firmware versions and firewall rules.
- The internal networks of the appliances must be the same.
- The appliances must have different real internal IP addresses, but should share the same virtual IP address.
- The synchronization interface ports of the appliances must be connected either directly or thorough a hub or a switch.

  For example, if the DMZ is the synchronization interface, then the DMZ/WAN2 ports on the appliances must be connected to each other.

Note
The synchronization interface need not be dedicated for synchronization only. It may be shared with an active internal network.

You can configure HA for any internal network, except the OfficeMode network.

Note
You can enable the DHCP server in all the IP45 security platforms. The DHCP server of a passive gateway starts answering DHCP requests only when the active gateway fails.

Nokia IP45 v4.0, in addition to the IP address of the interface, supports a virtual IP address that can be assigned to each WAN port. Assigning a virtual IP address to the WAN interface allows you to configure a secondary gateway to be accessible for remote management and connected to the service center at all times by using the primary IP address of the WAN interface). If the primary gateway fails, the secondary gateway automatically takes over the virtual IP address, ensuring continuous service availability.

Note
To create a WAN virtual IP, the type of Internet connection must be *Static IP. PPP* based connections and dynamic IP connections are not supported.

You can also configure WAN IP by using command-line interface. For information, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

Configuring High-Availability

The following sections provide information about configuring HA parameters by using the CLI and the GUI.

For information about the commands, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

Configuring High-Availability by Using the GUI

This section describes how to configure high-availability by using the graphical user interface (GUI).

Note
Before configuring high-availability, set the internal IP addresses of the device and the network range. Each device must have a different internal IP address. For more information, see "Changing IP Addresses" on page 113.

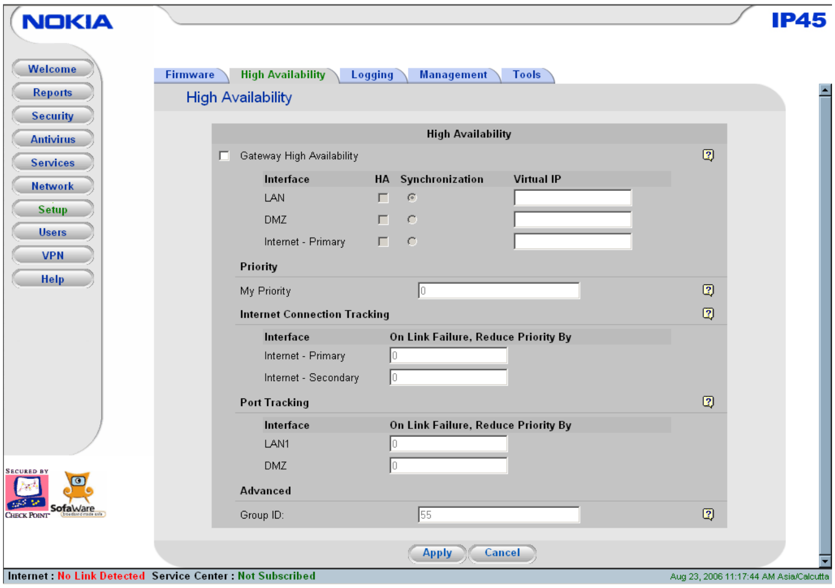
To configure high-availability by using GUI

1. Choose Setup from the main menu.

   The Firmware page opens.

2. Click High Availability.

   The High Availability page opens.



High Availability

High Availability

□ Gateway High Availability

Interface	HA	Synchronization	Virtual IP
LAN	□	●	
DMZ	□	○	
Internet - Primary	□	○	

Priority

My Priority: 0

Internet Connection Tracking

Interface	On Link Failure, Reduce Priority By
Internet - Primary	0
Internet - Secondary	0

Port Tracking

Interface	On Link Failure, Reduce Priority By
LAN1	0
DMZ	0

Advanced

Group ID: 55

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 11:17:44 AM Asia/Calcutta

3. Check the Gateway High Availability check box.

   All the existing internal interfaces are displayed.

4. To enable high availability, select HA next to the interface type.
5. Click the Synchronization radio button next to the type of interface to use as synchronization interface.
6. In the Virtual IP text box, enter the default gateway IP address. This can be any unused IP address, and must be same for all the devices.
7. In the My Priority text box, enter the priority value of the gateway.

Value: 1–255

8. Enter the value in Internet-Primary field. This field should contain the value to reduce the priority of the gateway if the primary Internet connection becomes inactive.

   Value: 0–255

9. Enter the value in Internet-Secondary field. This field should contain the value to reduce the priority of the gateway if the secondary Internet connection becomes inactive. For more information on configuring backup connection, see "Configuring a Backup Internet Connection" on page 93.

   Value: 0–255

10. In the text box next to LAN1 enter the amount to reduce the priority of the gateway if the Ethernet link of the LAN port is lost.

11. In the text box next to DMZ, type the amount to reduce the priority of the gateway if the Ethernet link of the DMZ/WAN2 port is lost.

12. Under Advanced, Group ID text box, type the Identity number of the cluster to which the gateway should belong.You need not change this value if only single HA cluster exists.

    Value:1-255

    Default value:55

13. Click Apply.

14. If desired, configure WAN high-availability for both the primary and secondary Internet connection. This setting should be the same for all the devices. For more information, see "Using the Setup Wizard" on page 73.

High-Availability over VPN

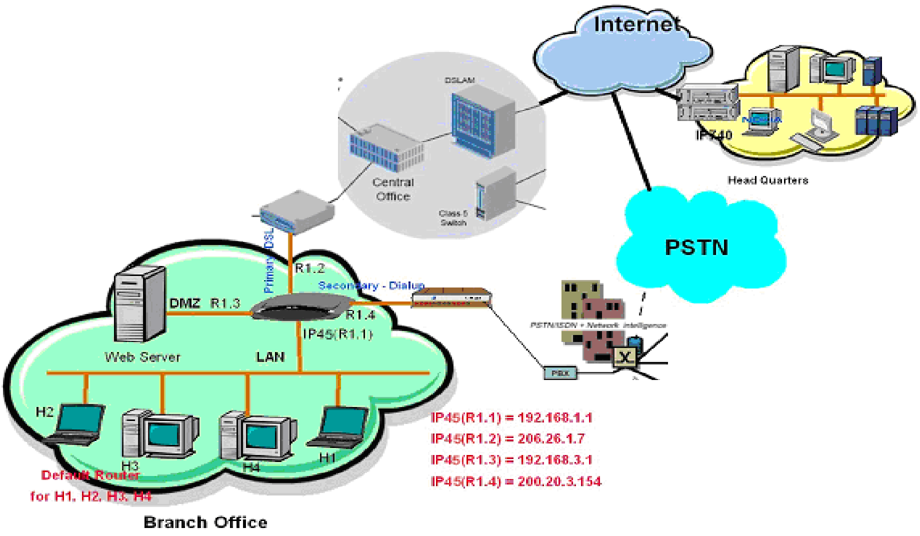
High-availability over VPN supports the following scenarios.This section includes the detailed description about the following topics:

- Dual Homing
- Generic High-Availability
- Advanced High-Availability

Dual Homing

The Nokia IP45 security platform v4.0 supports dual homing Internet connection that provides an uninterrupted connection to the ISP. The Internet connection that uses DSL or cable modem or static IP is the active and permanent connection. The dial-up connection is stated as the passive connection, which remains in backup mode. When the permanent connection fails, the dial-up connection automatically becomes active.

Figure 5 Dual Homing



Configuring for Dual Homing ISP Connectivity

The following sections give information about how to configure the Nokia IP45 dual homing feature:

- Configuring primary Internet profile for DSL/ Cable/Automatic DHCP (see "Configuring an Internet Connection" on page 73).
- Configuring secondary Internet profile for dial-up mode (see Chapter 5, "Configuring Dial-Up" on page 90)·
- Configuring modem parameters.

Use the following commands to configure modem parameters. For more information, see the *Nokia IP45 Security Platform CLI Reference Guide Version, 4.0*

```
set modem dialmode <tone | pulse>

set modem extrainit string

set modem manufacturer <standard | custom>

set modem rate <9600 | 19200 | 38400 | 57600 | 115200 | 230400 |460800>
```

Use the following commands to view the modem parameters:

```
show modem <all | dialmode | extrainit | manufacturer | rate>
```

Configuring ISP Dial-Up Profiles

Use the following command to configure ISP dial-up profiles by using the CLI wizard:

```
wizard dialup
```

For more information about how to use other dial-up commands, see the *Nokia IP45 Security Platform CLI Reference Guide*, *Version 4.0*.

Use the following commands to modify ISP dial-up profiles:

```
set dialup profile <id>
     user <username>
     password <password>
     number <telephone Number>
     [authentication <none | pap | chap | any>
     externalip <ip_address>
     mtu <value>
     staticdns <yes | no>
     dns1 <ip_address>
     dns2 <ip_address>
```

Use the following command to delete selected ISP dial-up profiles:

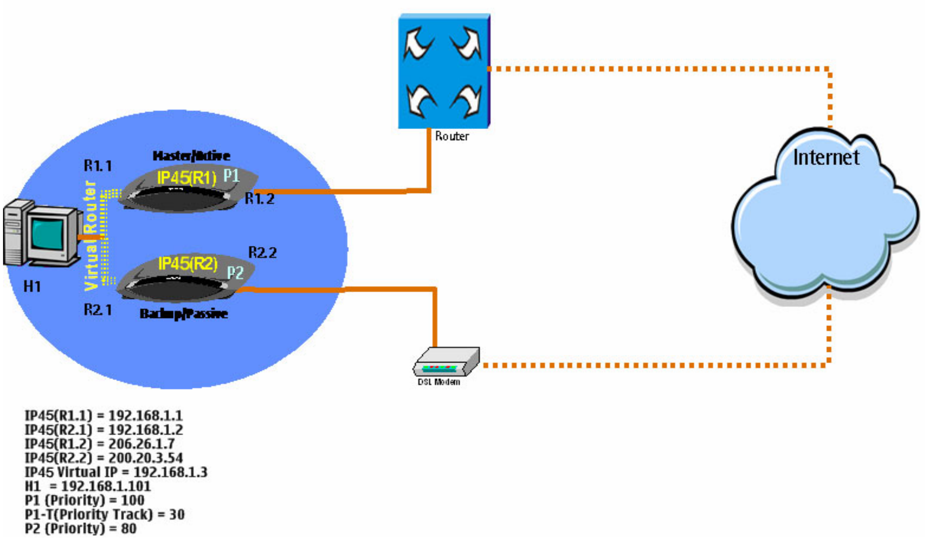
```
set dialup profile <id> disable
```

- **Advanced**—device monitors the status of BGP peers and dial-up, based on the WAN failover node. Generic High-Availability.

Generic High-Availability

Generic high-availability is implemented in Nokia IP45 v4.0. Using this option, you can create a high-availability cluster consisting of two IP45 devices. For example, you can install two IP45 devices on your network, one acting as the master, the default gateway through which all network traffic is routed, and the other as backup. If the master fails, the backup automatically and transparently takes over all the roles of the master. This ensures that your network is consistently protected by an IP45 device and is connected to the Internet.

Figure 6 Generic High-Availability



The gateways in a high-availability cluster have a separate IP address within the local network. In addition, the gateways share a single virtual IP address, which is the default gateway address for the local network. Control of the virtual IP address happens as follows:

- Each gateway is assigned a priority, which determines its role. The gateway with highest priority acts as the active gateway and uses the virtual IP address. The remaining gateways remain passive.
- The active gateway sends periodic signals, or heartbeats to the network through a synchronization interface.

Note
The synchronization interface can be any internal network existing on both gateways.

- If the heartbeat from the active gateway stops (indicating that the active gateway has failed), the gateway with the next highest priority becomes the new active gateway and takes over the virtual IP address.
- When a gateway that was offline becomes active again, or the priority of a gateway changes, the gateway sends a heartbeat notifying the other gateways in the cluster. The gateway with highest priority now becomes the active gateway.

The IP45 device supports Internet connection tracking, which means that each device tracks the status of its Internet connection and reduces its own priority by a user-specified value, if its Internet connection is inactive. If the priority of the active gateway drops below the priority of another gateway, then the gateway with highest priority becomes the active gateway.

While configuring high-availability, you can specify that only the active gateway should connect to the Internet. This is called WAN high-availability, and is useful in the following conditions:

- Your Internet subscription cost is based on connection time, and therefore having the passive device needlessly connected to the Internet costs you.

- Multiple devices need to share the same static IP address on a WAN interface without creating an IP address conflict. WAN high-availability avoids an IP address change, and thereby ensures virtually uninterrupted access from the Internet to internal servers at your network.

Before configuring high-availability, make sure that you meet the following requirements:

You must have at least two identical IP45 devices with:

- identical firmware versions and firewall rules
- same internal networks
- different real internal IP addresses, but sharing the same virtual IP address
- the devices' synchronization interface ports connected either directly, or through a switch. For example, if the DMZ is the synchronization interface, then the DMZ/WAN2 ports on the devices must be connected to each other.

Note
You can enable the DHCP server in all the IP45 devices. The DHCP server of a passive gateway starts answering the DHCP requests only if the active gateway fails.

Advanced High-Availability

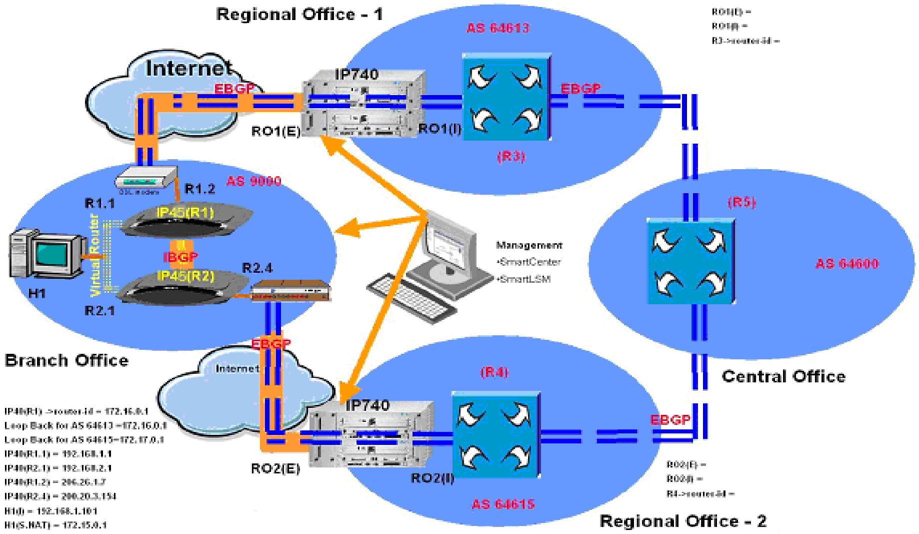
The following sections describe the advanced high-availability feature.

Route-Based VPN and BGP

The Nokia IP45 security platform has built-in features to automatically detect the failure of an IPSec VPN connection from a remote office or branch office to the headquarters. On failure, it forwards the traffic by using an alternative link (dial backup or VPN) through another ISP.

The IP45 security platform uses Border Gateway Protocol (BGP) to detect IPSec VPN connection failures, and to activate alternative links. The IP45 monitors each IPSec VPN tunnel in association with a BGP neighbor at the headquarters.

Figure 7 Dynamic VPN



To detect IPSec VPN connection failure, the Nokia IP45 security platform monitors the reachability of the remote BGP peers associated with the VPN tunnel. On failure, the passive link is activated to establish an alternative IPSec VPN connection to reach the associated BGP remote peer.

The Nokia IP45 continues to monitor the remote BGP peer reach ability on the preferred (primary) connection to the headquarters. Nokia IP45 falls back to preferred VPN connection as soon as the associated BGP remote peer becomes accessible.

A pair of loopback addresses (active and passive) are defined on the Nokia IP45 security platform with restricted BGP route advertisement of LAN and static NAT addresses. This scenario is supported with Check Point SmartLSM. The VPN policy installed on the Nokia IP45 includes the topology of immediate protected network behind the central office gateway only. This enables the traffic between these two networks tunneled, including the communication between BGP peers. The central office BGP peer advertises the CO networks to the IP45 and BGP. The traffic originating from the IP45 LAN destined to the central office network is tunneled and sent.

Border Gateway Protocol

The Nokia IP45 security platform participates in Autonomous System (AS), and can establish a neighbor relationship, and exchange routes with other non-adjacent routers.

An AS is a network or group of networks under common administration and with common routing policies.

The Nokia IP45 supports a limited set of BGP-4 features for route-based VPN and failover.

Note
You can configure BGP by using the Nokia IP45 CLI only. This feature is not supported in the IP45 GUI. Use the command-line options from a command shell (such as Hyper terminal) to configure these options. A brief list of important commands are included in this guide to provide an introduction. For more information about these commands, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

Configuring the BGP

The following sections provide the list of commands, which should be used to configure BGP.

Enabling BGP Routing

Use the following command to enable the BGP routing protocol:

```
set bgp daemon <restart | enable | disable>
```

Configuring the Local AS and Router-ID

Use the following command to configure the local AS:

```
set bgp as <value>
      router-id <value ipaddress>
```

Configuring for BGP Route Advertisement

The network and redistribute commands are used to inject routes into the BGP table. The network-mask portion of the IP address allows supernetting and subnetting.

Use the following commands to configure route advertisements:

```
add bgp
     network <value ipaddress | netmask-length>
     redistribute <connected | kernel | static>
```

Use the following commands to delete BGP route advertisement:

```
delete bgp
     network <value ipaddress | netmake-length >
     redistribute < connected | kernel | static >
```

Monitoring BGP

Use the following show commands to monitor BGP activity:

```
show bgp config all

show bgp summary

show bgp config running
```

Viewing Debugging Information

Use the following debug commands to display information on BGP logs for inbound or outbound events, or both:

```
set bgp debug
     event <on | off >
     keepalive <on | off >
     update <on | off >
     fsm <on | off >
```

Adding a BGP Peer to the Nokia IP45 Security Platform

The Nokia IP45 security platform v4.0 supports both internal and external BGP neighbors. Internal neighbors are in the same autonomous system; external neighbors are in different autonomous systems. Normally, external neighbors are adjacent to each other and share a subnet, while internal neighbors can be anywhere in the same autonomous system.

Use the following command to add BGP neighbors:

```
add bgp neighbor <value ip_address> remote-as <value>
```

Use the following command to delete a BGP neighbor:

```
delete bgp neighbor <value ip_address>
```

Clearing BGP

Clearing a BGP neighbor session resets BGP connections to enable inbound and outbound policy changes. Use the following commands to clear a BGP neighbor session:

```
clear bgp <neighbor <value ip_address> | neighbors>
```

Creating Prefix Lists on the Nokia IP45 Security Platform

Prefix lists are used to filter the updates *to* and *from* a peer on the basis of network prefixes, and masks. A prefix list is associated with a sequence number and prefix length range for a specified prefix and mask. The sequence number determines the order of the lookup and permits heavily used prefixes. Prefix lists filtering is easier to use and is more efficient than access lists.

Use the following commands to add prefix lists:

```
add bgp prefix-list <list-name>
      seq-no <value> action <permit | deny>
      any prefix <value>
```

Use the following commands to delete prefix lists:

```
delete bgp prefix-list <all-unused |name <value> [seq-no <value>] >
```

Creating Access- Lists on the Nokia IP45 Security Platform

Access lists are filters that enable you to restrict the routing information a router advertises to a neighbor. BGP uses address-based access lists.

Use the following commands to configure access lists:

```
add bgp access-list <list-name>
      action < permit | deny >
      any prefix <value>
```

Use the following commands to delete access lists:

```
delete bgp access-list all-unused | name <value>
```

Creating Route Maps on the Nokia IP45 Security Platform

Route maps are used to control distribution of routing updates. Route maps consist of a list of *match* and *set* commands. The *match* commands specify match criteria and the *set* commands specify the action to be taken if match criteria are met. Only those routes that pass through the route-map (inbound route maps) are accepted or forwarded (outbound routes).

Use the following commands to add route-maps:.

```
add bgp route-map name <map-name>
      action <permit | deny> seq-no <value>
      match <ip-address <value> | ip-next-hop <value> |
        metric <value> |>
      set ip-next-hop <value ip_address>
      local-preference <value>
      weight <value>
      metric <value>
      as-path-prepend <value>
```

Use the following commands to delete route-maps:

```
delete bgp route-map <all-unused | name <value> [seq-no <value>]>
```

Configuring Routing Policies on the Nokia IP45 Security Platform

Routing policies for a remote peer include all of the configurations such as route-map, distribute list, prefix-list, and filter-list that might affect inbound or outbound routing table updates.

Use the following commands to configure the routing policies for the created BGP Peer:

```
set bgp neighbor <value ip_address>
     dont-capability negotiate <on | off>
     ebgp-multihop <on | off>
     keepalive <value> holdtime <value>
     maximum-prefix <value <value> [warning-only <on | off>|] off>
     next-hop-self <on | off>
     no-shutdown
     passive <on | off >
     peer-group < value <value> | off >
     port < value <value> | off>
     prefix-list <value> direction <in |out | both> state <on | off>
     route-map <value> direction <in |out | both> state <on | off>
     route-reflector-client <on | off>
     update-source <value> state <on | off>
     weight <value <value>| off>
     shutdown
     distribute-list <value> direction <in |out | both> state <on |
      off>
```

Configuring a Remote BGP Peer with MD5 Authentication

You can invoke MD5 authentication with a remote BGP peer such that each segment sent on the TCP connection between the peers is verified. This feature must be configured with the same password on both BGP peers or the connection between them is not established. The authentication feature uses the MD5 algorithm. Invocation of this feature enables Nokia IP45 to generate and check the MD5 digest of every segment sent on the TCP connection. If authentication is invoked and a segment fails authentication, a message appears on the console.

Note
MD5 authentication with remote BGP peer is implemented external to the BGP routing process on Nokia IP45. This authentication mechanism has stronger coupling with VPN modules. Therefore, this feature is not supported for clear text BGP updates.

Use the following commands to configure BGP remote peers:

```
add bgp remote-peer <value ip_address>
      vpn-peer <value ip_address>
      priority <normal | high>
      [gateway <value>
       password <value>]
```

Configuring a Local Loopback Interface

Loopback interfaces enable your BGP connection to stay connected to the interface used to reach the neighbor. Configure this loopback interface IP address as the source address for the BGP process to communicate with a remote BGP peer.

Use the following commands to configure loopback interface:

```
set interface loopback id <value> address <value> mask-length <value>
```

Use the following commands to view a loopback interface:

```
show interface loopback <all | id <value>>
```

Use the following commands to delete a loopback interface:

```
delete interface loopback id <value>
```

Configuring Criteria for Path Selection

A VPN tunnel established with the given VPN peer is assumed to be disconnected or unavailable if the corresponding BGP peer is unreachable.

HA enforces the primary Internet connection as the path for each high priority BGP peer and its associated VPN peer by inserting static routes towards primary Internet connection. This ensures continuous status monitoring of high priority BGP peers.

Use the following command to configure a remote-peer:

```
add bgp remote-peer <value ip_address>
      vpn-peer <value ip_address>
      priority <normal | high>
      [gateway <value>
        password <value>]
```

Use the following command to delete a remote peer:

```
delete bgp remote-peer <value-ip_address>
```

High-Availability Options

The following are the high-availability options available with the Nokia IP45 device.

- **Generic**—device monitors WAN link and decides on failover and fallback, based on the synchronization interface and interface tracking feature.

  This is used in dual device HA, and is independent of BGP. For more information, see "Generic High-Availability" on page 219.

- The following are the options available for advanced high-availability solution.
  - **dialup**—used in *Single Device HA*. This mode is useful if device has dial-up as primary Internet connection with multiple dial-up profiles. In this mode, device uses dial-up profiles for fail over. If the BGP peer becomes unreachable using one profile, the device automatically switches to the next dial-up profile. This process continues in round-robin fashion until the BGP peer becomes reachable.
  - **secondary**—used in *Single Device HA*. This mode is useful if the device has LAN/PPPOE/PPTP/DHCP/ as primary Internet connection and *dial-up* as secondary Internet connection (optionally with multiple profiles). In this mode, device fails over to

secondary Internet connection (dial-up) if all high priority BGP peers become unreachable. It continues to monitor the status of high priority BGP peers and falls back to primary Internet connection if any one high priority BGP peer becomes reachable. It drops the dial-up connection when device falls back to primary Internet connection.

- **BGP**—this mode is useful if device has LAN/PPPOE/PPTP/DHCP as primary Internet connection and has no dial-up connection. Primary device of the dual device HA scenario is configured to operate in this mode. In this scenario, you have another device acting as *backup*. The backup device can have either dial-up or LAN/PPPOE/PPTP/DHCP for Internet connection. primary and backup devices establish internal BGP (IBGP) session with each other. The fail-over automatically takes place in the primary device based on the availability of CO routes. (external or internal BGP (EBGP or IBGP)).
- **BGP-external**—this mode is useful if the device has LAN/PPPOE/PPTO/DHCP as primary Internet connection and DMZ as secondary Internet connection. In this mode, DMZ is assumed to be secure and the traffic passing through DMZ will not be encrypted. So, DMZ can be connected to an external VPN device or a router connected to frame relay network. In this mode, the IP45 uses DMZ as backup to the primary Internet connection. The traffic is tunneled as long as BGP peer is reachable over VPN through primary Internet connection. As soon as the BGP peer becomes unreachable, the traffic goes in plain text through DMZ interface. Similar to the other modes, device continues to monitor the status of high priority BGP peers and falls back to primary Internet connection if at least one high priority BGP peer becomes reachable.

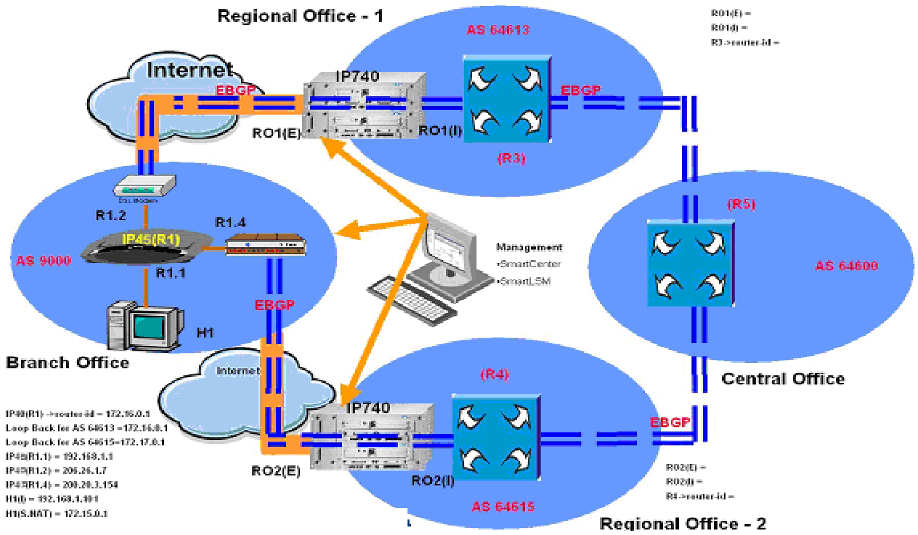
  HA triggers VPN tunnels associated with normal priority BGP peers if it finds all of the high priority BGP peers, unreachable. HA continues to monitor the status of high priority peers and drops the tunnels associated with lower priority BGP peers as soon as at least one of the high-priority BGP peers becomes reachable.
- **none**—no high availability.

High-Availability Solutions

Nokia IP45 v4.0 supports the following high-availability solutions using single and dual IP45 devices.

High-Availability Solutions with a Single Nokia IP45 Device

Figure 8 Single Device HA



In this scenario, the branch office is always securely connected to the central office on the Internet with a single Nokia IP45 device by using DSL or cable connection or dial-up as backup. The Nokia IP45 (R1) connects to the RO1 and establishes VPN connection on DSL (preferred connection). The Nokia IP45 (R1) and BGP peer (R3) located in RO1 establishes a BGP connection over VPN. If this BGP session fails because of any service interruption, dial-up is activated. The Nokia IP45 (R1) connects to RO2 and establishes a VPN connection. R1, and the BGP peer (R4) located in RO2 establish a BGP connection over VPN, and the traffic from the branch office flows through this alternative path. As soon as the IP45 (R1) detects the established BGP session on the DSL connection, the dial-up connection to RO2 is discontinued.

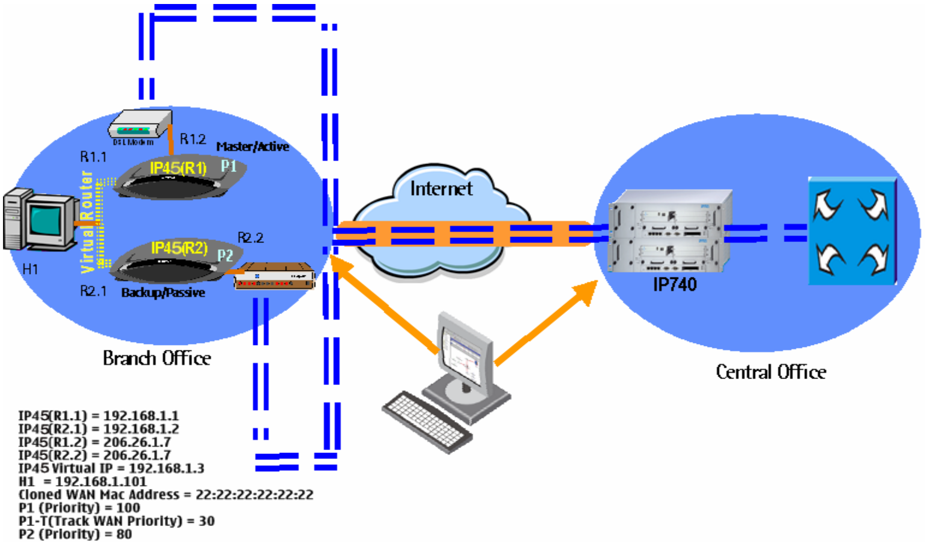
High-Availability Solutions with Dual Nokia IP45 Devices

High-availability solution by using Nokia IP45 can be achieved by the following two methods:

- Generic HA
- HA coupled with BGP (advanced HA solution)

Generic HA

Figure 9 Generic HA Solution - Dual Nokia IP45 devices

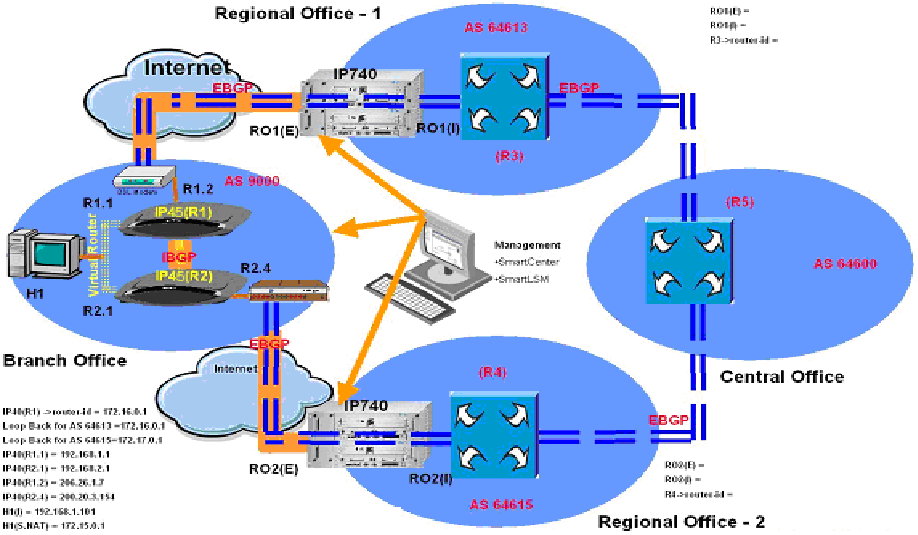


IP45(R1.1) = 192.168.1.1
IP45(R2.1) = 192.168.1.2
IP45(R1.2) = 206.26.1.7
IP45(R2.2) = 206.26.1.7
IP45 Virtual IP = 192.168.1.3
H1 = 192.168.1.101
Cloned WAN Mac Address = 22:22:22:22:22:22
P1 (Priority) = 100
P1-T(Track WAN Priority) = 30
P2 (Priority) = 80

This scenario supplements the single device HA solution to cater to device failures coupled with WAN link failures. In the illustration shown below, IP45 devices in an HA cluster are configured with same WAN IP address. WAN high-availability is enabled in the backup device, which means that backup device establishes connection to Internet only when WAN link for the master device fails. When an IP45 device (R1) fails to connect to the Internet, R2 takes over as master and starts forwarding internal traffic to central office through the VPN tunnel. As soon as R1 becomes active again, the WAN connectivity through R2 is discontinued and R1 becomes the master.

HA Coupled With BGP

Figure 10 HA Solution Coupled with BGP



This scenario supplements the single device HA solution cater to device failures at branch office coupled with dedicated link between the Nokia IP45 security platforms on DMZ ports and internal BGP to synchronize the route updates from central office on both the devices. The dedicated links between both the Nokia IP45 devices is secured with IPSec VPN.

Nokia IP45 (R1) acts as the default virtual router for the branch office network, and is connected to RO1 by using DSL or a cable connection (preferred path). If any service interruption occurs in the R1 LAN, Nokia IP45 (R2) takes over as the default virtual router and forwards the branch office traffic on the DMZ to RO1 securely. If the IP45 (R1) device fails, R2 becomes master and dial-up is activated. Now R2 connects to RO2 and establishes a VPN connection. R2,and the BGP peer (R4) located in RO2 establish a BGP connection over VPN, and the traffic from branch office flows through this alternative path. As soon as IP45 (R1) detects the established BGP session on the DSL connection, the dial-up connection to RO2 on R2 is discontinued.

12 Configuring Nokia IP45 Through Out-of-Band Management

This chapter explains how to configure the Nokia IP45 security platform using out-of-band management (OOB) and includes the following topics:

- Configuring OOB from the Nokia IP45 Security Platform GUI
- Secure Shell and HTTPS Access Through Out-of-Band Dial-In
- Remote Configuration Mode in the Nokia IP45 Security Platform

Overview

The Nokia IP45 security platform supports remote management by using Out-Of-Band management (OOB), where the IP45 device acts as a remote access server (RAS) and waits for the incoming call. To use OOB, connect a modem to the AUX port of your device with dial-up Internet connection.

Out Of Band management is useful in the cases where you cannot connect to your device locally by using either LAN, WAN or DMZ ports. In these cases, you can use OOB to connect the device for normal operations. Nokia IP45 supports ISDN terminal adaptor or analog modems for modem dial-in.

You can dial into the device using a dial-up Internet connection, and use HTTPS, SSH, and SNMP protocols to configure or monitor the device. By default, OOB is enabled (factory defaults) in the IP45 security platform.

To connect a modem to the Nokia IP45 security platform

1. Connect a modem to the AUX port of your IP45 device.
2. Dial in to the device from a computer that is configured with the dial-up connection.
3. Use the username and password already defined to log in.

Configuring OOB from the Nokia IP45 Security Platform GUI

Configure the modem settings from the IP45 GUI before you use the OOB feature.

To configure the modem settings from the IP45 security platform GUI

1. Choose Network from the main menu.

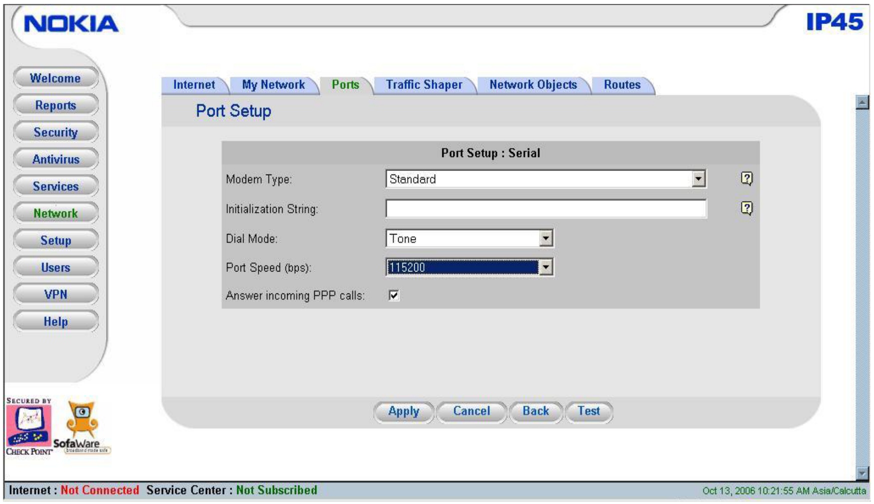
   The Internet page opens.

2. Click the Ports tab.

   The Ports page opens.

3. Click Setup next to Serial.

   The Port Setup page opens.



Port Setup : Serial

Modem Type: Standard

Initialization String:

Dial Mode: Tone

Port Speed (bps): 115200

Answer incoming PPP calls: ☑

Internet : Not Connected Service Center : Not Subscribed

Oct 13, 2006 10:21:55 AM Asia/Calcutta

4. Select Standard from the Modem Type drop-down list.

Note
To select a Custom Modem, use the command-line interface. This option is not supported in GUI.

5. Enter a suitable string next to Initialization String.This string is used to access additional modem features.

   For example, to disable the modem speakers, enter the initialization string ATM 0.

Note
To find the suitable init string, see the user manual of your modem.

6. Select Tone or Pulse from the Dial Mode drop-down list.

7. Select the port speed in bps from the Port Speed drop-down list.

   This speed defines the modem port speed. The values can be 9600, 19200, 38400, 57600, 115200, 230400, or 460800 bps.

8. Check Answer incoming PPP calls, to answer the incoming PPP calls.
9. Click Apply to save your modem settings.
10. Click Test to verify whether your modem settings are working.

Note
You cannot configure all of the OOB parameters from the IP45 GUI. The parameters that cannot be configured from the GUI, such as the address of the OOB interface, destination address of the OOB interface, and set IP header compression, have default values. You can only use the CLI to change these values.

Secure Shell and HTTPS Access Through Out-of-Band Dial-In

You can access and configure the Nokia IP45 security platform by using SSH or HTTPS. When you dial in to Nokia IP45 from a modem (see "To connect a modem to the Nokia IP45 security platform" on page 233 for details), you can establish a normal SSH or HTTPS session.

For details on using the Secure Shell, see "Telnet Access" on page 201, and for details on using HTTPS see "Enabling HTTPS Web Access" on page 206.

Note
Allow SSH and HTTPS access on Nokia IP45 before you establish the sessions from OOB dial-in. For more details, see "Configuring Virtual Servers" on page 149.

Remote Configuration Mode in the Nokia IP45 Security Platform

You can use remote configuration mode to configure and manage your IP45 security platform from a remote location. In this mode, firewall allows access to SSH/HTTPS from OOB for a time period of 30 minutes, irrespective of the current firewall filters.

To boot your Nokia IP45 in Remote Configuration Mode, hold the Reset button and connect the power to the device. The default username and password for OOB are *admin* and *password* respectively, if the first time password is not set

In this mode, the device is set to factory defaults.

13 Configuring Device Functions

This chapter describes how to configure common device functions such as setting the host name, configuring the date and time, and system logging. The chapter also discusses how to load the factory default configuration, perform a firmware upgrade, and upgrade the product key and covers the following topics:

- Host Name Configuration by Using the CLI
- Date and Time Configuration
- System Logging Configuration
- Exporting the Configuration
- Upgrading Firmware
- Resetting the Nokia IP45 Security Platform to Factory Defaults

Host Name Configuration by Using the CLI

Use the following commands to view or change your platform host name:

```
show hostname
```

```
set hostname name
```

For more information on setting the host name, see *the Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

Date and Time Configuration

For information on setting the date and time, see "Setting the Nokia IP45 Security Platform Time" on page 52.

For advanced date and time configuration using the NTP server, see the *Nokia IP45 Security Platform CLI Reference Guide, Version 4.0.*

System Logging Configuration

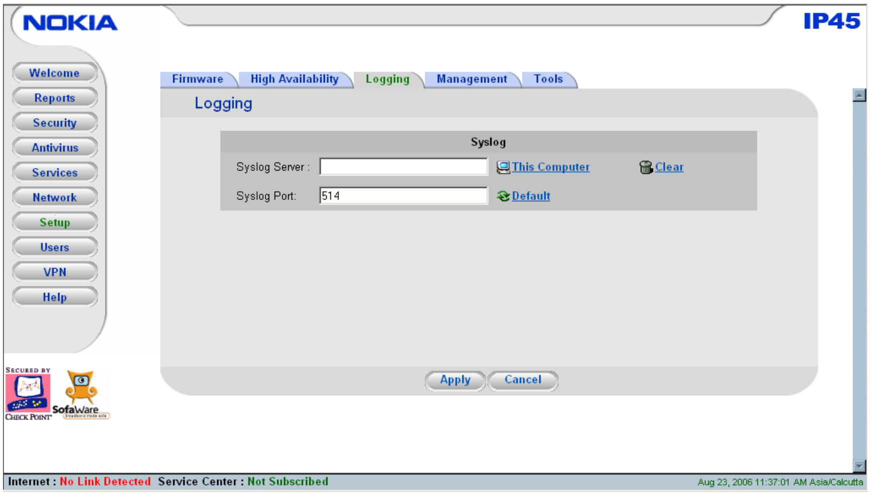
You can configure the Nokia IP45 security platform to send event logs to a syslog server that resides in your internal network or on the Internet. The logs store the event details like the date and the time as they occur. If the event is a communication attempt that was rejected by the firewall, the event details include the source and destination IP address, the destination port, and the protocol used for the communication attempt (for example, TCP or UDP).

Nokia IP45 supports local event logging, which you can view from Reports > Event Log. Up to 100 events can be logged here. You can also configure an external syslog server by using the following method.

To configure an external syslog server

1. Choose Setup from the main menu, and select the Logging tab.

   The Logging page opens.



Logging

Syslog

Syslog Server :

Syslog Port: 514

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 11:37:01 AM Asia/Calcutta

2. Enter the IP address for the syslog server in the Syslog Server field.
3. To enter the IP address of your computer, click *This Computer*.

Note
The syslog server can run either on a computer outside your network, or on a computer inside your IP45 network.

4. Specify the port number where the syslog server should run. The default port number is 514.
5. Click Apply.

Setting the Syslog Server by Using the CLI

Use the following commands to set the syslog server by using the CLI:

```
set syslog
     address - Syslog server address
     port    - Syslog server port
```

For more information about how to set the syslog server, see the *Nokia* IP45 *Security Platform CLI Reference Guide, Version 4.0.*

Network Utilities

You can use the following network utilities from the IP45 security platform GUI:

- Ping
- Traceroute
- WHOIS

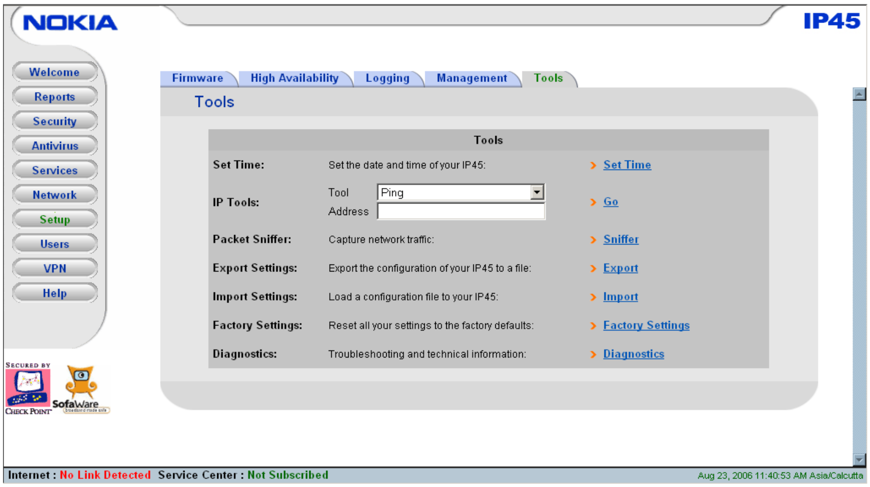
In addition to the above utilities, you can also use the following utilities by using the command *exec:*

- arp
- netstat
- nslookup
- ping
- tcpdump
- traceroute

To use the network utilities from the Nokia IP45 GUI

1. Choose Setup from the main menu, and select the Tools tab.

   The Tools page opens.



Tools

Tools		
Set Time:	Set the date and time of your IP45:	> Set Time
IP Tools:	Tool Ping Address	> Go
Packet Sniffer:	Capture network traffic:	> Sniffer
Export Settings:	Export the configuration of your IP45 to a file:	> Export
Import Settings:	Load a configuration file to your IP45:	> Import
Factory Settings:	Reset all your settings to the factory defaults:	> Factory Settings
Diagnostics:	Troubleshooting and technical information:	> Diagnostics

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 11:40:53 AM Asia/Calcutta

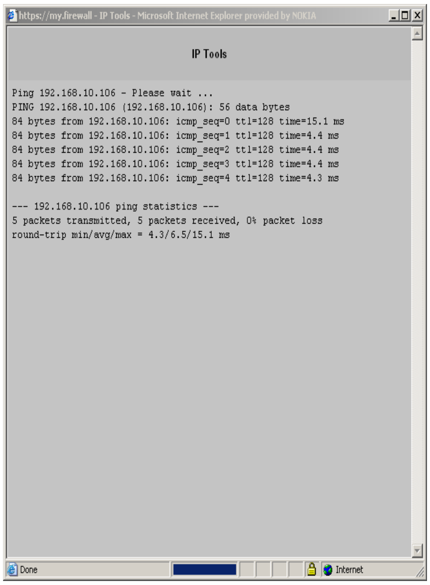
2. Select either ping, traceroute, or WHOIS from the IP Tools drop-down list, depending on the tool you want to use.

3. Enter the IP address in the Address field.

   Click Go on the right.

4. The IP Tools window opens, providing the statistics of the network.

   The following window is an example of ping tool usage.


https://my.firewall - IP Tools - Microsoft Internet Explorer provided by NOKIA
Done
Internet

IP Tools

```
Ping 192.168.10.106 - Please wait ...
PING 192.168.10.106 (192.168.10.106): 56 data bytes
84 bytes from 192.168.10.106: icmp_seq=0 ttl=128 time=15.1 ms
84 bytes from 192.168.10.106: icmp_seq=1 ttl=128 time=4.4 ms
84 bytes from 192.168.10.106: icmp_seq=2 ttl=128 time=4.4 ms
84 bytes from 192.168.10.106: icmp_seq=3 ttl=128 time=4.4 ms
84 bytes from 192.168.10.106: icmp_seq=4 ttl=128 time=4.3 ms

--- 192.168.10.106 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.3/6.5/15.1 ms
```

Managing the Configuration

You can export or import the existing configuration of your Nokia IP45 security platform.

This procedure is useful to upgrade the firmware of your device without losing the current configuration. You can also use this feature when the device is accidentally misconfigured, and the original configuration needs to be restored.

To backup and restore the settings, you can use the configuration file (*.cfg), which includes all the IP45 settings.

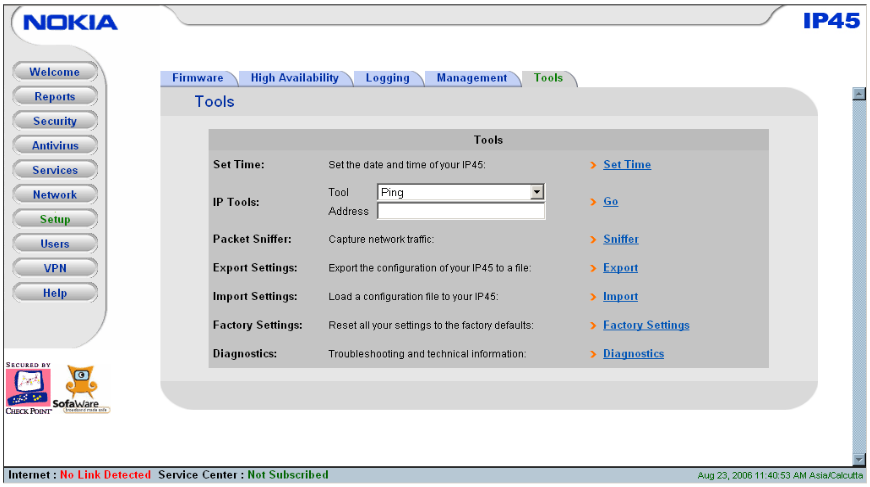
Exporting the Configuration

You can export the Nokia IP45 security platform configuration to a *.cfg file, and use this file to back up and restore IP45 settings, as needed.The configuration file includes all of your settings.

To export the configuration

1. Choose Setup from the main menu, and click the Tools tab.

   The Tools page opens.



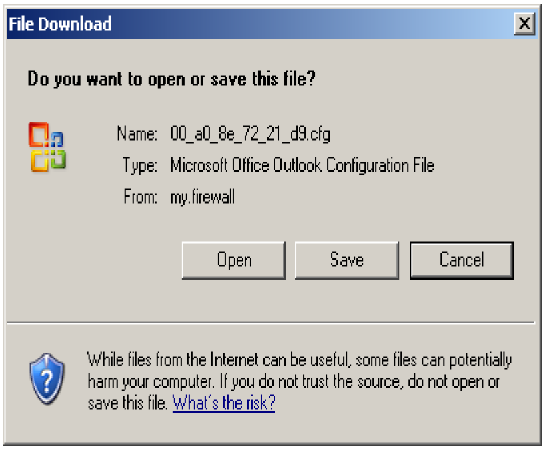
Tools

Tools		
Set Time:	Set the date and time of your IP45:	> Set Time
IP Tools:	Tool Ping Address	> Go
Packet Sniffer:	Capture network traffic:	> Sniffer
Export Settings:	Export the configuration of your IP45 to a file:	> Export
Import Settings:	Load a configuration file to your IP45:	> Import
Factory Settings:	Reset all your settings to the factory defaults:	> Factory Settings
Diagnostics:	Troubleshooting and technical information:	> Diagnostics

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 11:40:53 AM Asia/Calcutta

2. Click Export.

A standard File Download dialog box appears.



File Download

Do you want to open or save this file?

Name: 00_a0_8e_72_21_d9.cfg

Type: Microsoft Office Outlook Configuration File

From: my.firewall

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

3. Click Save, to save this file to disk.

   The Save As dialog box appears.

4. In the Save As dialog box, Click Browse to select a destination directoryof your choice.

5. Type a name for the configuration file and click Save.

   The *.cfg configuration file is created and saved to the specified directory.

Importing the Configuration

To restore the configuration of your device from a configuration file, you must import the file:

Note
While importing a configuration file in the local portal, the portal displays the result of each command, executed. From this, you can analyze the errors that might occur while processing the configuration file.

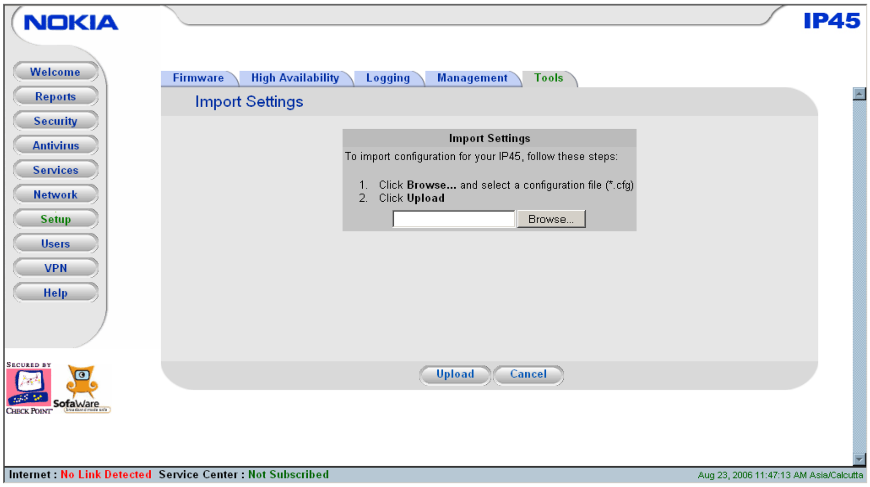
To import the configuration

1. Choose Setup in the main menu, and click the Tools tab.

   The Tools page opens.

2. Click Import.

The Import Settings page opens.



Import Settings

Import Settings

To import configuration for your IP45, follow these steps:

1. Click **Browse...** and select a configuration file (*.cfg)
2. Click **Upload**

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 11:47:13 AM Asia/Calcutta

3. Do one of the following:

- In the Import Settings field, type the full path to the configuration file.

or

- Click Browse to select the configuration file.

4. Click Upload.

A Confirmation message appears.

5. Click OK.

The IP45 settings are imported.

A success message appears.

6. Click OK.

Note
You can use the HTTP, TFTP, FTP, SCP protocols through the IP45 CLI for configuration export and import. For additional information, see the *Nokia IP45 Security Platform CLI Reference Guide, Version 4.0.*

Upgrading Firmware

You can upgrade the Nokia IP45 security platform to a new firmware version of the product. If you are subscribed to Software Updates, firmware updates are performed automatically. These updates include new product features and protection against new security threats.

If you are not subscribed to the Software Updates service, you must update your firmware manually.

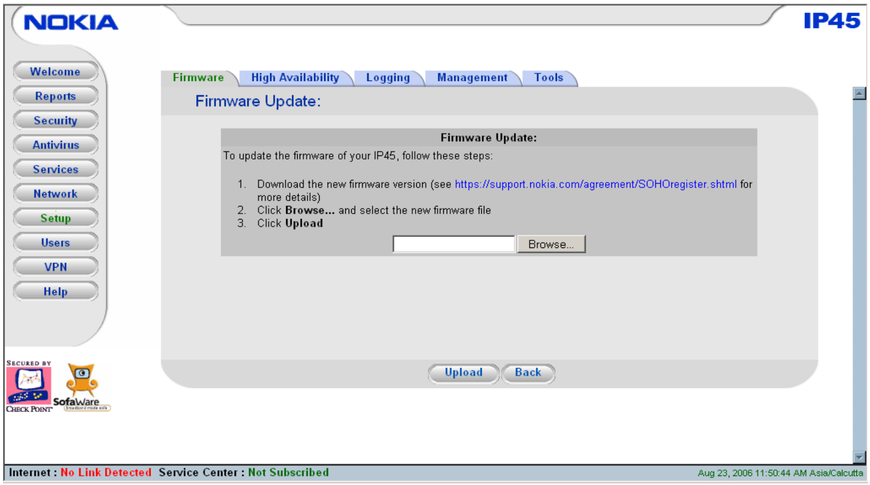
To update firmware manually

1. Choose Setup from the main menu.

   The Firmware page opens.

2. Click Firmware Update.

   The Firmware Update page opens.



Firmware Update:

Firmware Update:

To update the firmware of your IP45, follow these steps:

1. Download the new firmware version (see https://support.nokia.com/agreement/SOHOregister.shtml for more details)
2. Click **Browse...** and select the new firmware file
3. Click **Upload**

Internet : No Link Detected Service Center : Not Subscribed

Aug 23, 2006 11:50:44 AM Asia/Calcutta

3. Click Browse.

   A browse window opens.

4. Select the firmware file that you purchased.
5. Click Upload.
6. The IP45 firmware is updated.This might take one minute approximately.

   When the update is complete, the IP45 restarts automatically.

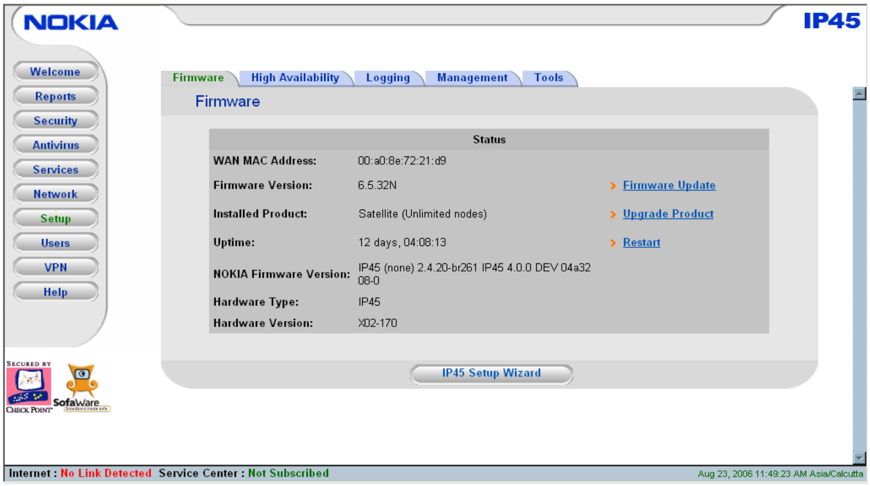
Installing your Product Key

The Nokia IP45 security platform is identified by the product key that is obtained when you purchase the device. You can purchase and upgrade to any of the other versions of the IP45.

To install a product key

1. Choose Setup from the main menu.

   The Firmware page opens.



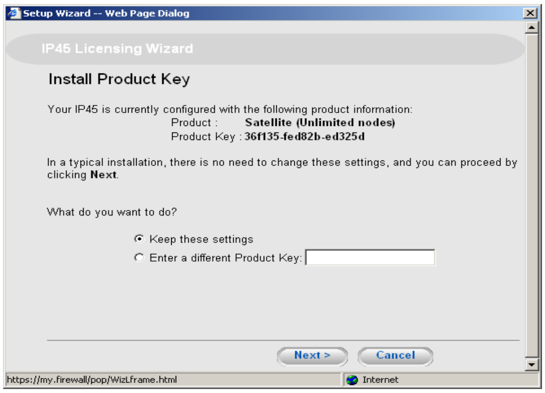
Firmware

Status		
WAN MAC Address:	00:a0:8e:72:21:d9	
Firmware Version:	6.5.32N	› Firmware Update
Installed Product:	Satellite (Unlimited nodes)	› Upgrade Product
Uptime:	12 days, 04:08:13	› Restart
NOKIA Firmware Version:	IP45 (none) 2.4.20-br261 IP45 4.0.0 DEV 04a32 08-0	
Hardware Type:	IP45	
Hardware Version:	X02-170	

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 11:49:23 AM Asia/Calcutta

2. Click Upgrade Product.

   The Setup wizard opens, displaying the Install Product Key window.


Setup Wizard -- Web Page Dialog
IP45 Licensing Wizard
Next >
Cancel
https://my.firewall/pop/WizLframe.html
Internet

Install Product Key

Your IP45 is currently configured with the following product information:
Product : **Satellite (Unlimited nodes)**
Product Key : **36f135-fed82b-ed325d**

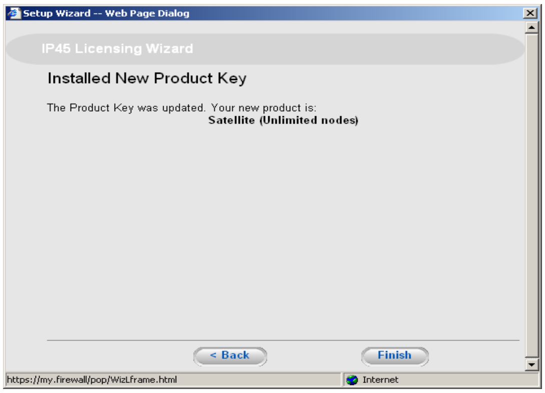
In a typical installation, there is no need to change these settings, and you can proceed by clicking **Next**.

What do you want to do?

● Keep these settings
○ Enter a different Product Key:

3. To retain the existing settings, click *Keep these settings*.
4. To enter a new product key, click *Enter a different Product Key.*
5. Type the new value.
6. Click Next.

The Installed New Product Key window opens.



Setup Wizard -- Web Page Dialog
IP45 Licensing Wizard

Installed New Product Key

The Product Key was updated. Your new product is:
Satellite (Unlimited nodes)

< Back
Finish
https://my.firewall/pop/WizLframe.html
Internet

7. To register your IP45, check I want to register my product.
8. Click Next.

   A new browser window opens with https://support.nokia.com/agreement/SOHOregister.html.
9. Click Finish.

   The IP45 restarts and the Welcome page opens.

Dynamic DNS

The Nokia IP45 security platform supports the use of a domain name without requiring a permanent IP address on the Internet. This is useful for Nokia Horizon Manager to locate the IP45 devices that it manages by the host names that are used at remote office and branch offices.

The Dynamic Domain Name Server (DDNS) feature on the Nokia IP45 updates the ISP-provided IP address to the DNS located at the headquarters. The DDNS feature works with DNS supporting BIND-8.2.x, BIND-9.x, and Windows DNS.

Configuring DDNS

You can configure DDNS through the CLI.

Note
Before you configure DDNS, make sure DNS is configured.

Use the following command to configure DDNS:

```
set ddns <server | client >
```

Use the following command to add DDNS:

```
add ddns server <ip address>
```

For more information about DDNS commands, see the *Nokia IP45 Security Platform CLI Reference Guide, Version 4.0.*

Resetting the Nokia IP45 Security Platform to Factory Defaults

You can reset the Nokia IP45 to its default settings. When you reset the IP45, it reverts to the state it was originally in when you purchased it, and your firmware reverts to the version that was shipped with the device.

Caution
Resetting to factory defaults deletes all of your settings and password information. You must set a new password and reconfigure your IP45 for Internet connection.

You can reset the IP45 device to defaults through the Web management interface (software) or by manually pressing the Reset button (hardware) located at the rear end of the device.

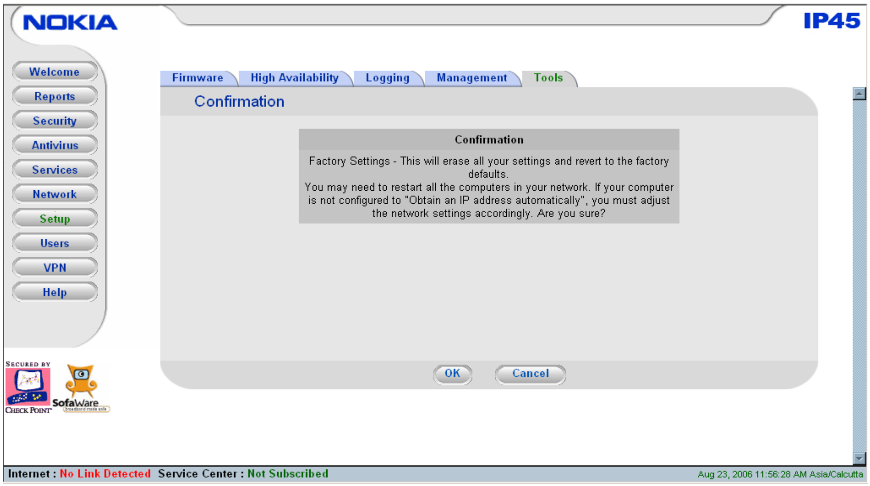
To reset the IP45 security platform to factory defaults through the Web interface

1. Choose Setup from the IP45 main menu, and click the Tools tab.

   The Tools page opens.

2. Click Factory Settings.

   A confirmation message appears.



Confirmation

Confirmation

Factory Settings - This will erase all your settings and revert to the factory defaults.
You may need to restart all the computers in your network. If your computer is not configured to "Obtain an IP address automatically", you must adjust the network settings accordingly. Are you sure?

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 11:56:28 AM Asia/Calcutta

3. Click OK.

- The *Please Wait* page opens.
- The IP45 returns to its factory defaults.
- The IP45 restarts.

  This can take up approximately a minute.
- The Login page reappears.

Note
Since the network settings change, you cannot access the device immediately. Release, and renew the IP address by running the Refresh IP tool located in the tools folder on the CDROM, and then access the IP45 GUI portal.

Resetting the Nokia IP45 Security Platform by Using the Reset Button

The Restore Defaults button is inside a hole on the back panel of the IP45 device. To press this button, use a large flat-tipped object, such as a thick paper clip. Pressing the Restore Defaults button for seven seconds restores all the IP45 settings back to factory defaults. The button works only after booting is complete, and the green light must be illuminated to activate the button.

The status light goes off while defaults are being restored, and relights after defaults are restored and the IP45 begins to reboot. It takes over two minutes approximately to restore defaults. An Amber light is displayed while rebooting. Until the first-time login and password are set, the green light blinks. A blinking green states that the device is set to factory defaults.

Note
You can also reset the IP45 device to factory defaults by using the GUI, or the CLI, and remote config mode.

Restarting the Nokia IP45 Security Platform by Using the GUI

The following procedure describes about how to restart your IP45 security platform.

To restart your Nokia IP45 security platform

1. Choose Setup from the main menu.

   The Firmware page opens.
2. On the Firmware page, click the Restart tab.

   A confirmation message appears.
3. Click OK.

14 Viewing Reports

This chapter provides an overview of the reports that you can view from the Nokia IP45 security platform GUI, and the procedure involved in viewing them and includes the following topics:

- Viewing the Event Log
- Viewing Active Computers
- Viewing Connections
- Viewing the Diagnostics Summary
- Viewing the Traffic Monitor

Viewing Reports on the Nokia IP45 Security Platform

You can view the following reports on the IP45 GUI:

- Event log
- Active computers
- Active connections
- VPN tunnels

Viewing the Event Log

You can track network activity by using the event log. The event log displays the last 100 events in the following categories:

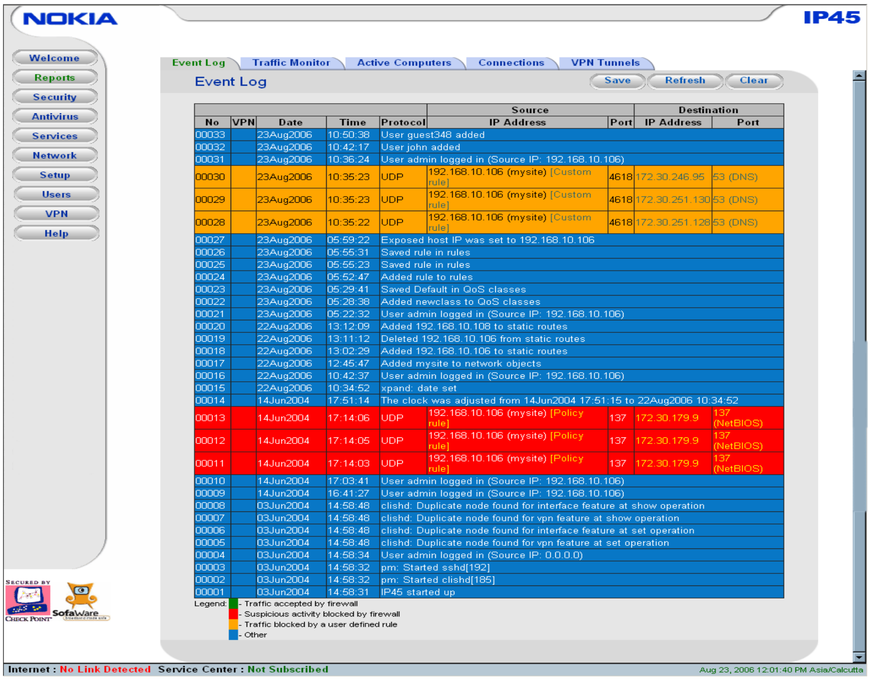
- Events highlighted in Green indicate the traffic accepted by the firewall.
- Events highlighted in Blue indicate changes in your setup that you made or that are the result of a security update implemented by your service center.
- Events highlighted in Red indicate connection attempts that your firewall blocked.
- Events highlighted in Orange indicate connection attempts that your custom security rules blocked.

The logs detail the date and time of the events as they occur, and their type. If the event is a communication attempt that was rejected by the firewall, the event details include the source and destination IP address, the destination port, and the protocol used (TCP, UDP, and so on) for the communication attempt.

To view the event log

1. Choose Reports from the IP45 main menu.

   The Event Log page opens.



					Source		Destination	
No	VPN	Date	Time	Protocol	IP Address	Port	IP Address	Port
00033		23Aug2006	10:50:38	User guest348 added				
00032		23Aug2006	10:42:17	User john added				
00031		23Aug2006	10:36:24	User admin logged in (Source IP: 192.168.10.106)				
00030		23Aug2006	10:35:23	UDP	192.168.10.106 (mysite) [Custom rule]	4618	172.30.246.95	53 (DNS)
00029		23Aug2006	10:35:23	UDP	192.168.10.106 (mysite) [Custom rule]	4618	172.30.251.130	53 (DNS)
00028		23Aug2006	10:35:22	UDP	192.168.10.106 (mysite) [Custom rule]	4618	172.30.251.128	53 (DNS)
00027		23Aug2006	05:59:22	Exposed host IP was set to 192.168.10.106				
00026		23Aug2006	05:55:31	Saved rule in rules				
00025		23Aug2006	05:55:23	Saved rule in rules				
00024		23Aug2006	05:52:47	Added rule to rules				
00023		23Aug2006	05:29:41	Saved Default in QoS classes				
00022		23Aug2006	05:28:38	Added newclass to QoS classes				
00021		23Aug2006	05:22:32	User admin logged in (Source IP: 192.168.10.106)				
00020		22Aug2006	13:12:09	Added 192.168.10.108 to static routes				
00019		22Aug2006	13:11:12	Deleted 192.168.10.106 from static routes				
00018		22Aug2006	13:02:29	Added 192.168.10.106 to static routes				
00017		22Aug2006	12:45:47	Added mysite to network objects				
00016		22Aug2006	10:42:37	User admin logged in (Source IP: 192.168.10.106)				
00015		22Aug2006	10:34:52	xpand: date set				
00014		14Jun2004	17:51:14	The clock was adjusted from 14Jun2004 17:51:15 to 22Aug2006 10:34:52				
00013		14Jun2004	17:14:06	UDP	192.168.10.106 (mysite) [Policy rule]	137	172.30.179.9	137 (NetBIOS)
00012		14Jun2004	17:14:05	UDP	192.168.10.106 (mysite) [Policy rule]	137	172.30.179.9	137 (NetBIOS)
00011		14Jun2004	17:14:03	UDP	192.168.10.106 (mysite) [Policy rule]	137	172.30.179.9	137 (NetBIOS)
00010		14Jun2004	17:03:41	User admin logged in (Source IP: 192.168.10.106)				
00009		14Jun2004	16:41:27	User admin logged in (Source IP: 192.168.10.106)				
00008		03Jun2004	14:58:48	clishd: Duplicate node found for interface feature at show operation				
00007		03Jun2004	14:58:48	clishd: Duplicate node found for vpn feature at show operation				
00006		03Jun2004	14:58:48	clishd: Duplicate node found for interface feature at set operation				
00005		03Jun2004	14:58:48	clishd: Duplicate node found for vpn feature at set operation				
00004		03Jun2004	14:58:34	User admin logged in (Source IP: 0.0.0.0)				
00003		03Jun2004	14:58:32	pm: Started sshd[192]				
00002		03Jun2004	14:58:32	pm: Started clishd[185]				
00001		03Jun2004	14:58:31	IP45 started up				

Legend: 🟩 - Traffic accepted by firewall
🟥 - Suspicious activity blocked by firewall
🟧 - Traffic blocked by a user defined rule
🟦 - Other

2. Do any of the following:

   - Click Save to save the Event Log.
   - Click Refresh to refresh the display.
   - Click Clear to clear all events.
   - If an event is highlighted in red, indicating a blocked attack on your network, you can view the attacker's details by clicking the IP address of the attacking computer.

Nokia IP45 queries the Internet WHOIS server, and a window displays the name of the entity to whom the IP address is registered and their contact information. This information is useful in tracking down external attacks.

Viewing the Traffic Monitor

Nokia IP45 v4.0 supports traffic monitoring tool, which the administrator can use to identify the trends and anomalies in the network and fine tune the QoS class assignments.

The network patterns are displayed in graphical representation using the legend as described in the following sections Color legend:

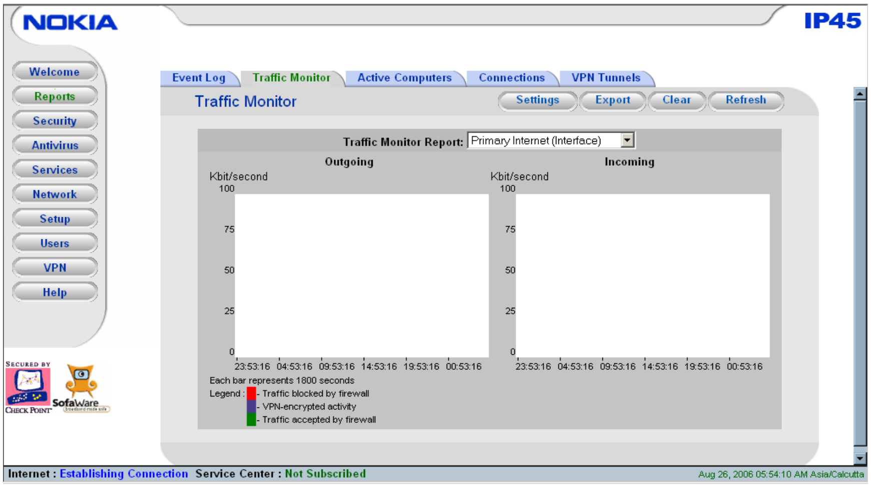
- **Red**—traffic (suspicious activity) blocked by firewall
- **Blue**—VPN encrypted activity (other)

- **Green**—traffic accepted by firewall

To view the traffic monitor

1. Choose Reports from the main menu and click Traffic Monitor.

   The Traffic Monitor page opens.



Traffic Monitor

Traffic Monitor Report: Primary Internet (Interface)

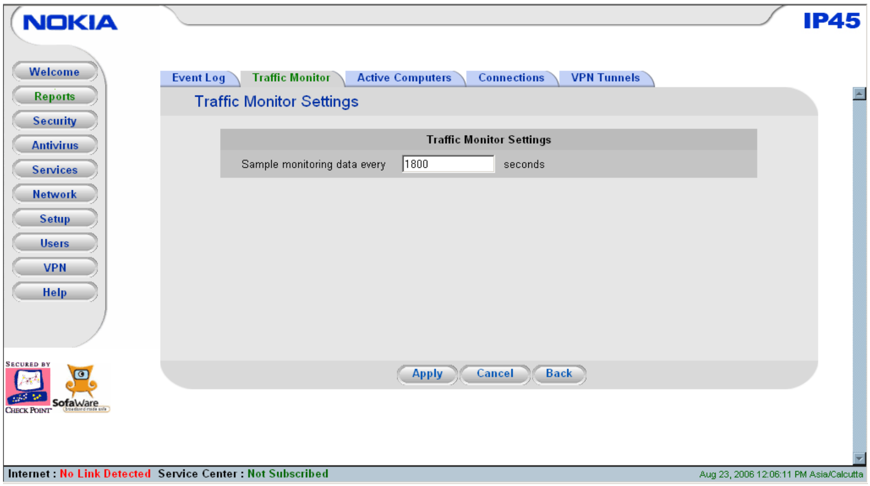
Each bar represents 1800 seconds

Legend : 🟥 - Traffic blocked by firewall
🟦 - VPN-encrypted activity
🟩 - Traffic accepted by firewall

Internet : Establishing Connection Service Center : Not Subscribed Aug 26, 2006 05:54:10 AM Asia/Calcutta

2. To view the traffic monitor report, select the interface from the drop-down list.
3. To set the monitoring time, Click Settings.

   The Traffic Monitor Settings page opens.



Traffic Monitor Settings

Traffic Monitor Settings

Sample monitoring data every 1800 seconds

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 12:06:11 PM Asia/Calcutta

4. Enter the time in the Sample monitoring data every text box.
5. Click Apply.

Viewing Active Computers

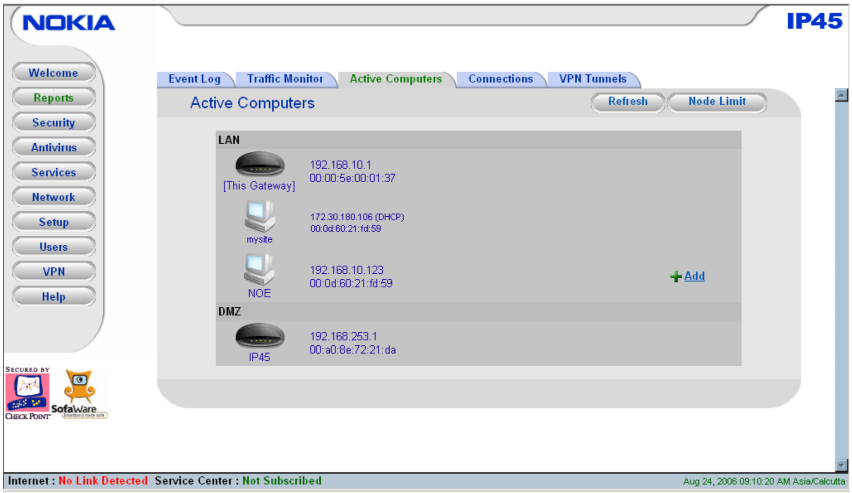
The Active Computers option in the IP45 GUI allows you to view the currently active computers on your network.

In the Active Computers report, licensed computers are shown in green. Computers that did not pass through the firewall (and therefore not a node) are displayed in blue. Computers that attempt to exceed the license are displayed in red and are blocked from accessing the Intranet. If a formerly active computer does not pass traffic through the firewall for a certain period of time, it is considered inactive, and is shown in blue. Another node can pass through the firewall instead.

To view the active computers

1. Choose Reports from the main menu and click Active Computers.

   The Active Computers page opens.



Active Computers

LAN

[This Gateway] 192.168.10.1 00:00:5e:00:01:37

mysite 172.30.180.106 (DHCP) 00:0d:60:21:fd:59

NOE 192.168.10.123 00:0d:60:21:fd:59

DMZ

IP45 192.168.253.1 00:a0:8e:72:21:da

Internet : No Link Detected Service Center : Not Subscribed Aug 24, 2006 09:10:20 AM Asia/Calcutta

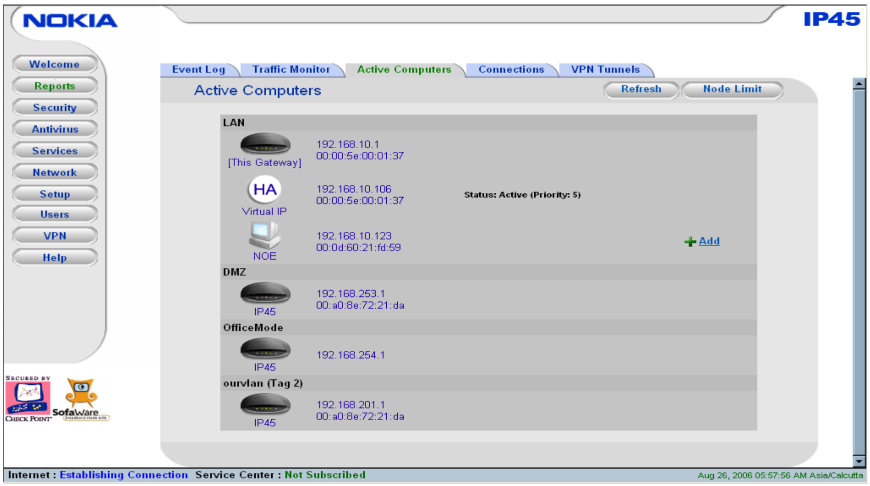
If your network exceeds the maximum number of computers allowed by your license, a warning message appears, and the computers that exceed the node limit are marked in red. These computers might not be able to access the Internet through IP45.

Note

To increase the number of computers that your license allows, you must upgrade your product.

Click Refresh to refresh the display.

When you configure high-availability feature, the GUI page for Active Computers appears as follows:



Active Computers

LAN
[This Gateway] 192.168.10.1 00:00:5e:00:01:37
Virtual IP 192.168.10.106 00:00:5e:00:01:37 Status: Active (Priority: 5)
NOE 192.168.10.123 00:0d:60:21:fd:59

DMZ
IP45 192.168.253.1 00:a0:8e:72:21:da

OfficeMode
IP45 192.168.254.1

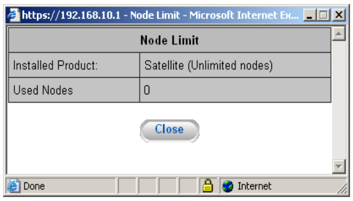
ourvlan (Tag 2)
IP45 192.168.201.1 00:a0:8e:72:21:da

Internet : Establishing Connection Service Center : Not Subscribed Aug 26, 2006 05:57:56 AM Asia/Calcutta

2. To view node limit information:

a. Click Node Limit.

The Node Limit window opens with the installed software product displaying the number of nodes used.


https://192.168.10.1 - Node Limit - Microsoft Internet Ex...
Close
Done
Internet

Node Limit	
Installed Product:	Satellite (Unlimited nodes)
Used Nodes	0

b. Click Close to close the window.

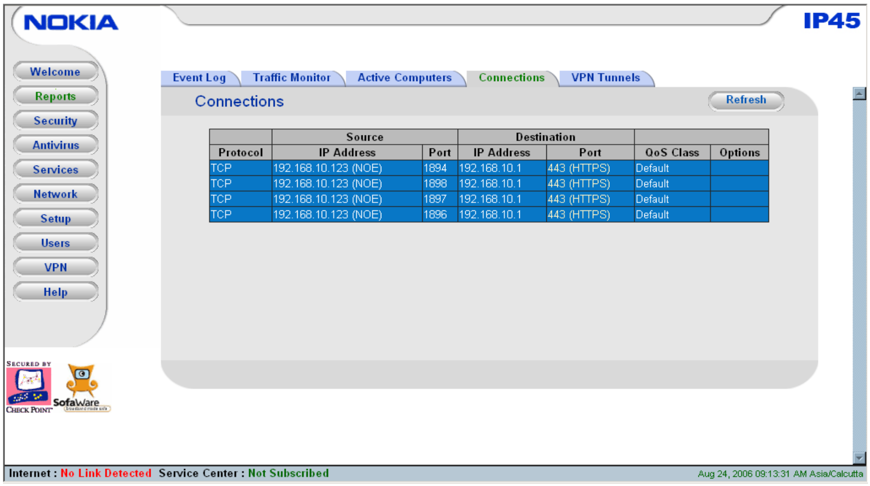
Viewing Connections

The Connections option in the IP45 GUI allows you to view the currently active connections between your network and the external world. The active connections are displayed as a list, specifying source IP address, destination IP address and port, and the protocol used (TCP, UDP, and so on).

To view active connections

1. Choose Reports from the main menu, and then click Connections.

   The Connections page opens.



Connections

	Source		Destination			
Protocol	IP Address	Port	IP Address	Port	QoS Class	Options
TCP	192.168.10.123 (NOE)	1894	192.168.10.1	443 (HTTPS)	Default	
TCP	192.168.10.123 (NOE)	1898	192.168.10.1	443 (HTTPS)	Default	
TCP	192.168.10.123 (NOE)	1897	192.168.10.1	443 (HTTPS)	Default	
TCP	192.168.10.123 (NOE)	1896	192.168.10.1	443 (HTTPS)	Default	

Internet : No Link Detected Service Center : Not Subscribed Aug 24, 2006 09:13:31 AM Asia/Calcutta

2. Do the following:

- Click Refresh to refresh the display.
- To view information about the destination computer, click the corresponding Port.

  The IP45 queries the Internet WHOIS server, and a window displays the name of the entity to whom the IP address is registered and their contact information.

Viewing the Diagnostics Summary

You can view the diagnostics summary for your device from the IP45 GUI. The diagnostics summary provides useful information about your device, such as node limit, network status, primary network status, secondary network status, my network status, setup state, users state, security, and subscription services. Apart from this, you can get the following basic information about your IP45 from the diagnostics summary.

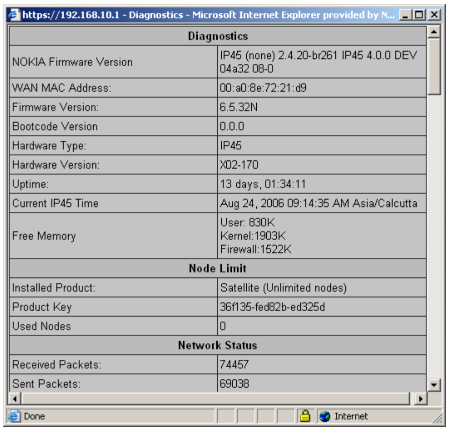
To view the diagnostics summary

1. Choose Setup from the main menu, and click Tools.

   The Tools page opens.

2. Click Diagnostics on the right of the page.

3. The Diagnostics window opens.The following figure shows a sample section of the diagnostics window that displays information about your IP45.



https://192.168.10.1 - Diagnostics - Microsoft Internet Explorer provided by N...
Done
Internet

Diagnostics	
NOKIA Firmware Version	IP45 (none) 2.4.20-br261 IP45 4.0.0 DEV 04a32 08-0
WAN MAC Address:	00:a0:8e:72:21:d9
Firmware Version:	6.5.32N
Bootcode Version	0.0.0
Hardware Type:	IP45
Hardware Version:	X02-170
Uptime:	13 days, 01:34:11
Current IP45 Time	Aug 24, 2006 09:14:35 AM Asia/Calcutta
Free Memory	User: 830K Kernel:1903K Firewall:1522K
Node Limit	
Installed Product:	Satellite (Unlimited nodes)
Product Key	36f135-fed82b-ed325d
Used Nodes	0
Network Status	
Received Packets:	74457
Sent Packets:	69038

4. Use the scroll bar to view more information.

15 Working with VPNs

This chapter describes how to use Nokia IP45 as a VPN client, server or gateway. It includes the following topics:

About VPN

In addition to a full firewall functionality, Nokia IP45 Tele 8, and Nokia Satellite X enable secure telecommuter access from home to the office network through the virtual private network (VPN) functionality.

VPN consists of at least one VPN server or gateway, and several VPN clients. A VPN server makes the corporate network remotely available to authorized users, such as employees working from home, who connect to the VPN server by using VPN clients. A VPN gateway can be connected to another VPN gateway in a permanent, bidirectional relationship. The two connected networks function as a single network.

A connection between two VPN sites is called a VPN tunnel. VPN tunnels encrypt and authenticate all traffic passing through them. Through these tunnels, you can safely use your company network resources when you work at home. For example, you can securely read email, use your company intranet, or access your company database from home.

Nokia IP45 Tele 8, and Satellite 16/32/U licenses provide VPN functionality. Nokia IP45 Tele 8 contains a VPN client and can act as a VPN server. Nokia IP45 Satellite 16/32/U can act as a VPN client, a VPN server, or a VPN gateway.

Both Nokia IP45 Tele 8, and Nokia IP45 Satellite X enables a number of solutions to support your VPN connectivity needs that are explained in the following sections.

Figure 11 VPN Topologies

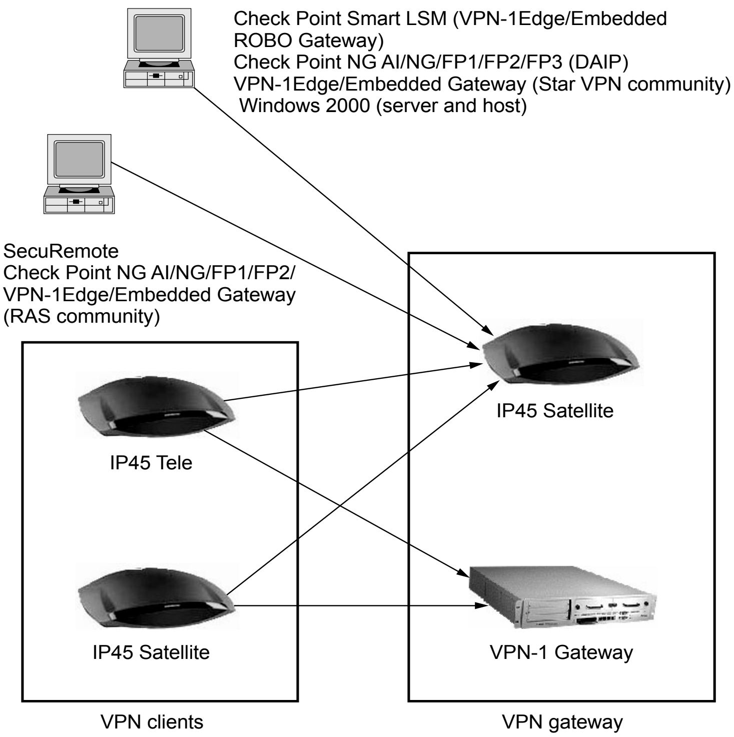

Check Point Smart LSM (VPN-1Edge/Embedded
ROBO Gateway)
Check Point NG AI/NG/FP1/FP2/FP3 (DAIP)
VPN-1Edge/Embedded Gateway (Star VPN community)
Windows 2000 (server and host)
SecuRemote
Check Point NG AI/NG/FP1/FP2/
VPN-1Edge/Embedded Gateway
(RAS community)
IP45 Satellite
IP45 Tele
IP45 Satellite
VPN-1 Gateway
VPN clients
VPN gateway

Table 56 VPN Topologies

VPN Client	Gateway
SecuRemote, R55/R56 VPN Client	Nokia IP45 Satellite
Nokia IP45 Tele	Nokia IP45 Satellite
Nokia IP45 Tele	Check Point NG AI, NG, FP3, FP2, FP1
Nokia IP45 Tele	Check Point NG AI using VPN-1 Edge/ Embedded Gateway (RAS Community)
Nokia IP45 Satellite (gateway)	Nokia IP45 Satellite (gateway)
Nokia IP45 Satellite (gateway)	Check Point NG AI, NG, FP3, FP2, FP1
Nokia IP45 Satellite	Check Point NG AI using VPN-1 Edge/ Embedded Gateway Check Point Smart LSM using VPN-1 Edge/Embedded ROBO gateway.

Table 56 VPN Topologies (*continued*)

VPN Client	Gateway
Nokia IP45 Satellite	Check Point NG AI using VPN-1 Edge/ Embedded Gateway (Star Community)
Nokia IP45 Satellite	Windows 2000, Nokia CryptoCluster series, CISCO PIX

Setting Up the Nokia IP45 Security Platform as a VPN Server

Using the Nokia IP45 security platform, you can make your network remotely available to authorized users by setting up your Nokia IP45 as a VPN server. Remote access users can connect to the VPN server through Check Point SecuRemote or a Nokia IP45 VPN client in remote access VPN mode.

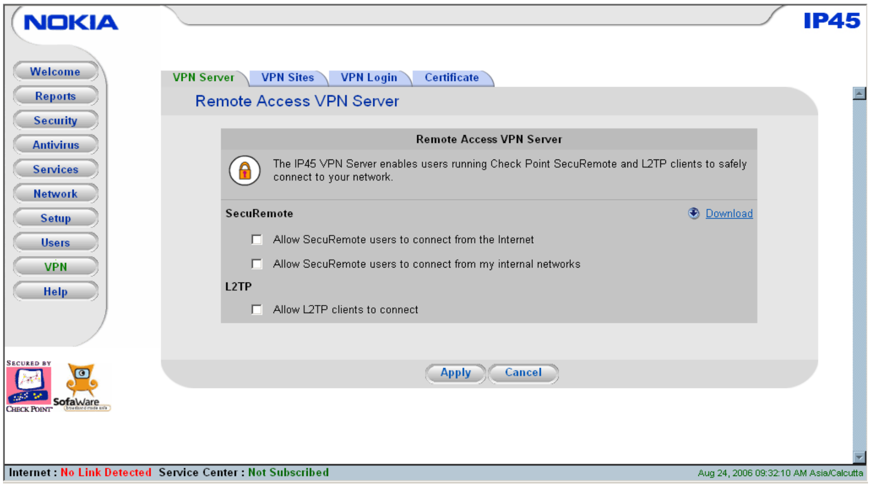
IP45 includes an integrated L2TP IPSec VPN Server. Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol that supports remote access virtual private networks. When this server is enabled, IP45 appliance can provide secure remote access to desktop or mobile clients running a Microsoft Windows L2TP IPSec VPN.

IP45 Tele and Satellite both provide VPN functionality. Nokia IP45 Tele license contains a VPN client and can act as a VPN server. Nokia IP45 satellite can act as a VPN client, a VPN server, or a VPN gateway.

To set up the IP45 device as a SecuRemote VPN server

1. Choose VPN from the IP45 main menu.

   The SecuRemote VPN Server page opens.



Remote Access VPN Server

Remote Access VPN Server

The IP45 VPN Server enables users running Check Point SecuRemote and L2TP clients to safely connect to your network.

SecuRemote Download

□ Allow SecuRemote users to connect from the Internet

□ Allow SecuRemote users to connect from my internal networks

L2TP

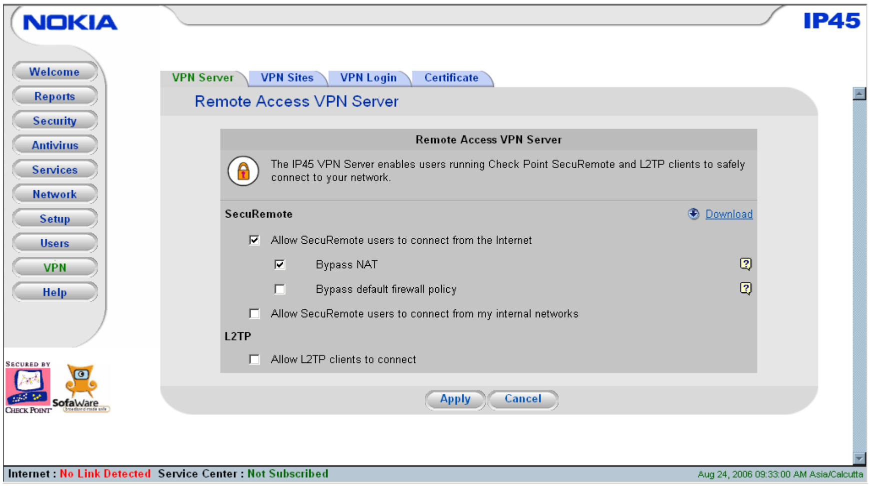
□ Allow L2TP clients to connect

Apply Cancel

Internet : No Link Detected Service Center : Not Subscribed Aug 24, 2006 09:32:10 AM Asia/Calcutta

2. Click Allow the SecuRemote users to connect from the Internet.

The following page opens.



Remote Access VPN Server

Remote Access VPN Server

The IP45 VPN Server enables users running Check Point SecuRemote and L2TP clients to safely connect to your network.

SecuRemote Download

☑ Allow SecuRemote users to connect from the Internet

☑ Bypass NAT

☐ Bypass default firewall policy

☐ Allow SecuRemote users to connect from my internal networks

L2TP

☐ Allow L2TP clients to connect

Apply Cancel

Internet : No Link Detected **Service Center :** Not Subscribed Aug 24, 2006 09:33:00 AM Asia/Calcutta

3. To allow authenticated users connecting from the Internet to bypass NAT when connecting to your internal network, click Bypass NAT check box.

4. To allow authenticated users connecting from the Internet to bypass the firewall and access your internal network without restriction, click Bypass default firewall policy check box.

5. Click Apply.

Note

To allow authenticated users to bypass NAT and access your internal network without restriction, select Bypass NAT. To bypass the firewall, select Bypass default firewall policy.

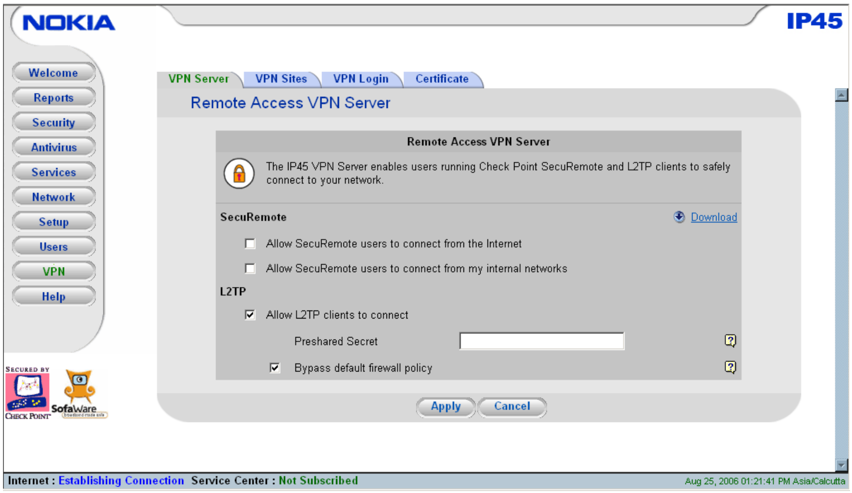
To allow L2TP clients to connect

1. From the main menu, choose VPN.

Remote Access VPN Server page opens.

2. Check Allow L2TP clients to connect check box.

L2TP options get displayed as shown in the following page:



Remote Access VPN Server

Remote Access VPN Server

The IP45 VPN Server enables users running Check Point SecuRemote and L2TP clients to safely connect to your network.

SecuRemote

□ Allow SecuRemote users to connect from the Internet

□ Allow SecuRemote users to connect from my internal networks

L2TP

☑ Allow L2TP clients to connect

Preshared Secret

☑ Bypass default firewall policy

Internet : Establishing Connection Service Center : Not Subscribed Aug 25, 2006 01:21:41 PM Asia/Calcutta

3. Enter a pre-shared secret to use to secure the L2TP IPSec tunnel in the Preshared Secret text box.
4. To enable or disable, check or uncheck the Bypass default firewall policy. By default, this option is enabled.
5. Click Apply.

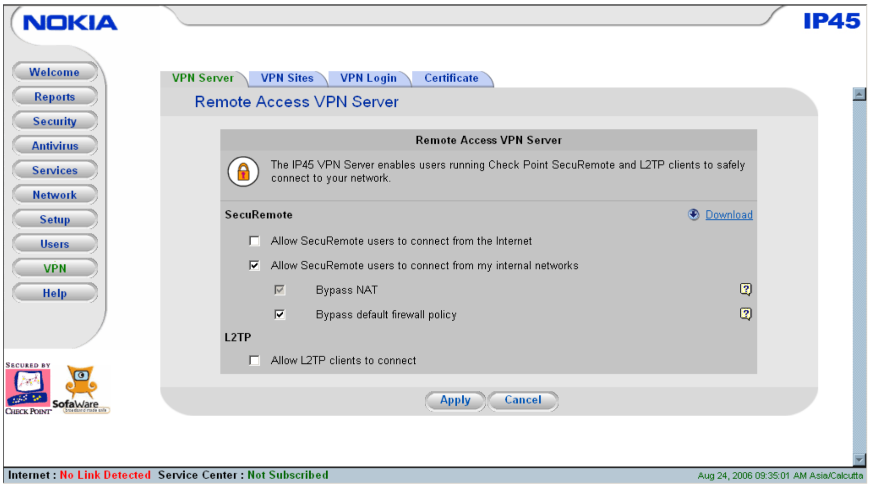
   The L2TP settings are saved.

You can set the L2TP settings by also using the command-line interface. For more information about L2TP VPN server commands, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0.*

To allow SecuRemote users from the Internal network

1. Choose VPN from the main menu.
2. Click Allow SecuRemote users to connect from my internal networks on VPN> VPN Server GUI page.

The following page opens.



Remote Access VPN Server

Remote Access VPN Server

The IP45 VPN Server enables users running Check Point SecuRemote and L2TP clients to safely connect to your network.

SecuRemote Download

□ Allow SecuRemote users to connect from the Internet

☑ Allow SecuRemote users to connect from my internal networks

☑ Bypass NAT

☑ Bypass default firewall policy

L2TP

□ Allow L2TP clients to connect

Apply Cancel

Internet : No Link Detected Service Center : Not Subscribed Aug 24, 2006 09:35:01 AM Asia/Calcutta

3. Click Bypass default firewall policy checkbox, to bypass firewall rules.
4. Click Apply.

Note
If you configured the internal VPN Server, install SecuRemote on the desired internal network computers.

To Install SecuRemote

1. Choose VPN from the IP45 main menu.
2. Click VPN Server.

   The SecuRemote VPN Server page opens.
3. Click *Download* link to download SecureRemote.
4. Follow the wizard instructions to complete the installation.

Configuring Remote Access VPNs

The following procedures describe how to configure a remote access VPN and VPN site.

To configure a remote access VPN

1. Choose VPN from the main menu, and click the VPN Sites tab.
2. Click New Site at the bottom of the page.

   The IP45 VPN site wizard appears.
3. If you select Remote Access VPN, the VPN Gateway Address dialog box appears.

To configure a remote access VPN site

1. Enter the IP address of the VPN gateway.
2. Click Next.
3. The VPN Network Configuration window opens.
4. Do one of the following:
   - To obtain the network configuration by downloading it from the VPN site, select Download Configuration. This option automatically configures your VPN settings by downloading the network topology definition from the VPN server.

   Note
   You can download the network configuration only if you are connecting to a Check Point VPN-1 or to the Nokia IP45 security platform.

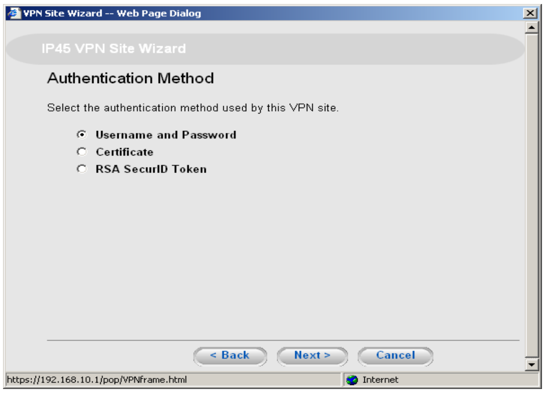
   - To provide the network configuration manually, select Specify Configuration.
   - To route all network traffic through the site, including Internet traffic, select Route All Traffic in the GUI wizard.

   This option increases the network security. For example, if your VPN consists of a central office and a number of remote offices, and the remote offices are allowed to access the Internet resources through the central office only, you can choose route all traffic from the remote offices through the central office.

   Note
   You can configure only one VPN site to route all traffic.

5. Click Next.

   If you chose Download Configuration or Route All traffic, the Authentication Method window opens.



VPN Site Wizard -- Web Page Dialog
IP45 VPN Site Wizard

Authentication Method

Select the authentication method used by this VPN site.

● Username and Password
○ Certificate
○ RSA SecurID Token

< Back
Next >
Cancel
https://192.168.10.1/pop/VPNframe.html
Internet

6. Choose the authentication method.

7. If you choose Specify Configuration, a second VPN Network Configuration dialog box appears. Do the following:

   a. In the Destination network column, enter up to three destination network addresses at the VPN site to which you want to connect.

   b. In the Subnet mask column, select the subnet masks for the destination network addresses.

Note
Obtain the destination networks and subnet mask addresses from the VPN gateway system administrator.

   c. In the Configure Backup Gateway column, type the name of the VPN gateway to use if the primary VPN gateway fails.

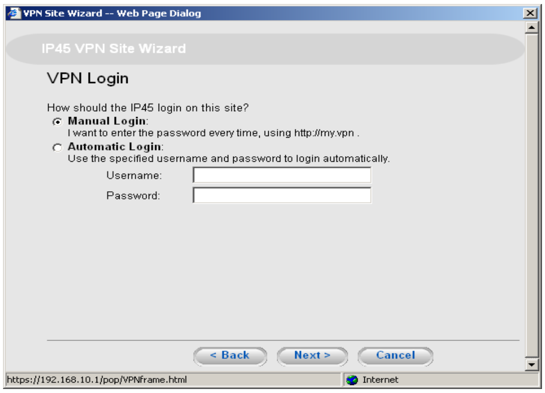
Note
The backup gateway can be configured only if you are using Check Point Multiple Entry Point. For information about how to configure the primary and secondary Check Point management stations, see the *Check Point Multiple Entry Point* document.

   d. Click Next.

   The Authentication method window opens. Choose the authentication method.

8. Click Next.

   The VPN Login window opens.



VPN Login

How should the IP45 login on this site?

● **Manual Login**:
I want to enter the password every time, using http://my.vpn .

○ **Automatic Login**:
Use the specified username and password to login automatically.

Username:

Password:

https://192.168.10.1/pop/VPNframe.html

9. Do one of the following:

   a. To configure the site for manual login, select Manual Login. Enter a username and password to be used for logging on to the VPN site.

   b. To enable the IP45 to log on to the VPN site automatically, select Automatic Login.

Note

While automatic login provides all of the computers on your home network with constant access to the VPN site, manual login connects only to the computer you are currently logged from, and only when the appropriate username and password are entered. The automatic login option in the GUI is supported for Nokia IP45 Satellite X and manual login is available for Nokia IP45 Tele license.

For more information about automatic and manual login, see "Logging On to a VPN Site" on page 271.

10. Enter the username and password.

Note

You can use a maximum of 19 characters for username and a maximum of 31 characters for password.

11. Click Next

    The Connecting window opens.

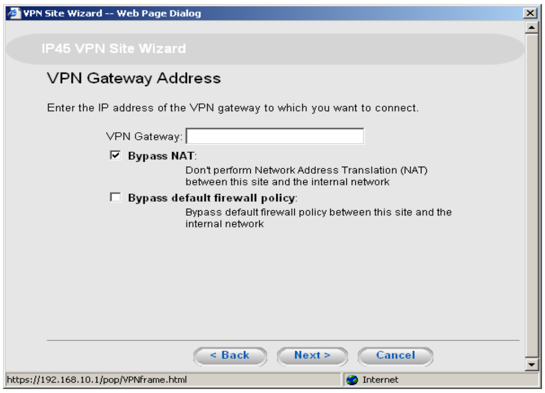
    The Contacting VPN Site window opens.

12. Click Next.

    Proceed to "Completing Site Creation" on page 268.

Configuring Site-to-Site VPN

If you select Site-to-Site VPN from VPN> VPN Sites > New Site page, the VPN Gateway Address window opens.



VPN Site Wizard -- Web Page Dialog

IP45 VPN Site Wizard

VPN Gateway Address

Enter the IP address of the VPN gateway to which you want to connect.

VPN Gateway:

☑ **Bypass NAT**:
Don't perform Network Address Translation (NAT) between this site and the internal network

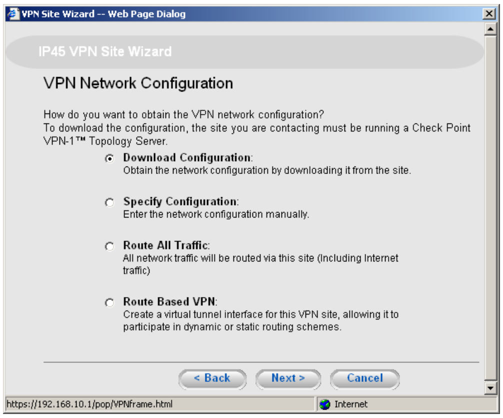
☐ **Bypass default firewall policy**:
Bypass default firewall policy between this site and the internal network

https://192.168.10.1/pop/VPNframe.html

To configure a Site-to-Site VPN gateway

1. Enter the IP address of the VPN gateway as given to you by the network administrator.
2. Check the Bypass NAT check box to bypass the NAT rules, and to allow the VPN site to access your internal network without restrictions.
3. Click Next.

   The VPN Network Configuration window opens.



VPN Network Configuration

How do you want to obtain the VPN network configuration?
To download the configuration, the site you are contacting must be running a Check Point VPN-1™ Topology Server.

● **Download Configuration**:
Obtain the network configuration by downloading it from the site.

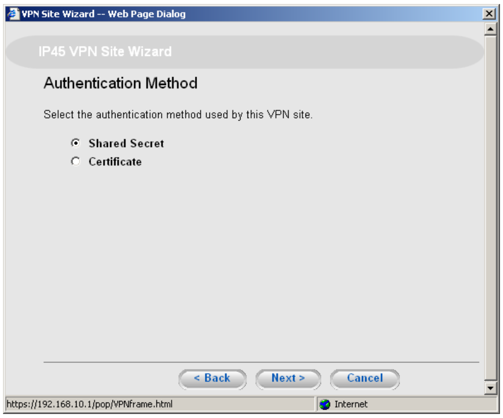
○ **Specify Configuration**:
Enter the network configuration manually.

○ **Route All Traffic**:
All network traffic will be routed via this site (Including Internet traffic)

○ **Route Based VPN**:
Create a virtual tunnel interface for this VPN site, allowing it to participate in dynamic or static routing schemes.

4. Select Download Configuration, and click next.

   The Authentication Method window opens.



VPN Site Wizard -- Web Page Dialog
IP45 VPN Site Wizard

Authentication Method

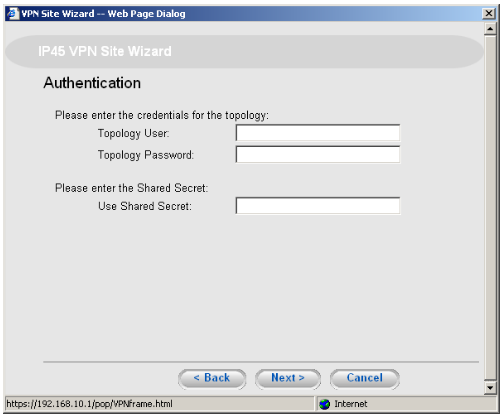
Select the authentication method used by this VPN site.

● **Shared Secret**
○ **Certificate**

< Back
Next >
Cancel
https://192.168.10.1/pop/VPNframe.html
Internet

5. Select the authentication method.
6. Click Next.

If you select the authentication method to be Shared Secret, the following window opens:


VPN Site Wizard -- Web Page Dialog
IP45 VPN Site Wizard

Authentication

Please enter the credentials for the topology:

Topology User:

Topology Password:

Please enter the Shared Secret:

Use Shared Secret:

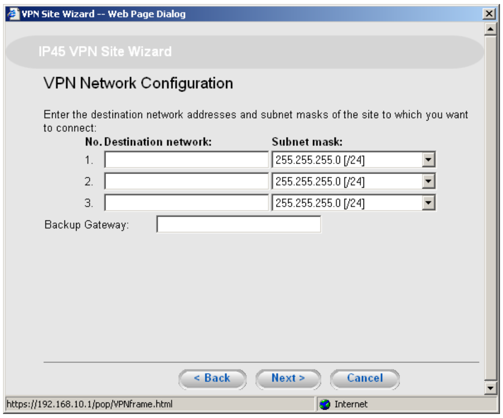
< Back
Next >
Cancel
https://192.168.10.1/pop/VPNframe.html
Internet

7. If the topology is to be downloaded,

   Enter the Topology username, and Topology password.

8. Enter the Shared Secret.

   If you select Specify Configuration from VPN Network Configuration window, the VPN Network Configuration window opens.


VPN Site Wizard -- Web Page Dialog
IP45 VPN Site Wizard

VPN Network Configuration

Enter the destination network addresses and subnet masks of the site to which you want to connect:

No.	Destination network:	Subnet mask:
1.		255.255.255.0 [/24]
2.		255.255.255.0 [/24]
3.		255.255.255.0 [/24]

Backup Gateway:

< Back
Next >
Cancel
https://192.168.10.1/pop/VPNframe.html
Internet

a. In the Destination Network column, enter up to three destination network addresses at the VPN site to which you want to connect.

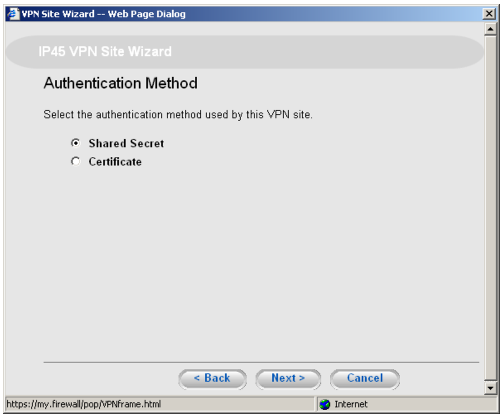
b. In the Subnet mask column, select the subnet masks for the destination network addresses.

Note

Obtain the destination networks and subnet masks from the VPN site system administrator.

c. Click Next.

The Authentication Method window opens.



VPN Site Wizard -- Web Page Dialog
IP45 VPN Site Wizard
< Back
Next >
Cancel
https://my.firewall/pop/VPNframe.html
Internet

Authentication Method

Select the authentication method used by this VPN site.

● Shared Secret
○ Certificate

d. Select the authentication method.

e. Click Next.

If the Route All Traffic option is selected, you are ready to complete your VPN site. See Completing Site Creation on page 268.

Completing Site Creation

When you configure a VPN site, the Site Name window opens in the IP45 VPN site wizard.

To complete VPN site creation

1. Enter a name for the VPN site.
2. Click Next.

   The Site Name window opens.

   a. Type the Site Name.

   b. If the Keep Alive Option is selected, enter the host IP address.

   The connection is kept active by sending packets to the IP address that you enter.
3. Click Finish.

   The VPN Sites page reappears. If you added a VPN site, the new site appears in the VPN Sites list. If you edited a VPN site, the modifications are reflected in the VPN Sites list.

Note
You can see the downloaded topology on your IP45 device from http://my.firewall/vpntopo.html.

Configuring Route-Based VPNs

Route-based VPNs allow administrators to extend dynamic routing protocols from headquarters to remote locations over the VPN tunnel, improving network and VPN management efficiency for a large network. Route-based VPNs combined with OSPF dynamic routing is a good solution for constantly changing the networks.

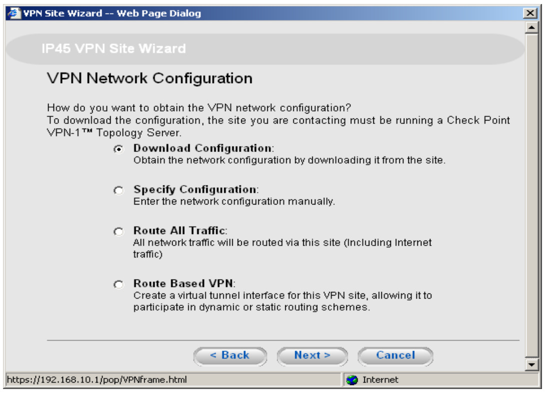
Every VPN tunnel is represented as virtual tunnel interface (VTI) and assigned an IP address, enabling the encapsulation of OSPF traffic.These virtual adapters can be used to establish integrated dynamic routing configurations with the routing domains in protected networks. Organizations can make frequent changes to the network topology by combining OSPF and route-based VPNs.

To configure route-based VPNs

1. Choose VPN from the main menu and select VPN Sites.
2. Click New Site.

   The VPN Site wizard opens.
3. Type the VPN Gateway IP Address, and set the options for Bypass NAT and Bypass firewall.
4. Click Next.

   The VPN Network Configuration window opens.



VPN Network Configuration

How do you want to obtain the VPN network configuration?
To download the configuration, the site you are contacting must be running a Check Point VPN-1™ Topology Server.

● **Download Configuration**:
Obtain the network configuration by downloading it from the site.

○ **Specify Configuration**:
Enter the network configuration manually.

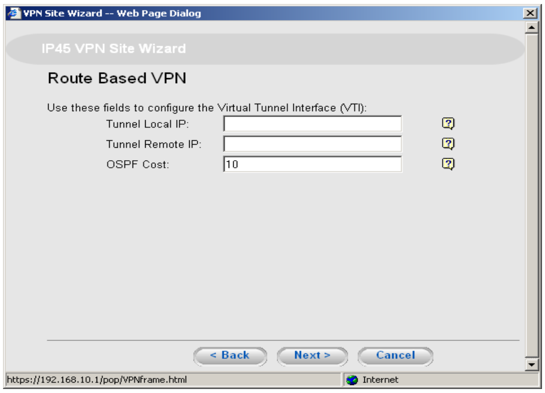
○ **Route All Traffic**:
All network traffic will be routed via this site (Including Internet traffic)

○ **Route Based VPN**:
Create a virtual tunnel interface for this VPN site, allowing it to participate in dynamic or static routing schemes.

https://192.168.10.1/pop/VPNframe.html

5. Select Route Based VPN, click Next.

   The Route Based VPN window opens.



VPN Site Wizard -- Web Page Dialog
IP45 VPN Site Wizard
< Back
Next >
Cancel
https://192.168.10.1/pop/VPNframe.html
Internet

Route Based VPN

Use these fields to configure the Virtual Tunnel Interface (VTI):

Tunnel Local IP:

Tunnel Remote IP:

OSPF Cost: 10

6. Enter the information in the VTI fields using Table 57.

Table 57 Virtual Tunnel Interface fields

Field	Description
Tunnel Local IP	Type a local IP address for the local end of VPN tunnel.
Tunnel Remote IP	Type the IP address of the remote end of the VPN tunnel.
OSPF Cost	Type the cost of this link for dynamic routing purposes. Default value: 10

7. Click Next and proceed as per the wizard prompts to complete the site creation.

   For more information, see "Completing Site Creation" on page 268.

Deleting a VPN Site

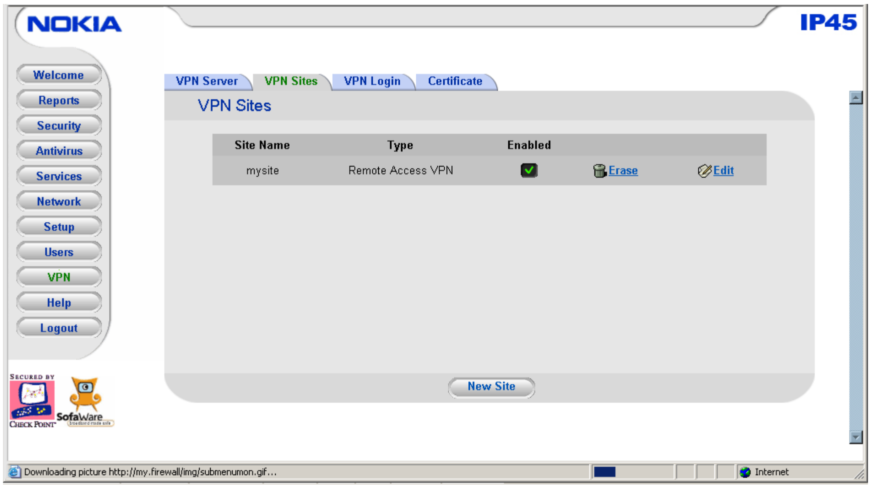
You can delete a VPN site from IP45 Tele 8 and IP45 Satellite X.

To delete a VPN site

1. Choose VPN from the IP45 main menu.

   The VPN Server page opens.
2. Click VPN Sites.

The VPN Sites page opens with a list of VPN sites.

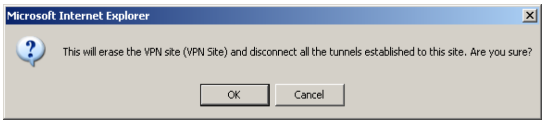


VPN Sites

Site Name	Type	Enabled		
mysite	Remote Access VPN	✓	Erase	Edit

3. To delete a VPN site, click the Erase icon, next to the VPN site.

   A confirmation message appears.



This will erase the VPN site (VPN Site) and disconnect all the tunnels established to this site. Are you sure?

4. Click OK.

   The VPN site is deleted.

Logging On to a VPN Site

If you chose automatic login, a VPN tunnel is created automatically when you try to access the VPN site.

If you chose manual login, you need to log on to a VPN site every time you want to access the VPN site.

You can log on to a VPN site either through the Nokia IP45 GUI or the *my.vpn* page. When you log on, a VPN tunnel is established. Only the computer from which you logged on can use the tunnel. To share the tunnel with other computers in your home network, you must log on to the VPN site from those computers, using the same username and password.

Note
You can use a single username and password for each VPN destination gateway computer.

Logging On from the Nokia IP45 Security Platform GUI

The following sections provide information how to log on to the IP45 security platform by using GUI.

To log on from IP45 GUI

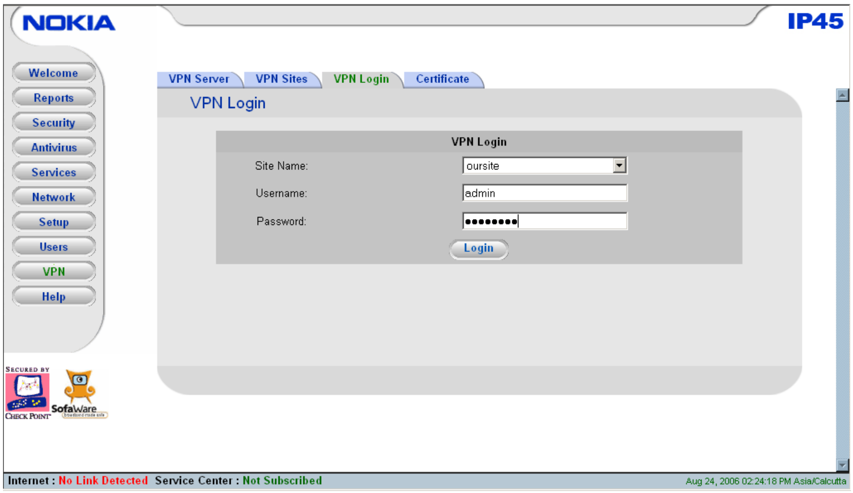
To log on to a VPN site from the Nokia IP45 GUI, use the following procedure:

1. Choose VPN from the IP45 main menu.

   The VPN Sites page opens, with the list of configured VPN sites.

2. In the VPN submenu, click VPN Login.

   The VPN Login page opens.



VPN Login

VPN Login

Site Name: oursite

Username: admin

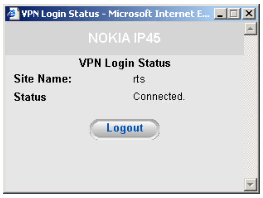
Password: ••••••••

Login

Internet : No Link Detected Service Center : Not Subscribed Aug 24, 2006 02:24:18 PM Asia/Calcutta

3. Select the site to log on to.
4. Type your username and password in the appropriate fields.
5. Click Connect.
   - If the IP45 device is configured to automatically download the network configuration, the IP45 downloads the network configuration.
   - If you specified a network configuration when you add the VPN site, the IP45 attempts to create a tunnel to the VPN site.
   - The VPN Login Status dialog box and the Connecting page appears. When the IP45 is finished connecting, the Status field changes to Connected. The VPN Login Status dialog box remains open until you log off from the VPN site.

- When the IP45 is finished connecting, the status changes to connected.



VPN Login Status - Microsoft Internet E...

NOKIA IP45

VPN Login Status

Site Name: rts

Status Connected.

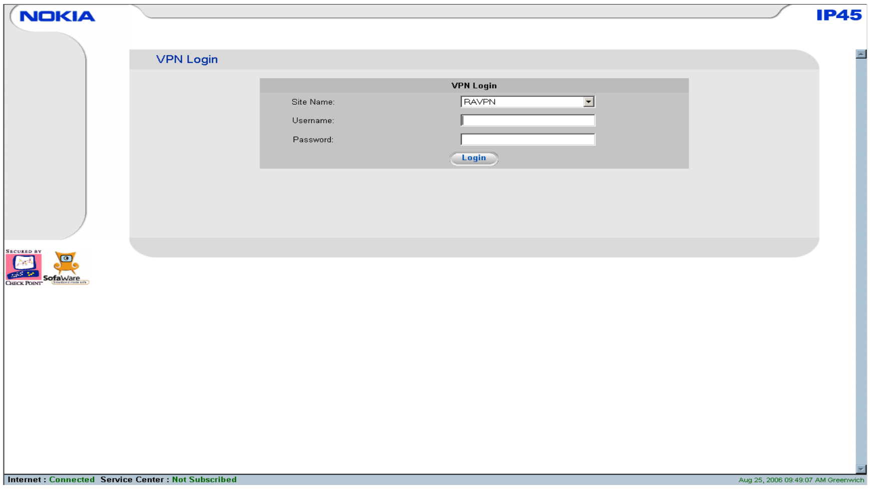
Logging On Through my.vpn

Use the following procedure to log on through my.vpn:

Note
You do not need to know the my.firewall page administrator's password to use the my.vpn page.

To log on to a VPN site through the my.vpn page

1. Go to http://my.vpn.The VPN Login page opens.



VPN Login

Site Name: RAVPN

Username:

Password:

Internet : Connected Service Center : Not Subscribed

Aug 25, 2006 09:49:07 AM Greenwich

2. Select the site to log on to.
3. Enter your username and password in the appropriate fields.
4. Click Login.
   - If the IP45 is configured to automatically download the network configuration, the IP45 downloads the network configuration.
   - When adding the VPN site, if you specified a network configuration, the IP45 attempts to create a tunnel to the VPN site.
   - The VPN Login Status dialog box appears. The Status field tracks the progress of the connection.

- When the IP45 is finished connecting, the Status field changes to Connected.
- The VPN Login Status box remains open until you log off from the VPN site.

Logging Off a VPN Site

You need to manually log off from a VPN site if:

- You are using IP45 Tele license.
- The VPN site is a remote access VPN site configured for manual login.

To log off from a VPN site, click *Close* in the VPN Login Status dialog box. All open tunnels from the IP45 to the VPN site are closed, and the VPN Login Status dialog box closes.

Closing the browser or dismissing the VPN Login Status box also terminates the VPN session within a short time.

VPN Certificates

A secure means of authenticating the Nokia IP45 security platform to other VPN gateways is a digital certificate. The Certificate Authority (CA) issues the certificate to entities such as gateways, users or computers. The entity then uses the certificate to identify itself and provide verifiable information. For instance, the certificate includes the distinguishing name (DN) of the entity, as well as the public key (information about itself). After two entities exchange and validate each other's certificates, they can begin encrypting information between themselves by using the public keys in the certificates.

IP45 v4.0 supports establishing certificates-based VPNs with multiple trusted CA. To use this capability, IP45 must be managed by Smart Center.

Installing a Certificate

Nokia IP45 supports certificates encoded in the PKCS#12 format. You can install the VPN certificate by:

- Generating a self-signed certificate—you can generate a self-signed certificate by using the Certificate wizard, supported by the IP45 GUI. See "Generating a Self-Signed Certificate" on page 275.
- Importing a certificate—importing a certificate from a location. See "Importing a Certificate" on page 277.

Note
The Nokia IP45 security platform supports certificates encoded in the personal information exchange syntax standard (PKCS) format. The PKCS #12 file must have a .p12 file extension. If you do not have a PKCS # 12, obtain it from your network security administrator.

Note
To use certificates authentication, each Nokia IP45 security platform should have an unique certificate. Do not use the same certificate for more than one gateway.

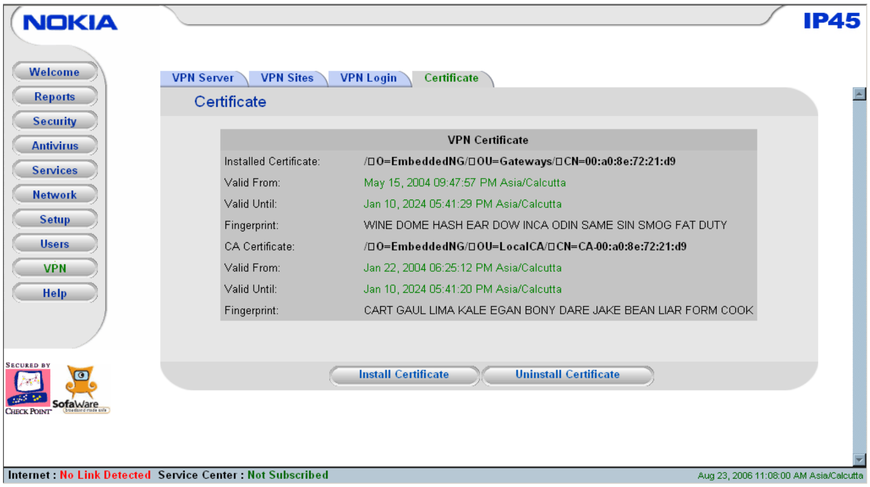
Generating a Self-Signed Certificate

You can now generate self-signed certificate by using http://my.firewall.

To generate a self-signed certificate

1. Choose VPN from the IP45 main menu and click Certificate.

   The VPN Certificate page opens.



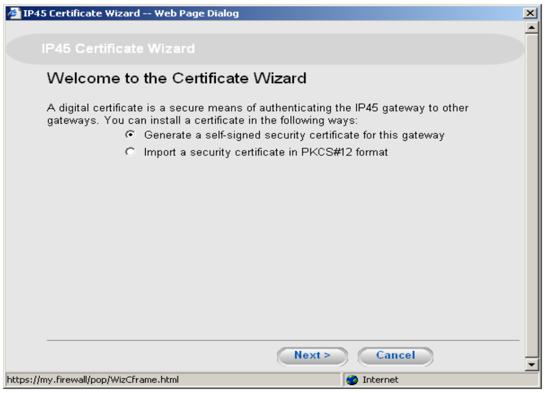
Certificate

VPN Certificate	
Installed Certificate:	/□O=EmbeddedNG/□OU=Gateways/□CN=00:a0:8e:72:21:d9
Valid From:	May 15, 2004 09:47:57 PM Asia/Calcutta
Valid Until:	Jan 10, 2024 05:41:29 PM Asia/Calcutta
Fingerprint:	WINE DOME HASH EAR DOW INCA ODIN SAME SIN SMOG FAT DUTY
CA Certificate:	/□O=EmbeddedNG/□OU=LocalCA/□CN=CA-00:a0:8e:72:21:d9
Valid From:	Jan 22, 2004 06:25:12 PM Asia/Calcutta
Valid Until:	Jan 10, 2024 05:41:20 PM Asia/Calcutta
Fingerprint:	CART GAUL LIMA KALE EGAN BONY DARE JAKE BEAN LIAR FORM COOK

Internet : No Link Detected Service Center : Not Subscribed Aug 23, 2006 11:08:00 AM Asia/Calcutta

2. Click Install Certificate.

   The Certificate wizard opens.


IP45 Certificate Wizard -- Web Page Dialog
IP45 Certificate Wizard
Next >
Cancel
https://my.firewall/pop/WizCframe.html
Internet

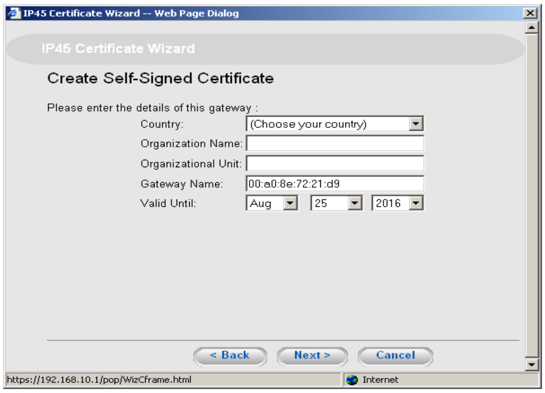
Welcome to the Certificate Wizard

A digital certificate is a secure means of authenticating the IP45 gateway to other gateways. You can install a certificate in the following ways:

● Generate a self-signed security certificate for this gateway
○ Import a security certificate in PKCS#12 format

3. Click Generate a self-signed security certificate for this gateway.
4. Click Next.

The Create self-signed certificate window opens.



IP45 Certificate Wizard -- Web Page Dialog
IP45 Certificate Wizard

Create Self-Signed Certificate

Please enter the details of this gateway :

Country: (Choose your country)

Organization Name:

Organizational Unit:

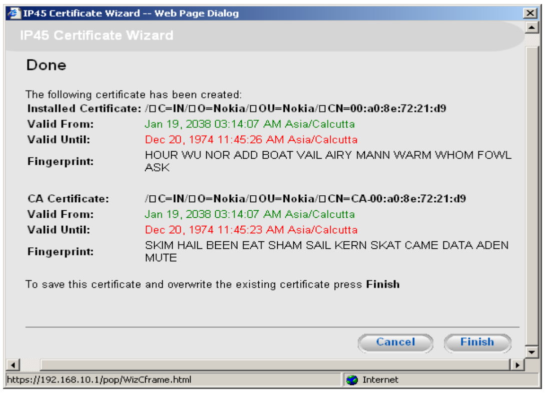
Gateway Name: 00:a0:8e:72:21:d9

Valid Until: Aug 25 2016

< Back
Next >
Cancel
https://192.168.10.1/pop/WizCframe.html
Internet

5. Complete the fields following the information provided in“Certificate fields” on page 276.
6. Click Next.

   It may take few minutes for the IP45 to generate the certificate. Once the certificate is generated, the Done window opens with details of the certificate generated.



Done

The following certificate has been created:

Installed Certificate: **/□C=IN/□O=Nokia/□OU=Nokia/□CN=00:a0:8e:72:21:d9**
Valid From: Jan 19, 2038 03:14:07 AM Asia/Calcutta
Valid Until: Dec 20, 1974 11:45:26 AM Asia/Calcutta
Fingerprint: HOUR WU NOR ADD BOAT VAIL AIRY MANN WARM WHOM FOWL ASK

CA Certificate: **/□C=IN/□O=Nokia/□OU=Nokia/□CN=CA-00:a0:8e:72:21:d9**
Valid From: Jan 19, 2038 03:14:07 AM Asia/Calcutta
Valid Until: Dec 20, 1974 11:45:23 AM Asia/Calcutta
Fingerprint: SKIM HAIL BEEN EAT SHAM SAIL KERN SKAT CAME DATA ADEN MUTE

To save this certificate and overwrite the existing certificate press **Finish**

7. Click Finish.

Note
The already installed certificate, if any will be re-written by the generated certificate. The Certificate window now displays the information about the new certificate installed.

Table 58 Certificate fields

Field	Action
Country	Select your country name from the drop-down list.
Organization Name	Type the name of your organization.

Table 58 Certificate fields (*continued*)

Field	Action
Organizational Unit	Type the name of your division.
Gateway Name	Type the name of the gateway. This name appears on the certificate and can be viewed by the remote users, inspecting the certificate. Default value: MAC address of the gateway.
Valid Until	Select the validity period from the drop-down list. Select the Month, Date and Year.

Importing a Certificate

You can import a VPN certificate by using the GUI or the CLI.

Importing a Certificate by Using the GUI

To install a certificate by using the GUI, follow the procedure below:

To install a certificate by importing

1. Choose VPN from the IP45 main menu and click Certificate.

   The VPN Certificate page opens.

2. Click Install Certificate.

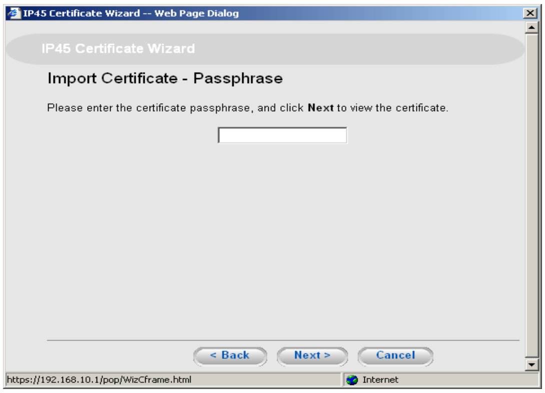
   The Certificate wizard opens.

3. Click Import a security certificate in PKCS#12 format.
4. Click Next.

   The Import Certificate window opens.

5. Click Browse to locate the file to import.
6. Select the file and click Next.

The Import Certificate Passphrase window opens.



IP45 Certificate Wizard -- Web Page Dialog
IP45 Certificate Wizard
< Back
Next >
Cancel
https://192.168.10.1/pop/WizCframe.html
Internet

Import Certificate - Passphrase

Please enter the certificate passphrase, and click **Next** to view the certificate.

7. Type the passphrase that you received from the administrator.
8. Click Next.
9. The Done window opens with details of the certificate.
10. Click Finish.

    The Certificate page displays the new certificate details, including the name of the CA that issued the certificate, and the name of the gateway to which this certificate was issued.

Installing Certificates by Using the CLI

You can also download and install the VPN certificate by using the command line interface.

Use the following command to install the certificate on the device:

```
set vpn certificate <file name>
```

Installing VPN Certificates from SmartCenter

VPN certificates are used to authenticate a VPN connection established between Check Point SmartCenter NG AI that uses Check Point Large Scale Manager and the dynamically configured IP45 security platform that uses the DAIP.

You can upload the certificate created on the Check Point NG AI to the IP45 Satellite.

To upload VPN certificates and to create a dynamic VPN site by using Check Point Smart LSM

1. Choose Services from the main menu, and then choose Connect.

   The Subscription Services wizard appears.
2. Enter the IP address of the Check Point NG AI Management station.

   The Connecting window opens.
3. Enter the Gateway ID and Registration Key that are used while creating the IP45 Dynamic Object on the LSM.

4. The Connecting window opens.

   When the connection is complete, the list of services downloaded is displayed.

5. Click Finish.

6. Click the VPN Sites tab to view the Dynamic VPN tunnel created between your Nokia IP45 device and the Check Point NG AI management station.

Uninstalling the VPN Certificate

Follow the below procedure to uninstall VPN certificate from the Nokia IP45 security platform.

To uninstall a certificate from Nokia IP45

1. Choose VPN from the IP45 main menu, and then choose Certificate.

   The Certificate page opens.

2. Click Uninstall Certificate to delete the certificate.

   A confirmation message appears.

3. Click OK.

Viewing VPN Tunnels

You can view a list of currently established VPN tunnels.

After you log on to the site, whenever your computer attempts to communicate with a computer at the VPN site, a VPN tunnel is created. When you log off, all open tunnels connecting to a VPN site are closed.

The active VPN Tunnels report now displays both the currently active phase-1 (IKE) and their associated establish phase-2(IPSec) VPN tunnels. For each tunnel, the source and destination IP addresses or address ranges are shown, as well as the selected security methods tunnel establishment time.

To view VPN tunnels

1. Choose Reports from the IP45 main menu.

   The Event Log page opens.

2. In the submenu, click VPN Tunnels.

   The VPN Tunnels page opens with a list of open tunnels to VPN sites.

   Table 59 VPN Tunnels includes the following columns

Table 59 VPN Tunnels

Column	Description
Type	Type of encryption used to secure the connection, followed by the type of authentication used to verify the user's identity. This information is presented in the following format: Encryption Type/ Authentication Type.
Source	Source of the connection
Destination	Destination of the connection
Security	VPN properties for Phase1 and Phase2 algorithms
Established	Time when the VPN Tunnel is established. This information is presented in the following format: Hour:Minute:Second
Site	VPN site name.
Username	User logged on to the VPN site.
Encryption Type	Type of encryption used to secure the connection, followed by the type of authentication used to verify the user's identity. This information is presented in the following format: Encryption Type/ Authentication Type.
Established Time	Time when the VPN Tunnel is established. This information is presented in the following format: Hour:Minute:Second.
VPN Gateway	IP Address of the VPN Gateway to which the tunnel is connected.

You can refresh the table by refreshing the browser.

Viewing IKE Traces

The following procedures describes how to view the IKE traces.

To view IKE traces

1. Establish a VPN tunnel to the VPN site with which you are experiencing connection problems.
2. For information on when and how VPN tunnels are established, see "Viewing VPN Tunnels" on page 279.
3. Click Reports in the main menu, and click the VPN Tunnels tab.
4. The VPN Tunnels page opens with a table of open tunnels to VPN sites.
5. Click Save IKE Trace.

   A File Download dialog box appears.
6. Click Save.

   The Save As dialog box appears.
7. Browse to a destination directory of your choice.
8. Type a name for the *.elg file and click Save.

   The *.elg file is created and saved to the specified directory. This file contains the IKE traces of all currently-established VPN tunnels.
9. Use the IKE View tool to open and view the *.elg file.
10. To clear the current IKE traces, click Clear IKE Traces.

Downloading the Precompiled Security Policy

For traditional policy management solutions, create a customized policy for each individual customer. You can upload the customized High-Medium-Low *.pfz file from the SmartCenter server to the Nokia IP45 security platform. The Check Point INSPECT engine enables you to dynamically update a security policy, adding support for new applications and attaching signatures to a firewall. The downloading procedure is as follows.

1. The Check Point policy editor generates an INSPECT code.

   Note
   The INSPECT library can be manually edited by a network security professional in order to add support for special applications.

2. The policy editor adds policy rules to the INSPECT library and compiles a *.pfz (single compressed signed file) file.
3. The *.pfz file is then downloaded to the Nokia IP45 security platform by using the CLI.

Use the following commands to download the security policy:

```
download policy
     url urlname
     [user username]
     [password password]
```

Use the following commands to install the security policy manually:

```
set vpn policy <file name>
```

filename is the name of the file, downloaded.

VPN Scenarios

The Nokia IP45 security platform supports the following VPN scenarios:

- Nokia IP45 Security Platform as a VPN Server
- Nokia IP45 Security Platform as VPN Client

Note
The following sections provide only an introduction to the VPN scenarios supported by the Nokia IP45 security platform. They *do not* discuss the complete usage scenario. For more information about usage scenarios, contact the Nokia support site.

Nokia IP45 Security Platform as a VPN Server

Nokia IP45 as a VPN server, supports the following scenario:

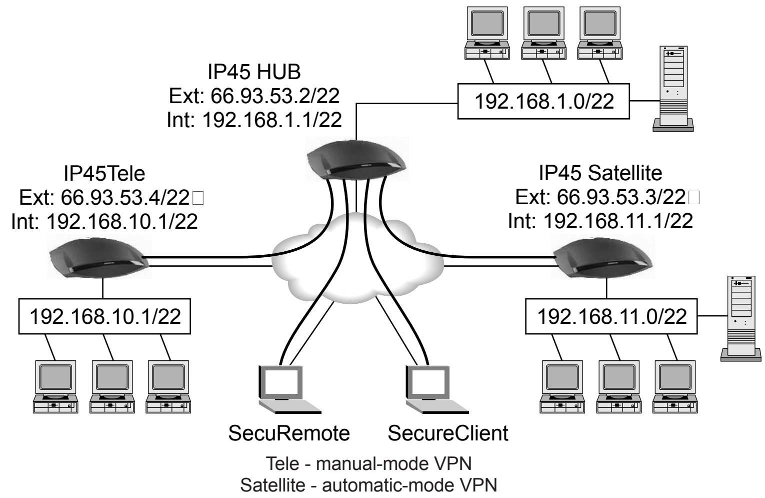
SecuRemote to Nokia IP45 Satellite X (VPN Client to Gateway)

This VPN topology enables Nokia IP45 Tele 8, Nokia IP45 Satellite X, Check Point SecuRemote, and SecureClient VPN clients to connect to an IP45 Satellite X acting as a VPN server.

Note
In this configuration, the IP45 Satellite X VPN server must have a static IP address and domain name.

The following example shows a sample implementation of the VPN client-to-IP45 Satellite X VPN server solution, in which two IP45 devices, a Check Point SecuRemote and a Check Point SecureClient act as VPN clients that download topology information from the IP45 Satellite X VPN server.

Figure 12 SecuRemote and SecureClient to Satellite X



Setting Up Nokia IP45 Satellite X

Configure a VPN tunnel between SecuRemote and IP45 Satellite X.

To set up IP45 Satellite X

1. Add a User.
2. Enable VPN Access for the user.
3. Enable a VPN server.

Setting Up SecuRemote

Define your VPN sites as IP45 Satellite X to set up SecuRemote.

For information about how to configure a remote-to-site VPN between Nokia IP45 Satellite x and a VPN client by using hybrid mode authentication with a RADIUS server, see *Hybrid mode authentication of Nokia IP45* whitepaper.

Note
While establishing a remote to site VPN between Nokia IP45 Satellite x and SecuRemote R55/ R56, ensure that IP45 has a VPN certificate installed in the device.

For more information about how to configure SecuRemote, see *Check Point Desktop Security Guide.*

Nokia IP45 Security Platform as VPN Client

IP45 v4.0 supports the following client scenarios.

- Remote access VPN with another IP45
- Remote access VPN with Check Point VPN-1

Authentication Methods

The Nokia IP45 v4.0 remote access VPN client supports the following new authentication methods:

- X.509 certificates for remote access VPN sites in automatic log-in mode.

  To get X.509 support, Choose from the main menu, Services > Connect to connect to the Check Point management and download a certificate.
- RSA Secure ID tokens for VPN sites in manual log-in mode.

  While authenticating to the VPN site, you must provide a four-digit PIN code and SecureID passcode. The RSA SecureID token generates a new passcode every minute.

For more information about remote access VPNs, see "Configuring Remote Access VPNs" on page 262.

Setting Up Nokia IP45 Tele 8 as a VPN Client

You can configure the IP45 Tele 8 as a VPN client.

To enable the VPN client functionality in your IP45 device

- If you have subscribed to security services, then connect with your service provider or enterprise and receive a security subscription.
- If you are using the IP45 in a standalone mode, add the license manually.

Adding VPN Sites by Using Nokia IP45 Tele 8

You can define only remote access VPN sites using IP45 Tele 8 licenses. To define site-to-site VPN gateways, you must have IP45 Satellite X license.

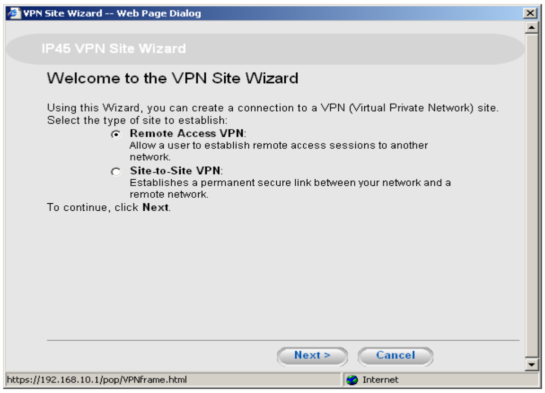
VPN sites represent VPN gateways to which you can connect. You must define VPN sites before you connect to them.

To add or edit VPN sites

1. Choose VPN from the IP45 main menu and click VPN Sites.

   The VPN Sites page opens, with the list of VPN sites configured.
2. To add a VPN site, click New Site.
3. To edit a VPN site, click Edit in the VPN site row.

If you click New Site, the Nokia VPN Site Wizard opens.


VPN Site Wizard -- Web Page Dialog
IP45 VPN Site Wizard

Welcome to the VPN Site Wizard

Using this Wizard, you can create a connection to a VPN (Virtual Private Network) site.
Select the type of site to establish:

● **Remote Access VPN**:
Allow a user to establish remote access sessions to another network.

○ **Site-to-Site VPN**:
Establishes a permanent secure link between your network and a remote network.

To continue, click **Next**.

Next >
Cancel
https://192.168.10.1/pop/VPNframe.html
Internet

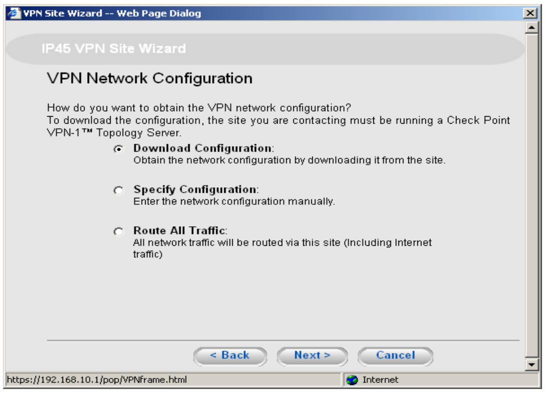
4. Click Next.

   The VPN Gateway Address dialog box appears.

5. Enter the IP address of the VPN gateway to connect to as given by the network administrator.

6. Click Next.

   The VPN Network Configuration window opens.



VPN Network Configuration

How do you want to obtain the VPN network configuration?
To download the configuration, the site you are contacting must be running a Check Point VPN-1™ Topology Server.

● **Download Configuration**:
Obtain the network configuration by downloading it from the site.

○ **Specify Configuration**:
Enter the network configuration manually.

○ **Route All Traffic**:
All network traffic will be routed via this site (Including Internet traffic)

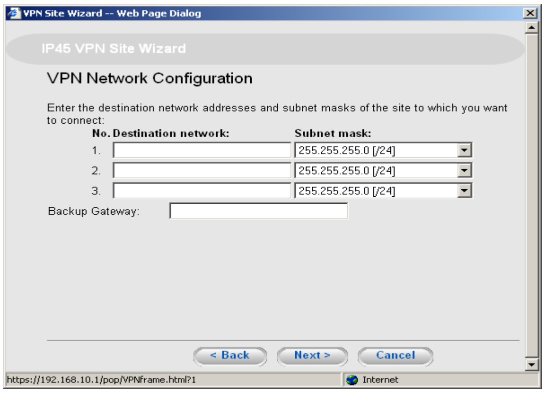
7. Select one of the following:

   - **Download Configuration**—to obtain network configuration from a VPN site. This option automatically downloads the network topology (gateway information and rules) from the VPN site.
   - **Specify Configuration**—to provide the network configuration manually.
   - **Route All Traffic**—to route all network traffic from the VPN site.

Note
You can download the network configuration only if you are connecting to a Check Point VPN-1 or Nokia IP45 Satellite X VPN Gateway.

To specify configuration

8. If you chose Specify Configuration in the preceding procedure, the following window opens.


VPN Site Wizard -- Web Page Dialog
IP45 VPN Site Wizard
< Back
Next >
Cancel
https://192.168.10.1/pop/VPNframe.html?1
Internet

VPN Network Configuration

Enter the destination network addresses and subnet masks of the site to which you want to connect:

No.	Destination network:	Subnet mask:
1.		255.255.255.0 [/24]
2.		255.255.255.0 [/24]
3.		255.255.255.0 [/24]

Backup Gateway:

9. Enter the destination network address and subnet mask of the site to connect to.

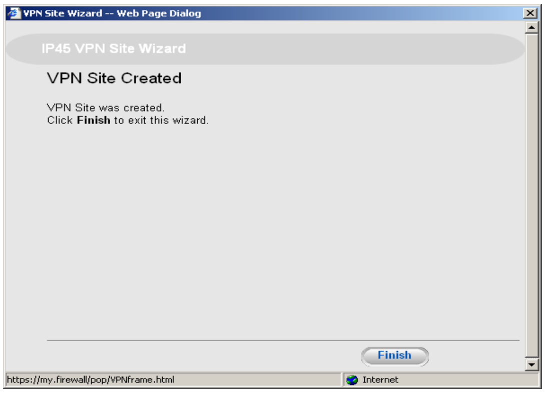
Note
Obtain destination network and subnet mask from the VPN gateway system administrator.

10. Click Next.

The Site Name dialog box appears.

11. Enter a name for the VPN site.

12. Click Next.The VPN Site Created window opens.


VPN Site Wizard -- Web Page Dialog
IP45 VPN Site Wizard
Finish
https://my.firewall/pop/VPNframe.html
Internet

VPN Site Created

VPN Site was created.
Click **Finish** to exit this wizard.

13. Click Finish.

14. Click the VPN Login tab.

Log in if you need to authenticate each time a VPN tunnel is created.

All of the computers connected to the LAN network of the Nokia IP45 Tele 8 user must manually log in with the same user name and password on all of the login pages of the connected computers.

Note
The Automatic Login feature is not available for the IP45 Tele 8 license.

To download configuration

1. From the VPN Network Configuration page, choose Download Configuration in Adding VPN sites by using IP45 Tele 8. A dialog box appears.
2. Click Next, the Network Topology is downloaded from the specified VPN gateway.

   The VPN Login page opens.
3. Follow steps 9 to 13 in "To specify configuration" on page 286, to proceed.

The VPN sites page updates with the added VPN sites. If you edited a VPN site, the modifications are reflected in the VPN sites list.

To route all traffic

If you chose Route All Traffic in Adding VPN sites by using the IP45 Tele 8, the VPN Network Configuration dialog box appears with the following message:

> Only one VPN Profile can be configured as Route All Traffic.

1. Check either Download Configuration or Specify Configuration, depending on how you want to obtain the VPN network configuration.
2. Follow steps 9 to 13 in "To specify configuration" on page 286, to proceed.

Nokia IP45 Site-to-Site VPNs support

The following sections describe site-to-site VPNs, and the modes they support.

Adding VPN Sites by Using Nokia IP45 Satellite X

You can define each VPN site according to the function you want IP45 Satellite X to perform while connecting to the site:

- **VPN Client**—define the VPN site as a remote access VPN site using the following procedure.
- **VPN Gateway**—do the following:
  - Define the second VPN site as a site-to-site VPN gateway by using the following procedure.
  - Define the first VPN site as a site-to-site VPN gateway.

To add or edit VPN sites by using Nokia IP45 Satellite X

1. Choose VPN from the main menu.

   The VPN Server page opens.

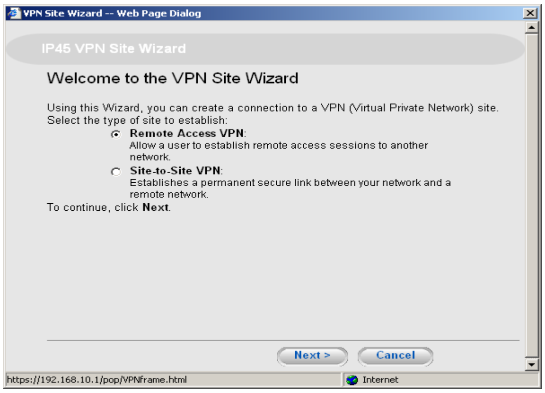
2. In the VPN submenu, click VPN Sites.

   The VPN Sites page opens with a list of VPN sites.

3. Do either of the following:

   - To add a VPN site, click New Site.
   - To edit a VPN site, click Edit in the desired VPN site row.

   The IP45 VPN Site wizard opens, with the Welcome to the VPN Site wizard window is displayed.



VPN Site Wizard -- Web Page Dialog
IP45 VPN Site Wizard

Welcome to the VPN Site Wizard

Using this Wizard, you can create a connection to a VPN (Virtual Private Network) site.
Select the type of site to establish:

● **Remote Access VPN**:
Allow a user to establish remote access sessions to another network.

○ **Site-to-Site VPN**:
Establishes a permanent secure link between your network and a remote network.

To continue, click **Next**.

Next >
Cancel
https://192.168.10.1/pop/VPNframe.html
Internet

4. Do one of the following:

   - Select Remote Access VPN to establish remote access from your VPN client to a VPN server or gateway.
   - Select Site-to-Site VPN to create a permanent bidirectional connection to another gateway.

5. Click Next.

   The VPN Gateway Address dialog box appears.

6. Enter the IP address of the VPN gateway to connect, as given to you by the network administrator.

7. Click Next.

8. The VPN Network Configuration dialog box appears. To proceed, see "Setting Up the Nokia IP45 Security Platform as a VPN Server" on page 259.

9. Choose Reports > VPN tunnels to view the active VPN tunnels with Phase-I negotiation.

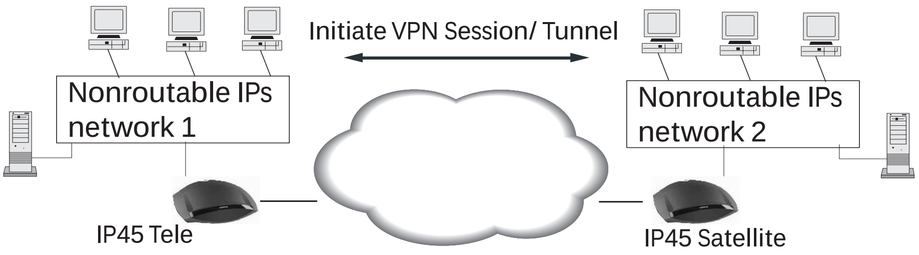
10. In order to see the Phase-II negotiation choose Reports > Active Connections and click the lock symbol of the FTP, HTTPS, or SSH traffic passing through the VPN tunnel.

Nokia IP45 Tele to IP45 Satellite X (VPN Client to Gateway)

Nokia IP45 Tele 8 functions in VPN client mode, in which connection is initiated by the VPN client.

Nokia IP45 Tele 8 uses a manual mode VPN connection. To select the VPN gateway to which you want to establish a VPN connection, go to http://my.vpn.

Figure 13 IP45 Tele 8 as VPN Client


Initiate VPN Session/ Tunnel
Nonroutable IPs network 1
Nonroutable IPs network 2
IP45 Tele
IP45 Satellite

If the VPN client is enabled, the IP45 GUI main menu includes a VPN menu option. In addition, the Reports pages include VPN Tunnels submenu that allows you to view the active VPN tunnels.

Setting Up Nokia IP45 Tele 8

Configure a VPN tunnel between an IP45 Tele 8 and an IP45 Satellite X.

Setting Up Nokia IP45 Satellite X

Configure a VPN tunnel between a Nokia IP45 Tele 8 and an Nokia IP45 Satellite X.

To set up Nokia IP45 Satellite X

1. Add a User.
2. Enable VPN remote access for the user you added.
3. Enable the VPN server.

Nokia IP45 Tele 8 to Check Point FP1, FP2, FP3, NG, NG AI, NGX R60 or NGX R61

You can use the IP45 Tele 8 as a VPN client to establish a Remote to Site VPN connectivity with a Check Point server by using version 4.1, FP1, FP2, FP3, NG, NG AI, NGX R60 and NGX R61.

For more information, see related Check Point documentation.

Setting Up Nokia IP45 Tele 8

Configure a VPN tunnel between an IP45 Tele 8 and an IP45 Satellite X.

Setting Up Check Point Server

Open the Check Point policy editor and select the Firewall-1/ VPN -1 workstation object that will receive the VPN-1 Edge/Embedded gateway session request.

For more information, see Check Point FP3 documentation.

Nokia IP45 Tele 8 to Check Point NG AI

You can use Nokia IP45 Tele 8 as a VPN client to establish a VPN connectivity with a Check Point NG AI server using a VPN-1 Edge/Embedded gateway dynamic object. This topology uses a remote-access VPN community.

IP45 Tele 8 uses a manual-mode VPN connection only. To select the VPN gateway to establish a VPN connection, go to http://my.vpn.

Setting Up Nokia IP45 Tele 8

To configure a VPN tunnel between Nokia IP45 Tele 8 and Check Point FP3, on IP45 Tele 8, (VPN client) add a VPN site.

Setting Up Check Point NG AI

Configure a VPN-1 Edge/Embedded gateway object on the Check Point Smart Dashboard.

To set up Check Point NG AI

1. Create a gateway by choosing Check Point > VPN-1 Edge/Embedded gateway.
2. Create a user and add the user to the VPN users group.
3. Create a remote access VPN community.
   - Include NG AI firewall object in the participating gateway.
   - Include the Users group in the participating users.
4. In the policy editor, create a rule with the following parameters:

   Source User: any

   Destination: any

   Through: remote access community

   Target: NG AI firewall object

Note
You can also use Check Point FP3 or FP4 in place of NG AI.

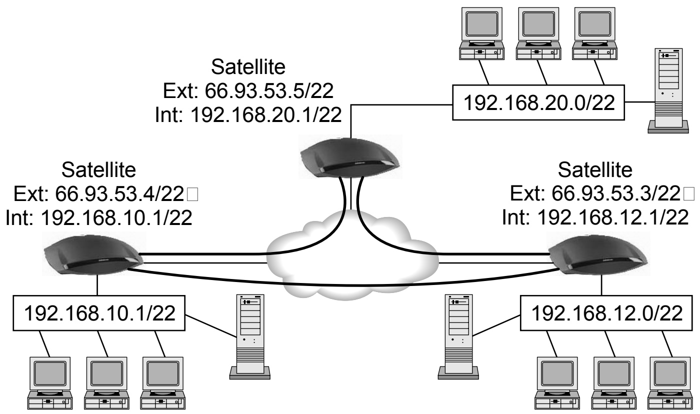
Nokia Satellite X to Nokia Satellite X (VPN Gateway-to-Gateway)

The VPN configuration between Nokia IP45 Satellite X and another Nokia IP45 Satellite X enables you to establish site-to-site VPN connections between two Nokia IP45 site-to-site VPN gateways.

Note
In this configuration, both Nokia IP45 Satellite X site-to-site VPN gateways must have a static IP address.

Figure 14 on page 291 shows a sample implementation of the Satellite X to Satellite X solution with three Satellite X devices. Each Nokia IP45 device acts as a Site-to-Site VPN gateway for a fully secure network. The networks communicate through VPN connections.

Figure 14 Nokia IP45 Satellite X to Nokia IP45 Satellite X



Setting Up Nokia IP45 Satellite X

Configure a VPN tunnel between two Nokia IP45 Satellite X devices (site-to-site VPN).

To set up the IP45 Satellite X

1. Specify the IP address of Nokia IP45 Satellite X on the remote Nokia IP45 Satellite X.
2. Enter the shared secret (a password that is known to both the IP45 Satellite X devices).

To set up the remote Nokia IP45 Satellite X

1. Specify the IP address of your IP45 Satellite X.
2. Enter the shared secret (a password that is known to both the IP45 Satellite X devices.)

Nokia IP45 Satellite X in NAT and Bypass NAT Modes

VPN configuration allows you to choose how your VPN should function. Use of NAT and No-NAT modes offer great flexibility.

NAT mode allows you to define VPNs at peer gateway sites without knowing the protected network behind the IP45 devices.

To access a resource that is protected by a VPN in NAT mode, you must contact the hiding (Internet) address of the VPN gateway. Your request is then forwarded to the correct computer in the protected network according to the defined security rules.

To access a resource that is protected by a VPN in bypass-NAT mode, you must contact the IP address of the last computer in the destination network that you want to reach.

Note
You can establish VPN tunnels between a combination of NAT and no-NAT devices. This possibility is not discussed in this guide.

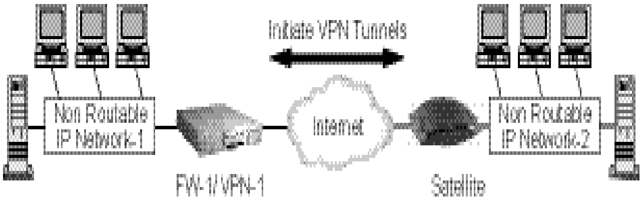
NAT Mode

Use NAT mode in site-to-site VPNs, where bidirectional initiation of traffic between networks using public IP addresses is required.

Note
The IP45 NAT engine allows multiple PPTP/IPSec clients to communicate simultaneously through the firewall even when NAT is in use.

Figure 15 shows two instances of site-to-site VPN gateways in NAT mode.

Figure 15 NAT Mode



Solution A: Nokia IP45 Satellite X to VPN-1 (Site-to-Site VPN)

Hosts on Network 1 establish the TCP/IP connection to the external IP address of the IP45 Satellite X site-to-site VPN gateway. The IP45 Satellite X device is configured through the IP45 GUI Security page to port forward the inbound traffic to the defined host.

Solution B: Nokia IP45 Satellite X to Satellite X (Site-to-Site VPN)

IP45 Satellite X supports the creation of site-to-site VPN connections between two or more IP45 Satellite X devices. Hosts on either network can directly initiate traffic to hosts on the peer network. The IP45 Satellite X is configured through the IP45 GUI Security page to port forward the inbound traffic to the defined host.

Bypass NAT

The Nokia IP45 security platform supports the bypass NAT option. When this feature is enabled, NAT is not performed on the internal network for authenticated remote users.

Bypass Firewall

When the bypass firewall feature is enabled, firewall rules are not applied to the internal network for authenticated remote users.

To enable bypass NAT or bypass firewall

1. Choose VPN from the IP45 main menu.

   The VPN Server page opens.
2. To disable NAT, select Bypass NAT.
3. To disable firewall rules, select Bypass Firewall.
4. Click Apply.

Defining a Backup VPN Gateway

You can define a backup VPN gateway to support the main or primary VPN gateway. If the primary VPN gateway fails, the backup gateway takes over.

To define a backup VPN Gateway

1. Choose VPN from the IP45 main menu, and click the VPN Sites tab.
2. Click New Site at the bottom of the page.

   The VPN Site wizard appears.
3. Select Site-to-Site VPN, and click Next.

   The VPN Gateway address window opens.
4. Enter the IP address of the primary Check Point management station with enforcement module, and click Next.

   The VPN Network Configuration window opens.

5. In the Destination Network text box 1, enter the network address behind the primary Check Point management station with enforcement module.

   Select 255.255.255.0/24 as the subnet mask.

6. In the Destination Network text box 2, enter the network address behind the secondary Check Point management station with enforcement module.

   Select 255.255.255.0/24 as the subnet mask.

7. Enter the IP address of the secondary Check Point management station in the Backup Gateway field.

For information about how to configure the primary and secondary Check Point management stations, see *Check Point Multiple Entry Point* document.

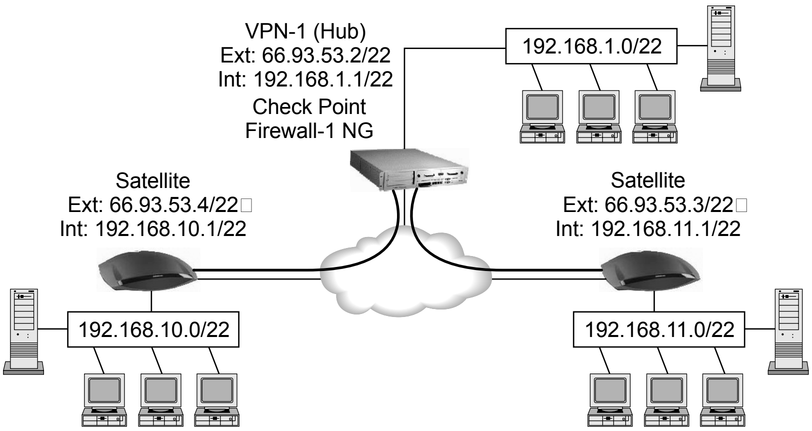
Nokia IP45 Satellite X to VPN-1 (Site-to-Site VPN)

Nokia IP45 Satellite X to VPN-1 or Check Point v4.1, FP1, FP2, FP3, NG, or NG AI configuration enables you to establish site-to-site VPN connections between an IP45 Satellite X site-to-site VPN gateway and a VPN-1 site-to-site VPN gateway.

Note
In this solution model, both the VPN-1 and IP45 Satellite X site-to-site VPN gateways must have a static IP address.

Figure 16 shows an implementation of the IP45 Satellite X to Check Point VPN-1 solution, in which two IP45 Satellite X devices are connected to a VPN-1 site-to-site VPN gateway.

Figure 16 Nokia IP45 Satellite X to VPN-1



Setting Up Nokia IP45 Satellite X

Configure a VPN tunnel between a Nokia IP45 Satellite X and Check Point VPN-1 server or gateway.

To configure Nokia IP45 Satellite X

1. Specify the IP address of Nokia IP45 Satellite X on the VPN-1 server.
2. Enter the shared secret (a password that is known to both the IP45 Satellite X and the VPN-1 Server).

Note
For information about how to set up VPN-1, see the *Check Point Virtual Private Network* documentation.

Nokia IP45 Satellite X to Check Point FP3 or DAIP

You can use Nokia IP45 Satellite X as a VPN server to establish a VPN connectivity with Check Point FP3 server by using a Check Point FP3 DAIP object.

Setting Up Check Point FP3

Configure a VPN tunnel between an IP45 Satellite X and Check Point FP3 server.

To set up Check Point FP3

1. Define a DAIP object.
2. Enable IKE.
3. Use the VPN export tool to create a .p12 certificate from the internal certificate defined for the DAIP object.
4. Configure a rule, set with the following parameters:

   Source: internal network of the IP45 DAIP object

   Destination: internal network of FP3

   Select Encrypt.
5. Push the policy onto the FP3 firewall object.
6. Import the certificate to the computer to which the IP45 Satellite X is connected.

   Use FTP or a floppy disk to import the certificate.

Setting Up Nokia IP45 Satellite X

Configure a VPN tunnel between an IP45 Satellite X and Check Point FP3 server.

To set up Nokia IP45 Satellite X

1. On the IP45 GUI main page, click VPN.

   The VPN Server page opens.
2. Click Certificate > Install Certificate, browse for the certificate.

   Click Upload.
3. Enter the Certificate pass phrase that you use to create the certificate.
4. Click OK.

When you create a VPN connection between IP45 Satellite X and Check Point FP3, select Use Certificate instead of Use Shared Secret.

Nokia IP45 Satellite X to Check Point SmartCenter FP3/NG AI

You can use Nokia IP45 Satellite X as a VPN server to establish VPN connectivity with SmartCenter FP3/NG AI server by using VPN-1 Edge/Embedded gateway or using VPN-1 Edge/Embedded ROBO gateway when you use Smart LSM (VPN Star Community).

Setting Up Check Point SmartCenter FP3/NG AI

Configure the Check Point SmartCenter FP3 for a VPN connection with Nokia IP45 Satellite X.

To set up Check Point SmartCenter FP3/NG AI

1. Define a VPN-1 Edge/Embedded Gateway.
2. Create a new Star Community.
3. Configure a VPN central gateway as the FP3 firewall object.
4. Configure VPN-1 Edge/Embedded gateway as a Satellite X gateway.
5. Define access rules with the following parameters:

   Source: any

   Destination: any

   If Via: Remote access

   Action: accept

   Install On: FP3 firewall object

Setting Up Nokia IP45 Satellite X for VPN Connection with SmartCenter FP3

The following sections describe how to set up Nokia IP45 Satellite X for VPN configuration with SmartCenter FP3:

To configure IP45 Satellite X for VPN connection with SmartCenter FP3

1. Specify the IP address of Nokia IP45 Satellite X on the VPN-1 server.
2. Enter the shared secret (a password that is known to both the IP45 Satellite X and the VPN-1 Server).

Setting Up Check Point SmartCenter NG AI by Using Certificates with Smart LSM

Configure the Check Point SmartCenter NG AI for a VPN connection with Nokia IP45 Satellite X using Certificates with Smart LSM.

To set up Check Point Smart LSM

1. Define a VPN-1 Edge/Embedded ROBO gateway with a dynamic IP address on the Smart LSM.
2. Create a Check Point Smart LSM object on the Check Point Smart Dashboard.
3. Create a new Star Community.
4. Configure a VPN central gateway as the NG AI firewall object.
5. Configure VPN-1 Edge/Embedded gateway as a Satellite X gateway.
6. Define access rules with the following parameters:

   Source: Any

   Destination: Any

   If Via: Star Community

   Action: Accept

   Install On: NG AI firewall object

To configure IP45 Satellite X for VPN connection with SmartCenter NG AI using Certificates.

1. Choose Services from the IP45 main menu, and choose Connect.

   The Subscription Services wizard appears.
2. Enter the IP address of the Check Point NG AI Management station.

   The Connecting window opens.
3. Enter the Gateway ID and Registration Key that is used while creating the IP45 dynamic object on the LSM.

4. The Connecting window opens.

   After the connection is complete, the list of Services downloaded page opens.
5. Click Finish.
6. Choose VPN from the main menu and click the VPN Certificate tab.
7. Click the VPN Sites tab and click New Site.
8. Specify the IP address of the Check Point NG AI management station and check Unrestricted.
9. Click Next.
10. Select Specify Configuration.
11. Enter the Destination network and the subnet mask.
12. Click Next.
13. Click Use Certificate.
14. Click Next.
15. Click Finish.

Note
To download the certificate from Check Point NG AI and create a VPN site manually on Nokia IP45, use the VPN-1 Edge/Embedded gateway on the Smart Dashboard and create a Star VPN community.

Site-to-Site VPN with Windows 2000

You can configure for VPN connectivity between Nokia IP45 Satellite X and Microsoft Windows 2000 / XP IPSec for site-to-site VPN.

Authentication supported: preshared secret

The following scenarios are supported:

- **Windows Gateway to Nokia IP45 Satellite X *in* bypass NAT mode**—NAT is not performed to the internal network for authenticated remote users.
- **Windows gateway to Nokia IP45 Satellite X *in* bypass firewall mode**—firewall rules are not applied to the internal network for authenticated remote users.
- **Windows host to Nokia IP45 Satellite X in bypass NAT mode**— NAT is not performed to the internal network for authenticated remote users.
- **Windows host to Nokia IP45 Satellite X *in* bypass firewall mode**—firewall rules are not applied to the internal network for authenticated remote users.

For more information about how to configure the Windows 2000 server, see *SofaWare's Configuring Windows 2000/ XP IPSec to Site-to-Site VPN*.

Site-to-Site VPN with Nokia CryptoCluster

You can configure for VPN connectivity between Nokia IP45 Satellite X and a Nokia VPN Gateway (CryptoCluster) for site-to-site VPN.

Authentication supported: preshared secret

Perfect Forward Secrecy: supported

The following scenario is supported:

- **Nokia VPN gateway to Nokia IP45 Satellite X *in* bypass NAT and bypass firewall mode**—NAT is not performed to the internal network for authenticated remote users.

For more information about how to configure CryptoCluster, see *Configuring Nokia CryptoCluster to Nokia IP45 Site-to-Site VPN*.

Site-to-Site VPN with Cisco PIX

You can configure for VPN connectivity between Nokia IP45 Satellite X and the Cisco secure PIX firewall (using PDM 2.0 and above) for site-to-site VPN.

Authentication supported: preshared secret

The following scenario is supported:

- **Cisco PIX Gateway to Nokia IP45 Satellite X in Bypass NAT mode**—NAT is not performed to the internal network for authenticated remote users.

For more information about how to configure CISCO PIX, see SofaWare's *Configuring Site-to-Site VPN with CISCO PIX*.

VPN Routing Between two Nokia IP45 Security Platforms

VPN routing is designed to fulfill the need for gateways to encrypt with each other indirectly, through a central VPN-1 module that acts as a VPN router by decrypting the traffic coming from one gateway and encrypting it to forward to another gateway. This feature is useful in scenarios such as:

- DAIP (VPN-1 Module with a Dynamic IP address) to DAIP encryption. Since the DAIP Modules are not aware of each others dynamically assigned IP address, one solution is to forward traffic through a central VPN-1 router, to which both DAIP modules connect.
- Using the IPSec VPN to mimic the architecture of Frame Relay networks for an easier migration from traditional networks to IP based network.
- Enabling simple configuration for branch offices by hiding the entire network from them, while allowing them full connectivity.

IPSec NAT Traversal

Nokia IP45 v4.0 can establish site-to-site VPN tunnels along with remote-to-site VPNs that pass through NAT devices. VPN peers automatically negotiate NAT traversal mode when needed.

Mesh VPN Support

This section describes mesh VPN support between different Nokia IP45 security platforms using Check Point R55 with HotFix 4 and above. Nokia IP45 v4.0 also supports mesh VPN between different Nokia IP45 security platforms using SofaWare management Portal v4.11 and later.

The Nokia IP45 security platform supports mesh VPN topology using Check Point where different IP45 security platforms are configured as site-to-site VPNs within a mesh topology. The limitation in this scenario is that the IP45 configured on Check Point should have a static WAN IP address.

Enhanced MEP Support

Nokia IP45 v4.0 supports all multiple entry point (MEP) and interface resolving options available in SmartCenter NG AI R55, including:

- MEP load distribution
- Partially overlapping encryption domains
- Fully overlapping encryption domains
- Interface resolving (automatically determining the closest reachable interface for VPN connections to gateways with multiple interfaces)

The following three basic configurations are tested:

Primary backup—multiple backup gateways provide high availability for a primary gateway. The remote VPN peer is configured to work with the primary gateway, and switches to the backup gateway if the primary gateway stops functioning.

You might use this configuration if you have two Check Point gateways in a MEP environment. The computer with high performance can be configured as primary gateway and the other computer as secondary gateway.

Figure 17 Partially Overlapping Encryption Domain

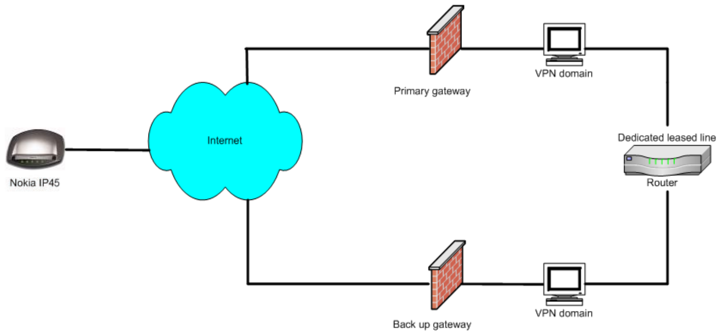
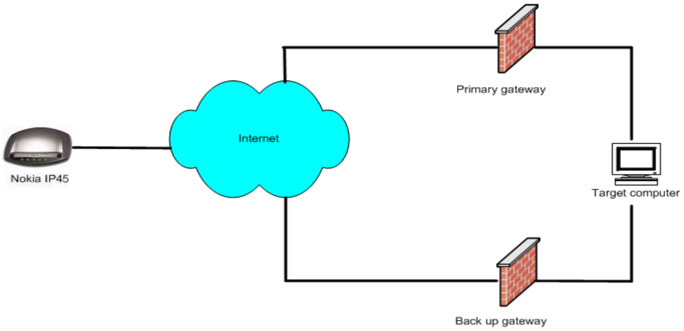


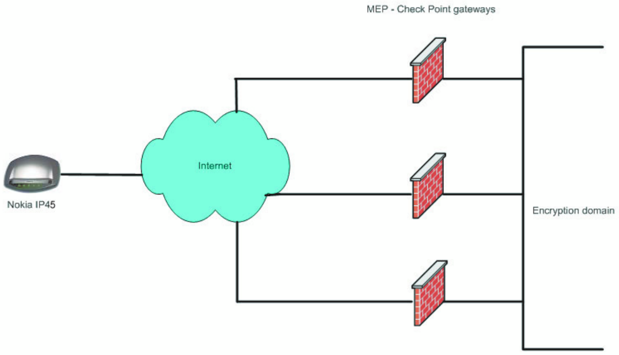
Figure 18 Fully Overlapping Encryption Domain



Load distribution—the remote VPN peers randomly select a gateway to open a VPN session. For each IP source and destination address pair, a new gateway is selected randomly.

You can enable load distribution when you have a number of working Check Point VPN gateways in your network with equal performance abilities.

Figure 19 Load Distribution



First to respond—the first gateway to reply to the peer gateway is chosen. That is, when two gateways are made available with the MEP configuration, the gateway located at the nearest geographical end responds first.

16 Using Managed Services

You can integrate your IP45 security platform into an overall enterprise security policy, for maximum security. The Check Point Security Management Architecture (SMART) delivers a single enterprise-wide security policy that you can centrally manage and automatically deploy an unlimited number of the IP45 gateways.

This chapter describes how to start and use subscription services, such as automatic software and security policy updates, content filtering, email virus scanning, and remote logging. It includes the following topics:

- Starting your Subscription Services
- SofaWare Security Management Portal
- Automatic and Manual Updates
- Managing with the Nokia Horizon Manager
- Check Point SmartCenter LSM

For information about how to use SofaWare Management Center to configure subscription services like Web filtering, email antivirus, and software updates, see "Deploying Nokia IP45 with SofaWare Management Portal" on page 71.

Starting your Subscription Services

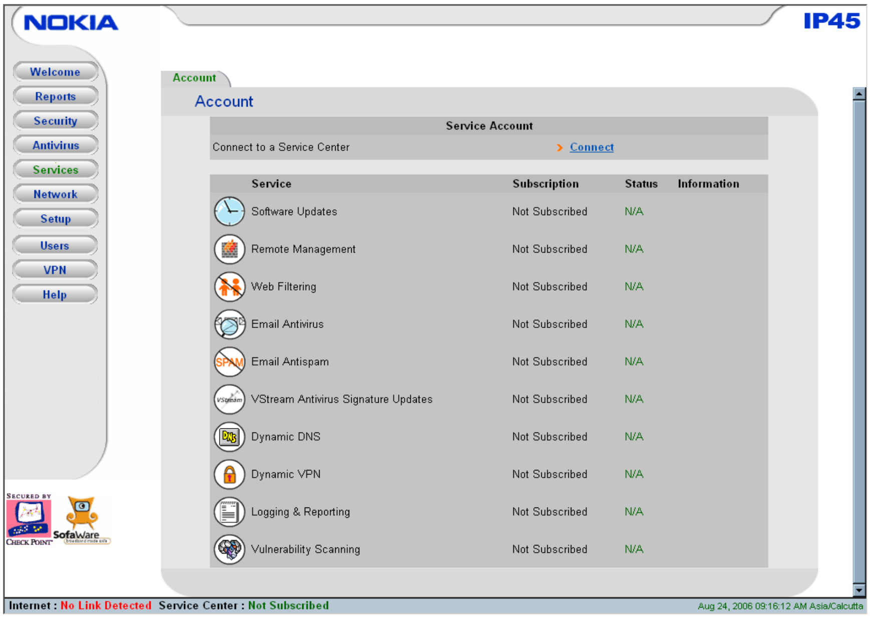
The following sections provide you information about how to start your subscription services.

Note
These services work on the Nokia IP45 security platform. Nokia does not offer these services directly.

To start your subscription

1. Choose Services from the main menu, and click the Account tab.

   The Account page opens.



Account

Service Account	
Connect to a Service Center	› Connect

Service	Subscription	Status	Information
Software Updates	Not Subscribed	N/A	
Remote Management	Not Subscribed	N/A	
Web Filtering	Not Subscribed	N/A	
Email Antivirus	Not Subscribed	N/A	
Email Antispam	Not Subscribed	N/A	
VStream Antivirus Signature Updates	Not Subscribed	N/A	
Dynamic DNS	Not Subscribed	N/A	
Dynamic VPN	Not Subscribed	N/A	
Logging & Reporting	Not Subscribed	N/A	
Vulnerability Scanning	Not Subscribed	N/A	

Internet : No Link Detected Service Center : Not Subscribed Aug 24, 2006 09:16:12 AM Asia/Calcutta

2. In the Service Account area, click Connect.

   The Setup Wizard opens, with the Subscription Services dialog box displayed.

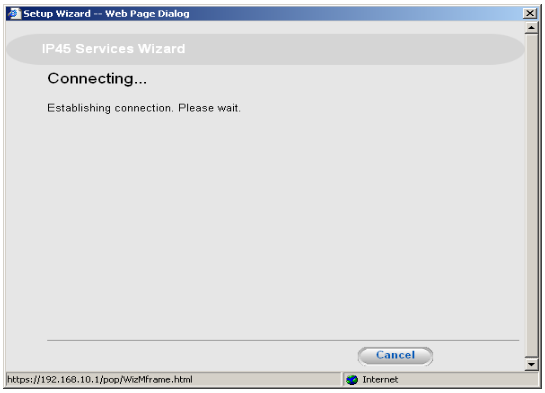
3. Make sure that I wish to connect to a Service Center check box is checked.

4. Do the following:

   - To specify a Service Center, do the following:
     - Select Specified IP.
     - In the Specified IP text box, enter the IP address of the desired Service Center, as given to you by the service center.

5. Click Next.

   - The Connecting window opens.

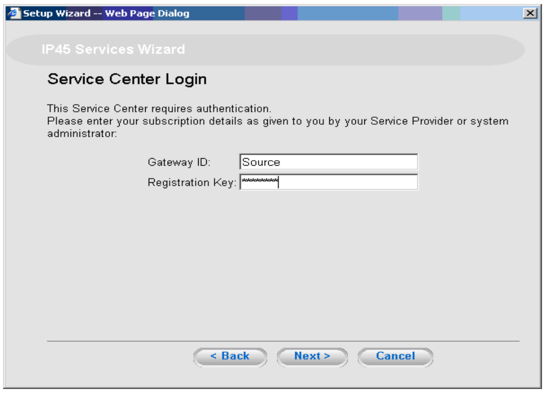


Connecting...

Establishing connection. Please wait.

https://192.168.10.1/pop/WizMframe.html

- If the Service Center requires authentication, a second Service Center Login dialog box appears.



Service Center Login

This Service Center requires authentication.
Please enter your subscription details as given to you by your Service Provider or system administrator.

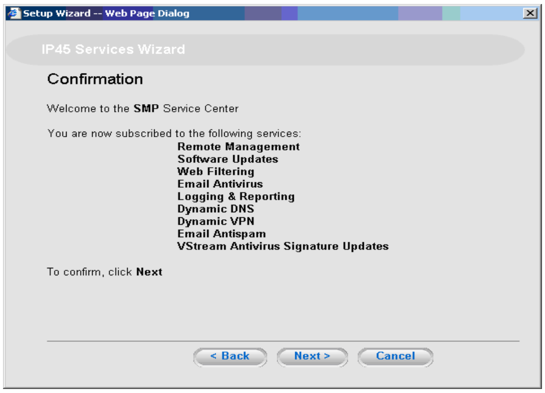
Gateway ID: Source
Registration Key: ********

Do the following:

a. Enter your gateway ID and registration key in the appropriate fields, as given to you by your service provider.

b. Click Next.

- The Connecting window opens.
- The Confirmation dialog box appears with a list of services to which you are subscribed.



Confirmation

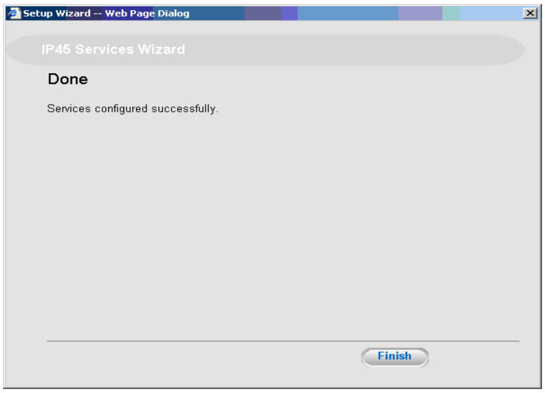
Welcome to the **SMP** Service Center

You are now subscribed to the following services:
Remote Management
Software Updates
Web Filtering
Email Antivirus
Logging & Reporting
Dynamic DNS
Dynamic VPN
Email Antispam
VStream Antivirus Signature Updates

To confirm, click **Next**

6. Click Next.

The Done window opens with a success message.



Done

Services configured successfully.

7. Click Finish.

   Following are the results:

   - If a new firmware is available, the IP45 downloads it. This can take several minutes. When the download is complete, the IP45 restarts by using the new firmware.
   - The Welcome page opens.
   - The services to which you are subscribed are now available on your IP45 and are listed on the Account page. For more information, see "Viewing Service Information from the Account Page" on page 306.

Note
A local administrator cannot locally modify the settings that the service center configures remotely. To change these settings locally, disconnect from the service center.

Viewing Service Information from the Account Page

The following table provides the information about your subscription:

Table 60 Account Page Fields

Field	Description
Service Center Name	Name of the Service Center to which you are connected (if known).
Subscription will end on	Date on which your subscription to services ends.
Service	Services available in your service plan.
Subscription	Status of your subscription to each service: • Subscribed • Not Subscribed

Table 60 Account Page Fields (*continued*)

Field	Description
Status	Status of each service: • Connected: you are connected to the service through the Service Center. • N/A: the service is not available.
Mode	Mode to which each service is set. For further information, see sections on Web Filtering, Virus Scanning and Automatic and Manual Updates.

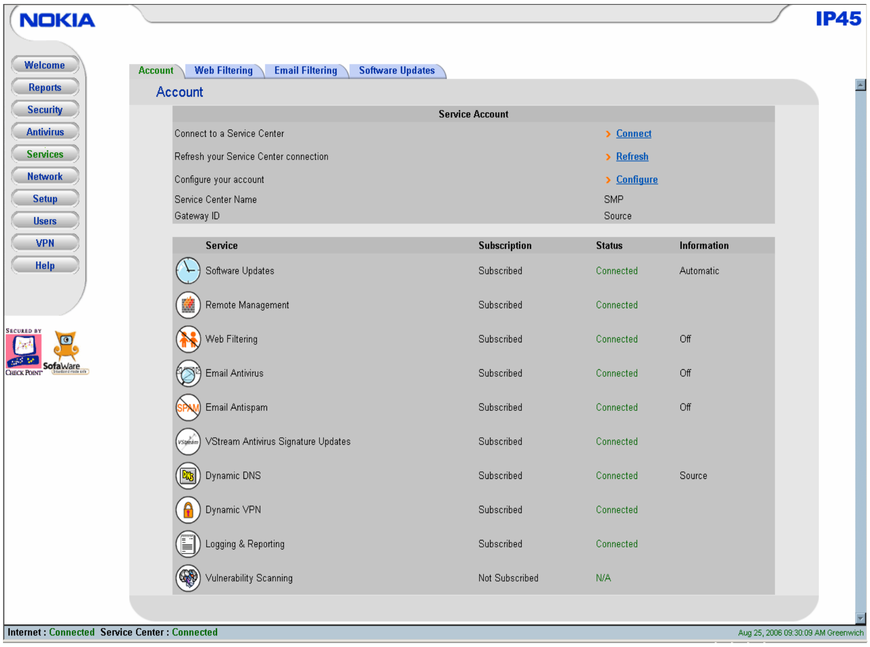
Refreshing your Service Center Connection

The refresh option restarts the connection to the service center and refreshes the service settings of your device.

To refresh your service center connection

1. Choose Services from the main menu, and click the Account tab.

   The Account page opens.



Account

Service Account	
Connect to a Service Center	› Connect
Refresh your Service Center connection	› Refresh
Configure your account	› Configure
Service Center Name	SMP
Gateway ID	Source

Service	Subscription	Status	Information
Software Updates	Subscribed	Connected	Automatic
Remote Management	Subscribed	Connected	
Web Filtering	Subscribed	Connected	Off
Email Antivirus	Subscribed	Connected	Off
Email Antispam	Subscribed	Connected	Off
VStream Antivirus Signature Updates	Subscribed	Connected	
Dynamic DNS	Subscribed	Connected	Source
Dynamic VPN	Subscribed	Connected	
Logging & Reporting	Subscribed	Connected	
Vulnerability Scanning	Not Subscribed	N/A	

Internet : Connected Service Center : Connected Aug 25, 2006 09:30:09 AM Greenwich

2. In the Service Account area, click Refresh.

   The IP45 reconnects to the Service Center.

   Your service settings are refreshed.

Note
When you connect to a service center using a DNS name, the DNS address is saved, and periodically looked up again. This process allows you to change the IP address of the service center without disconnecting all the connected devices.

Configuring your Account

You may access your service center Web site, for additional configuration options of your account.

To configure your account

1. Choose Services in the main menu, and click the Account tab.

   The Account page opens.

2. In the Service Account area, click Configure.

   Note
   If no additional settings are available from your service center, this button does not appear.

   Your service center Web site opens.

3. Follow the instructions on the window.

Disconnecting from your Service Center

If desired, you can disconnect from your Service Center.

To disconnect from your service center

1. Choose Services from the main menu, and click the Account tab.

   The Account page opens.

2. In the Service Account area, click Connect.

   The Setup Wizard opens, with the first Subscription Services dialog box displayed.

3. Uncheck the I wish to connect to a service center check box.
4. Click Next.

   The Done window opens with a success message.

5. Click Finish.

Following are the results:

- You are disconnected from the Service Center.
- The services to which you were subscribed are no longer available on your IP45.

SofaWare Security Management Portal

The SofaWare Security Management Portal (SMP) is a security platform that enables centralized management of a large number of firewalls embedded in broadband access devices or gateways.

Note
Configure the management servers by using SMP, before you can use subscription services such as Web filtering, email antivirus, and software updates.

Using the Sofaware Management Portal, you can:

- Browse and update your user database.
- Update security policies and user interface files.
- Configure and fine-tune SofaWare management servers.

To create a gateway of type IP45 on SofaWare Security Management Portal

1. Click New Gateway in the main menu of SMP portal.

   The new gateway page opens.

2. Select a new gateway type, IP45.

   The registration key is automatically generated.

3. Save the settings that you made.

Click the Servers on the main menu for a list of server groups and management servers.

For more information, see SofaWare Management Portal/SofaWare Management Center documents.

Web Filtering

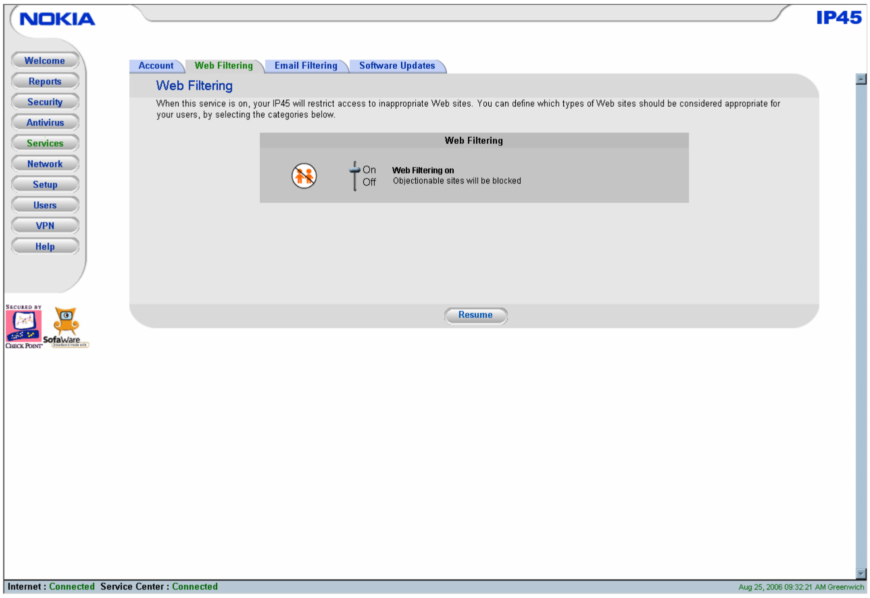
When Web filtering is enabled, access to Web content is restricted according to the categories specified under Allow Categories. Adult users can view Web pages with no restrictions, only after they provide the administrator password from the Web filtering popup window.

Note
If you are remotely managed, contact your service center to change these settings.

To enable or disable Web filtering

1. Choose Services from the main menu, and click the Web Filtering.

   The Web Filtering page opens.



Web Filtering

When this service is on, your IP45 will restrict access to inappropriate Web sites. You can define which types of Web sites should be considered appropriate for your users, by selecting the categories below.

Web Filtering

On
Off

Web Filtering on
Objectionable sites will be blocked

Internet : Connected Service Center : Connected   Aug 25, 2006 09:32:21 AM Greenwich

2. Move the On/Off lever upwards or downwards.

   Web Filtering is enabled or disabled for all internal network computers.

Selecting Categories to Block

You can define which types of Web sites are considered appropriate for your family or office members, by selecting the categories. Categories marked with a check mark remain visible, while categories marked with a plus mark (+) are blocked and require the administrator password for viewing.

Note
If you are remotely managed, contact your service center to change these settings.

To allow or block a category

1. In the Allow Categories area, click the check mark or the plus sign (+) next to the desired category.
2. Click Apply.

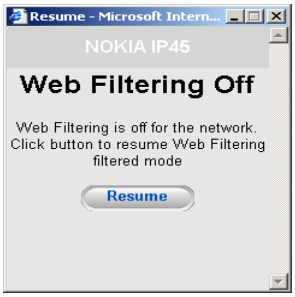
To temporarily disable Web filtering

1. Choose Services from the main menu, and click the Web Filtering tab.

   The Web Filtering page opens.

2. Click Snooze.

   - Web filtering is temporarily disabled for all internal network computers.
   - Snooze changes to Resume.
   - The Web Filtering Off popup window opens.



Web Filtering Off

Web Filtering is off for the network. Click button to resume Web Filtering filtered mode

3. To re-enable the service, click Resume, either in the popup window, or on the Web Filtering page.

   - The service is re-enabled for all internal network computers.
   - If you clicked Resume in the Web Filtering page, the button changes to Snooze.
   - If you clicked Resume in the Web Filtering Off popup window, the popup window closes.

Virus Scanning

Enabling this option results in automatic scanning of your email for the detection and elimination of all known viruses and vandals.

Enabling or Disabling Email Antivirus

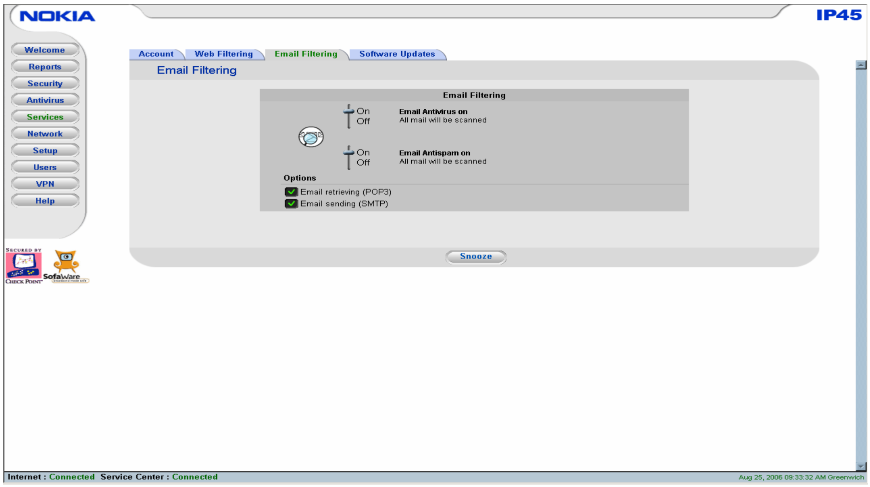
This section gives you information about how to enable or disable the email antivirus option.

Note
If you are remotely managed, contact your service center to change these settings.

To enable or disable email antivirus

1. Choose Services from the main menu, and click the Email Antivirus tab.

   The Email Antivirus page opens.



Email Filtering

Email Filtering

On / Off — Email Antivirus on
All mail will be scanned

On / Off — Email Antispam on
All mail will be scanned

Options

☑ Email retrieving (POP3)

☑ Email sending (SMTP)

Internet : Connected Service Center : Connected Aug 25, 2006 09:33:32 AM Greenwich

2. Drag the On/Off lever upwards or downwards.

   Email Antivirus is enabled or disabled for all internal network computers.

Selecting Protocols for Scanning

If you are locally managed, you can define which protocols should be scanned for viruses:

- Email retrieving (POP3). If enabled, all incoming email in the POP3 protocol is scanned.
- Email sending (SMTP). If enabled, all outgoing email is scanned.

Protocols marked with a check mark are scanned, while those marked with cross mark (x) are not.

Note
If you are remotely managed, contact your service center to change these settings.

To enable virus scanning for a protocol

1. In the Protocols area, click the check mark or plus sign (+) next to the desired protocol.
2. Click Apply.

Temporarily Disabling Email Antivirus

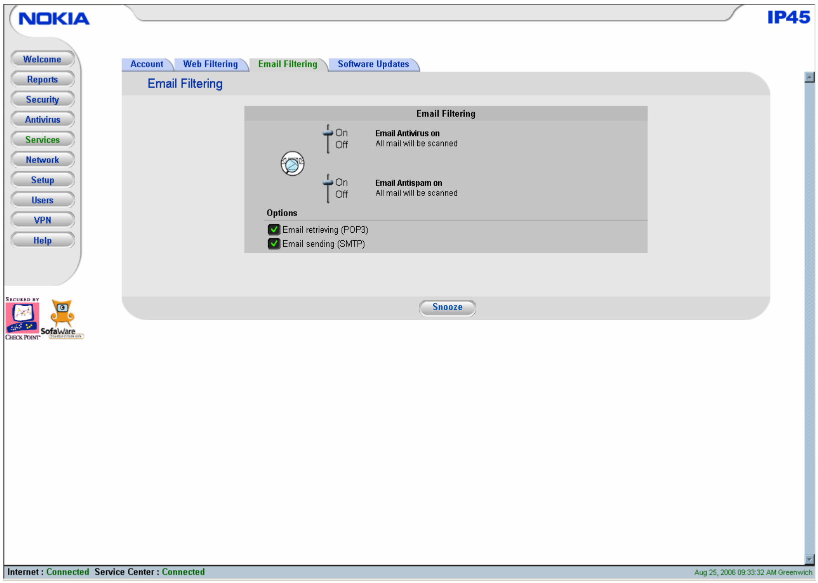
If you are having problems sending or receiving email you can temporarily disable the email antivirus service.

To temporarily disable Email Antivirus

1. Choose Services form the main menu, and click the Email Antivirus tab.

   The Email Antivirus page opens.

2. Click Snooze.
   - Email antivirus is temporarily disabled for all internal network computers.
   - Snooze changes to Resume.



Email Filtering

Email Filtering

On / Off — **Email Antivirus on** — All mail will be scanned

On / Off — **Email Antispam on** — All mail will be scanned

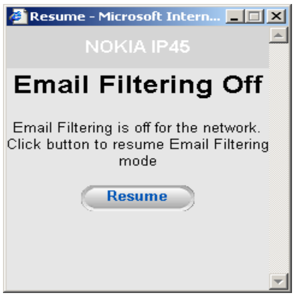
Options

☑ Email retrieving (POP3)

☑ Email sending (SMTP)

Internet : Connected Service Center : Connected Aug 25, 2006 09:33:32 AM Greenwich

   - The Email Antivirus Off popup window opens.



Email Filtering Off

Email Filtering is off for the network. Click button to resume Email Filtering mode

3. To re-enable the service, click Resume, either in the popup window, or on the Email Antivirus page.
   - The service is re-enabled for all internal network computers.
   - If you clicked Resume in the Email Antivirus page, the button changes to Snooze.
   - If you clicked Resume in the Email Antivirus Off popup window, the popup window closes.

Automatic and Manual Updates

If you are subscribed to Software Updates, you can check for new security and software updates.

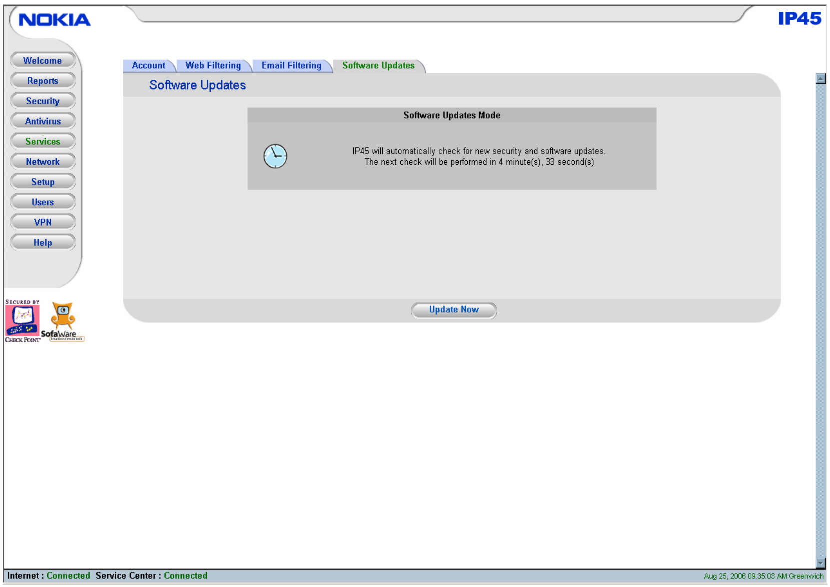
Checking for Software Updates when Locally Managed

If your Nokia IP45 security platform is locally managed, you can set it to automatically check for software updates, or you can set it so that software updates can be checked manually.

To configure software updates when locally managed

1. Choose Services from the main menu, and click the Software Updates tab.

   The Software Updates page opens.



Software Updates

Software Updates Mode

IP45 will automatically check for new security and software updates.
The next check will be performed in 4 minute(s), 33 second(s)

Internet : Connected Service Center : Connected

Aug 25, 2006 09:35:03 AM Greenwich

2. To set the IP45 to automatically check for and install new software updates, drag the Automatic/Manual level upwards.

   The IP45 checks for new updates and installs them according to its schedule.

Note
When the Software Updates service is set to Automatic, you can still manually check for updates.

3. To set the IP45 so that software updates must be checked for manually, drag the Automatic/ Manual level downwards.

   The IP45 does not check for software updates automatically.

4. To manually check for software updates, click Update Now.

The system checks for new updates and installs them.

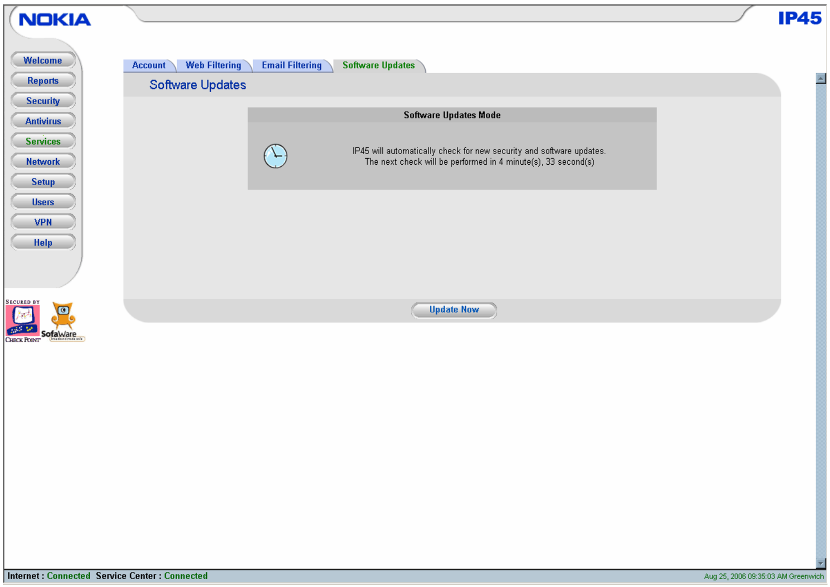
Checking for Software Updates when Remotely Managed

If your IP45 is remotely managed, it automatically checks for software updates and installs them without user intervention. However, you can still *Check for updates Manually*, if needed.

To manually check for security and software updates

1. Choose Services from the main menu, and click Software Updates.

   The Software Updates page opens.



Software Updates

Software Updates Mode

IP45 will automatically check for new security and software updates.
The next check will be performed in 4 minute(s), 33 second(s)

Internet : Connected Service Center : Connected

Aug 25, 2006 09:35:03 AM Greenwich

2. Click Update Now.

   The system checks for new updates and installs them.

Managing with the Nokia Horizon Manager

You can manage your Nokia IP45 security platform by using Nokia Horizon Manager. Nokia Horizon Manager is a software application designed to manage and configure a large number of Nokia security platforms (devices) that reside on a corporate enterprise, managed service provider (MSP), or hosted applications service provider network (ASP).

Note
You can manage the IP45 by using the Nokia Horizon Manager 1.5 SP1 and later only.

To use Nokia Horizon Manager to access and manage your IP45 security platform from the GUI:

1. Choose Setup from the main menu, and choose Management.
2. Choose IP Address Range next to SSH, and specify the IP address of Nokia Horizon Manager.
3. Click Apply.

To use Nokia Horizon Manager Interface to access and manage your IP45 security platform:

1. Click Devices in the main menu and choose Create Devices to create an IP45 device.
2. Click Nokia Small Office Series Platform - IP45 for device type.
3. In the Device text box, type the Device Name (IP45) or the IP address.
4. Click Yes for Use Secure connection.
5. Type the device login and password.
6. Click OK at the bottom of the menu.Your IP45 device is created.

For more details see *Nokia Horizon Manager User Guide*.

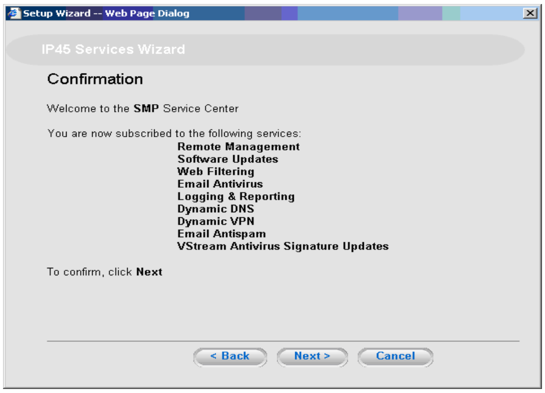
Check Point SmartCenter LSM

Check Point SmartCenter Large Scale Manager (LSM) allows you to manage many Check Point Remote Office/Branch Office (ROBO) gateways from a single SmartCenter Server. The Check Point LSM concept is based on Gateway Profiles, which are defined in the standard Check Point SmartDashboard. Each Gateway Profile represents many ROBO gateways.

For additional information on installing and configuring LSM, see *Check Point SmartCenter LSM documentation.*

To configure NG AI and IP45 for site-to-site by using LSM profiles on the IP45 Side

1. Connect the IP45 to the SmartCenter.
   - Click Services on the main menu and choose Connect.
   - Specify the IP address of Check Point LSM, and click Next.
   - Type the Gateway ID and registration key as defined in VPN-1 Edge/Embedded ROBO gateway, and click Next to continue.
   - After successful connection, the Confirmation window opens giving a list of services to which you have subscribed.



Confirmation

Welcome to the **SMP** Service Center

You are now subscribed to the following services:

Remote Management
Software Updates
Web Filtering
Email Antivirus
Logging & Reporting
Dynamic DNS
Dynamic VPN
Email Antispam
VStream Antivirus Signature Updates

To confirm, click **Next**

2. Open http://my.firewall and verify the following before you proceed:
   a. Enterprise site was added to the VPN site page.
   b. The LSM profile object certificate was synchronized to the device.
   c. Topology was loaded to the device. This should be verified from http://my.firewall/vpntopo.html.
3. You can verify that the tunnel is open by sending packets from the IP45 to the VPN-1 gateway.

To configure NG AI and the Nokia IP45 security platform for site-to-site by using LSM profiles on Check Point

1. Enable LSM: in the command prompt, type LSMenabler on, and reset the FW services.
2. Open SmartDashboard and define a new VPN-1 edge embedded ROBO profile.
3. Name the LSM profile, and click OK.
4. Click Save on SmartDashboard and close.Open SmartLSM.
5. Define a new VPN-1 edge embedded gateway, and select the LSM profile you defined. Make sure to choose the correct HA type (IP45).
6. Open SD again, and define a Star Community.

   Place VPN-1 GW in the Central Gateway, and the LSM profile in the Satellite Gateway.
7. Define a new UDP service on ports to 9281-9282, and name it SW.
8. Place the SW service in the excluded services of the Star Community you defined.
9. Create the rule base, or policy used for managing your device.
10. Install the policy.

17 Troubleshooting

This chapter provides troubleshooting tips, problems your Nokia IP45 security platform might encounter, and solutions for them and includes the following topics:

- Debugging
- Configuring Debugging Levels
- Frequently Asked Questions
- Resetting the IP45 Security Platform to Factory Defaults
- Failsafe Mode
- Running Diagnostics
- Using Packet Sniffer

Debugging

Debugging commands serves as a troubleshooting tool for advanced customers and support engineers by displaying feature-specific information to the enabling console and optionally to the log file. You can configure debug levels by using CLI, for the following features:

- DDNS
- Dial-up
- HA
- Kernel-bgp

The performance of the device does not get affected even if debugging is disabled. But when debugging is enabled for many features, it can affect the primary firewall and VPN task of the Nokia IP45. Debugging should be enabled judiciously and for brief periods.

The debugging commands enable debugging messages based on customer-defined criteria of feature and level.

Configuring Debugging Levels

Use the following commands to configure DDNS debugging levels:

```
set debug ddns level<0-9>
```

Use the following commands to configure dial-up debugging levels:

```
set debug dialup level<0-9>
```

Use the following commands to configure HA debugging levels:

```
set debug ha level<0-9>
```

Use the following commands to configure kernel-bgp debugging levels

```
set debug kernel-bgp level<0-9>
```

Viewing Debugging Levels

Use the following commands to view debugging levels:

```
show debug <ddns | dialup | ha | kernel bgp>
```

For more information about debug commands, see the *Nokia IP45 Security Platform CLI Reference Guide Version 4.0*

Frequently Asked Questions

Please list the modems that are supported.

The following modems are supported:

- Analog modem 56 Kbps (DTE speed: up to 115200)
- ISDN TA (using PPP) 64 Kbps (DTE speed: up to 230400)
- ISDN TA (using MLPPP) 128 Kbps (DTE speed: up to 460800)

I cannot access the Internet. What should I do?

Check for the following:

- Check if the PWR LED is active. If not, check the power connection to the IP45.
- Check if the WAN LED is on. If not check the network cable to the modem and make sure the modem is turned on.
- Check if the LAN LED for the port that your computer uses is on. If not, check if the network cable linking your computer to the IP45 is connected properly.
- Use your web browser to go to http://my.firewall and check whether *connected* appears on the status bar. Make sure that the IP45 network settings are configured according to your service center directions.
- Check your TCP/IP configuration according to Chapter 2.
- If the firewall level is set to High, try setting it to Medium or Low.
- If Web filtering or email antivirus scanning are on, try turning them off.
- Erase all your block rules through the security menu.
- Check with your ISP for possible service outage.

- Check whether you are exceeding the maximum number of computers allowed by your license. See "Viewing Active Computers" on page 252.

I cannot access http://my.firewall or http://my.vpn. What should I do?

- Verify that the IP45 is operating (PWR LED is active).
- Check if the LAN LED for the port that your computer uses is on. If not, check that the network cable, linking your computer and the IP45 is connected properly.
- Try surfing to 192.168.1.2 instead of to my.firewall.

Note
192.168.1.2 is the default value, and it might vary if you changed it in the My Network page.

- Check your TCP/IP configuration according to Chapter 2.
- Restart the IP45 and your broadband modem by disconnecting the power and reconnecting after five seconds.
- If your Web browser is configured to use an HTTP proxy to access the Internet, add my.firewall or my.vpn to your proxy exceptions list.

Every time I start Internet Explorer, the application searches for an Internet connection. This is unnecessary, since I am connected through the IP45. What should I do?

For Internet Explorer, versions 5 and 6, do the following:

1. Open the browser.
2. On the Tools menu, click Internet Options then click the Connections tab.
3. For each item in the Dial-up Settings list, do the following:
    a. Select the item.
    b. Select Never dial a connection.
4. Click Apply.
5. Click OK.
6. Close all active browsers and try again.

Every time I start Outlook Express, the application searches for an Internet connection. This is unnecessary, since I am connected through the IP45. What should I do?

For Outlook Express, versions 5 and 6, do the following:

1. Open Outlook Express.
2. On the Tools menu, click Accounts, then click the Mail tab.
3. For each of the accounts configured in the mail window, do the following:
4. Click Properties, then click the Connection tab.
5. Clear the Always connect to this account using check box.
6. Click OK.
7. Click Close.

8. Close all active browsers and try again.

I run a public Web server at home but it cannot be accessed externally, although it is accessible to the computers on my network. What should I do?

Surf to the security page and use the Servers submenu to allow access to your server.

My network seems extremely slow. What should I do?

- The Ethernet cables might be faulty. For proper operation, the IP45 requires STP CAT5 (shielded twisted pair category five) ethernet cables. Make sure that this specification is printed on your cables.
- Your Ethernet card might be faulty or incorrectly configured. Try replacing your Ethernet card.

I cannot play a certain network game. What should I do?

- Turn the IP45 security to Low and try again.
- If the game still does not work, set the computer you wish to play from to be the DMZ server.
- When you are finished playing the game, make sure to clear the DMZ setting, otherwise your security might be compromised.

I have forgotten my password. What should I do?

Reset the IP45 to factory defaults by using the Reset button as detailed in "Resetting the IP45 Security Platform to Factory Defaults" on page 326.This will erase all your settings.

I cannot connect to a VPN site using the IP45 Satellite or the IP45 Tele. What should I do?

Check whether your VPN client has a problem.

Do one of the following:

- If you are using the IP45 Tele, add the demo Check Point VPN site, using the procedure "Adding and Editing VPN Sites using the IP45 Tele," as follows:
  - In the VPN Gateway Address dialog box, enter 207.40.230.20 in the VPN Gateway field.
  - In the VPN Network Configuration dialog box, select Download Configuration.
- If you are using IP Satellite, add the demo Check Point VPN site, using the procedure Adding and Editing VPN Sites using the IP45 Tele, as follows:
  - In the Welcome to the VPN Site Wizard dialog box, select Remote Access VPN.
  - In the VPN Gateway Address dialog box, enter 207.40.230.20 in the VPN Gateway field.
  - In the VPN Network Configuration dialog box, select Download Configuration.
- Log on to the demo site, using vpndemo as your username and password.
- Surf to http://207.40.230.22

The Check Point VPN-1 SecuRemote Demo Site should open and inform you that you successfully created a VPN tunnel.

I changed the network settings to incorrect values and am unable to correct my error. What should I do?

Reset the network to its default settings by using the reset button at the rear panel of the IP45 device.

I am using the Nokia IP45 security platform with another DSL/Cable router, and I am having problems with some applications.

The IP45 performs network address translation (NAT). You can use the IP45 behind another device that performs NAT, such as a DSL router or wireless router, but the device will block all incoming connections from reaching your IP45.

To fix this problem, do one of the following. (The solutions are listed in order of preference.)

- Consider whether you really need the router. You can use the IP45 as a replacement for your router, unless you need it for some additional functionality that it provides, such as wireless access.
- If possible, disable NAT in the router. For instructions on how to do this, see the router's documentation.

The following suggestions will work only if the router is connected to the WAN port of the IP45:

- If the router has a DMZ computer option, set it to the IP45 external IP address.
- Set the router to direct all incoming connections to the external IP address of the IP45.

Keep in mind that if you use the IP45 behind another NAT device, you might lose some of the advantages of the IP45, such as broad application support and high performance.

I cannot open http://my.firewall page when the LAN address is changed. What should I do?

Renew the IP address of the computer by using ipconfig.

I cannot connect to the HTTPS server in the DMZ. What should I do?

Ensure that HTTPS access to the device is enabled.

I cannot establish HTTPS session to the device even when the HTTPS access to the device is permitted. What should I do?

Ensure that the browser supports 128-bit cipher strength.

I cannot send SMTP or POP3 traffic across the Device what should I do?

Do one of the following: (The solutions are listed in order of preference)

- If antivirus scanning is on, try turning it off.
- If the antivirus is required, then make sure that the CVP server and SMTP server in the server page of SMP are correctly configured.

I cannot send HTTP traffic across the IP45. What do I do?

Do one of the following (The solutions are listed in order of preference.):

- If Web-filtering scanning is on, try turning it off.
- If the URL filtering is required, then make sure the UFP server in the server page of SMP is correctly configured.

I cannot connect to SmartCenter FP3 VPN site using the IP45 Satellite X when using Dynamic IP with certificate support (DAIP). What should I do?

- Check for the installed certificate in VPN > Certificate.
- Check for the following error messages in Reports > Event:

Error Message	Verify
Failed to Create VPN tunnel:client Encrypt Notification	Ensure that on the FP3 management station the authentication mechanism followed is 3DES/SHA1.
Failed to Create VPN tunnel:could not validate my certificate	Ensure that the certificate used in the device is the one associated to the certificate created for this gateway on Smart Center FP3.
Failed to Create VPN tunnel:invalid certificate	Ensure that the certificate used is not expired.
Failed to Create VPN tunnel:invalid cert encoding	Ensure that the certificate used is PKCS#12 format.

I cannot connect to the Check Point SmartCenter FP3 VPN site by using the IP45 Satellite configured using VPN Communities. What should I do?

Check for the following error messages in Reports > Event Log:

Error Message	Verify
Failed to Create VPN tunnel: payload malformed	Ensure that the safe@gateway object defined for this device at Smart Center FP3 uses the same shared secret.
Extended Authentication Failure	Check for the correct username, password given for the VPN site during login.

I cannot connect to the IP45 Satellite VPN site by using the IP45 Satellite X. What should I do?

Check for the following error messages in Reports >Event Log:

Error Message	Verify
Failed to Create VPN tunnel: payload malformed	Ensure that both gateways use the same shared secret.
Failed to Create VPN tunnel: N/A	Check for the validity of the user on the remote IP45 gateway.

I cannot download the certificate. What should I do?

Ensure that the device date and management date matches.

I have a VPN established between my IP45 device and Check Point; I am not able to mount drives from the server on to the client. The Linux computer behind the Check Point is the NFS server and the Linux computer behind the IP45 is the NFS client. What should I do?

This problem is caused because of packet fragmentation.

Most of the applications send packets to the network according to the MTU size. The packet size is determined based on the *rsize* and *wsize* parameters of the NFS; the values being 4k and 8k respectively. Set the NFS parameters that match the packet size so that no fragmentation occurs.

When I try to save the IKE traces from the IP45 devices, they are being stored in HTML format instead of .elg format.

This problem is observed only with IE v5.5 and not later versions. Do the following to resolve this problem:

- Go to Reports > VPN Tunnels on the IP45 GUI.
- Click Save IKE Trace tab.
- On the pop-up window, select save this file to disk.
- The to be save file format will be HTML.
- Click Cancel.
- From the pop-up window, select the option open the file from its current location.

  No file is opened and the other option on the pop-up window, save this file to disk gets automatically selected.
- Click OK.

  The file will be saved as .elg format.

I am unable to access the IP45 GUI through HTTPS. The browser displays an error message Received a message with incorrect message authentication code. What should I do?

This problem occurs when you use Netscape Navigator.

Generate and install a new self-signed/CA signed HTTPS certificate to resolve this problem.

Viewing Firmware Status

The firmware is the software program embedded in the IP45.

You can view your current firmware version and additional details.

To view the firmware status, choose Setup from the main menu. The Firmware page opens with information about the firmware version and other information.

The Firmware page displays the following information:

Table 61 Firmware Status

Field	Description
Firmware Version	the current version of the firmware
Hardware Type	the type of the current IP45 hardware
Hardware Version	the current hardware version of the IP45
Installed Product	the licensed software and the number allowed nodes
Uptime	the time that elapsed from the moment the unit was turned on

Resetting the IP45 Security Platform to Factory Defaults

You can reset to factory defaults with the GUI or by manually pressing the Reset button.

For more information, see "Resetting the Nokia IP45 Security Platform by Using the Reset Button" on page 248.

Failsafe Mode

The Nokia IP45 security platform enters failsafe mode when the main kernel gets corrupted. If the main kernel becomes corrupted, the IP45 loads a failsafe kernel to the RAM. For the device to function properly, it must be upgraded with a new firmware.

You can upgrade the firmware by using OOB or by using the console and LAN.

If the device is booted in failsafe mode, you receive the following login prompt:

```
Welcome to IP45 (failsafe)

login:
```

The username and password are *admin* and *password* respectively.

Upgrading Firmware in Failsafe Mode by Using Console

When the IP45 goes to failsafe mode, you can use the following procedure to upgrade the firmware.

To upgrade the firmware using the console and LAN

1. Connect to the console.Use *admin* and *password* as the default username and password. The following message appears:

```
Welcome to IP45 (failsafe)

login: admin

password:
```

You will see the following message displayed on the console:

```
Device is running in failsafe mode. You must upgrade the device
immediately.
```

2. Specify the LAN IP address and netmask when prompted.

The device waits for the FTP client to upload the firmware once the LAN interface is configured.

You will see the following message displayed on the console:

```
Device is waiting for ftp client to upload the firmware.
```

You must close FTP session using quit command after uploading firmware.

Press Ctrl+C to Cancel.

3. FTP to the configured LAN IP address and upload the firmware.
4. The device requests your confirmation for firmware upgrade after successful firmware upload.Press Y to confirm.

The device displays the appropriate message depending on success or failure of firmware upgrade.

Upgrading Firmware from Failsafe Kernel

If the firmware of your device gets corrupted, and your device is not working properly, you need to reload the firmware in it. You can reload your firmware by using the Failsafe Kernel.

You can use the OOB feature in the IP45 for remote HTTPS or SSH access and to perform firmware upgrades.

Note
Failsafe kernel does not provide any other function other than reloading the firmware.

To upgrade firmware through OOB from the failsafe kernel

1. Boot in to the failsafe kernel. See "Failsafe Mode" on page 326 for more details.
2. After booting, dial in to the device with username *admin* and password *password*.

Note
The IP45 uses the IP address 192.168.40.1 for the dial-up interface.

3. Open a Telnet session to the IP45 by using the preceding IP address and username/password information.
4. Upload the firmware file to the device by using FTP or TFTP. You are prompted to confirm firmware upgrade when the upload is completed.
5. Upgrade the device firmware by clicking Yes. The IP45 verifies whether the firmware file you uploaded is valid before upgrading.

Running Diagnostics

You can view technical information about the Nokia IP45 security platform hardware, firmware, license, network status, and subscription services.

This information is useful for troubleshooting. You can copy and paste the information into the body of an email and send it to technical support.

To run diagnostics

1. Choose Setup from the main menu.

   The Firmware page opens.
2. Click Tools and then click Diagnostics.

   Technical information about the Nokia IP45 appears in a new window.
3. To refresh the contents of the window, click Refresh.

   The contents are refreshed.
4. To close the window, click Close.

Using Packet Sniffer

The Nokia IP45 v4.0 supports a packet sniffer tool that enables you to capture packets and use them for troubleshooting purpose. A filter expression can be specified to capture the packets. If no filter expression is specified, all the packets on the selected interface will be saved.

The saved results can be read by using free protocol analyzers such as Ethereal.

Note
You can use the packet sniffer only by using the GUI, command-line interface is not supported.

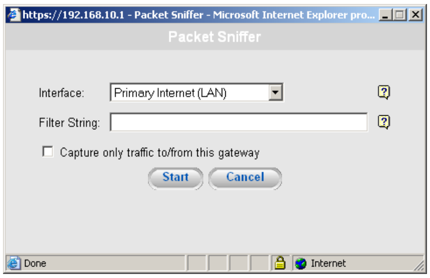
To use packet sniffer

1. Choose Setup from the main menu.

   The Firmware page opens.

2. Click Tools and then click Sniffer.

   The Packet Sniffer window opens.



https://192.168.10.1 - Packet Sniffer - Microsoft Internet Explorer pro...

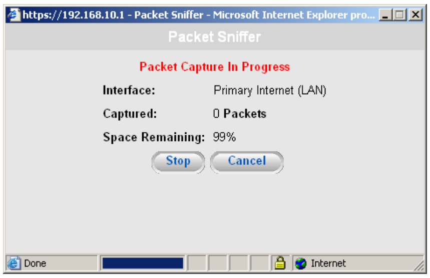
Packet Sniffer

Interface: Primary Internet (LAN)

Filter String:

□ Capture only traffic to/from this gateway

3. Select the interface from the drop-down list.
4. Enter a filter string. Example: port 80
5. Click Start.
6. The Packet Capture in Progress window opens with information about the captured packets.



https://192.168.10.1 - Packet Sniffer - Microsoft Internet Explorer pro...

Packet Sniffer

Packet Capture In Progress

Interface: Primary Internet (LAN)

Captured: 0 **Packets**

Space Remaining: 99%

   Once the packets are captured, a window is displayed providing the information about the packets.

7. Click Stop to go to the previous window.
8. Click Cancel to exit packet sniffer.

A Specifications

Technical Specifications

Table 62 Specifications

Height 1.2 inches	Input DC Power - 12V
Width - 8.0 inches	Power Consumption - 13.5 W
Length - 4.8 inches	Power Supply - 100 V AC, 120 V AC or 240 V AC
Weight - 1.8 lbs	

Safety Precautions

Read the following safety instructions before attempting to install or operate the Nokia IP45 security platform. Read the installation and operation procedures provided in this User Guide. Failure to follow the instructions can result in damage to equipment, and or personal injuries.

⚠ **Warning**
Do not use any accessories other than those approved by Nokia. Failure to do so might result in loss of performance, damage to the product, fire, electric shock or injury, and voids the warranty.

⚠ **Warning**
Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

⚠ **Caution**
Before cleaning the IP45, unplug the power cord. Use only a soft cloth dampened with water for cleaning.

⚠ **Caution**
Any changes or modification to this product not explicitly approved by the manufacturer could void any assurances of safety or performance and could result in violation of part 15 of the FCC Rules.

⚠ **Caution**
When installing the IP45, ensure that the vents are not blocked.

⚠ **Caution**
Do not use the IP45 outdoors.

⚠ **Caution**
Do not expose the IP45 to liquid or moisture.

⚠ **Caution**
Do not expose the IP45 to extreme high or low temperatures.

⚠ **Caution**
Do not drop, throw, or bend the IP45 since rough treatment could damage it.

⚠ **Caution**
Do no disassemble or open the IP45. Failure to comply voids the warranty.

⚠ **Caution**
Do not route the cables in a walkway or in a location that will crimp the cables.

B Compliance Information

This appendix contains the following compliance information:

- Declaration of Conformity
- Compliance Statements
- FCC Notice (US)

Declaration of Conformity

According to ISO/IEC Guide 22 and EN 45014:

Manufacturer's Name:	Nokia Inc.
Manufacturer's Address:	313 Fairchild Drive Mountain View, CA 94043-2215 USA

declares that the product:

Product Name:	IP45
Model Number:	EM3100
Date First Applied:	2003

conforms to the following standards:

Safety:	UL60950, 3rd Edition; EN60950-1:2001+A11; IEC60950-1:2001.
EMC:	EN55024 1998, EN55022B 1998, EN61000-3-2, EN61000-3-3

Supplementary information:

Pursuant to directive 1999/5/EC this product complies with the requirements of the Low Voltage Directive 73/23/EEC and the EMC Directive 89/336/EEC with Amendment 93/68/EEC.

NOKIA

Christopher Saleem
Compliance & Reliability Engineering Manager
Security & Mobile Connectivity, Enterprise Solutions
Mountain View, California
May 2006

Tom Furlong
Vice President and General Manager
Security & Mobile Connectivity, Enterprise Solutions
Mountain View, CA

Compliance Statements

This hardware complies with the standards listed in this section.

Emissions Standards

FCC part15 SubpartB Class B	US/Canada
EN55022 (CISPR22 Class B).	European Community (CE)

Immunity Standards

EN55024:	European Community (CE)
EN61000-4-2	
EN61000-4-3	
EN61000-4-4	
EN61000-4-5	
EN61000-4-6	
EN61000-4-11	

Harmonics and Voltage Fluctuation

EN61000-3-2	European Community (CE)
EN61000-3-3	European Community (CE)

Safety Standards

UL/EN60950	US/European Community (CE).
CAN/CSA-C22.2 No. 60950	Canada

FCC Notice (US)

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this device does cause harmful interference to radio or television reception, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the computer and receiver.
- Connect the computer into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

⚠ **Caution**
Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

060425

Index