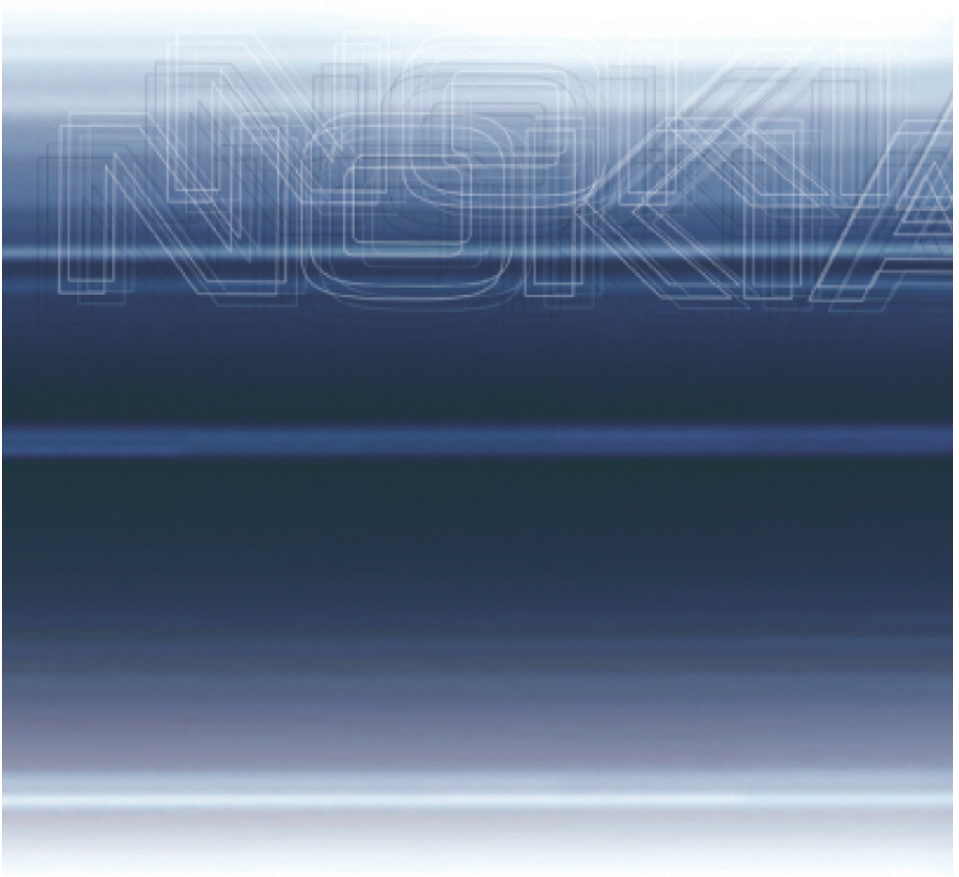


Nokia IP30

User Guide



NOKIA
CONNECTING PEOPLE

N450829001 Rev A
October 2002

COPYRIGHT

©2002 Nokia. All rights reserved.

Rights reserved under the copyright laws of the United States.

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.

SofaWare, Safe@Home, Safe@Home Pro, Safe@Office, Safe@Office Plus, Security Management Portal (SMP) and Security Management Console (SMC) are registered trademarks of SofaWare Technologies Ltd., a CheckPoint Company.

Nokia Contact Information

Corporate Headquarters

Web Site	http://www.nokia.com
-----------------	---

Telephone	1-888-477-4566 <i>or</i> 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: ipsecurity.na@nokia.com
Europe	Nokia House, Summit Avenue Southwood, Farnborough Hampshire GU14 ONG UK	Tel: 00800 5543 1816 <i>or</i> 1+44 (0) 8700 555 777 email: ipsecurity.emea@nokia.com
Asia-Pacific		Tel: +358 9 692 7156 email: ipsecurity.apac@nokia.com

Nokia Customer Support

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

Contents

About this Guide	11
Document Organization	11
Document Conventions	12
Cautionary Icons	12
Menu Items	12
1 Introduction	13
About the Nokia IP30	13
Nokia IP30 Firewall	14
Nokia IP30 Tele	14
Nokia IP30 Satellite	14
Nokia IP30 Satellite Plus	15
Nokia IP30 Features and Compatibility	15
Connectivity	15
Security	15
Management	16
Security Services	16
VPN	16
Package Contents	17
Network Requirements	17
IP30 Rear Panel	17
IP30 Front Panel	18
2 Installing the IP30	21
Before You Install the IP30	21
Windows 98/Millennium Operating Systems	22

Setting up on XP/ Windows 2000 Operating System	24
Connecting the IP30 to the Network	26
Installing Your Network	26
Configuring the IP30 for Internet Connection	27
Administrator Password	28
Using the Setup Wizard	29
Cable Connection Settings	31
DSL Connection Settings	32
Using Advanced Setup	35
LAN Connection	37
Cable Connection	38
xDSL PPPoE Connection	39
xDSL PPTP Connection	40
Static Routes	41
Installing Your Product Key	42
3 Configuring the IP30	45
Logging On to the IP30	45
Accessing the IP30 securely	46
Nokia IP30 GUI	48
Logging Off	49
Managing Your Network	49
Viewing Network Activity Information	49
Quick Internet Connection and Disconnection	50
Configuring Network Settings	51
Enabling and Disabling the DHCP Server	51
Changing IP Addresses	52
Enabling and Disabling NAT	53
Accessing the IP30 from a Remote Location	54
Managing IP30 Firewall from a Remote Location	55
Viewing Reports	56
Viewing the Event Log	56
Viewing Active Computers	57
Viewing Active Connections	59
Viewing VPN Tunnels	59

Setting up the IP30 Security Policy	62
Setting the Firewall Security Level	62
Configuring Virtual Servers	63
Creating Rules	65
Allow and Block Rules	65
Demilitarized Zone	68
Using Subscription Services	69
Starting Your Subscription Services	70
Viewing Services Information	73
Canceling Subscription Services	73
Web Filtering	74
Enabling Web Filtering When Locally Managed	74
Selecting Categories for Blocking	75
Snoozing Web Filtering When Remotely Managed	75
E-mail Anti Virus	77
Enabling E-mail Anti Virus Scan When Locally Managed	77
Selecting Protocols for Scanning	78
Snoozing Anti virus When Remotely Managed	78
Automatic and Manual Updates	79
Software Updates for Locally Managed IP30	80
Software Updates for Centrally Managed IP30	80
Refreshing Your Service Center Connection	81
Configuring Your Account	81
Configuring for Nokia Horizon Manager	82
Managing Users	83
Changing Your Password	83
Adding Users	85
Viewing and Editing Users	85
Deleting Users	87
Setting Up Remote VPN Access for Users	88
4 VPN Configuration	89
SecuRemote to Satellite (VPN Client to Gateway)	92
Setting up IP30 Satellite	93
Setting up SecuRemote	94
IP30Tele to IP30 Satellite (VPN Client to Gateway)	94
Setting up IP30 Tele	94

Setting up IP30 Satellite.	95
IP30 Tele to Check Point v4.1/ NG/ FP1/ FP2	95
Setting up IP30 Tele	95
Setting up Check Point Server.	95
IP30 Tele to Check Point FP3	95
Setting up IP30 Tele	96
Setting up Check Point FP3.	96
Satellite to Satellite (VPN Gateway to Gateway).	97
Setting up IP30 Satellite.	98
Satellite to VPN-1 (Site-to-Site VPN).	98
Setting up IP30 Satellite.	99
IP30 Satellite to Check Point FP3	100
Setting Up Check Point FP3	100
Setting up IP30 Satellite.	101
IP30 Satellite to Check Point SmartCenter FP3	101
Setting Up Check Point SmartCenter FP3.	101
Setting up IP30 Satellite.	102
IP30 Satellite in NAT and No-NAT Modes.	102
No-NAT Mode	103
NAT Mode	104
IP30 Satellite to Windows 2000.	104
Using IP30 Tele.	105
Adding VPN Sites by Using IP30 Tele.	105
Adding VPN Sites by Using IP30 Satellite.	110
To add or edit VPN sites by using IP30 Satellite	110
Configuring a Remote Access VPN Site	111
Configuring a Site to Site VPN Gateway	114
Completing Site Creation	115
Setting Up IP30 Satellite as VPN Server.	115
To set up your IP30 as a VPN server	116
Deleting a VPN Site	116
Logging on to a VPN Site	117
Logging On Using IP30 GUI	117
Logging On Through my.vpn	119
Logging Off a VPN Site	120

5	Troubleshooting	121
	Frequently Asked Questions	121
	Viewing Firmware Status	127
	Resetting the IP30 to factory defaults.	127
	Rebooting the IP30.	129
	Running Diagnostics.	129
A	Specifications	133
	Technical Specifications.	133
	Safety Precautions.	133
B	Warranty	135
C	End User License Agreement	143
D	Compliance Information	153
	Compliance Statement.	154
	FCC Notice (US)	155
	Index	157

About this Guide

This guide provides information and procedures for how to install and configure the Nokia IP30 security platform. The User Guide provides information about the new features incorporated into Nokia IP30. This version of Nokia IP30 uses SofaWare's Safe@v3.0.xx software.

For a quick reference on configuring features in Nokia IP30, see the *Nokia IP30 Quick Start Guide* and the *IP30 Online Help* that is part of the graphical user interface (GUI) in the device.

Document Organization

This guide is organized into the following chapters:

Chapter 1 [Introduction](#) provides the information you need to know before you install the Nokia IP30.

Chapter 2 [Installing the IP30](#) explains how to install the device, operating system requirements, protocols and how to establish a network connection.

Chapter 3 [Configuring the IP30](#) explains how to configure the features provided in the IP30.

Chapter 4 [VPN Configuration](#) explains how to configure a VPN using the IP30.

Chapter 5 [Troubleshooting](#) discusses problems users might encounter and proposes solutions.

Appendix A explains the [Specifications](#) of IP30.

Appendix B explains the [Warranty](#) on IP30.

Appendix C explains the [End User License Agreement](#).

Appendix D explains [Compliance Information](#).

Document Conventions

This section explain document conventions including notices, menu items, and IP address notation conventions used in this guide.

Cautionary Icons



Warning

Warnings advise the user that bodily injury might occur because of a physical hazard.

Note

Notes provide information of special interest or recommendations.

Menu Items

Items in Nokia IP30 menus are separated by the greater than sign, with spaces before and after the 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.

1 Introduction

About the Nokia IP30

The Nokia IP30 is an advanced Internet security appliance that enables secure high-speed Internet access from the home or office. The IP30 uses Safe@ v3.0.xx software from SofaWare Technologies. The Safe@ firewall, based on the Check Point FireWall-1 Stateful Inspection technology, inspects and filters all incoming and outgoing traffic, blocking all unauthorized traffic.

The IP30 is a hardware appliance and is easy to install. It allows you to share your Internet connection among several computers, other network devices and enables advanced home and office networking, besides providing protection for your entire network.

With the IP30, home users can subscribe to security services, such as firewall security updates, parental control and so on. Business users can securely connect to the corporate network.

The IP30 is available with the following software configurations:

- Nokia IP30 Firewall
- Nokia IP30 Tele
- Nokia IP30 Satellite
- Nokia IP30 Satellite Plus

All of these versions of IP30 provide a Web-based management interface that enables you to manage and configure the IP30 operation and options.

The IP30 comes with a pre-installed with the product of your choice. The IP30 can be upgraded to the more advanced product, without replacing the hardware. Just contact your software provider.

Nokia IP30 Firewall

The IP30 Firewall protects your home network from hostile Internet activity. It is intended for home users and up to five computers and users can use it.

Nokia IP30 Tele

The IP30 Tele provides virtual private networking (VPN) functionality in addition to the Firewall. The IP30 Tele contains a VPN client that enables employees working from home to securely connect to the corporate network.

The IP30 Tele supports telecommuting and enables you to connect to a corporate network. Up to 5 computers and users can use it.

Nokia IP30 Satellite

The Nokia IP30 Satellite provides all the benefits of Firewall and Tele, along with expanded VPN functionality. It can function as a VPN client as well as a VPN server or gateway that is installed at your office to protect the company VPN and make it available to telecommuting employees. IP30 Satellite can also be configured as a VPN gateway that allows permanent bidirectional connections between two gateways, such as two company offices.

IP30 Satellite is intended both for companies with extended enterprise networks and for their employees working from home. Up to 10 computers and users can use it.

Nokia IP30 Satellite Plus

Nokia IP30 Satellite Plus extends the IP30 Satellite functionality to support up to 25 computers and users.

Nokia IP30 Features and Compatibility

The IP30 provides the following features:

Connectivity

- Four-port 10/100 Mbit/s Ethernet switch
- Internet connection sharing: network address translation (NAT)
- PPPoE and PPTP support
- DHCP server and client
- MAC Cloning

Security

- Advanced Stateful Inspection Firewall security
- Protection from Denial of Service (DoS) attacks
- Anti spoofing protection
- Intrusion logging
- Customized security policy
- Protocol support for TCP/IP, ICMP, GRE, ESP and UDP
- H323 fully supported with NAT off

Management

- Local Web-based interface
- Remote management by service center or central office
- Remote firmware updates
- Remote management through HTTPS
- Remote management by service center or corporate, using the SofaWare security management platform (SMP)
- Nokia Horizon Manager v1.2 SP1 support
- SmartCenter FP3 supports managing gateways

Security Services

- Automatic firewall security updates
- Parental control
- Content filtering
- E-mail anti virus protection
- Centralized logging and intrusion detection
- VPN management

VPN

- IPSEC VPN remote access server (Nokia IP30 Satellite only)
- IPSEC VPN site-to-site gateway (Nokia IP30 Satellite only)
- IPSEC VPN remote access client (Nokia IP30 Tele and Satellite only)
- Support for IKE hybrid mode authentication
- AES encryption for better performance (Nokia IP30 Satellite-to-Satellite only)
- Split DNS
- UDP encapsulation supported in VPN client
- VPN keep alive
- DAIP with VPN certificates
- NAT Traversal

Package Contents

- Nokia IP30 internet security appliance
- CAT5 straight-through ethernet cable
- Power adapter
- Quickstart Guide
- This User Guide

Network Requirements

- A broadband Internet connection by cable or DSL modem with Ethernet interface (RJ-45)
- 10BaseT or 100BaseT 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 to use either Microsoft Internet Explorer 5.5 or higher, or Netscape Navigator 4.7 or higher.

IP30 Rear Panel

All physical connections (network and power) to the IP30 are made through the rear panel.

Figure 1 Rear View of Nokia IP30



The items on the rear panel of the IP30 are explained in Table 1.

Table 1 Rear Panel of the IP30

Label	Description
PWR	A power jack used for supplying power to the device. Connect the power adapter to this jack. The device connects to the power source.
RESET	Used to reboot/ reset the IP30 to its factory defaults. Use a sharp object to press this button. Short press: reboots IP30 Long press (7 seconds): resets the IP30 to its factory defaults. This results in loss of all security services and passwords. DO NOT RESET UNIT WITHOUT CONSULTING NOKIA SUPPORT.
WAN	An ethernet port (RJ-45) used to connect your cable or xDSL modem.
LAN 1-4	Four Ethernet ports (RJ-45) used to connect computers or other network devices.

IP30 Front Panel

You can monitor the IP30 operations by viewing the LEDs on the front panel. The Nokia IP30 includes 11 status LEDs.

Figure 2 Front Panel of Nokia IP30



The items on the front panel of the IP30 are explained in Table 2.

Table 2 Front Panel of Nokia IP30

LED	Description
PWR/SEC	Off: Power Off Flashing quickly (Green): System boot-up Flashing slowly (Green): Establishing Internet connection On (Green): Normal Operation Flashing (Red):- Hacker attack blocked On (Red): Error
LAN 1-4/ WAN	LINK/ ACT off, 100 Off: Link is down. LINK/ ACT On, 100 Off: 10 Mbps link established for the corresponding period. LINK/ ACT On, 100 On: 100Mbps link established for the corresponding port. LINK/ ACT Flashing: Data is being transmitted or received.

2 Installing the IP30

This chapter describes the set up and installation procedures for the IP30 in a networking environment. The chapter covers the following topics:

- Checking the computer's TCP/IP Configuration
- Installing the TCP/IP protocol on your computer (if not installed)
- Configuring the TCP/IP settings for different platforms
- [Connecting the IP30 to the Network](#)
- [Configuring the IP30 for Internet Connection](#)

Before You Install the IP30

Before you connect and set up the IP30, you must check the following:

- If TCP/IP is installed on your computer.
- If your computer's TCP/IP settings to make sure it obtains its IP address automatically.

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

Windows 98/Millennium Operating Systems

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

To check the TCP/IP Installation

1. Choose Start > Settings > Control Panel.

The Control Panel window appears.



2. Double click the **Network** icon. The Network window appears.

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 this section.

To Install TCP/IP

1. In the Network window, click Add.
The Select Network Component Type window appears.
2. Choose Protocol and click Add. The Select Network Protocol window appears.
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 the Windows asks 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.

To set TCP/IP Settings

If you are connecting the IP30 to an existing LAN, consult your network manager for the correct configuration.

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.

2. Click Gateway tab and remove any installed gateways.
3. Click DNS Configuration tab and click Disable DNS.
4. Click the IP Address tab and select 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 PC. To assign a static IP address, select Specify an IP address and enter an IP address in the range of 192.168.10.129-254. Enter 255.255.255.0 as the Subnet Mask. Click OK to save the new settings.

5. Click Yes when prompted for “Do you want to restart your computer?”

Your computer restarts for the new settings to take effect.

Your computer is now ready to access the IP30.

Setting up on XP/ Windows 2000 Operating System

Windows XP has an Internet Connection Firewall option. Nokia recommends that you disable the Firewall option if using IP30.

To Check the TCP/IP installation

1. Click Start > Settings > Control Panel.
The Control Panel window appears.
2. Double click the Network and Dial-up Connections icon.
The Network and Dial-up Connections window appears.
3. Right-click the Local Area Connection icon and select Properties from the drop down menu.
The Local Area Connection Properties window appears.
4. Check for TCP/IP in the Component list and if it is configured with the Ethernet card that is installed on your computer.
If TCP/IP does not appear in the Components list, install it as described in the following section.

To Install TCP/ IP

1. In the Local Area Connection Properties window, click Install.
The Select Network Component Type window appears.
2. Choose Protocol and click Add.
The Select Network Protocol window appears.

-
3. In the Select Network Protocol window, choose Internet Protocol (TCP/IP) and click OK to install the TCP/IP protocol on your computer.

To set TCP/IP settings

1. In the Local Area Connection Properties window double-click Internet Protocol (TCP/IP) component and click Properties.
The Internet Protocol (TCP/IP) Properties window opens.
2. Select 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 PC. To assign a static IP address, select Specify an IP address and enter an IP address in the range of 192.168.10.129-254. Enter 255.255.255.0 as the Subnet Mask. Click OK to save the new settings.

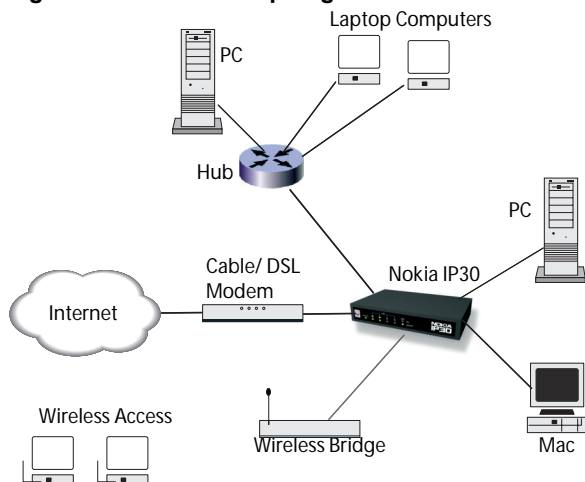
3. Click 'Obtain DNS server address automatically.'
4. Click OK to save the new settings.

Your computer is now ready to access your IP30.

Connecting the IP30 to the Network

The Nokia IP30 can be connected to your network in various ways. Figure displays the various possible setups.

Figure 3 Nokia IP30 Topologies



Installing Your Network

Plan your network and the location of the IP30, then install your network.

To install the network

1. Connect the LAN cable:
 - Connect one end of the Ethernet cable to one of the LAN ports at the back of the unit.
 - Connect the other of the ethernet cable to the computer, hubs, or another network device.

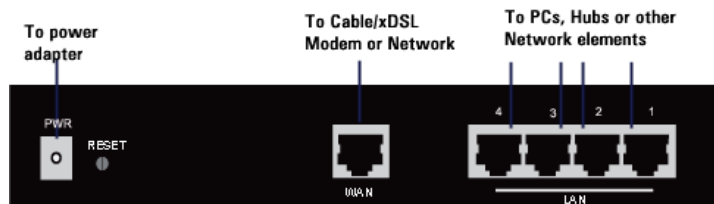
2. Connect the WAN cable:
 - Connect one end of the Ethernet cable to the WAN port at the back of the unit.
 - Connect the other end of the Ethernet cable to a cable modem, xDSL modem, or a corporate network.
3. Connect the power adapter to the power socket, labeled PWR, at the back of the device.
4. Plug in the AC power adapter to the wall electrical outlet.



Warning

The AC adapter is compatible with either 120 V AC or 230 V AC input power. Verify that the wall outlet voltage is compatible with the voltage specified on your power supply. Failure to observe this warning can result in injuries or damage to equipment.

Figure 4 Rear Panel Connections



Configuring the IP30 for Internet Connection

Configure the Internet connection to IP30 before you can access the Internet through the IP30.

To configure the Internet connection

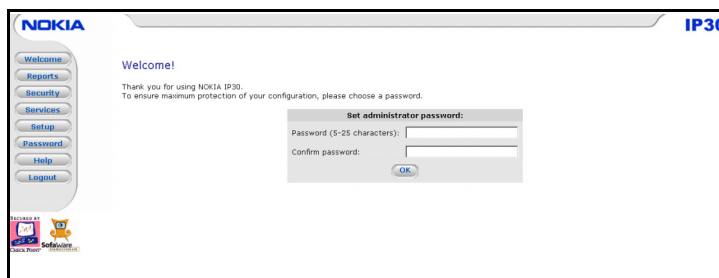
1. Set up your password.
2. Configure your Internet connection using either of the following setup tools:
 - The Setup Wizard: guides you through the configuration process step by step.
 - Advanced Setup: offers advanced setup options.

Note

You must configure the Internet connection on initial operation and after all reset to defaults operations.

Administrator Password

1. Enter `http://my.firewall`.

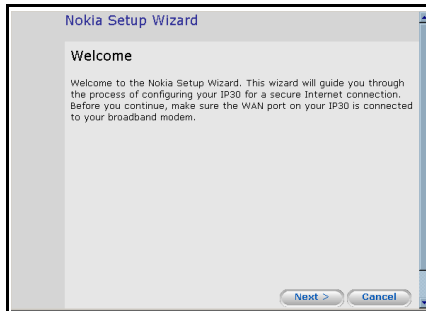


2. On the IP30 Login page, enter a password. Re-enter the password to confirm.

Note

The password must be between five to eleven alphanumeric characters. To change the Password, click Setup on the navigation bar and click Password.

The Setup Wizard opens.



You can now configure the Internet connection for IP30.

Configure the Internet connection for the IP30 by doing one of the following:

- To manually configure the connection settings, click Cancel to abort the Setup Wizard, and use Advanced Setup. For further information, see “Using Advanced Setup.”
- To have the Setup Wizard take you through the configuration process step by step, see “Using the Setup Wizard.”

Using the Setup Wizard

The Setup Wizard allows you to configure your IP30 for Internet connection quickly and easily through the use of a user friendly interface. The setup wizard automatically pops up on successful login.

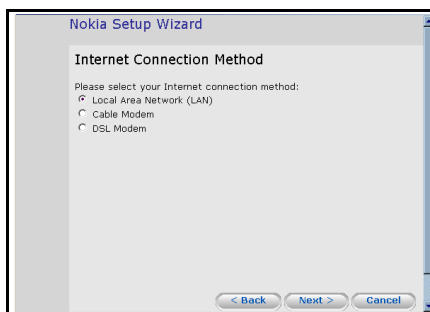
You can choose between three modes of broadband connection:

- Local area network (LAN)
- Cable modem
- xDSL modem

To configure the Internet connection using Setup Wizard

Follow the on-screen instructions to set up your Internet connection.

1. Click Next. The Internet Connection Method screen appears.



2. Select the Internet connection method to use for connecting to the Internet and click Next.

Note

For Static WAN IP address, choose LAN regardless of the connection type.

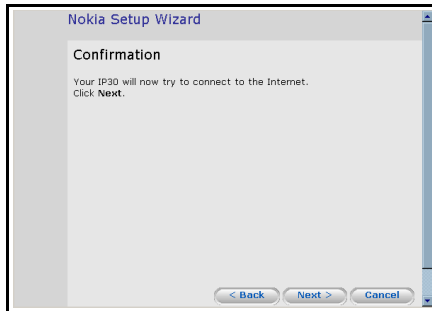
Note

If you select DSL Modem, do not use dial up software to connect to the Internet.

3. Click Next.

A Connecting message appears followed by a Connected message.

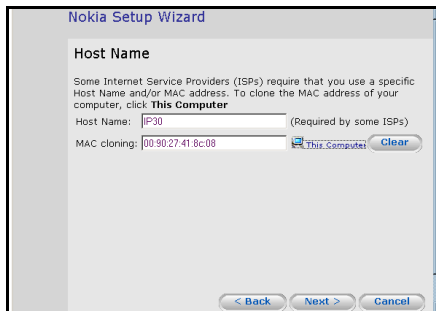
Once connected, the wizard prompts you to register your details and set up your subscription options, which vary from product to product.



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

Cable Connection Settings

If you selected cable connection in the previous procedure, the Host Name screen appears.



MAC Cloning. Some ISPs require registration of MAC addresses of the computer behind the cable modem before an Internet connection can be established.

The Safe@ gateway takes the place of the computer behind the Cable modem and the local user can use MAC Cloning to enter the

original PC MAC address without contacting the ISP for changing that information.

To configure for cable connection

1. Enter the Host name.

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.

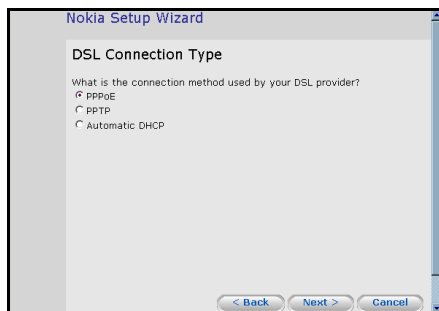
The system attempts to connect to the Internet.

At the end of the connection process the Connected message appears. Once connected, the wizard will prompt 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.

DSL Connection Settings

If you selected a DSL connection method, the following screen appears.



To connect using DSL Connection

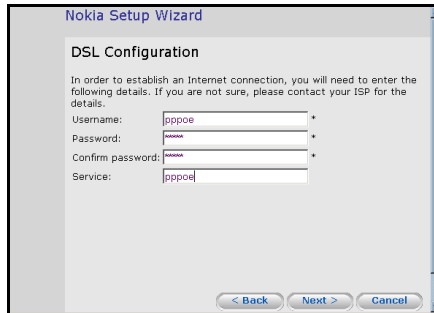
1. Select the connection method that your DSL provider uses.
2. Click Next.

Note

Most DSL providers use PPPoE. If you are uncertain about which connection method to use, contact your DSL provider.

Using PPPoE

If you selected PPPoE, the PPPoE Configuration window appears.



In the PPPoE dialog box enter the following,

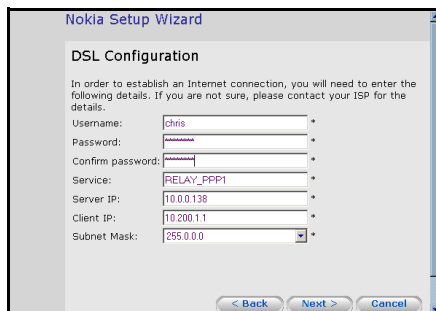
1. Your Username, Password and confirm the Password.
2. The service name.
This is optional.
3. Click Next.

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

Using PPTP

If you select PPTP, the PPTP configuration window appears.



The screenshot shows the 'Nokia Setup Wizard' window with the 'DSL Configuration' tab selected. The window contains the following fields and values:

Field	Value
Username:	chris
Password:	password
Confirm password:	password
Service:	RELAY_PPP1
Server IP:	10.0.0.138
Client IP:	10.200.1.1
Subnet Mask:	255.0.0.0

At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

1. Enter the Username, Password and confirm the Password.
2. Enter the service name.
3. The IP address of the DSL modem in the Server IP field.
4. The IP address required to access the DSL modem in the Client IP field.
5. The Subnet Mask of the DSL modem in the Subnet Mask field.
6. Click Next.

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

Using Automatic DHCP

If you enabled automatic DHCP, no further settings are required. The Confirmation message appears.

1. Click Next.

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

Once connected, the wizard will prompt you to register your details, install the product key and set up your subscription options, which may vary from product to product.

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

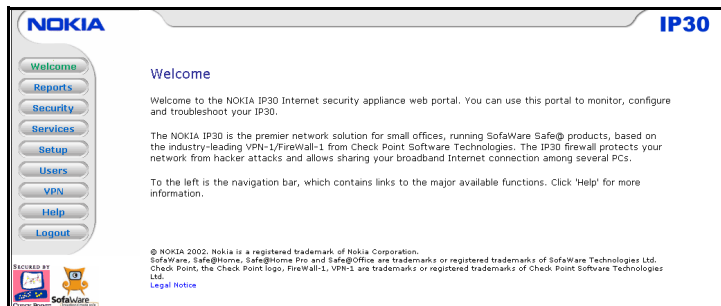
Using Advanced Setup

You can configure the advanced features in the IP30 using Advanced Setup.

To configure the Internet connection

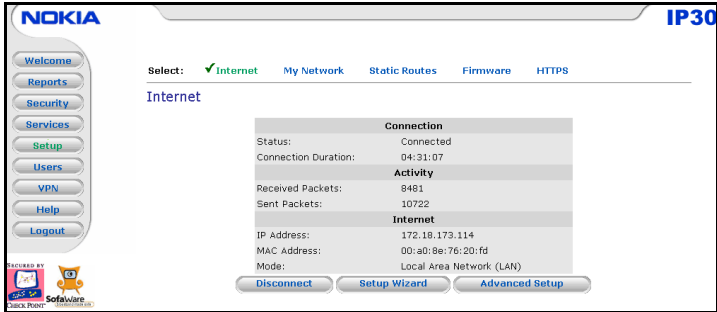
1. Click Cancel on the Welcome page of the Setup Wizard.

The Welcome page appears.



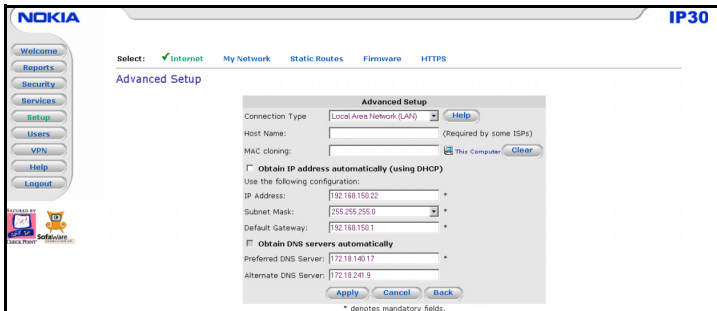
2. In the Navigation Bar, click Setup.

The Internet page appears.



3. Click on Advanced Setup.

The Advanced Setup page appears



4. From the Connection Type drop-down list, select the Internet connection you are using or intend to use.

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

LAN Connection

If using a LAN connection, enter the following:

1. Enter the Host name.

This field is optional. If a service center requires it, they will provide it.

2. If you do not want the IP30 to obtain an IP address automatically using DHCP, do the following:

- a.** Clear the Obtain IP address automatically (using DHCP) check box.
- b.** Enter the IP address by which your internal IP addresses will be hidden (NAT).

The screenshot shows the Nokia IP30 Advanced Setup screen. The 'Connection Type' is set to 'Local Area Network (LAN)'. The 'Host Name' field is empty. The 'MAC cloning' field is empty. The 'Obtain IP address automatically (using DHCP)' checkbox is unchecked. The 'Obtain DNS servers automatically' checkbox is checked. The IP Address field contains 192.168.150.22, Subnet Mask contains 255.255.255.0, Default Gateway contains 192.168.150.1, Preferred DNS Server contains 172.18.140.17, and Alternate DNS Server contains 172.18.241.9. There are 'Apply', 'Cancel', and 'Back' buttons at the bottom.

- c.** Select the Subnet mask that applies to the IP address you e entered.
- d.** Enter the IP address of the default gateway of your Service Center.
- e.** Enter the Primary DNS server IP address.
- f.** Enter the Secondary DNS server IP address.

3. To assign an IP address automatically using DHCP, but not configure DNS servers automatically, do the following:

- a.** Clear the Obtain DNS Servers automatically check box.
- b.** Enter the Primary DNS server IP address.
- c.** Enter the Secondary DNS server IP address.

4. Click Apply.

Cable Connection

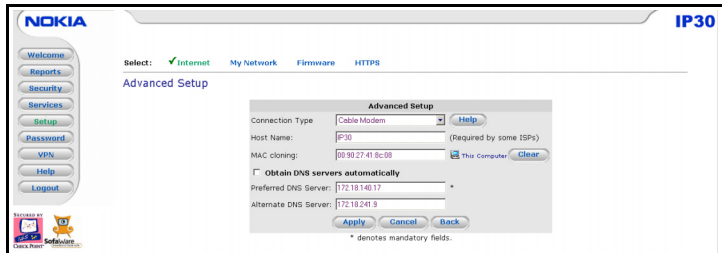
If using a cable connection, enter the following:

1. Enter the Host name.

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

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

- a. Clear the Obtain DNS servers automatically check box.
- b. Enter the Primary DNS server IP address.
- c. Enter the Secondary DNS server IP address.



2. Click Apply.

xDSL PPPoE Connection

If using an xDSL PPPoE connection, enter the following information:

1. Enter your Username and Password and confirm the Password.
2. Enter the service name as given by your service center.

The screenshot shows the Nokia IP30 web interface. On the left is a navigation menu with buttons: Welcome, Reports, Security, Services, Setup, Password, VPN, Help, and Logout. The 'Setup' button is highlighted. The main area has a 'Select:' dropdown menu with 'Internet' selected, and tabs for 'My Network', 'Firmware', and 'HTTPS'. Below this is the 'Advanced Setup' section. It contains a 'Connection Type' dropdown set to 'PPPoE' with a 'Help' button. Below are input fields for 'Username' (containing 'pppoe'), 'Password' (containing 'pppoe'), 'Confirm password' (containing 'pppoe'), 'Service' (empty), and 'MTU' (empty). There is a 'MAC cloning' section with a 'This Computer' button and a 'Clear' button. A checkbox 'Obtain DNS servers automatically' is checked. Below it are 'Preferred DNS Server' (172.16.140.17) and 'Alternate DNS Server' (172.16.241.9). At the bottom are 'Apply', 'Cancel', and 'Back' buttons. A small note at the bottom right says '* denotes mandatory fields'.

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 center.

3. If you are not using automatic configuration of DNS servers, do the following:
 - a. Clear the Obtain DNS servers automatically check box.
 - b. Enter the Primary DNS server IP address.
 - c. Enter the Secondary DNS server IP address.

4. Click Apply.

xDSL PPTP Connection

If using an xDSL PPTP connection, enter the following information:

1. Enter your Username and Password and confirm the Password.
2. Enter the service name as given by your Service Center.
3. Enter the IP address of the PPTP server as given by your Service Center.

The screenshot shows the Nokia IP30 web interface. On the left is a sidebar with buttons: Welcome, Reports, Security, Services, Setup, Password, VPN, Help, and Logout. The main area has a top bar with 'Select: Internet My Network Firmware HTTPS' and a sub-header 'Advanced Setup'. Below this is a form titled 'Advanced Setup' with the following fields:

- Connection Type: PPTP (dropdown menu)
- Username: jchs
- Password: jchs
- Confirm password: jchs
- Service: RELAY_PPTP
- Server IP: 10.0.0.138
- Client IP: 10.200.1.1
- Subnet Mask: 255.255.255.0 (dropdown menu)
- MTU: (empty field)
- MAC cloning: (checkbox) This Computer
- Obtain DNS servers automatically: (checkbox)
- Preferred DNS Server: 172.18.140.17
- Alternate DNS Server: 172.18.241.9

At the bottom of the form are buttons for 'Apply', 'Cancel', and 'Back'. A small note at the bottom right states '* denotes mandatory fields.'

4. Enter the IP address of the PPTP client as given by your Service Center.
5. Select the PPTP client subnet as given by your Service Center.
You can configure the MTU size. Nokia recommends that you leave this field empty. Consult your Service Center to modify the default MTU.
6. If you are not using automatic configuration of DNS servers, do the following:
 - a. Clear the Obtain DNS servers automatically check box.
 - b. Enter the Primary DNS server IP address.

- c. Enter the Secondary DNS server IP address.
7. Click Apply.

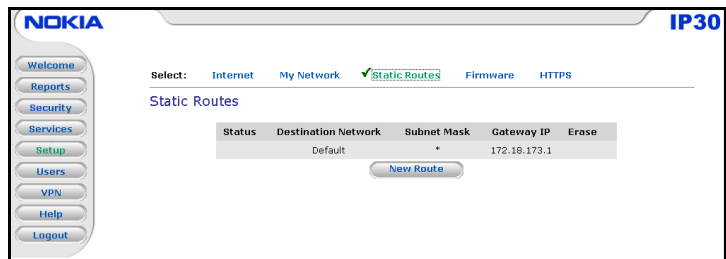
Static Routes

Static routes allow you to route all traffic to a specified network or host through a specified router. In IP30 Satellite, upto 5 static routes can be configured in LAN or when using a Cable modem.

To configure a Static Route

1. Click Setup > Static Routes.

The Static Routes page appears.



2. Click New Route.
The Static Route dialog box appears.
3. Enter the following information:
 - Destination Network
 - Subnet Mask
 - IP address of the gateway
4. Click Add Route.

Note

Static Routes can be added only for gateways on the WAN.

Installing Your Product Key

Your IP30 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 IP30.

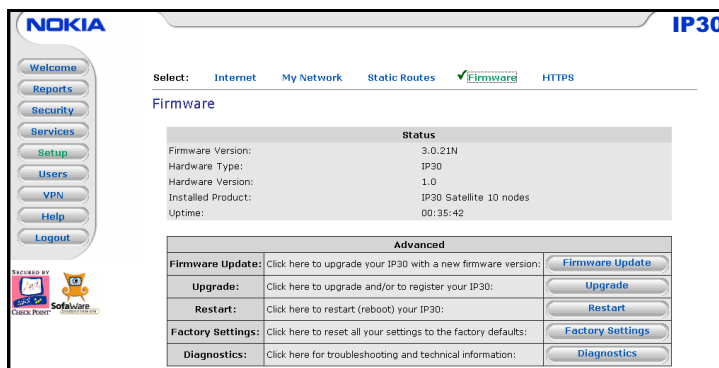
To install a product key

1. In the Navigation Bar click Setup.

The Internet page appears.

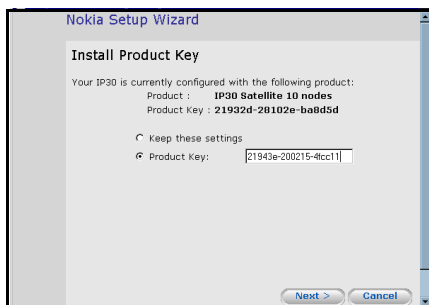
2. Click the Firmware tab.

The Firmware page appears.



3. In the Advanced area, click Upgrade.

The Setup Wizard opens, with the Install License dialog box displayed.

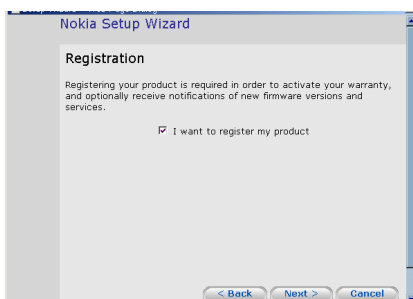


4. Select Product Key.
5. In the Product Key field, enter the new product key.
6. Click Next.

The Installed New Product Key dialog box appears.



7. To register your IP30, 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 IP30 restarts and the Welcome page appears.

Firmware Upgrade

You can upgrade the IP30 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. In the Navigation Bar click Setup.

The Internet page appears.

2. Click Firmware.

The Firmware page appears.



3. Click Firmware Update.
The Firmware Update page appears
4. Click Browse.
A browse window appears.
5. Select the firmware file that you have purchased.
6. Click Upload.
7. The IP30 firmware is updated - this may take one minute.
Upon updating, the the IP30 restarts automatically.

3 Configuring the IP30

This chapter explains the steps and procedure to perform to configure the IP30.

Logging On to the IP30

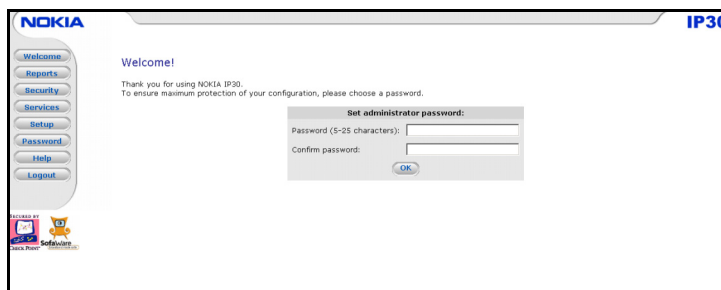
Once connected to the internet, you can configure your IP30. You can configure and manage the IP30 using the GUI.

To access the user interface of the IP30,

1. Open your Web browser, enter `http://my.firewall`.

Click Enter.

The Nokia IP30 initial login page appears.



2. Enter the Password.

If you are using IP30 Satellite or Satellite Plus, enter Username and Password.

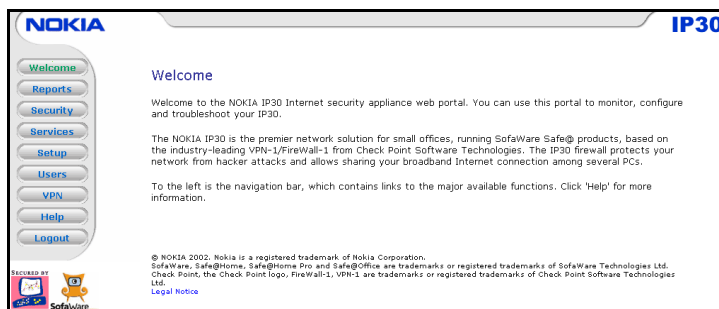
You need to define your password in two instances:

- At the initial Login
- When you reset the device to defaults.

Note

The password should be five to eleven alphanumeric characters.

After the initial login, the Welcome screen appears.



Accessing the IP30 securely

You can access the IP30 graphical user interface (GUI) through HTTPS either remotely or locally (from your internal network).

Note

First configure HTTPS to access the IP30 GUI from a remote location.

To access the IP30 locally

1. Enter **https://my.firewall:981** in the address bar of your browser. (the URL starts with *https*, not *http*).

The IP30 GUI welcome page appears.

2. To access the IP30 from a remote location,

Enter **https://<firewall_IP_address>:981** in the address bar of your browser. (Note that the URL starts with *https*, not *http*.)

If you are accessing the IP30 for the first time, the security certificate in the IP30 is not yet known to the browser, so a Security Alert appears.

Click Yes to install the security certificate of the IP30 that you are trying to access. If using Internet Explorer 5.0 or later, do the following:

- a. Click View Certificate.

The Certificate information screen appears, with the General tab displayed.

- b. Click Install Certificate.

The Certificate Import Wizard opens.

- 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.

- e. Click Finish.

The Root certificate Store message appears.

- f. Click Yes.

The certificate is installed.

The IP30 GUI appears.

Nokia IP30 GUI

The Nokia IP30 GUI includes three major elements:

1. The **Navigation Bar** – used for navigating between the seven main menus and options:
 - Welcome
 - Reports: provides reporting capabilities such as event logging.
 - Security: allows you to set up the security of a computer in the network.
 - Services: allows you to manage your Subscription Services.
 - Setup: allows you to configure your Internet connections.
 - Help: provides context sensitive on-line help.
 - Logout: logs you out of the web interface.

If you are using IP30 Tele, Satellite/ Satellite Plus, the Navigation Bar includes the following additional main menus:

- VPN: lets you manage, configure, and log on to VPN sites.
 - Users: allows you to manage users.
2. The **Main Frame** – displays the relevant information and controls related to the selected topic. These topics differ depending on whether you use IP30 Firewall, Tele or Satellite.
 3. The **Status Bar** – displays the status of your Internet connection and managed services as well as your current services plan, along the bottom of each page.
 - Internet: your internet connection status
 - Connected
 - Not Connected
 - Establishing Connection
 - Contacting Gateway
 - Service Center: your subscription services
 - Not Subscribed

- Connection Failed
- Connecting
- Connected

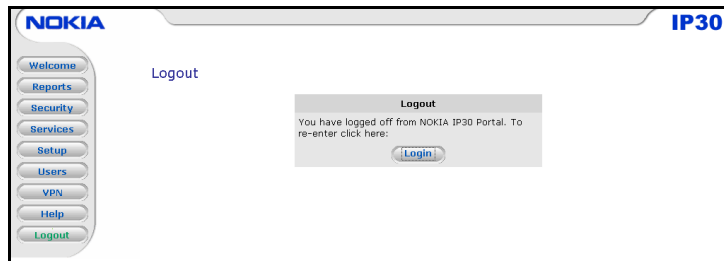
Logging Off

Logging off terminates the IP30 session. To connect to the IP30 again, enter the password.

To log out of IP30, perform one of the following procedures:

- If you are connected locally, click Logout.

The Logout screen appears.



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

Managing Your Network

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

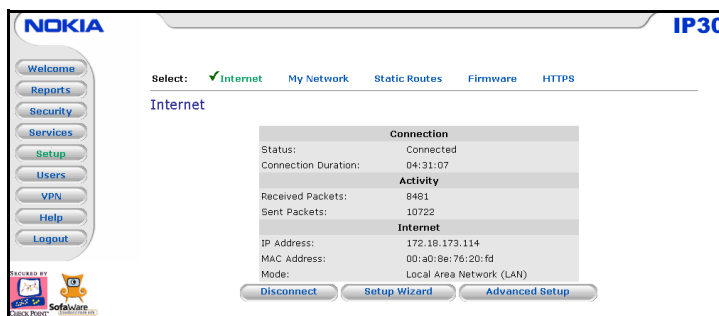
Viewing Network Activity Information

You can view network activity information.

To view network activity information

- In the Navigation Bar, click Setup.

The Internet page appears displaying a brief view of the network activity and status.



The following information is displayed:

- Connection: provides information on the connection status and the connection duration, if it is active.
- Activity: details the amount of data packets sent and received in the active connection.
- Internet: provides information on the user's IP and MAC addresses as well the connection mode used.

Click Setup to go back to the setup page.

Quick Internet Connection and Disconnection

Click the Connect or Disconnect button (depending on the connection status) to establish quick Internet connection by using the currently selected connection type. In the same manner, you can terminate the active connection.

Configuring Network Settings



Warning

Network Settings are advanced settings. Nokia recommends that these settings are not changed unless it is necessary and you are qualified to do so. Changing network settings might result in losing the IP30 configuration.

If you change the network settings to incorrect values and are unable to correct the error, reset the IP30 to its factory default settings.

To reset the IP30 to its factory default settings, choose Setup > Firmware > Factory Defaults.

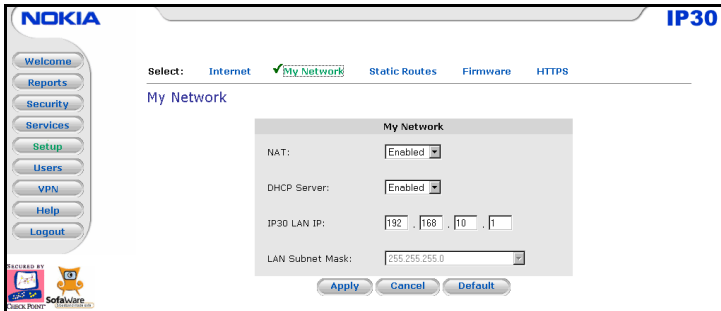
Enabling and Disabling the DHCP Server

The IP30 operates as a DHCP (Dynamic Host Configuration Protocol) server enabled by default. This allows the IP30 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 IP30. Nokia recommends that you leave this setting enabled.

To enable or disable the DHCP server,

1. In the Navigation Bar, click Setup > My Network.
The My Network page appears.



The My Network page is different for IP30 Satellite

2. In the DHCP Server list, select Enabled or Disabled.
3. Click Apply.
4. If you do not have another DHCP server in your network, and your computers were originally configured differently, do the following:
 - Reconfigure all the devices on your network.
 - Use DHCP to disable the Obtain IP address automatically setting in the TCP/IP settings.

Changing IP Addresses

You can change the IP address of your IP30. With IP30 Satellite, you can also change the entire range of IP addresses in your network. You might want to do this if, for example, you are adding the IP30 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 IP30, that assigns addresses within a different range.

If you change the IP address of your IP30, 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,

1. In the Navigation Bar, click Setup > 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. The following things happen:
 - If you changed the internal network range to X.X.X.X, the IP address of the IP30 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 (using DHCP), and the DHCP server in your IP30 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 using the TCP/IP settings.

Enabling and Disabling NAT

Network Address Translation (NAT) enables you to share a single IP address among several computers.

Note

NAT can only be disabled in IP30 Satellite and Satellite Plus. NAT is enabled by default. If NAT is disabled, you need to buy an IP address range.

To enable NAT

1. In the Navigation Bar, click Setup > My Network.
The My Network page appears.

2. Select Enabled.
3. Click Apply.
NAT is enabled.

Accessing the IP30 from a Remote Location

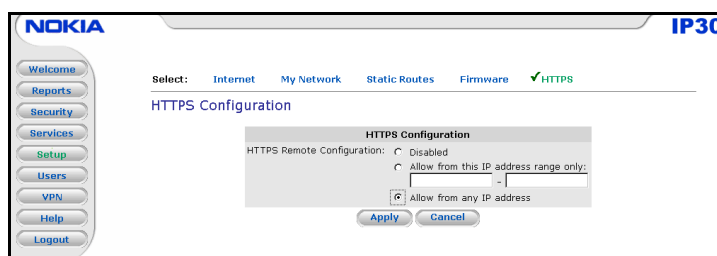
You can allow users to access IP30 from a remote location through the Internet. To allow remote access, you must first configure HTTPS.

Note

If your IP30 is managed from a central location, the central location must configure HTTPS access for you.

To configure HTTPS

1. In the Navigation Bar, click Setup > HTTPS.
The HTTPS Configuration page appears.



2. Do one of the following:
 - a. Select Disabled to disable remote HTTPS capability.
 - b. To allow access to IP30 from a specific range of IP addresses, select Allow from this IP address range only and enter the IP address range.

Note

You can use HTTPS to access the IP30 from your internal network even if remote HTTPS is disabled, by going to <https://my.firewall>.

- c. To allow access to the IP30 from any IP address, select Allow from any IP address.

**Warning**

If HTTPS is enabled, the IP30 settings can be changed remotely, so make sure all IP30 passwords are difficult to guess.

3. Click Apply.

The HTTPS configuration is saved. You can now access IP30 from a remote location through the Internet.

Managing IP30 Firewall from a Remote Location

You can manage an IP30 from a remote location using a Safe@object configured on Check Point SmartCenter FP3. The Checkpoint Smart Dashboard has three profiles to manage Firewall remotely they are "Low", "Medium", "High" and a pre-configured "Hi-med-Low" profile.

They are derived from a Rule base and packaged together into a single security policy which can be enforced onto the IP30.

Viewing Reports

You can view the following reports in the IP30 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 blue indicate changes in your setup that you made or as a 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 attempts that your custom security rules blocked.

The logs detail the date and time the event occurred, and its 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. In the Navigation Bar click Reports.
The Event Log page appears.

Select: ☒ Event Log ☐ Active Computers ☐ Active Connections ☐ VPN Tunnels

Event Log Refresh Clear

You can view the event log for the last 100 events.

#	Date	Time	Protocol	Source		Destination	
				IP Address	Port	IP Address	Port
00043	Oct 18	17:16:21	User	admin	logged in		
00042	Oct 18	17:15:14	UDP	192.168.10.85 (HYDT0009)	137 (NETBIOS)	172.18.140.10	137 (NETBIOS)
00041	Oct 18	17:14:58	UDP	192.168.10.85 (HYDT0009)	137 (NETBIOS)	172.18.140.10	137 (NETBIOS)
00040	Oct 18	17:14:45	UDP	192.168.10.85 (HYDT0009)	137 (NETBIOS)	172.18.140.10	137 (NETBIOS)
00039	Oct 18	17:12:54	UDP	192.168.10.85 (HYDT0009)	137 (NETBIOS)	172.18.140.10	137 (NETBIOS)
00038	Oct 18	17:12:42	UDP	192.168.10.85 (HYDT0009)	137 (NETBIOS)	172.18.140.10	137 (NETBIOS)
00037	Oct 18	17:10:55	UDP	192.168.10.85 (HYDT0009)	137 (NETBIOS)	172.18.140.10	137 (NETBIOS)
00036	Oct 18	17:10:45	UDP	192.168.10.85 (HYDT0009)	137 (NETBIOS)	172.18.140.10	137 (NETBIOS)
00035	Oct 18	17:08:49	UDP	192.168.10.85 (HYDT0009)	137 (NETBIOS)	172.18.140.10	137 (NETBIOS)
00034	Oct 18	17:08:37	UDP	192.168.10.85 (HYDT0009)	137 (NETBIOS)	172.18.140.10	137 (NETBIOS)
00033	Oct 18	17:06:49	UDP	192.168.10.85 (HYDT0009)	137 (NETBIOS)	172.18.140.10	137 (NETBIOS)

2. Do any of the following:

- Click the Refresh button to refresh the display.
- Click the Clear button to clear all events.
- If an event is highlighted in red, indicating a blocked attack on your network, you can display the attacker's details, by clicking on the IP address of the attacking machine.

The IP30 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 hackers.

Viewing Active Computers

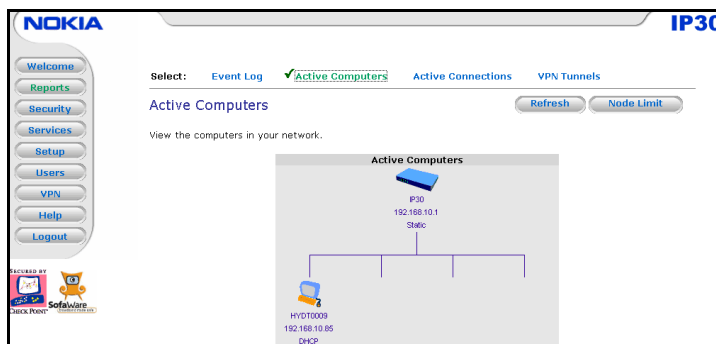
The Viewing Active Computers option allows you to view the currently active computers on your network. The active computers are graphically displayed, each with its name, IP address, and settings (DHCP, Static, and so on).

You can also view node limit information.

To view the active computers

1. In the Navigation Bar click Reports > Active Computers.

The Active Computers page appears.



If you exceed the maximum number of computers allowed by your license, a warning message appears, and the computers over the node limit are marked in red. These computers might not be able to access the Internet through the IP30.

Note

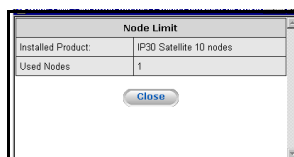
To increase the number of computers that your license allows, you must upgrade your product.

If desired, click the Refresh button to refresh the display.

2. To view node limit information:

a. Click Node Limit.

The Node Limit window appears with installed software product and the number of nodes used.



b. Click Close to close the window.

Viewing Active Connections

The Viewing Active Connections option 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 the active connections,

1. In the Navigation Bar click Reports > Active Connections.

The Active Connections page appears.

Protocol	Source		Destination	
	IP Address	Port	IP Address	Port
UDP	192.168.10.85 (HYDT0009)	2868	172.18.173.14	161 (SNMP)
UDP	192.168.10.85 (HYDT0009)	2832	172.18.173.14	161 (SNMP)
UDP	192.168.10.85 (HYDT0009)	2889	172.18.173.14	161 (SNMP)
UDP	192.168.10.85 (HYDT0009)	2888	172.18.173.14	161 (SNMP)
UDP	192.168.10.85 (HYDT0009)	2890	172.18.173.14	161 (SNMP)
UDP	192.168.10.85 (HYDT0009)	2879	172.30.178.7	161 (SNMP)
UDP	192.168.10.85 (HYDT0009)	2869	172.30.178.7	161 (SNMP)
UDP	192.168.10.85 (HYDT0009)	2870	172.30.178.7	161 (SNMP)
UDP	192.168.10.85 (HYDT0009)	2886	172.30.178.7	161 (SNMP)
UDP	192.168.10.85 (HYDT0009)	2887	172.30.178.7	161 (SNMP)

2. Do the following:

- Click the Refresh button to refresh the display.
- To view information on the destination machine, click on its IP address.

The IP30 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 VPN Tunnels

You can view a list of currently established VPN tunnels.

Note

This feature is applicable for IP30 Tele and Satellite.

A VPN tunnel is created whenever your computer attempts to communicate with a computer at the VPN site, after you have logged on to the site. When you log off, all open tunnels connecting to a VPN site are closed.

VPN tunnels are created and closed as follows:

- Remote Access VPN sites configured for automatic login:

A tunnel is created whenever your computer attempts to communicate with a computer at the VPN site. The tunnel is closed when not in use.

Note

Although the VPN tunnel is automatically closed, the site remains open, and if you attempt to communicate with the site, the tunnel is re established.

- Remote Access VPN sites configured for site-to-site VPN gateways:

A tunnel is created whenever your computer attempts to communicate with a computer at the VPN site. The tunnel is closed when not in use.

- Remote Access VPN sites configured for Manual Login:

A tunnel is created whenever your computer attempts to communicate with a computer at the VPN site, after you have manually logged on to the site. All open tunnels connecting to the site are closed when you manually log off.

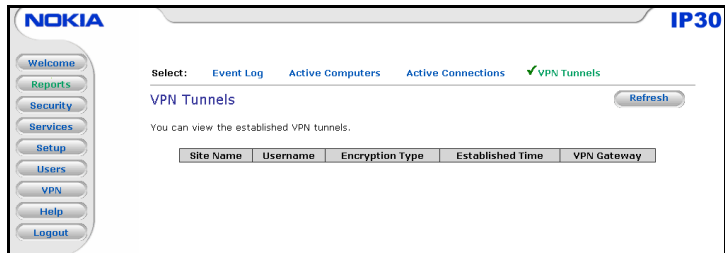
To view VPN tunnels

1. Click Reports.

The Event Log page appears.

2. In the submenu, click VPN Tunnels.

The VPN Tunnels page appears with a table of open tunnels to VPN sites.



The VPN Tunnels table includes the following columns:

Table 3 VPN Tunnels

Column	Information
Site	The VPN site's name
Username	The User logged on to the VPN site
Encryption Type	<p>The type of encryption used to secure the connection, followed by the type of authentication used to verify the user's identity.</p> <p>This information is presented in the following format - Encryption Type/ Authentication Type</p>
Established Time	<p>The Time when the VPN Tunnel is established.</p> <p>This information is presented in the following format - Hour:Minute:Second</p>
VPN Gateway	The IP Address of the VPN Gateway to which the Tunnel is connected

You can refresh the table by refreshing the browser.

Setting up the IP30 Security Policy

You can control the following security features from the IP30 GUI:

- Firewall security level
- Configuring Virtual servers
- Allowing specific ports and IP addresses
- Blocking specific ports and IP addresses
- Setting up a computer as a DMZ

You can also subscribe to services such as Web Filtering and Anti - virus scanning. For information on these services and the subscription process, see “Using Subscription Services.”

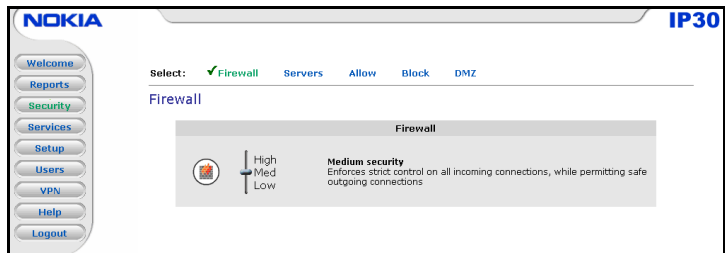
Setting the Firewall Security Level

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

- Low security - enforces basic control on incoming connections, while permitting all outgoing connections.
- Medium security - enforces strict control on all incoming connections, while permitting safe outgoing connections.
- High security - enforces strict control on all incoming and outgoing connections.

To change the firewall security level

1. In the Navigation Bar click Security.
The Firewall page appears.



2. To set the security level, drag the slider.
The IP30 security level changes accordingly.

Note

You may experience a temporary break in the service.

Configuring Virtual Servers

Note

If you do not intend to host any public Internet servers (Web server, mail server and so on) in your network, you can skip this section.

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

Note

If you configure a virtual server, you can not create an additional Allow Rule.

To allow a service to be run on a host

1. In the Navigation Bar click Security.
The Firewall page appears.

2. Click the Servers tab.

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

NOKIA **IP30**

Welcome Reports Security **Services** Setup Users VPN Help Logout

Select: Firewall ☒ Servers Allow Block DMZ

Virtual Servers

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

#	Allow	Category	Application Name	Host IP	VPN Only
1	<input checked="" type="checkbox"/>	Applications	Web Server	200.200.2.1 This Computer	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	Applications	FTP	This Computer	<input type="checkbox"/>
3	<input type="checkbox"/>	Applications	Telnet	This Computer	<input type="checkbox"/>
4	<input type="checkbox"/>	Applications	POP3	This Computer	<input type="checkbox"/>
5	<input type="checkbox"/>	Applications	SMTP	This Computer	<input type="checkbox"/>

Apply Cancel

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

If you are using IP30 Satellite, the appropriate check box in the VPN Only column is enabled.

4. To allow only connections made through a VPN, 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 will run the service (one of your network computers) or click the corresponding This Computer button 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.

To stop a service from running on a specific host

1. In the Navigation Bar, click Security > Servers.

The Virtual Servers page appears, 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.

Creating Rules

The IP30 checks the protocol used, the ports range, and destination IP address when deciding whether to allow or block traffic. User defined rules have priority over the default rules.

By default, in the Medium security level, the IP30 blocks all connection attempts from the Internet (WAN) to the LAN, and allows all outgoing connection attempts from the LAN to the Internet (WAN).

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 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.

To create a new rule

1. In the Navigation Bar, click Security.

The Firewall page appears.

2. Click Allow tab to create a new Allow rule or click the Block tab to create a new Block rule.

Depending on the tab you select, the Allow Rules or the Block Rules page appears.

The screenshot shows the Nokia IP30 web interface. On the left is a navigation bar with buttons: Welcome, Reports, Security (highlighted), Services, Setup, Users, VPN, Help, and Logout. The main content area has a header with 'NOKIA' and 'IP30'. Below the header, there's a 'Select:' section with tabs: Firewall, Servers, Allow (checked), Block, and DMZ. The title 'Allow Rules' is displayed. A message states: 'To allow additional inbound services not on the "Virtual Servers" list, specify the port ranges and protocols.' Below this is a table with columns: #, Protocol, Ports, Internet IP, Home IP, and VPN Only. A 'New:' row shows 'TCP' in the Protocol column, empty boxes in the Ports column, and empty boxes in the Internet IP and Home IP columns. There is a checkbox for 'This Computer' and 'Add' and 'Clear' buttons.

#	Protocol	Ports	Internet IP	Home IP	VPN Only
New:	TCP				<input type="checkbox"/> This Computer

The screenshot shows the Nokia IP30 web interface. On the left is a navigation bar with buttons: Welcome, Reports, Security (highlighted), Services, Setup, Users, VPN, Help, and Logout. The main content area has a header with 'NOKIA' and 'IP30'. Below the header, there's a 'Select:' section with tabs: Firewall, Servers, Allow, Block (checked), and DMZ. The title 'Block Rules' is displayed. A message states: 'To block outbound communication selected port ranges and protocols.' Below this is a table with columns: #, Protocol, Ports, Internet IP, Home IP, and Also VPN. A 'New:' row shows 'TCP' in the Protocol column, empty boxes in the Ports column, and empty boxes in the Internet IP and Home IP columns. There is a checkbox for 'This Computer' and 'Add' and 'Clear' buttons.

#	Protocol	Ports	Internet IP	Home IP	Also VPN
New:	TCP				<input type="checkbox"/> This Computer

Note

In IP30 Firewall or Tele, the Allow Rules page does not contain a VPN Only column, and the Block Rules page does not contain an Also VPN column.

3. To specify the port range to which the rule applies, in the Ports column, enter 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 is open-ended.

4. From the Protocol drop-down list, select the protocol for which you wish to create a rule.
5. In the Internet IP text box, do one of the following:
 - If you are creating an Allow rule, type the Internet IP address that should be allowed to access the defined ports of a specific computer inside your network.
 - If you are creating a Block rule, type the Internet IP address whose defined ports should not be accessible from a specific computer inside your network.

Note

When in No-NAT mode, you can leave the Internet IP field empty. The rule then applies to the entire Internet.

When you create Allow rules in NAT mode, you need to provide an IP address. This way the IP30 knows to which computer to forward incoming connections. On the other hand, when you define Block rules in NAT mode, you can leave the Internet IP field empty, which results in the IP30 blocking outgoing Internet connections of all computers in the local network on the specified ports.

6. In the Home IP text box, do one of the following:
 - If you are creating an Allow rule, type the IP address of the computer inside your network, to which the specified Internet IP address should be allowed access.

- If you are creating a Block rule, type the IP address of the computer inside your network for which access to the specified Internet IP address should be blocked.

Alternatively, you can specify your computer, by clicking This Computer.

7. In the Allow Rules page, select the VPN Only check box to allow only connections made through a VPN.
8. In the Block Rules page, select the Also VPN check box if you want the rule to apply not only to the Internet, but to the VPN as well.
9. Click Add.

The new rule is added to the list of rules.

To delete an existing rule

1. In the Navigation Bar click Security.
The Firewall page appears.
2. Click the Allow tab to delete an Allow rule or click the Block tab to delete a Block rule.
The Allow and Block Rules page appears.
3. Click the Delete icon of the rule you wish to delete.
A confirmation message appears.
4. Click OK.

The rule is deleted.

Demilitarized Zone

The IP30 allows you to define a DMZ, that is define a computer that is not protected by the firewall. This procedure is useful for setting up a public server. It allows unlimited incoming and outgoing connections between the Internet and that computer.



Warning

Entering an IP address might make the designated computer vulnerable to hacker attacks.

To define a computer as DMZ

1. In the Navigation Bar click Security > DMZ

The DMZ IP Address page appears.

2. In the DMZ IP Address text box, type the IP address of the computer you wish to define as DMZ.

Alternatively, you can click This Computer to define your computer as DMZ.

3. Click Apply.

The selected computer is now defined as DMZ.

Using Subscription Services

Subscription services offer valuable features, such as automatic software and security policy updates, content filtering, Anti virus scanning, and remote logging.

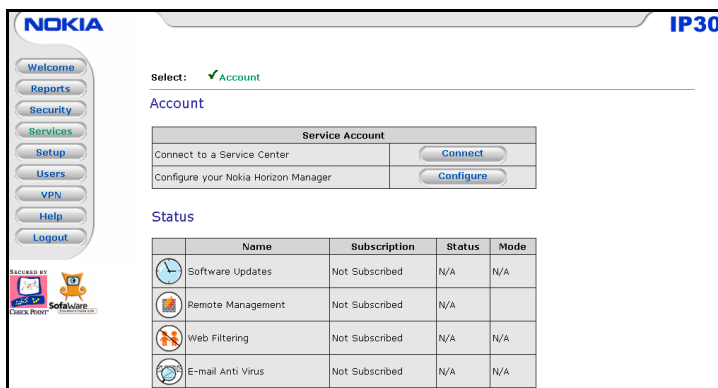
Starting Your Subscription Services

The subscription services option allows you to configure and start your services subscription.

To start your subscription

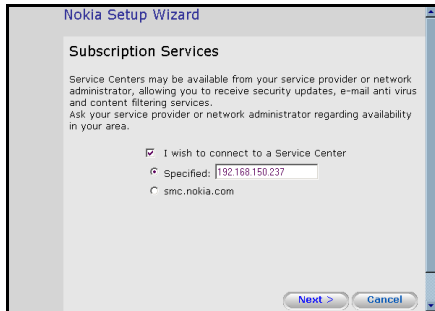
1. In the Navigation Bar, click Services.

The Account page appears.



2. In the Service Account area, click Connect.

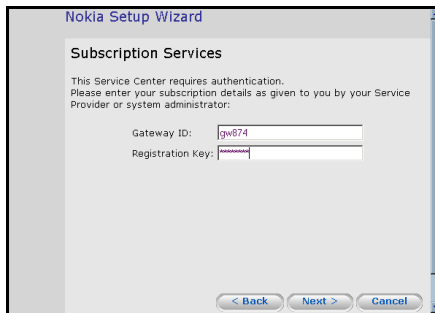
The Setup Wizard opens, with the first Subscription Services dialog box displayed.



3. Make sure the I wish to connect to a Service Center check box is selected.
4. Enter the desired service center IP address or the domain name in the Service Center text box, as given to you by your service provider.
5. Click Next.

The Connecting screen appears.

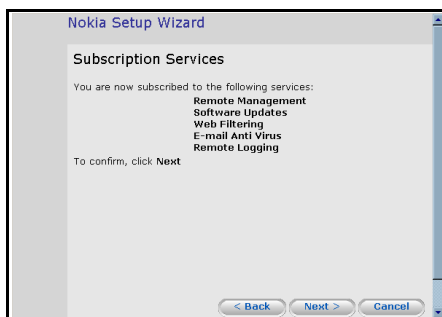
The second Subscription Services dialog box appears.



6. Enter your gateway ID and registration key in the appropriate fields, provided by your service provider.
7. Click Next.

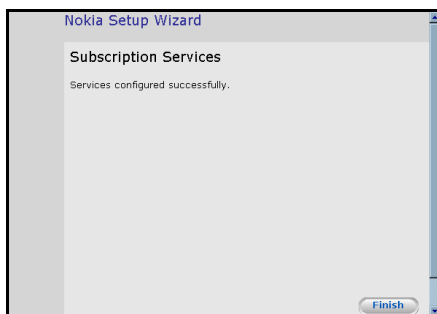
The Connecting screen appears.

The third Subscription Services dialog box appears with a list of services to which you are subscribed.



8. Click Next.

The final Subscription Services dialog box appears with a success message.



9. Click Finish.

The following things happen:

- If a new firmware was installed, the IP30 is restarted.
- The services to which you are subscribed to are now available on your IP30 and listed on the Account page.

The Services submenu includes the services you are subscribed to.

Viewing Services Information

The Account page Service Status area lists the services available in your service plan.

The following information is displayed for each service:

Name	Name of the service
Subscription	status of your subscription to the service (Subscribed or Not Subscribed)
Status	Status of the service
Connected	You are connected to the service from the Central Location.
N/A	Service not available
Mode	Mode to which the service is set. This depends on the IP30 management.

Canceling Subscription Services

You can cancel your subscription to the services provided by your service center.

To cancel your subscription

1. In the Navigation Bar, click Services > Connect.
2. In the Service Account area, click Connect.
The Setup Wizard opens, with the first Subscription Services dialog box displayed.
3. Clear the I wish to connect to a Service Center check box.
4. Click Next.
The final Subscription Services dialog box appears with a success message.
5. Click Finish.

The following things happen:

- You are disconnected from the service center.
- The services to which you were subscribed are no longer available on your IP30.

Web Filtering

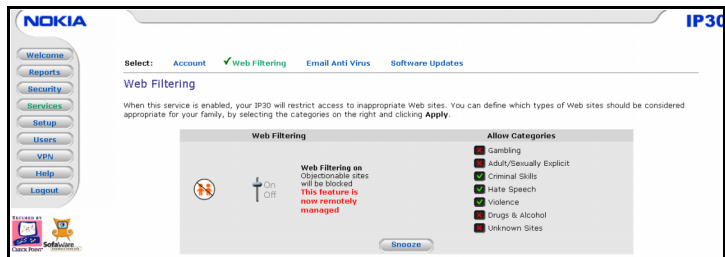
When enabled, access to Web content is restricted according to the categories specified under Allow Categories.

Enabling Web Filtering When Locally Managed

You can enable and disable Web filtering when your IP30 is locally managed.

To enable and disable Web Filtering when locally managed

1. In the Navigation Bar click Services.
The Account page appears.
2. In the Services submenu, click Web filtering.
The Web Filtering page appears.



3. Drag the On /Off lever upwards or downwards.

Web Filtering is enabled or disabled for all internal network computers.

Selecting Categories for Blocking

You can define which types of Web sites should be considered appropriate for users by selecting the categories. Visible and blocked categories are marked and will require the administrator password for viewing.

Note

If the configured plan is remotely managed but with services locally managed, then you can modify the services using the IP30 GUI

To allow and block a category

1. In the Allow Categories area, select the desired category.
2. Click Apply.

Snoozing Web Filtering When Remotely Managed

If the IP30 is remotely managed, your service center can remotely control snoozing. You can also snooze the Web Filtering service, temporarily disabling it.

To snooze Web Filtering when remotely managed

1. In the Navigation Bar click Services > Web Filtering.

The Web Filtering page appears.

Note

The On/Off slider and Allow Categories area on this page are read-only. Contact your service center to change these settings.

If the service is enabled, the On/Off is set to On.

2. Click Snooze.
 - Web Filtering is snoozed for all internal network computers.
 - The Snooze button changes to Resume
 - The Web Filtering Off popup window opens.



Note

Closing the Web Filtering Off popup window does not cause the Web Filtering service to resume.

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.
 - The Resume button changes to Snooze.

- If the Web Filtering Off popup window was open, it closes.

E-mail Anti Virus

Enabling the anti virus scanning option results in automatic scanning of email for the detection and elimination of all known viruses and vandals.

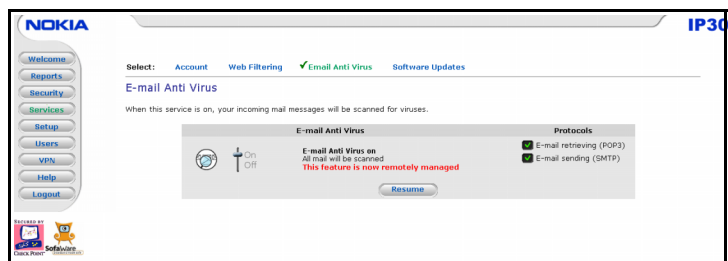
Enabling E-mail Anti Virus Scan When Locally Managed

You can enable the Anti virus scanning for outgoing SMTP and incoming POP3 email traffic.

To enable or disable email anti virus scan when locally managed

1. In the Navigation Bar click Services > Anti Virus.

The Anti Virus page appears.



2. Drag the On/Off slider upwards or downwards.

Anti virus scanning is enabled or disabled for all internal network computers.

Selecting Protocols for Scanning

If you are locally managed, you can define the protocols to be scanned for viruses:

- Email retrieving (POP3): if enabled, all incoming email in the POP3 protocol is scanned.
- E-mail sending (SMTP): if enabled, all outgoing email is scanned.

Protocols selected are scanned.

Note

If your IP30 is remotely managed, contact your service center to change these settings.

To enable virus scanning for a protocol

1. Select the desired protocol.
2. Click Apply.

Snoozing Anti virus When Remotely Managed

If the IP30 is remotely managed, your service center can remotely control this service.

If you are having problems sending or receiving email you can snooze the Anti virus service, temporarily disabling it.

To snooze Anti virus scanning when remotely managed

1. In the Navigation Bar click Services > Anti virus.
The Anti virus page appears.

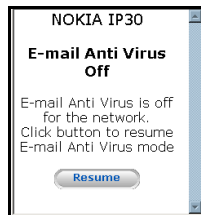
Note

The On/Off slider and Protocols area on this page are read-only. Contact your Service Center to change these settings.

If the service is enabled, the On/Off lever is set to On.

2. Click Snooze.

- Anti virus scanning is snoozed for all internal network computers.
- The Snooze button changes to Resume.
- The Anti virus Off popup window opens.



Note

Closing the E-mail Anti Virus Off popup window does not cause the Anti Virus service to resume.

3. To re-enable the service, click Resume, either in the popup window, or on the Anti virus page.

- The service is re enabled for all internal network computers.
- The Resume button changes to Snooze.
- If the Anti virus Off popup window was open, it closes.

Automatic and Manual Updates

If you are subscribed to software updates, you can check for new security and software updates.

Software Updates for Locally Managed IP30

If your IP30 is locally managed, you can set it to automatically check for software updates, or you can manually check for software updates.

To configure software updates when locally managed

1. In the Navigation Bar, click Services > Software Updates.
The Software Updates page appears.
2. To set the IP30 to automatically check for and install new software updates, drag the Automatic/Manual lever upwards.
The IP30 checks for new updates and installs them.

Note

When the Software Update service is set to Automatic, you can still manually check for updates. See step 5.

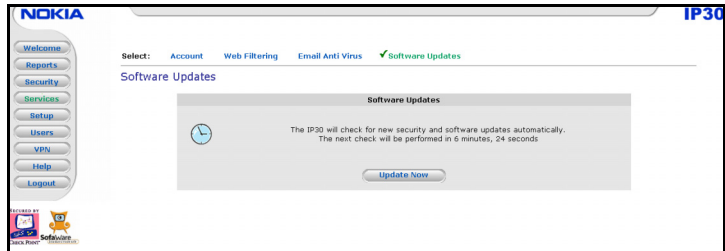
3. To set the IP30 so that software updates must be checked for manually, drag the Automatic/Manual lever downwards.
The IP30 does not check for software updates automatically.
4. To manually check for software updates, click Update Now.
The system checks for new updates and installs them.

Software Updates for Centrally Managed IP30

If your IP30 is managed from a central location, it automatically checks for software updates and installs them without user intervention. However, you can also check for updates manually.

To manually check for updates

1. In the Navigation Bar, click Services > Software Updates.
The Software Updates page appears.



2. Click Update Now.

The system checks for new updates and installs them.

Refreshing Your Service Center Connection

This option reconnects you to your Service Center and refreshes the IP30 services' settings.

To refresh your Service Center connection

1. In the Navigation Bar, click Services > Refresh.

IP30 reconnects to the Service Center. Your service settings are refreshed.

Configuring Your Account

The configure option allows you to access your service center, which offers additional configuration options for your account.

To configure your account

1. In the Navigation Bar, click Services > Configure.

The service center website opens.

Note

If no additional settings are available from your service center, this button does not appear.

2. Follow the on-screen instructions.

Configuring for Nokia Horizon Manager

You can configure your IP30 to be managed from Nokia Horizon Manager.

To configure Nokia Horizon Manager

1. In the Navigation Bar, Click Services > Configure (Select Nokia Horizon Manager).

The Nokia Horizon Manager wizard window opens.

2. Enter the following information:

IP Address of NHM

Port Number. Port Number 6654 is the default port.

Retry Timeout. The default timeout is 2 minutes

Host Name.

Select Allow HTTPS from NHM.

3. Click Connect.

Managing Users

Nokia IP30 Firewall and Tele have a single user called *admin*. You can change this user's password.

In Nokia IP30 Satellite, you can define multiple users and perform the following tasks:

Nokia Horizon Manager

You need to configure your IP30 to connect to Nokia Horizon Manager (NHM).

IP Address of NHM:

Port Number:

Retry Timeout (minutes):

Host Name:

Allow HTTPS from NHM: ☒

Note: This configuration is to be set only if this device is managed by NHM and the WAN is dynamic.

- Changing Your Password
- Adding Users
- Viewing and Editing Users
- Deleting Users
- Setting Up Remote VPN Access for Users

Changing Your Password

You can change your password at any time. How this task is performed depends on the IP30 that you are using (Firewall, Tele, or Satellite).

To change password using IP30 Firewall and Tele

1. In the Navigation Bar click Password.

The Password page appears.

NOKIA IP30

Welcome Reports Security Services Setup Users VPN Help Logout

Edit User

Details

Username:

Password (5-25 characters):

Confirm password:

Permissions

Administrator ☒

VPN Remote Access ☒

2. Edit the Password and Confirm password fields.

Note

Use 5 to 25 characters (letters or numbers) for the new password.

3. Click Apply.

Your changes are saved.

To change password using IP30 Satellite

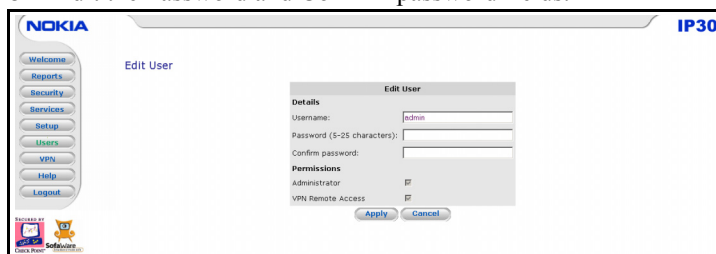
1. In the Navigation Bar click Users.

The Users page appears.

2. In the username row, click Edit.

The Edit User page appears.

3. Edit the Password and Confirm password fields.



Note

Use 5 to 25 alphanumeric characters for the new password.

4. Click Apply.

Your changes are saved.

Adding Users

You can perform this task only with IP30 Satellite. The number of IP30 users you can add is limited according to your software.

To add a user

1. In the Navigation Bar, click Users.
The Users page appears.
2. Click New User.
The Edit User page appears. The options that appear on the page depend on the software and services you are using.
3. Complete the fields using the information in Table 4.
4. Click Apply.

The new user is saved. The Edit User page appears.

Viewing and Editing Users

You can perform this task only with IP30 Satellite.

To view or edit users

1. In the Navigation Bar, click Users.
The Users page appears.
2. In the desired user's row, click Edit.
The Edit User page appears 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 using Table 4.
 - b. Click Apply.
The changes are saved.

4. To return to the Users page without making any changes, click Cancel.

Table 4 Users

Field	Action
Username	Enter a username for the user. You cannot change the admin user's username.
Password	Enter a password for the user. Use five to 25 alphanumeric characters for the new password.
Confirm Password	Re enter the user's password.
Administrator	Allows the user to log on to my.firewall. This option cannot be disabled for the admin user.
VPN Remote Access	Allows the user to connect to this IP30 using their VPN client. For further information on setting up VPN remote access, see "Setting Up Remote VPN Access for Users." This option is available in IP30 Satellite and Satellite Plus only.
Web Filtering Override	Allows the user to override family filters. This option only appears if the Web Filtering service is defined.

Deleting Users

You can delete users only with IP30 Satellite.

Note

The “admin” user cannot be deleted.

To delete a user

1. In the Navigation Bar, click Users.
The Users page appears.
2. In the desired user’s row, click the Delete icon.
A confirmation message appears.
3. Click OK.
The user is deleted.

Setting Up Remote VPN Access for Users

You can setup VPN access for users only with IP30 Satellite. If you are using IP30 as a VPN server, you can allow users to access it remotely through their VPN clients (a Check Point SecureClient, Check Point SecuRemote, IP30 Tele, or another IP30 Satellite).

To set up remote VPN access for a user

1. Enable your VPN server using the procedure in “Setting Up Your IP30 as a VPN Server.”
2. Add the user to the system, using the procedure in “Adding Users.”

You must select the VPN Remote Access option.

4 VPN Configuration

In addition to a full firewall functionality, the IP30 Tele, Satellite, and Satellite Plus enable secure telecommuter access from home to the office network through the virtual private network (VPN) functionality.

A 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 and enable the two connected networks to function as a single network.

A connection between two VPN sites is called a VPN tunnel. VPN tunnels encrypt and authenticate all traffic through them. Through these tunnels, you can safely use your company's 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.

IP30 Tele, IP30 Satellite and Satellite Plus provide VPN functionality.

The IP30 Tele acts as a VPN client and can establish secure VPN tunnels to your office VPN gateway.

IP30 Satellite and Satellite Plus can act as a VPN client, a VPN server, or a VPN gateway.

Note

If you have an IP30 Firewall and need VPN functionality, upgrade your IP30 to Tele, Satellite or Satellite Plus. Until you install your Tele or Satellite license, your IP30 functions as a Firewall. For information on how to install a license, see “Installing Your Software License.”

Both Tele and Satellite enable a number of solutions to support your VPN connectivity needs that are explained in the subsequent sections:

Figure 5 VPN Topologies

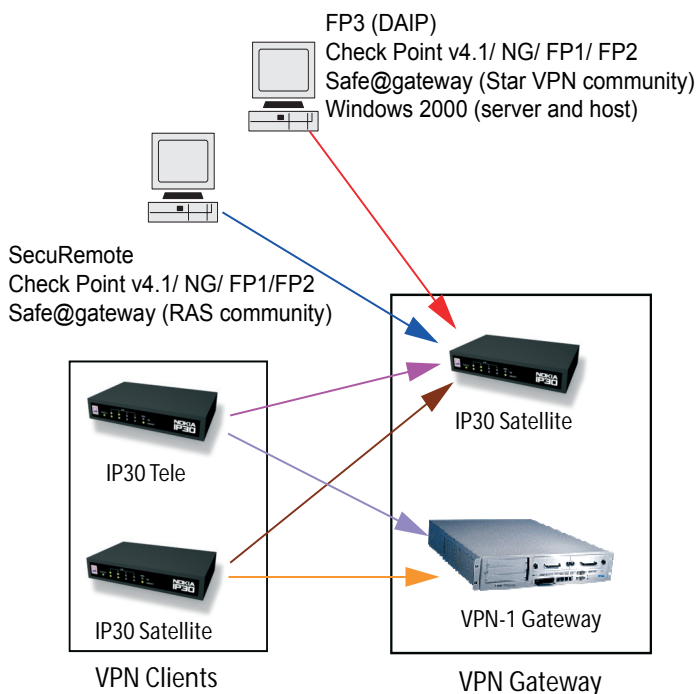


Table 5 VPN Topologies

VPN Client	Gateway
SecuRemote/ VPN Client	Satellite
Tele	Satellite
Tele	Check Point v4.1, NG, FP1, FP2, FP3
Tele	Check Point FP3 (RAS Community)
Satellite (Gateway)	Satellite (Gateway)
Satellite (Gateway)	VPN-1, Check Point v4.1, NG, FP1, FP2, FP3
Satellite	Check Point FP3 (DAIP object)
Satellite	Check Point FP3 (Star Community)
Satellite	Windows 2000

Note

To know more on Configuring VPN gateways, refer *SofaWare's Configuring Safe@* to *VPN-1 gateway to gateway VPNs with DAIP*.

SecuRemote to Satellite (VPN Client to Gateway)

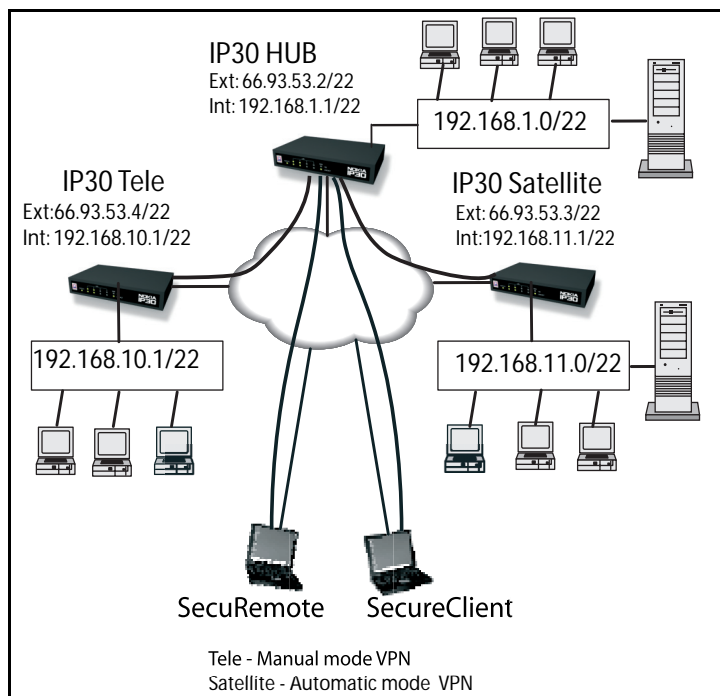
This VPN topology enables IP30 Tele, Satellite, Check Point SecuRemote and SecureClient VPN clients to connect to an IP30 Satellite VPN server.

Note

In this configuration, the IP30 Satellite VPN server must have a static IP address / domain name.

Below is a sample implementation of the VPN client-to-IP30 Satellite VPN server solution, in which two IP30 devices, a Check Point SecuRemote, and a Check Point SecureClient act as VPN clients that download topology information from the IP30 Satellite VPN server.

Figure 6 SecuRemote and SecureClient to Satellite



Setting up IP30 Satellite

Configure a VPN tunnel between SecuRemote and IP30 Satellite.

To set up IP30 Satellite

1. Add a User (refer "Managing Users" to Add a User).
2. Enable Remote Access for the User.
3. Enable VPN server.

Setting up SecuRemote

Define your VPN sites as IP30 Satellite to set up SecuRemote.

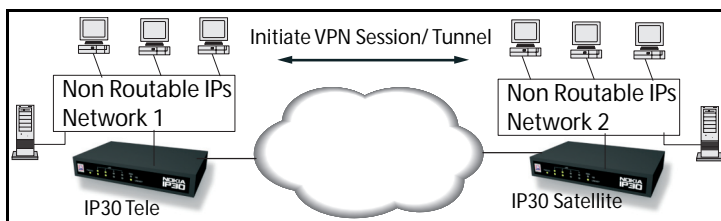
Refer Check Point *Desktop Security Guide*, VPN-1 SecuRemote Client” for information on how to Configure SecuRemote.

IP30Tele to IP30 Satellite (VPN Client to Gateway)

IP30 Tele functions in VPN client mode, in which connection is initiated only by the VPN client.

IP30 Tele uses only 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 7 IP30 Tele as VPN Client



If the VPN client is enabled, the IP30 GUI Navigation Bar includes a VPN menu option. In addition, the Reports pages includes an additional VPN Tunnels submenu that allows you to view the active VPN tunnels.

Note

You can use IP30 Tele only in NAT mode.

Setting up IP30 Tele

Configure a VPN Tunnel between an IP30 Tele and an IP30 Satellite.

On IP30 Tele (VPN client) add a VPN site.

Setting up IP30 Satellite

Configure a VPN Tunnel between an IP30 Tele and an IP30 Satellite.

To set up the IP30 Satellite

1. Add a User.
2. Enable VPN remote access for the user you added.
3. Enable the VPN Server.

IP30 Tele to Check Point v4.1/ NG/ FP1/ FP2

The IP30 Tele can be used as a VPN client to establish a VPN connectivity with a Check Point server using version 4.1, NG, FP1, FP2 or FP3.

Setting up IP30 Tele

Configure a VPN Tunnel between an IP30 Tele and an IP30 Satellite.

On IP30 Tele (VPN client) add a VPN site.

Setting up Check Point Server

Open the Check Point policy editor and select Firewall-1/ VPN -1 workstation object that will receive the Safe@VPN session request.

IP30 Tele to Check Point FP3

The IP30 Tele can be used as a VPN client to establish a VPN connectivity with Check Point FP3 server using a Safe@gateway

dynamic object. This topology uses a remote access VPN community.

An illustration of this topology is available in Figure 8.

IP30 Tele uses only a manual mode VPN connection. To select the VPN gateway to which you want to establish a VPN connection, go to <http://my.vpn>.

Setting up IP30 Tele

To configure a VPN Tunnel between an IP30 Tele and Check Point FP3, on IP30 Tele (VPN client) add a VPN site.

Setting up Check Point FP3

Configure a Safe@gateway dynamic object on the Check Point SmartBoard.

To set up Check Point FP3

1. Create a Safe@gateway as a dynamic object.
2. Create a user and add the user to the VPN users group.
3. Create a remote access VPN community.
Include FP3 firewall object in the participating gateway.
Include the Users group in the participating users.
4. In the policy editor, create a rule with
Source User - any
Destination - any
Via - remote access community
Target - FP3 firewall object

Satellite to Satellite (VPN Gateway to Gateway)

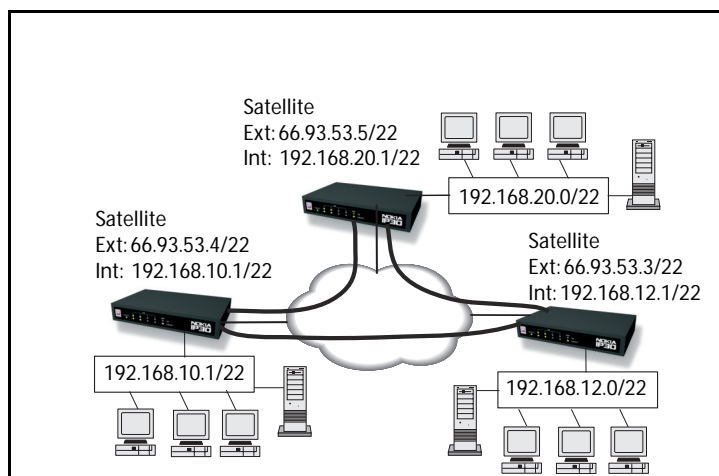
The VPN configuration between an IP30 Satellite and another IP30 Satellite enables you to establish site-to-site VPN connections between IP30 site-to-site VPN gateways.

Note

In this configuration, both IP30 Satellite Site-to-Site VPN gateways must have a static IP address.

The Figure below shows a sample implementation of the Satellite to Satellite solution with three Satellite devices. Each IP30 device acts as a Site-to-Site VPN gateway for a fully secure network. The networks communicate through VPN connections.

Figure 8 Satellite to Satellite



Setting up IP30 Satellite

Configure a VPN tunnel between two IP30 Satellite devices (site-to-site VPN).

To set up IP30 Satellite

1. Specify the IP address of IP30 Satellite on the remote IP30 Satellite.
2. Enter the Shared Secret (a password that is known to both of the IP30 Satellite devices).

To set up the remote IP30 Satellite

1. Specify the IP address of your IP30 Satellite.
2. Enter the Shared Secret (a password that is known to both the IP30 Satellite devices.)

Satellite to VPN-1 (Site-to-Site VPN)

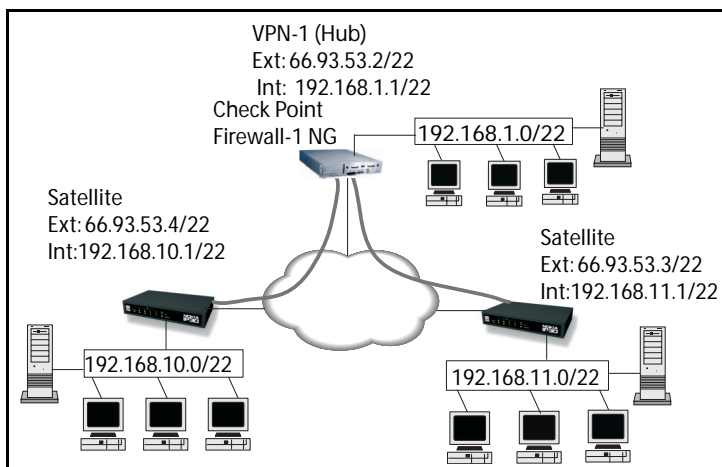
The IP30 Satellite to VPN-1 or Check Point v4.1, NG, FP1, FP2 or FP3 configuration enables you to establish site-to-site VPN connections between an IP30 Satellite site-to-site VPN gateway and a VPN-1 site-to-site VPN gateway.

Note

In this solution model, both the VPN-1 and IP30 Satellite Site-to-Site VPN gateways must have a static IP address.

The figure below shows an implementation of the IP30 Satellite to Check Point VPN-1 solution, in which two IP30 Satellite devices are connected to a VPN-1 site-to-site VPN gateway.

Figure 9 Satellite to VPN-1



Setting up IP30 Satellite

Configure a VPN Tunnel between an IP30 Satellite and Check Point VPN-1 server or gateway.

To configure IP30 Satellite

1. Specify the IP address of IP30 Satellite on the VPN-1 server.
2. Enter the Shared Secret (a password that is known to both the IP30 Satellite and the VPN-1 Server).

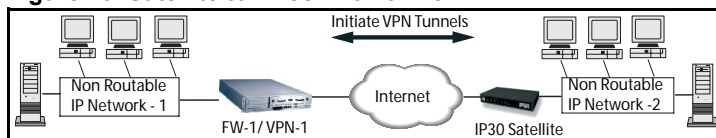
Note

For information on setting up VPN-1, refer to the *Check Point Virtual Private Networks*.

IP30 Satellite to Check Point FP3

The IP30 Satellite can be used as a VPN server to establish a VPN connectivity with Check Point FP3 server using Check Point FP3 DAIP object.

Figure 10 Satellite to Check Point FP3



Setting Up Check Point FP3

Configure a VPN Tunnel between an IP30 Satellite and Check Point FP3 server.

To set up Check Point FP3

1. Define a DAIP object.
Enable IKE.
2. Use VPN export tool to create a .p12 certificate from the internal certificate defined for the DAIP object.
3. Configure a rule set with the following:
Source: internal network of the IP30 DAIP object
Destination: internal network of FP3
Select Encrypt
Push the policy on to the FP3 firewall object.
4. Import the certificate to the computer to which the IP30 Satellite is connected.
Use FTP or a floppy disk to import the certificate.

Setting up IP30 Satellite

Configure a VPN Tunnel between an IP30 Satellite and Check Point FP3 server.

To set up IP30 Satellite

1. On the IP30 GUI, click VPN.
The VPN page appears.
2. Click Certificates.
On the Certificates page, browse for the certificate.
Click Upload.
3. Enter the Certificate pass phrase that you use to create the certificate.
4. Click OK.

When creating a VPN connection between IP30 Satellite and Check Point FP3, select Use Certificate instead of Use Shared Secret.

IP30 Satellite to Check Point SmartCenter FP3

The IP30 Satellite can be used as a VPN server to establish a VPN connectivity with SmartCenter FP3 server using Safe@gateway with a static IP address (VPN Star Community).

Setting Up Check Point SmartCenter FP3

Configure the Check Point SmartCenter FP3 for a VPN connection with IP30 Satellite.

To set up Check Point SmartCenter FP3

1. Define a Safe@ gateway with a static IP address.
2. Create a new Star Community.

3. Configure VPN central gateway as the FP3 firewall object.
4. Configure Safe@gateway as Satellite gateway.
5. In the VPN properties, select 3DES and SHA1.
6. Define access rules with the following:

Source: Any

Destination: Any

If Via: Remote Access

Action: Accept

Install On: FP3 firewall object

Setting up IP30 Satellite

Configure the IP30 Satellite for VPN connection with SmartCenter FP3.

1. Specify the IP address of IP30 Satellite on the VPN-1 server.
2. Enter the Shared Secret (a password that is known to both the IP30 Satellite and the VPN-1 Server).

IP30 Satellite in NAT and No-NAT Modes

VPN configuration allows you to choose how your VPN should function. Use of NAT and No-NAT modes offers great flexibility.

No-NAT is the default mode of operation, in which the protected networks at each site are known and predefined.

NAT mode allows you to define VPNs at peer gateway sites without knowing the protected network behind the IP30 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 No-NAT mode, you must contact the IP address of the final 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.

No-NAT Mode

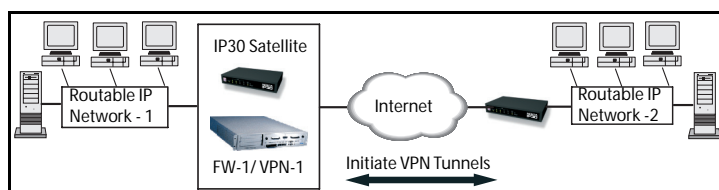
Use no-NAT mode in site-to-site VPNs, where bi-directional initiation of traffic within a VPN is required between hosts with routable IP addresses.

Note

You can only use No-NAT mode with IP30 Satellite.

The Figure below shows a site-to-site VPN in No-NAT mode. Both VPN peers are considered site-to-site VPN gateways, and traffic is directly established from the source host to the destination host. In this example, hosts on either network can initiate traffic to hosts on the peer network. Both Network 1 and Network 2 are using routable IP addresses.

Figure 11 No-NAT Mode

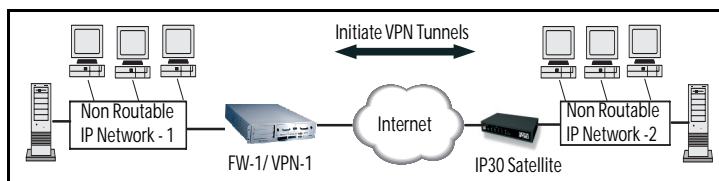


NAT Mode

NAT mode should be used in site-to-site VPNs, where bi-directional initiation of traffic between networks using private IP addresses is required.

The Figure below shows two instances of a site-to-site VPN gateways in NAT mode.

Figure 12 NAT Mode



Solution A: IP30 Satellite to VPN-1 (Site-to-Site VPN)

Hosts on Network 1 establish the TCP/IP connection to the external IP address of the IP30 Satellite site-to-site VPN gateway. The IP30 Satellite device is configured through the IP30 GUI Security page to port forward the inbound traffic to the defined host.

Solution B: Satellite to Satellite (Site-to-Site VPN)

IP30 Satellite supports the creation of site-to-site VPN connections between two or more IP30 Satellite devices. Hosts on either network can directly initiate traffic to hosts on the peer network. The IP30 Satellite is configured through the IP30 GUI Security page to port forward the inbound traffic to the defined host.

IP30 Satellite to Windows 2000

You can configure for VPN connectivity between the IP30 Satellite and a Windows 2000 server in the following scenarios:

- Windows gateway to IP30 Satellite in unrestricted mode

- Windows gateway to IP30 Satellite in restricted mode
- Windows Client to IP30 Satellite in unrestricted mode
- Windows Client to IP30 Satellite in restricted mode

For more information on how to configure the Windows 2000 server, refer *SofaWare's Configuring Windows 2000/ XP IPSec to Site-to-Site VPN*.

Using IP30 Tele

You can configure IP30 Tele as a VPN client.

To enable the VPN client functionality in your IP30

- 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 IP30 in a standalone mode, add the license manually.

Adding VPN Sites by Using IP30 Tele

With IP30 Tele, you can define only remote access VPN sites. To define site-to-site VPN gateways, you must have IP30 Satellite.

VPN sites represent VPN gateways to which you can connect. You must define VPN sites before you connect to them.

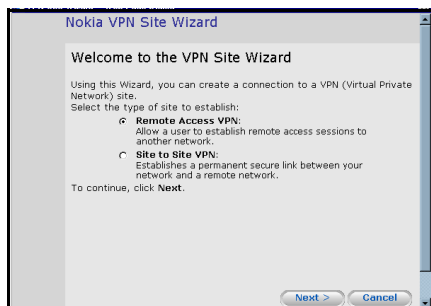
To add or edit VPN sites

1. In the Navigation Bar, click VPN.

The VPN Sites page appears, with a list of VPN sites.

2. Do either of the following:
 - a. To add a VPN site, click New Site.
 - b. To edit a VPN site, click Edit in the desired VPN site's row.

The Nokia VPN Site Wizard opens, as shown in the Figure below.

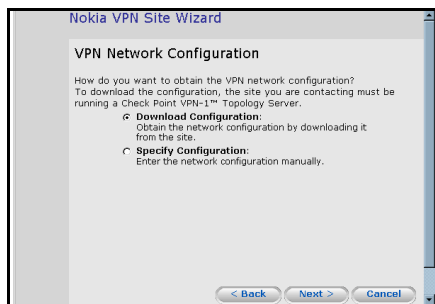


3. Click Next.

The VPN Gateway Address dialog box appears.

4. Enter the IP address of the VPN gateway to which you want to connect, as given by the network administrator.
5. Click Next.

The VPN Network Configuration dialog box appears.



6. Do 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.

Note

Downloading the network configuration is only possible if you are connecting to a Check Point VPN-1 or Nokia IP30 Satellite VPN Gateway.

Specify Configuration

7. If you chose Specify Configuration in the preceding procedure, a dialog box appears.

Nokia VPN Site Wizard

VPN Network Configuration

Enter the destination network address and subnet mask of the site gateway to which you want to connect:

#	Destination network:	Subnet mask:
1.	192.168.18.0	255.255.255.0
2.		
3.		

< Back Next > Cancel

8. Enter the destination network address and subnet mask of the site to which you want to connect.

Note

Obtain the destination network and subnet mask from the VPN gateway system administrator.

9. Click Next.

The VPN Login page appears.



10. In the VPN Login page,

- Choose Manual Login if you need to authenticate each time a VPN tunnel is created.
- Choose Automatic Login to authenticate using the specified Username and Password each time a VPN tunnel is created. If you choose Automatic Login, enter the Username and Password.

11. Click Next. The Contacting VPN Site screen appears.

Note

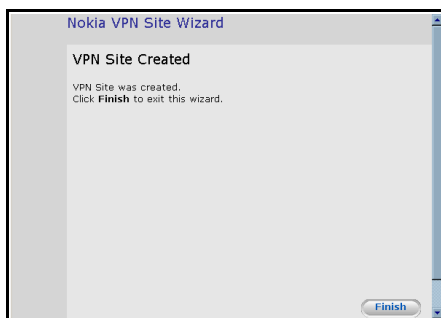
Automatic Login must be enabled by the management center. You can subscribe to this feature.

12. Click Next.

The Site Name dialog box appears.

13. Enter a name for the VPN site.

14. Click Next. The VPN Site Created screen appears.



15. Click Finish.

Download Configuration

If you chose Download Configuration in Adding VPN sites by using IP30 Tele, a dialog box appears.

- 1.** Click Next, the Network Topology will be downloaded from the specified VPN gateway.

The VPN Login page appears.

- 2.** Follow steps 9 to 13 in Specify Configuration.

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.

Adding VPN Sites by Using IP30 Satellite

You can define each VPN site according to the function you want IP30 Satellite to perform when connecting to the site:

VPN Client: Define the VPN site as a Remote Access VPN site using the procedure below.

VPN Gateway: Do the following:

- Define the second VPN site as a site-to-site VPN gateway by using the procedure below.
- Define the first VPN site as a site-to-site VPN gateway.

To add or edit VPN sites by using IP30 Satellite

1. In the Navigation Bar, click VPN.
The VPN Server page appears.
2. In the VPN submenu, click VPN Sites.
The VPN Sites page appears 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's row.

The IP30 VPN Site Wizard opens, with the Welcome to the VPN Site Wizard dialog box displayed.



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 bi-directional connection to another gateway.
5. Click Next.

The VPN Gateway Address dialog box appears.

6. Enter the IP address of the VPN gateway to which you want to connect, as given to you by the network administrator.
7. Click Next.

Configuring a Remote Access VPN Site

If you selected Remote Access VPN, the VPN Network Configuration dialog box appears.

1. 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

Downloading the network configuration is only possible if you are connecting to a Check Point VPN-1 or IP30 Satellite VPN gateway.

- To provide the network configuration manually, select Specify Configuration.
2. Click Next.

The following things happen in the order below:

- If you chose 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 masks from the VPN gateway system administrator.

- c. Click Next.
 - The VPN Login dialog box appears.



8. Do one of the following:
 - To configure the site for manual login, select Manual Login.
 - To enable the IP30 to log on to the VPN site automatically, do the following:
 - a. Select Automatic Login.
 - b. Enter a user name and password to be used for logging on to the VPN site.

Note

While Automatic Login provides all of the computers on your home network with constant access to the VPN site, Manual Login connects only the computer you are currently logged onto to the VPN site, and only when the appropriate user name and password are entered.

For further information on Automatic and Manual Login, see “Logging on to a VPN Site.”

The Connecting screen appears.

The Contacting VPN Site screen appears.

9. Click Next.

Continue at “Completing Site Creation.”

Configuring a Site to Site VPN Gateway

If you selected site-to-site VPN, the VPN Network Configuration dialog box appears.

To configure a site-to-site VPN gateway

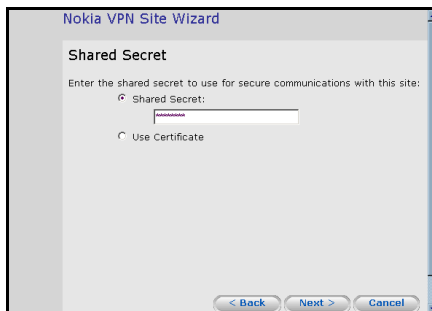
1. In the Destination network column, enter up to three destination network addresses at the VPN site to which you want to connect.
2. In the Subnet mask column, select the subnet masks for the destination network addresses.

Note

Obtain the destination networks and subnet masks from the VPN site's system administrator.

3. Click Next.

The Shared Secret dialog box appears.



4. Enter the shared secret to use for secure communications with the VPN site.

This shared secret is a string used to identify the VPN sites to each other. The secret can contain spaces and special characters.

5. Click Next.

You are ready to complete your VPN site. Continue at “Completing Site Creation.”

Completing Site Creation

Once you configure a VPN site, the Site Name dialog box appears.

To complete VPN site creation

1. Enter a name for the VPN site. You may choose any name.
2. Click Next.

The VPN Site Created screen appears.

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.

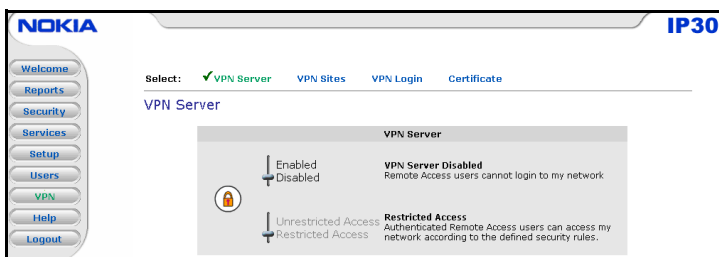
Setting Up IP30 Satellite as VPN Server

With IP30 Satellite, you can make your network remotely available to authorized users by setting up your IP30 as a VPN server.

To set up your IP30 as a VPN server

1. In the Navigation Bar, click VPN.

The VPN Server page appears.



2. Drag the On/Off lever to On.

The VPN server is enabled.

3. Follow the procedures in “Setting Up Remote VPN Access for Users.”

Deleting a VPN Site

You can delete a VPN site by using both IP30 Tele and IP30 Satellite.

To delete a VPN site

1. In the navigation bar, click VPN.

The VPN Server page appears.

2. Click VPN Sites.

The VPN Sites page appears with a list of VPN Sites.

3. In the desired VPN site row, click the Delete VPN icon.

A confirmation message appears.

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, 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 IP30 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.

Logging On Using IP30 GUI

To log on to a VPN site using IP30 GUI, do the following:

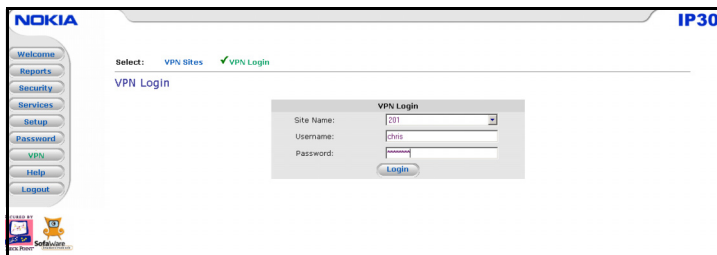
1. Click VPN.

The VPN Sites page appears, with a list of VPN sites.

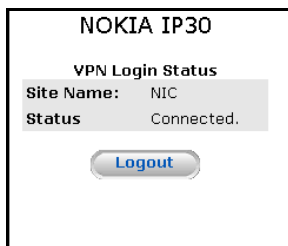
2. In the VPN submenu, click VPN Login.

The VPN Login page appears.

3. Select the site you want to log on.



4. Enter your username and password in the appropriate fields.
5. Click Connect.
 - If your IP30 is configured to automatically download the network configuration, the IP30 downloads the network configuration.
 - If when adding the VPN site, you specified a network configuration, the IP30 attempts to create a tunnel to the VPN site.
 - The VPN Login Status box appears. The Connecting screen appears. Once the IP30 has finished connecting, the Status field changes to Connected. The VPN Login Status box remains open until you log off of the VPN site.
 - Once the IP30 has finished connecting, the status changes to connected.



- The VPN Login Status box remains open until you log off the VPN site.

Logging 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 screen appears.



2. Select the site to which you want to log on.
3. Enter your user name and password in the appropriate fields.
4. Click Connect.
 - If the IP30 is configured to automatically download the network configuration, the IP30 downloads the network configuration.
 - If when adding the VPN site you specified a network configuration, the IP30 attempts to create a tunnel to the VPN site.
 - The VPN Login Status box appears. The Status field tracks the progress of the connection.
 - Once the IP30 has finished connecting, the Status field changes to Connected.
 - The VPN Login Status box remains open until you log off of the VPN site.

Logging Off a VPN Site

You need to manually log off of a VPN site if:

- you are using IP30 Tele.
- the VPN site is a remote access VPN site configured for manual login.

To log off a VPN site

1. In the VPN Login Status box, click Close.

All open tunnels from the IP30 to the VPN site are closed, and the VPN Login Status box closes.

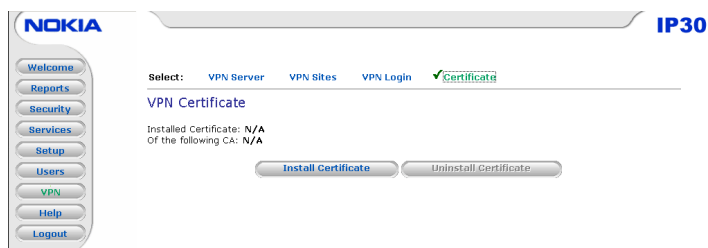
Note

Closing the browser or dismissing the VPN Login Status box also terminates the VPN session within a short time.

Using VPN Certificates

The VPN Certificates are used to authenticate a VPN connection established between Check Point SmartCenter FP3 and the dynamically configured IP30 using DAIP.

The manually created .p12 certificate can be uploaded on to the IP30 Satellite.



To upload VPN Certificates

- 1.** On the Navigation Bar, click VPN > Certificate.
The VPN Certificate screen appears.
- 2.** Click Install Certificate.
The Certificate Upload screen appears.
- 3.** Click Browse.
Select the .p12 certificate.
- 4.** Click Upload.
The screen prompts you to enter the Certificate Passphrase used when creating the .p12 certificate.
- 5.** Click OK.

5 Troubleshooting

If the IP30 does not function normally, refer Frequently Asked Questions, and perform the required tasks:

Frequently Asked Questions

I cannot access the Internet. What should I do?

Check for the following:

- Check if the PWR/SEC LED is active. If not, check the power connection to the IP30.
- Check if the WAN LINK/ACT LED is on. If not check the network cable to the modem and make sure the modem is turned on.
- Check if the LAN LINK/ACT LED for the port used by your computer is on. If not, check if the network cable linking your computer to the IP30 is connected properly.
- Using your web browser go to <http://my.firewall> and see whether “connected” appears on the status bar. Make sure that the IP30 network settings are configured as per 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 E-mail anti-virus 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. Refer Viewing Computers.

I cannot access `http://my.firewall` or `http://my.vpn`. What should I do?

- Verify that the IP30 is operating (PWR/SEC LED is active)
- Check if the LAN LINK/ACT LED for the port used by your computer is on. If not, check the network cable linking your computer and IP30 is connected properly.
- Try surfing to 192.168.10.1 instead of to my.firewall.

Note

192.168.10 is the default value, and it may vary if you changed it in the My Network page.

- Check your TCP/IP configuration according to Chapter 2.
- Restart the IP30 and your broadband modem by disconnecting the power and reconnecting after 5 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 IP30. 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 IP30. What should I do?

For Outlook Express, versions 5 and 6, do the following:

7. Open Outlook Express.
8. On the Tools menu, click Accounts, then click the Mail tab.
9. For each of the accounts configured in the mail window, do the following:
 - a. Click Properties, then click the Connection tab.
 - b. Clear the Always connect to this account using check box.
 - c. Click OK.
10. Click Close.
11. 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 may be faulty. For proper operation, the IP30 requires STP CAT5 (Shielded Twisted Pair Category 5) Ethernet cables. Make sure that this specification is printed on your cables.

- Your Ethernet card may be faulty or incorrectly configured. Try replacing your Ethernet card.

I cannot play a certain network game. What should I do?

- Turn the IP30 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 have 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 IP30 to factory defaults using the Reset button as detailed in “Resetting the IP30 to factory defaults.” Note that this will erase all your settings.

I purchased IP30 Tele or IP30 Satellite, but I only seem to have IP30 Firewall functionality. What should I do?

You have not installed your product key. See Installing Your Product Key.

I cannot connect to a VPN site using IP30 Satellite or IP30 Tele. What should I do?

Check whether there is a problem with your VPN client:

Do one of the following:

1. If you are using IP30 Tele, add the demo Check Point VPN site, using the procedure “Adding and Editing VPN Sites using IP30 Tele,” as follows:
 - a. In the VPN Gateway Address dialog box, enter 207.40.230.20 in the VPN Gateway field.
 - b. In the VPN Network Configuration dialog box, select Download Configuration.

2. If you are using IP Satellite, add the demo Check Point VPN site, using the procedure Adding and Editing VPN Sites using IP30 Tele, as follows:
 - a. In the Welcome to the VPN Site Wizard dialog box, select Remote Access VPN.
 - b. In the VPN Gateway Address dialog box, enter 207.40.230.20 in the VPN Gateway field.
 - c. In the VPN Network Configuration dialog box, select Download Configuration.
3. Log on to the demo site, using “vpndemo” as your username and password.
4. 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 using the button on the back of the IP30 unit.

I am using the IP30 with another DSL/Cable router, and I am having problems with some applications.

The IP30 performs Network Address Translation (NAT). It is possible to use the IP30 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 IP30.

To fix this problem, do ONE of the following. (The solutions are listed in order of preference.)

- Consider whether you really need the router. The IP30 can be used 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. Refer to the router's documentation for instructions on how to do this.

The following suggestions will work only if the router is connected to the WAN port of the IP30:

- If the router has a “DMZ Computer” option, set it to the IP30 external IP address.
- Set the router to direct all incoming connections to the external IP address of IP30.

Keep in mind that if you use the IP30 behind another NAT device, you may lose some of the advantages of the IP30, 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 using ipconfig

I cannot connect to the HTTPS server in the DMZ. What should I do?

Ensure that HTTPS access to the Device is disabled.

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 Box what should I do?

Do ONE of the following. (The solutions are listed in order of preference.):

- If Anti Virus scanning is on, try turning it off.
- If the anti virus is required then make sure that the CVP server and SMTP server in the Server page of SMC are correctly configured.

I cannot send HTTP traffic across the IP30. What do I do?

Do ONE of the following. (The solutions are listed in order of preference.):

- If Web Filtering scanning are on, try turning it off.

- If the URL filtering is required, then make sure the UFP server in the Server page of SMC is correctly configured.

I cannot connect to SmartCenter FP3 VPN site using IP30 Satellite or Satellite Plus when using Dynamic IP with certificate support (DAIP). What should I do?

- Check for the installed certificate VPN >Certificate.
- Check for the following error messages in Reports >Event Log:

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 using IP30 Satellite or Satellite Plus configured using VPN Communities. What should I do?

Check for the following error messages in Report >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 IP30 Satellite VPN site using IP30 Satellite or Satellite Plus. What should I do?

Check for the following error messages in Report->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 IP30 gateway

Viewing Firmware Status

The firmware is the software program embedded in the IP30.

You can view your current firmware version and additional details.

To view the firmware status

1. In the Navigation Bar click on Setup.

The Internet page appears.

2. Click the Firmware tab.

The Firmware page appears.

The Firmware page displays a table with the following information:

- Firmware Version - the current version of the firmware.
- Hardware Type - the type of the current IP30 hardware.
- Hardware Version - the current hardware version of the IP30.
- 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 IP30 to factory defaults

The IP30 allows you to reset its settings to factory defaults. When you reset the IP30, it reverts to the state it was originally in when you purchased it, and your firmware reverts to the version that shipped with the IP30.

You can reset to factory defaults using the GUI or by manually pressing the Reset button located at the back of the IP30.



Warning

This operation erases all your settings and password information. You will have to set a new password and reconfigure the IP30 for Internet connection.

To reset the IP30 to factory defaults using GUI

1. In the Navigation Bar click Setup.

The Internet page appears.

2. Click the Firmware tab.

The Firmware page appears.

3. Click Factory Settings.

A confirmation message appears.

4. Click OK.

The IP30 returns to its factory defaults - this process might take up 30-60 seconds to finish.

At the end of the process the gateway restarts automatically and the Gateway restart confirmation page appears.

5. Click OK.

The gateway is restarted and within one minute the IP30 Welcome page appears.

To reset the IP30 to factory defaults using Reset

1. Make sure the IP30 is powered on.
2. Using a sharp object, press the RESET button on the back of the IP30 steadily for a few seconds and then release it.
3. Allow the IP30 to boot-up until the system is ready (PWR/SEC LED flashes slowly or illuminates steadily in green light).



Warning

If you choose to reset the IP30 by disconnecting the power cable and then reconnecting it, be sure to leave the IP30 disconnected for at least three seconds, or the IP30 might not function properly until you reboot it as described below.

Rebooting the IP30

If the IP30 is not functioning properly, rebooting it will often solve the problem.

To reboot the IP30

1. In the Navigation Bar click Setup.

The Internet page appears.

2. Click the Firmware tab.

The Firmware page appears.

3. Click on Restart.

A confirmation message appears.

4. Click OK.

The IP30 is restarted (the PWR/SEC LED flashes quickly) and the following message appears.

The Login page appears.

Running Diagnostics

You can view technical information about IP30 hardware, firmware, license, network status, and subscription services.

This information is useful for troubleshooting. You can copy and paste it into the body of an email and send it to technical support.

To run diagnostics

1. In the Navigation Bar click Setup.

The Internet page appears.

2. Click the Firmware tab.

The Firmware page appears.

3. Click Diagnostics.

Technical information about the IP30 appears in a new window.

4. To refresh the contents of the window, click Refresh.

The contents are refreshed.

5. To close the window, click Close.



A Specifications

Technical Specifications

Table A-6 Specifications

Height 1.2 inches	Input AC Power - 9VAC
Width - 8.0 inches	Power Consumption - 13.5 W
Length - 4.8 inches	Power Supply - 100 VAC, 120 VAC or 230 VAC
Weight - 1.8 lbs	

Safety Precautions

Read the following safety instructions before attempting to install or operate the Nokia IP30. Read the installation and operation procedures provided in this User Guide. Failure to follow the instructions may result in damage to equipment and / or personal injuries.

- Before cleaning the IP30, unplug the power cord. Use only a soft cloth dampened with water for cleaning.

- 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.
- When installing the IP30, ensure that the vents are not blocked.
- Do not use the IP30 outdoors.
- Do not expose the IP30 to liquid or moisture.
- Do not expose the IP30 to extreme high or low temperatures.
- Do not drop, throw, or bend the IP30 since rough treatment could damage it.
- Do not use any accessories other than those approved by Nokia. Failure to do so may result in loss of performance, damage to the product, fire, electric shock or injury, and will void the warranty.
- Do not disassemble or open the IP30. Failure to comply will void the warranty.
- Do not route the cable in a walkway or in a location that will crimp the cables.

B Warranty

THE TERMS AND CONDITIONS SET FORTH ON THIS DOCUMENT CONSTITUTE THE ENTIRE AGREEMENT BETWEEN Nokia, Inc., A DELAWARE CORPORATION ("NOKIA"), AND CUSTOMER IN RESPECT OF THE NOKIA SOFTWARE INCLUDED IN THE PRODUCT PACKAGE, INCLUDING ANY DOCUMENTATION THERETO (the "SOFTWARE"). NOKIA WILL NOT BE BOUND BY ANY TERMS OF ANY PRIOR AGREEMENT OR UNDERSTANDING THAT ARE INCONSISTENT WITH THE TERMS HEREIN. THE SOFTWARE IS LICENSED ONLY ON THE CONDITION THAT THE CUSTOMER ACCEPTS THE TERMS OF THIS AGREEMENT. BY OPENING THE PACKAGE AND/OR BY MAKING USE OF THE ENCLOSED SOFTWARE YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT PLEASE IMMEDIATELY RETURN THE SOFTWARE IN THE PRODUCT PACKAGE TO THE PLACE YOU PURCHASED IT FOR FULL REFUND.

- 1. SOFTWARE LICENSE.** Unless Customer is an approved Managed Service Provider, Nokia grants to Customer a

personal, nonexclusive and nontransferable license to use the Software in object code form solely as embedded in equipment provided by Nokia. If Customer is an approved Managed Service Provider ("MSP"), Nokia grants a nonexclusive and non transferable license to demonstrate the Software to clients and prospective clients in order to market MSP's managed services and to use the Software to provide managed services provided that each copy of the Software is used solely on behalf of and for the benefit of a single client on the single piece of equipment provided by Nokia. An MSP may discontinue use of the Software on behalf of one client and use the Software to provide managed services to another single client.

Customer may make one (1) archival copy of the Software provided Customer affixes to such copy all copyright, confidentiality and proprietary notices that appear on the original. Customer shall not otherwise, in whole or in part, copy the Software or documentation; modify the Software or create derivative works thereof; reverse compile or reverse assemble all or any portion of the Software; rent, lease, distribute, sell, or use for time-sharing purposes, the Software; or use or allow the Software to be used for the direct benefit of any third party. Any fixes, updates or new releases of the Software, which may be made available to Customer, shall be deemed part of the "Software," subject to the restrictions and limitations contained in this license.

- 2. PROPRIETARY RIGHTS.** All right, title and interest in and to the Software and documentation, and any copies thereof provided by Nokia or which may be made by Customer, are and shall remain the exclusive property of Nokia or Nokia's licensors (Nokia and its licensors are collectively referred to as "Software Owners"). Each Software Owner shall have the right

to enforce this Agreement against the Customer as to such Software Owner's Software.

3. LIMITED WARRANTY.

- a. Software Warranty.** Nokia warrants that the Software will substantially conform to the published specifications for a period of ninety (90) days, plus a thirty (30) day transit allowance, from the date of shipment. If the Software is found to contain a substantial nonconformance, Nokia's sole obligation under this warranty shall be, at Nokia's option: (a) to correct, or provide a "work around" for any material programming error or defect in the Software, or (b) to refund to Licensee the purchase price paid and this Agreement shall terminate.
- b. Warranty Services.** In the event of a warranted problem with respect to the Software, Customer shall call its reseller for warranty services. All repair services are provided by Nokia's authorized reseller from whom the Customer has purchased the product on which the Software is imbedded.
- c. Exclusions.** The above warranty does not apply if the Software or the equipment on which it resides (1) has been altered, except as authorized by Nokia, (2) has not been installed, operated, repaired or maintained in accordance with any installation, handling, maintenance or operating instructions supplied by Nokia, (3) has been subjected to unusual physical or electrical stress, misuse, negligence or accident, (4) has been used in ultra-hazardous activities, or (5) has been used in such a way that Nokia cannot reasonably reproduce the Software error. Furthermore, the above warranty does not apply to any portion of the product supplied by a third party. In no event does Nokia warrant that the Software is error-free or that the Customer

will be able to operate it without problems or service interruptions.

d. DISCLAIMER. THE WARRANTY ABOVE IS IN LIEU OF, AND NOKIA DISCLAIMS, ALL OTHER WARRANTIES AND CONDITIONS, EXPRESSED OR IMPLIED, INCLUDING THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUALITY, NON-INFRINGEMENT, NON-INTERRUPTION OF USE, FREEDOM FROM BUGS OR OTHERWISE. NO DEALER OR RESELLER IS AUTHORIZED TO MAKE ANY MODIFICATIONS, EXTENSIONS, OR ADDITIONS TO THIS WARRANTY. NOKIA SPECIFICALLY DISCLAIMS ANY WARRANTY FOR THIRD PARTY SOFTWARE SUPPLIED WITH THE PRODUCT.

4. LIMITATION OF LIABILITY. IN NO EVENT WILL NOKIA, ITS SUPPLIERS OR RESELLERS BE LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY, TORT OR OTHER THEORY FOR DIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF PROFIT OR DATA), WHETHER OR NOT THEY BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS. IN THE EVENT THAT ANY EXCLUSION CONTAINED HEREIN SHALL BEHELD TO BE INVALID FOR ANY REASON AND NOKIA BECOMES LIABLE FOR LOSS OR DAMAGE THAT MAY LAWFULLY BE LIMITED, SUCH LIABILITY SHALL BE LIMITED TO THE PURCHASE PRICE. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF CERTAIN LIABILITIES OR DAMAGES,

SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO CUSTOMER BY LAW.

5. **EXPORT RESTRICTIONS.** Customer shall not export or transmit, directly or indirectly, the Software or any technical data (including processes and services) received from Nokia, nor the direct product thereof, outside of the United States without prior authorization of the U.S. Government if such authorization is required. Customer shall obtain all licenses, permits and approvals required by any government. Customer agrees to comply with all export laws, rules, policies, procedures, restrictions and regulations of the Department of Commerce or other United States or foreign agency or authority, and not to export, or allow the export or reexport of any goods in violation of any such restrictions, laws or regulations. Customer will indemnify and hold harmless Nokia for any violation or alleged violation by Customer of such laws, rules, policies, procedures, restrictions or regulations.
6. **CONFIDENTIAL INFORMATION.** Customer agrees that aspects of the Software and documentation, including the specific design and structure of individual programs and the composition of the whole, constitute trade secrets and/or copyrighted material of Nokia. Customer shall not itself, nor shall Customer permit others to, disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior consent of Nokia. Customer agrees to implement reasonable security measures to protect such trade secrets and copyrighted material. The obligations of confidentiality shall not apply to information, which has entered the public domain except where such entry is the result of Customer's breach of this Agreement.

- 7. FORCE MAJEURE.** Nokia shall not be liable for any delay or failure in performance whatsoever due to reasons beyond its reasonable control.
- 8. TERM AND TERMINATION.** This Agreement is effective until terminated. The license to the Software granted by Nokia will terminate upon any attempt by Customer to transfer or assign the Software, this Agreement or any rights or obligations hereunder without Nokia's prior written consent. In addition, Nokia may terminate this Agreement effective fifteen (15) days following the giving of written notice to Customer upon the occurrence of Customer's failure to perform any of its existing or future obligations hereunder if such breach shall remain uncured. Upon termination, Customer shall cease all use of the Software and shall destroy or return to Nokia the original(s) and all copies of the Software and documentation made or furnished hereunder. Customer may terminate the License at any time by destroying all copies of the Software and documentation. The provisions of Sections 2, 4, 6, 9, and 10 shall survive any termination.
- 9. APPLICABLE LAW.** This Agreement shall be governed by and construed in accordance with the laws of the State of California and the United States without regard to conflicts of laws provisions thereof and without regard to the United Nations Convention on Contracts for the International Sale of Goods. To the extent permitted by law, the parties waive any and all rights, privileges and obligations which may derive from any codification of the body of law generally referred to as the "Uniform Commercial Code".
- 10. MISCELLANEOUS.** No waiver of rights under this Agreement by either party shall constitute a subsequent waiver of this or any other right under this Agreement. In the event that any of the terms of this Agreement become or are declared to be illegal by any Court of competent jurisdiction, such term(s) shall be null and void and shall be deemed deleted from

this Agreement. All remaining terms of this Agreement shall remain in full force and effect. In the event of a breach of this Agreement, the breaching party shall pay to the other party any reasonable attorneys' fees and other costs and expenses incurred by the non-breaching party in connection with the enforcement of any provisions of this Agreement.

If the Software is licensed to a U.S. Governmental user, the following shall apply. The Software and documentation licensed in this agreement are "commercial items" and are deemed to be "commercial computer software" and "commercial computer software documentation." Consistent with the Federal Acquisition Guidelines and related laws, any use modification, reproduction, release, performance, display, or disclosure of such commercial software or commercial software documentation by the US. Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

C End User License Agreement

This EndUser License Agreement (the "Agreement") is an agreement between you (both the individual installing the Product and any legal entity on whose behalf such individual is acting) (hereinafter "You" or " Your") and SofaWare Technologies Ltd. (hereinafter " SofaWare ").

TAKING ANY STEP TO SET-UP OR INSTALL THE PRODUCT CONSTITUTES YOUR ASSENT TO AND ACCEPTANCE OF THIS END USER LICENSE AGREEMENT. WRITTEN APPROVAL IS NOT A PREREQUISITE TO THE VALIDITY OR ENFORCEABILITY OF THIS AGREEMENT AND NO SOLICITATION OF ANY SUCH WRITTEN APPROVAL BY OR ON BEHALF OF YOU SHALL BE CONSTRUED AS AN INFERENCE TO THE CONTRARY. IF YOU HAVE ORDERED THIS PRODUCT AND SUCH ORDER IS CONSIDERED AN OFFER BY YOU, SOFAWARE'S ACCEPTANCE OF YOUR OFFER IS EXPRESSLY CONDITIONAL ON YOUR ASSENT TO THE TERMS OF THIS AGREEMENT, TO THE EXCLUSION OF ALL OTHER TERMS. IF THESE TERMS ARE CONSIDERED AN OFFER BY SOFAWARE, YOUR ACCEPTANCE IS EXPRESSLY LIMITED TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH ALL THE TERMS OF THIS

AGREEMENT, YOU MUST RETURN THIS PRODUCT WITH THE ORIGINAL PACKAGE AND THE PROOF OF PAYMENT TO THE PLACE YOU OBTAINED IT FOR A FULL REFUND.

1. DEFINITIONS:

1.1 "Product" means the object code copy of the software program provided to You in connection with this Agreement, together with the associated original electronic media and/or associated hardware devices and all accompanying manuals and other documentation, and together with all enhancements, upgrades, and extensions thereto that may be provided by SofaWare to You from time to time, unless otherwise indicated by SofaWare. If You are a Standard User the Product shall be associated with the SofaWare S-box obtained by you, if you are a Managed Service Provider the Product shall be an object code copy that allows the management of SofaWare S-box Licensed Configurations for a defined amount of Service Customers.

1.2 "Licensed Configuration" means to the extent applicable, as indicated on the License Key, the choice of features and the maximum number of nodes (an internal computing device with an IP address) on the trusted side of the firewall or any other hardware or software specifications, as declared by You in Your purchase order, or request for License Key, if the Product purchased by You does not come with a License Key then the Licensed Configuration shall be the minimum configuration allowed by the user manual of SofaWare S-Box, and upon which the licensing fee was based.

1.3 "License Key" means the code provided to You by SofaWare which enables the Product to operate for the specified Licensed Configuration.

1.4 "Third Party Software" means any software programs provided by third parties contained in the Product as detailed in the Third Party Software Addendum attached to this Agreement.

1.5 "Third Party Software Provider" means the third party which has the right to provide and grant licenses for the use of Third Party Software.

1.6 You are a "Managed Service Provider" if (a) You are in the regular business of providing firewall, VPN, or IP addressing management for a fee to entities that are not Your affiliates ("Service Customers"); or if you are a Company that provides such managed services to Standard Users that are a part of your corporation or of your affiliated companies ("Clients"); (b) You indicated in Your purchase order or in requesting the License Key that You intend to use the Products on behalf of Service Customers or Clients; and (c) you purchased the managed service provider package.

1.7 You are a "Standard User" if You indicated in Your purchase order or in requesting the License Key that You intend to use the Products on Your own behalf, or you obtained the products from a Managed Service Provider, reseller, vendor or any other intermediate supplier.

2. LICENSE AND RESTRICTIONS:

2.1 License. Subject to the terms and conditions of this Agreement, SofaWare hereby grants only to You, a non-exclusive, non-sublicensable, non-transferable license to install and use the Product in accordance with the relevant end user documentation provided by SofaWare for the Licensed Configuration. You have no right to receive, use or examine any source code or design documentation relating to the Product.

2.2 Standard User Restrictions. If You are a Standard User, the Products are licensed to You solely for use by You for Your own operations. No Product, nor any portion thereof, may be used by or on behalf of, accessed by, re-sold to, rented to, or distributed to any other party.

2.3 Managed Service Provider Restrictions. If You are a Managed Service Provider, the Products are licensed to You for use by You to provide policy management for the operations of Your Service Customers or Clients from an authorized location. No Product, nor any portion thereof, may be used by or on behalf of, accessed by, re-sold to, rented to, or distributed to any other party, except for the

management of Your Clients or Service Customers who have made a valid purchase of the Product. Distribution of the Product to Service Customers requires that You enter into a Reseller and/or Managed Service Agreement with SofaWare or its authorized representative.

2.4 General Restrictions. You may not copy the Product, in whole or in part. The Product is licensed to You solely for your internal use by You and for You and the Product or any portion thereof may not be used or accessed by, sub-licensed to, re-sold to, rented to, or distributed to any other party. You agree not to allow others to use the Product and You will not use the Product for the benefit of third parties. You acknowledge that the source code of the Product, and the underlying ideas or concepts, are valuable intellectual property of SofaWare and You agree not to, except as expressly authorized and only to the extent established by applicable statutory law, attempt to (or permit others to) decipher, reverse translate, decompile, disassemble or otherwise reverse engineer or attempt to reconstruct or discover any source code or underlying ideas or algorithms or file formats or programming or interoperability interfaces of the Products by any means whatsoever. You will not develop methods to enable unauthorized parties to use the Product, or to develop any other product containing any of the concepts and ideas contained in the Product. You will not (and will not allow any third party to) modify Product or incorporate any portion of Product into any other software or create a derivative work of any portion of the Product. You will not (and will not allow any third party to) remove any copyright or other proprietary notices from the Product.

2.5 Specific Restrictions. The Product is licensed to You based on the applicable Licensed Configuration purchased. The License permits the use of the Product in accordance with the designated number of IP addresses. Without derogation from any applicable laws, it is a violation of this End User License Agreement to create, set-up or design any hardware, software or system which alters the number of readable IP addresses presented to the Product with the

intent, or resulting effect, of circumventing the Licensed Configuration.

2.6 Evaluation License. This Section 2.6 shall only apply if You are licensing the Product for an initial sixty (60) day evaluation period. The license is valid only for a period of sixty (60) days from the delivery of the Product, and is designed to allow You to evaluate the Product during such period. In the event that You wish to enter into a longer-term license agreement with SofaWare, the terms and conditions of this Agreement shall be applicable. In the event that You determine not to enter into a licensing transaction with SofaWare at the end of such sixty (60) day evaluation period, or in the event that SofaWare advises You that discussions with respect to a licensing transaction have terminated, then Your rights under this Agreement shall terminate and You shall promptly return all Product to the representative that supplied the Product.

3. MAINTENANCE AND SUPPORT:

SofaWare has no obligation to provide support, maintenance, upgrades, modifications, or new releases under this Agreement. Any purchase of upgrades shall be subject to this End User License Agreement, unless otherwise determined by SofaWare.

4. TITLE AND INTELLECTUAL PROPERTY:

All right, title, and interest in and to the Product shall remain with SofaWare and its licensors. The Product is protected under international copyright, trademark and trade secret and patent laws. The license granted herein does not constitute a sale of the Product or any portion or copy of it.

5. TERM AND TERMINATION:

This Agreement is effective until terminated. SofaWare may terminate this Agreement at any time upon Your breach of any of the provisions hereof. Upon termination of this Agreement, You agree to cease all use of the Product and to return to SofaWare or destroy the Product and all documentation and related materials in your possession, and so certify to SofaWare. Except for the license

granted herein and as expressly provided herein, the terms of this Agreement shall survive termination.

6. INDEMNIFICATION:

SofaWare shall have the right, but not the obligation, to defend or settle, at its option, any action at law against You arising from a claim that Your permitted use of the Product under this Agreement infringes any patent, copyright, or other ownership rights of a third party. You agree to provide SofaWare with written notice of any such claim within ten (10) days of Your notice thereof and provide reasonable assistance in its defense. SofaWare has sole discretion and control over such defense and all negotiations for a settlement or compromise, unless it declines to defend or settle, in which case You are free to pursue any alternative You may have.

**7. LIMITED WARRANTY, WARRANTY DISCLAIMERS
AND LIMITATION OF LIABILITY:**

7.1 Limited Warranty. SofaWare warrants to You that the encoding of the software program on the media on which the Product is furnished will be free from defects in material and workmanship, and that the Product shall substantially conform to its user manual, as it exists at the date of delivery as can be found on SofaWare's web page (www.sofaware.com or www.s-box.com), for a period of ninety (90) days from the date of purchase. SofaWare's entire liability and Your exclusive remedy shall be, at SofaWare's option, either: (i) return of the price paid to SofaWare for the Product, resulting in the termination of this Agreement, or (ii) repair or replacement of the Product or media that does not meet this limited warranty. **EXCEPT FOR THE LIMITED WARRANTIES SET FORTH IN THIS SECTION 7.1, THE PRODUCT AND ANY SERVICES ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. SOFAWARE DOES NOT WARRANT THAT THE PRODUCT WILL MEET YOUR REQUIREMENTS OR THAT ITS OPERATION WILL BE UNINTERRUPTED OR ERROR FREE. SOFAWARE**

DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, so the above limitations may not apply to You. This warranty gives You specific legal rights. You may have other rights which vary from jurisdiction to jurisdiction.

7.2 Limitation of Liability. EXCEPT FOR PERSONAL INJURY, IN NO EVENT WILL SOFAWARE BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DAMAGES ARISING OUT OF THE SUBJECT MATTER OF THIS AGREEMENT, THE PRODUCT OR ANY SERVICES UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY, FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS), OR FOR LOSS OF OR CORRUPTION OF DATA), OR FOR COST OF PROCUREMENT OF SUBSTITUTE GOODS OR TECHNOLOGY, IRRESPECTIVE OF WHETHER SOFAWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOFAWARE'S MAXIMUM LIABILITY FOR DAMAGES SHALL BE LIMITED TO THE LICENSE FEES RECEIVED BY SOFAWARE UNDER THIS LICENSE FOR THE PARTICULAR PRODUCT(S) WHICH CAUSED THE DAMAGES. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

8. GOVERNMENT REGULATION AND EXPORT CONTROL

8.1 Government Regulations. You agree that the Product will not be shipped, transferred, or exported into any country or used in any manner prohibited by law.

8.2 Export. The Product is subject to export control laws of the State of Israel and/or may be subject to additional export control laws applicable to You or in Your jurisdiction, including, without limitation, the United States. If the Product contains any

encryption device You must contact SofaWare's export regulation information page (www.sofaware.com or www.s-box.com) for specific information. You agree that You will not ship, transfer, or export the Product into any country, or make available or use the Product in any manner, prohibited by law.

8.3 You understand and acknowledge that upon entry of the Product into the United States it becomes subject to regulation by agencies of the U.S. government, including the U.S. Department of Commerce, which prohibit export or diversion of certain products and technology to certain countries. Any and all of Your obligations with respect to the Product shall be subject in all respects to such United States laws and regulations as shall from time to time govern the license and delivery of technology and products abroad by persons subject to the jurisdiction of the United States, including the Export Administration Act of 1979, as amended, any successor legislation, and the Export Administration Regulations ("EAR") issued by the Department of Commerce, International Trade Administration, and Bureau of Export Administration. You warrant that You will comply in all respects with the export and reexport restrictions applicable to the Product and will otherwise comply with the EAR or other United States laws and regulations in effect from time to time.

8.4 You warrant and agree that You are not: (i) located in, under the control of, or a national or resident of Cuba, Iraq, Libya, North Korea, Iran, Syria, Sudan or Yugoslavia, or (ii) on the U.S Treasury Department list of Specially Designated Nationals or the U.S. Commerce Department's Table of Deny Orders.

9. GENERAL:

9.1 Miscellaneous. You may not assign your rights or obligations under this Agreement without the prior written consent of SofaWare. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, that provision of the Agreement will be enforced to the maximum extent permissible so as to effect the intent of the Agreement, and

the remainder of the provisions of this Agreement shall remain in full force and effect. The laws of the State of Israel shall govern all issues arising under or relating to this Agreement, without giving effect to the conflict of laws principles thereof. All disputes arising under or relating to this Agreement shall be resolved exclusively in the appropriate Israeli court sitting in Tel Aviv, Israel. This Agreement will not be governed by the United Nations Convention on Contracts for the International Sales of Goods, the application of which is expressly excluded. This Agreement sets forth the entire understanding and agreement between You and SofaWare and may be amended only in writing signed by both parties.

9.2 Third Party Software. Certain Third Parties Software may be provided with the Product for use in connection with the Product subject to the licenses of their respective proprietors. The Third Parties Software may be used only in connection with the Products. The provisions of this Agreement shall apply to all Third Party Software Providers and to Third Party Software as if they were the Product and SofaWare, respectively.

9.3 Government Restricted Rights. This provision applies to Product acquired directly or indirectly by or on behalf of any Government. The Product is a commercial product, licensed on the open market at market prices, and was developed entirely at private expense and without the use of any U.S. Government funds. Any use modification, reproduction, release, performance, display, or disclosure of the Product by any Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement, and no license to the Product is granted to any government requiring different terms.

9.4 Questions? Should You have any questions concerning this Agreement contact the manufacturer at SofaWare Technologies Ltd., 3 Hilazon St., Ramat-Gan, Israel 52522.

D Compliance Information

Declaration of Conformity

according to ISO/IEC Guide 22 and EN 45104

Manufacturer's name: Nokia Corporation
Manufacturer's address: 313 Fairchild Drive
Mountain View, CA 94043- 2215
USA

declares that the product:

Product name: IP0530
Model number: IP530
Product options: All
Serial number: 1 to 100,000
Date first applied: 2000

conforms to the following standards:

Safety: EN60950:1992, A1,A2:1993,
A3:1995, A4:1997, A11:1998

with Japanese National Deviations

EMC: EN50024, EN55022A 1998, CISPR
22 Class A 1985, EN61000-3-2,
EN61000-3-3

Supplementary information:

“The product complies with the requirements of the **Low Voltage Directive 73/23/EEC** and the **EMC Directive 89/336/EEC**.”

NOKIA

Alan Hutchinson
Quality Engineer
Mountain View, California
USA

European contact: Greg Shortell
Nokia Telecommunications
2 Heathrow Blvd, 284 Bath Road
Heathrow, Middlesex UB7 ODQ
England

Compliance Statement

This hardware complies with the following standards:

Emissions

FCC Part 15, Subpart B, Class A	US and Canada
EN55022A: (CISPR 22, Class A)	European Community (CE)
EN6100-3-2	European Community (CE)
EN6100-3-3	European Community (CE)

Immunity

EN50024:	European Community (CE)
EN61000-4-2	
EN61000-4-3	
EN61000-4-4	
EN61000-4-5	
EN61000-4-6	
EN61000-4-8	
EN61000-4-11	
ENV50204	

Safety

UL1950	US
CAN/CSA 22.2, No. 950-M95	Canada
EN60950	European Community (CE,
TUV)	
EN60950	Japan
(with Japanese National Deviations)	

Telecom

T1	FCC Part 68, CS-03
V.35/X.21	I-CTR 2
ISDN	I-CTR 3

FCC Notice (US)

This device has been tested and found to comply with the limits for a Class A 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

Caution: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

Index

A

- Adding VPN Sites Using IP30 Tele 105
- Advanced Setup, Using 35
- Anti virus, Snoozing 78
- Automatic DHCP, Using 35

B

- Blocking Categories 75

C

- Canceling, Subscription Services 73
- Changing IP Addresses 52
- Changing Your Password 83
- Compliance Specifications 152
- compliance standards
 - emission 153
 - safety 153
- Configuration, Download 109
- Configuration, Specify 107
- configure HTTPS 54
- Configure, Network Settings 51
- Configuring Your Account 81
- Configuring, Nokia Horizon Manager 82
- Configuring, Remote Access VPN Site 111
- Configuring, Site to Site VPN Gateway 114

- Configuring, Virtual Servers 63
- Connection Settings, Cable 31
- Connection Settings, DSL 32
- Connection, Cable 38
- Connection, LAN 37
- Connection, xDSL PPPoE 39
- Connection, xDSL PPTP 40
- Connectivity 15
- Creating Rules 65
- Creating, Allow and Block Rules 65

D

- Diagnostics 129
- DMZ 68

E

- E-mail Anti Virus 77
- E-mail Anti Virus, Enabling 77
- emissions 152
- Enabling NAT 53
- Enabling, DHCP Server 51

F

- FCC Notice 153
- Frequently Asked Questions 121

I

- immunity 152
- Installing Your Network 26
- IP30 GUI 48
- IP30 Satellite in NAT and No-NAT Modes 102
- IP30 Satellite to Check Point FP3 100

IP30 Satellite to Check Point SmartCenter FP3 101
IP30 Satellite to Windows 2000 104
IP30 Tele to Check Point FP3 95
IP30 Tele to Check Point v4.1/ NG/ FP1/ FP2 95
IP30 Tele, Using 105
IP30, Configuring for Internet Connection 27
IP30, Connecting to Network 26
IP30, Front Panel 18
IP30, Logging Off 49
IP30, Logging On 45
IP30, Rear Panel 17
IP30, Rebooting 128
IP30, Remote Access 54
IP30, secure accessing 46
IP30, Setting up the Security Policy 62

L

Logging Off of a VPN Site 120
Logging On Through my.vpn 119
Logging on to a VPN Site 117
Logging On Using IP30 GUI 117

M

Mac Cloning 32
Management 16
Managing Your Network 49
Millennium 22

N

Network Requirements 17
Nokia Horizon Manager 82
Nokia IP30, About 13

- Nokia IP30, Features 15
- Nokia IP30, Firewall 14
- Nokia IP30, Satellite 14
- Nokia IP30, Satellite Plus 15
- Nokia IP30, Tele 14

P

- Package Contents 17
- Password, Administrator 28
- PPPoE, Using 33
- PPTP, Using 34
- Precautions, safety 131
- Product Key, Installing 42

Q

- Quick Internet Connection 50

R

- Reset to factory defaults 127

S

- safety 153
- Satellite to Satellite 97
- Satellite to VPN-1 98
- Scanning, Protocols 78
- SecuRemote to Satellite 92
- Security 15
- Security Services 16
- Setting the Firewall Security Level 62
- Setting Up IP30 Satellite as VPN Server 115
- Setup Wizard 29
- Software Updates 80

- Specifications 131
- specifications
 - compliance 152
 - emissions 152
 - safety 153
- Specifications, Technical 131
- Static Routes 41
- Subscription Services, Using 69

T

- TCP/IP Installation 22
- TCP/IP Settings 23
- TCP/IP, Installation 22
- TCP/IP, installation 24
- TCP/IP, Settings 23
- TCP/IP, settings 25
- Tele to Satellite 94
- Troubleshooting 121

U

- Updates, Automatic and Manual 80
- Users, Adding 85
- Users, Deleting 87
- Users, Managing 83
- Users, Remote VPN Access 88
- Users, Viewing and Editing 85

V

- Viewing, Active Computers 57
- Viewing, Active Connections 58
- Viewing, Event Log 55
- Viewing, Firmware Status 126

- Viewing, Network Activity Information 49
- Viewing, Reports 55
- Viewing, Services Information 73
- Viewing, VPN Tunnels 59
- VPN 16
- VPN Configuration 89

W

- Web Filtering 74
- Web Filtering, Enabling 74
- Web Filtering, Snoozing 75
- Windows 98 22
- Windows, 2000 24
- Windows, XP 24