



CBT Introduction

NetScreen Training Reference CBT is to be used as a entry level training guide for NetScreen's Value Added Resellers. It is not intended by any means to replace Authorized NetScreen instructor-led courses.

THE AUDIENCE FOR THIS CLASS

This material is for you if:

- You are a NetScreen Value Added Reseller.

NETSCREEN VAR TEST

When you complete this material, you may choose to complete the online NetScreen VAR Test. Please contact NetScreen to organize this testing.

TIME AND RESOURCES REQUIRED TO COMPLETE THIS MATERIAL

This material will take about 15-30 hours to complete depending on your networking, security technologies and NetScreen product experience.

Resources need to complete this material:

- Portions of this material will require the use of NetScreen devices in a lab environment
- Internetworking reference material.

PREREQUISITES FOR THIS MATERIAL

Before begining this material you should be familiar with basic internetworking technologies and terminologies such as:

- TCP/IP
- Routers, Bridges and Switches
- “The Internet”
- Web Browsers
- Terminal Software

NETSCREEN TRAINING MATERIAL MODULES

“NetScreen 5 Hardware and Software Description”

This chapter provides illustrations and descriptions of the NetScreen-5 front and back panel and an introduction to the Web User Interface (WebUI).

“Basic NetScreen-5 Network Connection”

Follow the instructions in this chapter to set up the NetScreen-5 hardware and to configure the software initially for Transparent or Network Address Translation (NAT) mode.

“NetScreen 10 & 100 Hardware and Software Description”

This chapter provides illustrations and descriptions of the NetScreen-10/100 front and back panels and an introduction to the Web user interface (WebUI).

“Connecting the NetScreen10 & 100 to the Network”

Follow the instructions in this chapter to set up the NetScreen-10/100 hardware and to configure the software for the first time.

“Configuring the NetScreen 10 & 100 for the First Time”

This chapter shows you how to configure your NetScreen-10/100 in Transparent mode and allow internal users to access the Internet while denying internal access from the Internet.

“Interfaces and Operational Modes”

This chapter describes the various physical, logical, and virtual interfaces and the three operational modes supported by NetScreen devices. The chapter is organized into the following sections:

- Interfaces
- Transparent Mode
- Network Address Translation
- Route Mode

“System Parameters”

This chapter focusses on the concepts involved in establishing system parameters affecting the following areas of a NetScreen security appliance:

- Firewall Protection
- Route Table Configuration
- DNS Support
- DHCP
- PPPoE
- URL Filtering
- Managing ScreenOS

“Administration”

This chapter describes various management methods and tools, ways to secure administrative traffic, and the administrative privilege levels that you can assign to admin users:

- Management Methods and Tools
- Levels of Administration
- Securing Administrative Traffic

“Building Blocks for Access Policies and VPNs”

This chapter discusses the concepts common to Access Policies and Virtual Private Networks (VPNs). The specific topics discussed are:

- Levels of Administration
- Address Book Entries
- VIPS (Virtual IP)
- MIPs (Mapped IP)
- Users
- Dialup User Groups
- Services
- Service Groups
- Schedules

“Access Policies”

This chapter describes what Access Policies do and how the various elements that comprise an Access Policy are related. It is divided into the following two main sections:

- Defined Access Policies
- Applied Access Policies

COPYRIGHT NETSCREEN TECHNOLOGIES INC. - VERSION 1.0

NetScreen 5 Hardware and Software Description

2

This chapter provides illustrations and descriptions of the NetScreen-5 front and back panel and an introduction to the Web User Interface (WebUI).

Before you install the NetScreen® device, you should unpack it on site and verify the contents against the packing slip.

HARDWARE DESCRIPTION

Figure 2-1 shows a front view of the NetScreen-5.

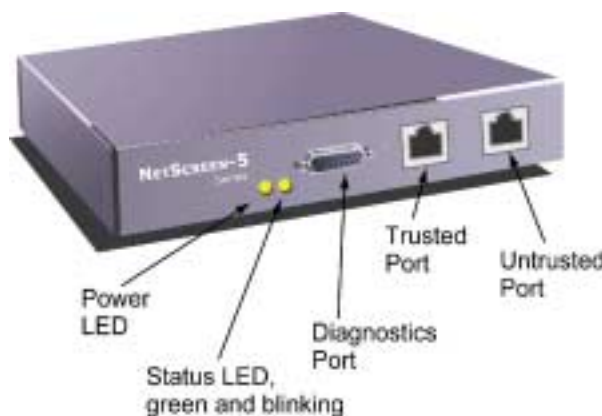


Figure 2-1 Front Panel of the NetScreen-5

The front panel of the NetScreen-5 contains the following features:

- **Power LED:** glows solid green when power is supplied to the NetScreen-5.
- **Status LED:** glows solid green when NetScreen-5 is first powered up and the unit first performs diagnostics. Then the unit goes into a startup phase, which takes up to one minute to complete. During startup, the LED blinks orange, after which the LED blinks green. If an error is detected, then the LED illuminates red.
- **Diagnostics Port:** DB9 serial port connector for local diagnostics.

- **Trusted Port:** Connect the NetScreen-5 to the LAN using a twisted pair cable with RJ45 connectors.
- **Untrusted Port:** Connect the NetScreen-5 to the router using a twisted pair cable with RJ45 connectors.
- **Trusted and Untrusted Ethernet LEDs:** Each Ethernet port has two link lights or LEDs, as shown in Figure 2-2. If the right LED is glowing, the link is connected to an active device. If the left LED is blinking, there is network traffic activity.
- **Power Outlet:** Use the universal power supply included with your NetScreen-5 unit to connect to the power outlet. The NetScreen-5 unit is powered when connected. The power specifications are as follows:

Input: 85–264 VAC

Output: 5 VDC @ 1.5 amps

DC Jack: 2.5 mm x 5.5 mm x 11 mm; polarity is center positive

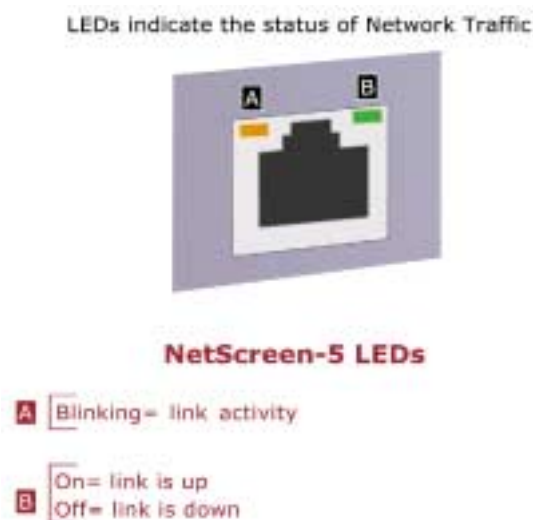


Figure 2-2 The NetScreen-5 Ethernet LEDs

Figure 2-3 on page 2-9 shows the back view of the NetScreen-5.

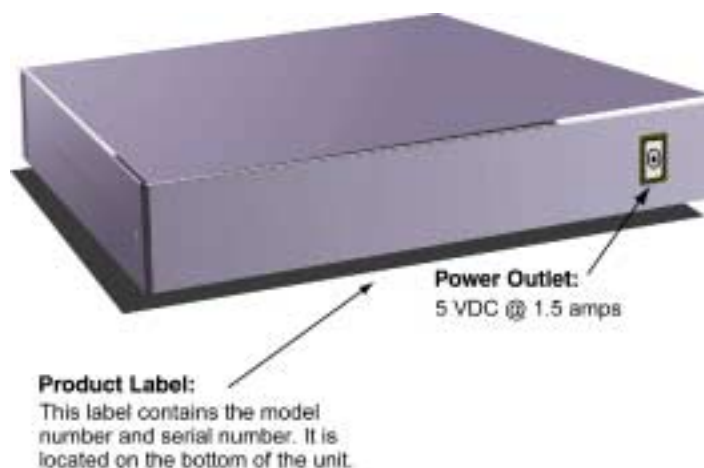


Figure 2-3 Back Panel of the NetScreen-5

GENERAL LAYOUT OF THE NETSCREEN-5 WEB UI

The Web UI Administration Tools page consists of two main logical sections:

- Figure 2-4 on page 2-10 shows the NetScreen-5 menu column and explains the features found under each button. The menu column consists of four functional categories: System, Network, Lists, and Monitor, each of which contain further sub-functions, represented by tabs in the central display area. During the configuration process, you first need to select a main functional category before choosing the various utilities offered within each sub-category.

**Figure 2-4** The NetScreen-5 Menu Column

- A *central display area*, shown in Figure 2-5, lists the information for each of the categories in the menu column, in either a tabular or graphical format. These pages generally contain links to dialog boxes through action links such as **Apply**, **OK**, **New Entry**, **Download Configuration**, **Edit**, **Remove**.

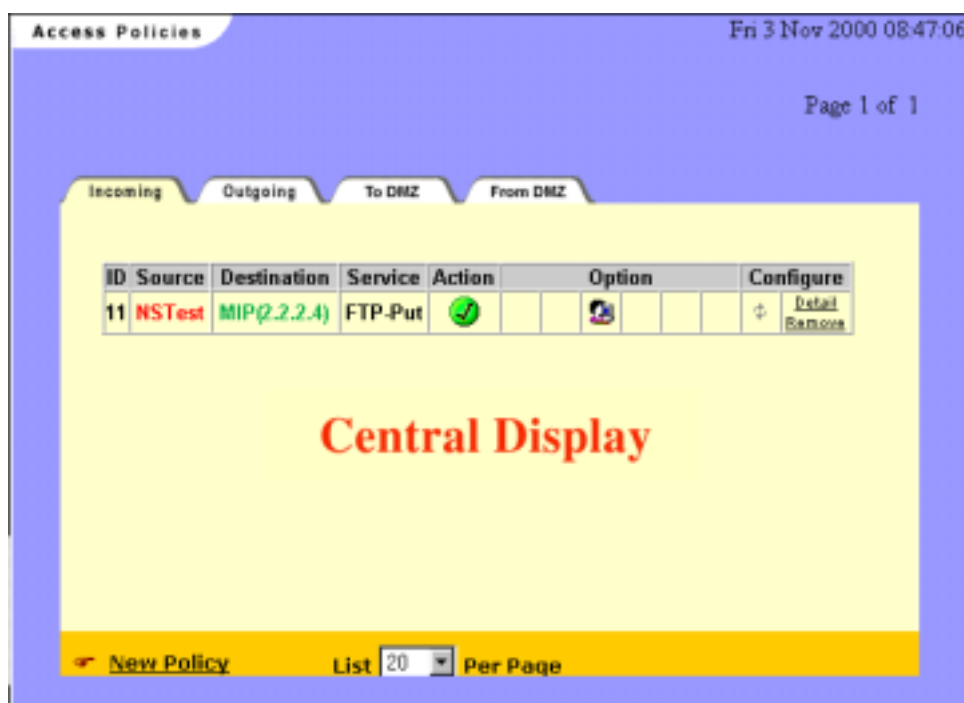


Figure 2-5 The NetScreen-5 Central Display

Basic NetScreen-5 Network Connection

3

Follow the instructions in this chapter to set up the NetScreen-5 hardware and to configure the software initially for Transparent or Network Address Translation (NAT) mode. See the *NetScreen Concepts and Examples ScreenOS Reference Guide*, for more configuration options.

CONNECTING THE NETSCREEN-5 TO NETWORKS AND DEVICES

This section explains how to set up the NetScreen-5 hardware connections.

Note: Check your router, hub, or computer documentation to determine if you should reconfigure the device or if you should switch off the power supply when connecting new equipment to the LAN.

1. Install the NetScreen-5 on a level surface.
2. Connect the universal power supply's DC side to the power outlet on the NetScreen-5 device, and the AC side to an AC outlet.

The NetScreen-5 takes up to one minute to start up. There is no ON/OFF switch. If you need to reboot at any point, unplug the NetScreen device for 30 seconds and then plug it back in again.

3. Connect the NetScreen-5 to the network as shown in one of the following illustrations:
 - Figure 3-1 “Typical Multiple-Workstation Configuration—Router Connected to the Untrusted Port, LAN Connected to the Trusted Port” on page 3-14
 - Figure 3-2 “Typical Single-Workstation Configuration—Router Connected to the Untrusted Port, Workstation Connected to the Trusted Port” on page 3-14

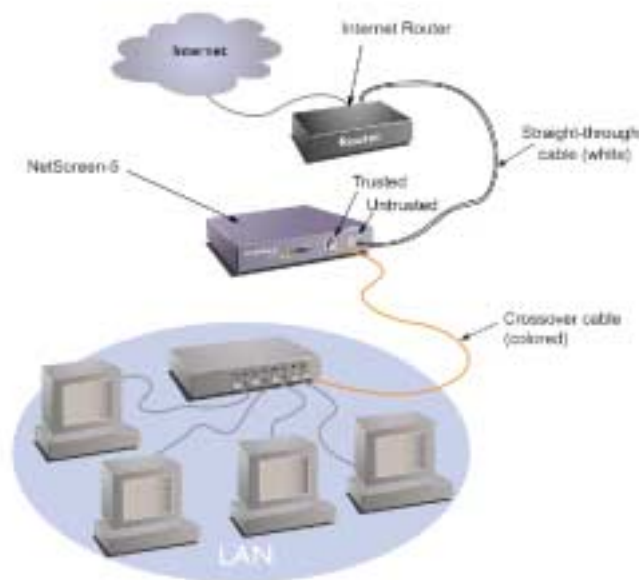


Figure 3-1 Typical Multiple-Workstation Configuration—Router Connected to the Untrusted Port, LAN Connected to the Trusted Port

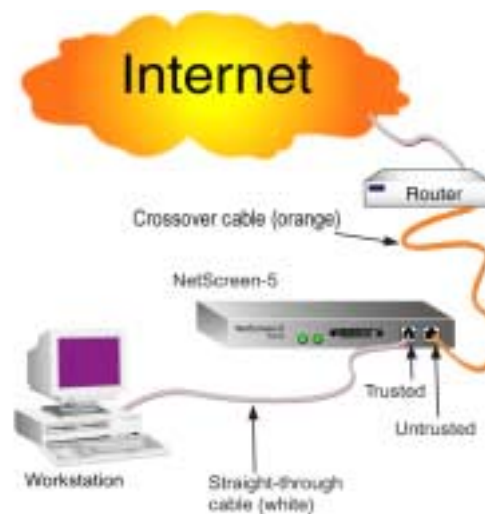


Figure 3-2 Typical Single-Workstation Configuration—Router Connected to the Untrusted Port, Workstation Connected to the Trusted Port

Note: You may have to supply additional cables, depending on your particular configuration. A straight-through cable is a 10/BaseT unshielded twisted pair (UTP) and is usually white. A crossover cable is a 10/BaseT UTP and is usually orange.

A DTE (Data Terminal Equipment) device cannot connect to a DTE port without a crossover cable. Conversely, a DCE (Data Communications Equipment) device cannot connect to a DCE port without a crossover cable.

Table 3-1 Typical NetScreen-5 Cable Connections

For a Device Connected to:	Untrusted Port (DTE)*	Trusted Port (DCE)
Workstation (DTE)	crossover	straight-through
Switch/Hub (DCE)	straight-through	crossover
Router [§] (DTE)	crossover	straight-through
*An Untrusted Ethernet port is not technically a DTE but for cabling purposes, should be treated as such.		
[§] Routers with uplink ports may behave in reverse.		

- If you have not already done so, turn on the power supply to the devices you have connected to the NetScreen-5.

If all cables are connected correctly, the link light for each connection illuminates.

CONFIGURING THE NETSCREEN-5

There are three ways to configure the NetScreen-5 for the first time:

- Using the Quick Start Program.
- Using a Web browser running on a workstation connected via a network to the Trusted port.
- Using CLI via either Telnet or the serial port.

Table 3-2 Administration Configuration Requirements

Configuration Method	Requirements
Quick Start	Netscape [®] Communicator [®] v4.5 or greater, or Microsoft [®] Internet Explorer v5.0 or greater TCP/IP network connection to the NetScreen-5
WebUI via a Web Browser	Netscape Communicator v4.5 or greater, or Microsoft Internet Explorer v 5.0 or greater TCP/IP network connection to the NetScreen-5
CLI	Via the console port, using Hilgraeve [®] Hyperterminal [®] or a VT100 terminal emulator on the administrator's workstation and an RS-232 Console cable Via Telnet, using TCP/IP network connection to the NetScreen device.

Table 3-3 Important Default Configuration Settings

Default System IP Address:	192.168.1.1
Default Trusted/Untrusted IP Addresses:	0.0.0.0 (transparent mode)
Default User Name:	netscreen
Default Password:	netscreen

Configuring Via the Quick Start Program

NetScreen-5 comes with The Quick Start disk for easy configuration.

1. Insert the Quick Start disk into the a: drive of Windows® 95/98 or Windows NT® v4.0 computer from which you will configure unit on the LAN.
2. On the Windows task bar, click the **Start** button, and then select **Run**.
3. At the Command Line, type `a:\nsqstart.exe`, then select **OK**.

The NetScreen Quick Start Welcome window appears as in Figure 3-3 on page 17.



Figure 3-3 NetScreen Quick Start Welcome

4. Read the information on the NetScreen Quick Start Welcome screen, then click the **Next** button.

If there is more than one network card on the computer, the Quick Start program displays their IP addresses and prompts you to select the one for the network on which you are installing the NetScreen-5, as shown in Figure 3-4.

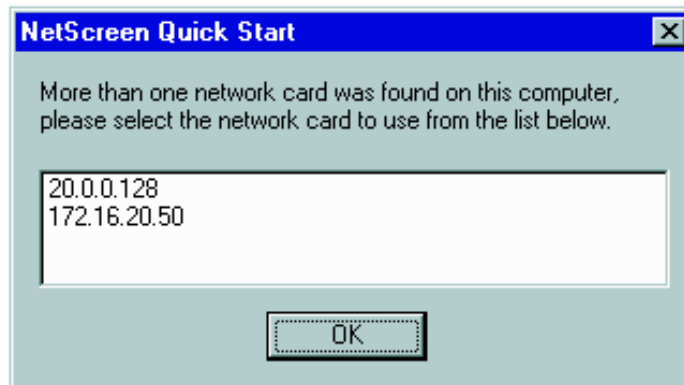


Figure 3-4 Network Card IP Address List

Select the appropriate network card, and then click **OK**.

Note: The Quick Start program can only find the NetScreen-5 devices on your network that still have the factory default configuration.

5. When the NetScreen Quick Start Select Device dialog box displays, select the NetScreen-5 you want to configure, as shown in Figure 3-5, then click the **Next** button.

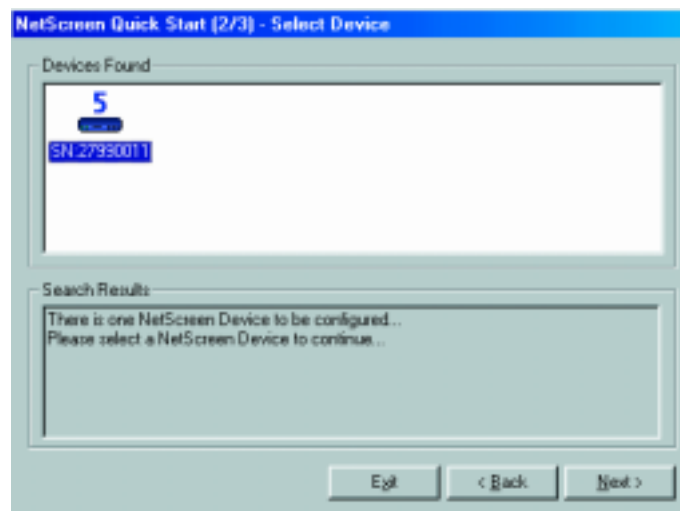


Figure 3-5 NetScreen Quick Start-Select Device

6. Enter the new System IP address for the NetScreen device you are configuring, as shown in Figure 3-6.

This value must be an available address on the Trusted subnet. This is the address that you will use to further manage the NetScreen-5.

Figure 3-6 NetScreen Quick Start-Configuration Dialog Box.

Selecting Transparent Mode

1. To launch your NetScreen-5 in Transparent mode, select **Transparent Mode as shown in Figure 3-6**.
2. Click **Finish**.

If you leave the **Launch web browser for further configuration** check box selected (the default), Quick Start opens your Web browser and displays the User name and Password dialog box as shown in Figure 3-11 on page 3-25.

If you clear the **Launch web browser for further configuration** check box, you must start your Web browser manually when Quick Start exits.

Selecting Network Address Translation

1. To launch your NetScreen-5 in NAT mode, select **Network Address Translation Mode (NAT)**.
2. Click **Next**.

The NAT Configuration screen shown in Figure 3-7 appears.

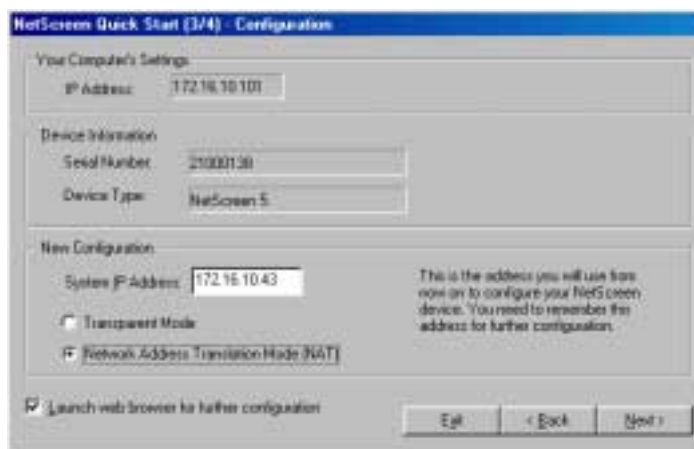


Figure 3-7 NetScreen Quick Start-Configuring NAT

3. Enter the IP address, subnet mask of the NetScreen-5 Trusted interface.
4. To configure the Untrusted interface, use one of the following three methods:
 - a. To use Dynamic Host Control Protocol, select **DHCP**.
 - b. To use Point-to-Point Protocol over Ethernet, select **PPPoE** and enter the **User name** and **Password** for the login prompt.
 - c. To assign an IP address, subnet mask, and gateway IP address manually, select **Manually Assign** and then enter the settings in the appropriate fields.
5. Select **Finish**.

If you leave the **Launch web browser for further configuration** check box selected (the default), Quick Start opens your Web browser and displays the Username and Password dialog box, as shown in Figure 3-11 on page 3-25.

If you clear the **Launch web browser for further configuration** check box, you must start your Web browser manually when Quick Start exits. For more information on logging in manually, see *"Logging On" on page 3-25*

Configuring Via the WebUI

You can also perform the initial configuration through a Web browser without the NetScreen-5 Quick Start disk. To do this, you need to

- Change the IP address of the management workstation to the same subnet as the NetScreen-5 default System IP address.

Then after making an Ethernet connection to the NetScreen-5, you can log on through a Web browser. The following section details this procedure.

Refer back to Table 3-2 on page 3-16 for administration requirements.

Making a Connection

Before you begin, be sure you connected the NetScreen-5 hardware to the network as outlined on page 3-13.

Setting the System IP Address

For remote administration of the NetScreen device over a network connection, you must change the system IP address. The NetScreen-5 ships from the factory with a default IP address of 192.168.1.1. To change this to an address on the same subnet as the other network devices to which the NetScreen-5 is connected, enter the following command:

1. Record your workstation's IP address and subnet mask. You must re-enter them later in this process.

Note: To find your workstation IP address: Start>>Settings>>Control Panel>Network>Configuration, select TCP/IP and then click Properties.

2. Change the IP address of the workstation to 192.168.1.2 and a subnet mask of 255.255.255.0. You might have to restart the workstation to enable these changes to take effect.

Note: For Windows NT users, ensure that you are logged on to the workstation as an administrator.

3. Start your Web browser.
4. In the URL field of the browser, enter the IP address of the NetScreen-5: http://192.168.1.1.

The Enter Network Password dialog box appears, as shown in Figure 3-8 on page 3-22.

Note: The NetScreen-5 ships from the factory with the IP address set to 192.168.1.1.

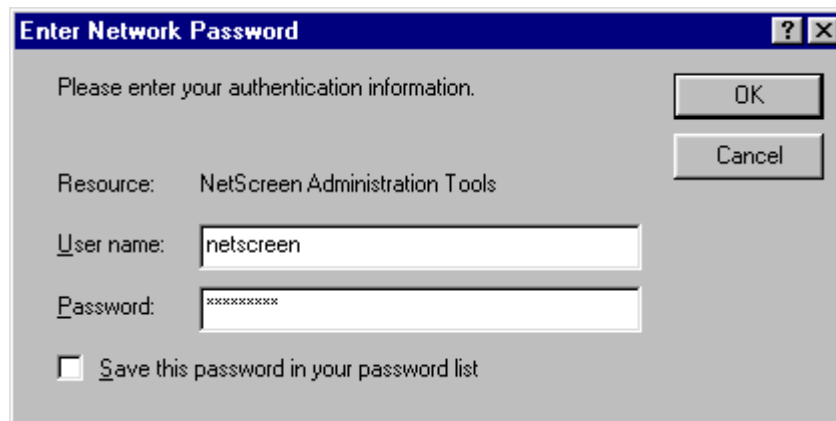


Figure 3-8 Enter Network Password Dialog Box

5. In the dialog box, type `netscreen` for both the user name and password, and then click **OK**.

Note: The user name and password are case-sensitive. After configuring the NetScreen device for the first time, change the default user name and password as described later in "Changing the Administrator Login Name and Password" on page 3-30.

6. An IP Address Configuration dialog box, as shown in Figure 3-9 on page 3-23 is displayed for first-time configuration.



Figure 3-9 Initial IP Address Configuration

7. Enter a new System IP address and subnet mask for the NetScreen-5, and then click **OK** to save your settings.

Note: The IP address must be a valid and available IP address on your local network, and the subnet mask must be an appropriate value for your local network.

The Configuring in Progress screen appears, as shown in Figure 3-10.

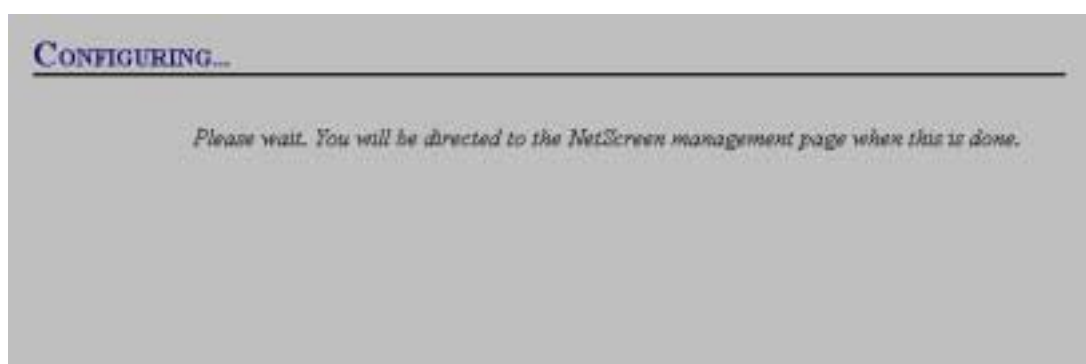


Figure 3-10 Configuring in Progress Screen

The NetScreen-5 is in Transparent mode. To change it to NAT mode, you must configure the Trusted and Untrusted interfaces. To do that, refer to chapter 2, “System Parameters” in the *NetScreen Concepts and Examples ScreenOS Reference Guide*.

8. Reconfigure your administration workstation IP address to the original settings that you recorded in the first step. Depending on the operating system, you might have to restart your workstation.

Logging On

Once the IP configuration is complete, you must again log on.

1. When the Web browser is activated, enter the newly created IP address of the NetScreen-5.

The User name and Password dialog box displays.

2. In the User name and Password dialog box, type `netscreen` for both the user name and password, and then click **OK**.

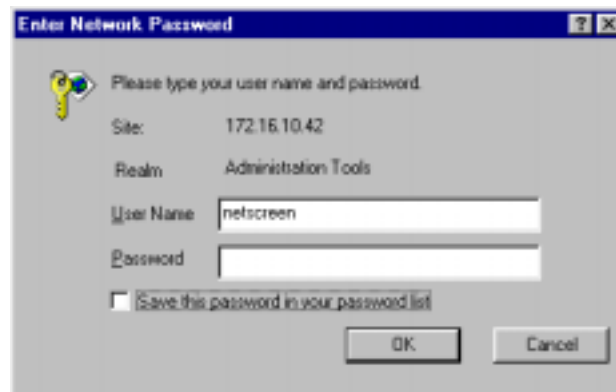


Figure 3-11 Username and Password Dialog Box

Note: The login name and password are case-sensitive.

After configuring the NetScreen-5 for the first time, change the user name and password. See “Changing the Administrator Login Name and Password” on page 3-30 for instructions.

Allowing Outbound Traffic

The NetScreen-5 ships with a default Access Policy allowing all traffic inside the network to access the Internet. The Access Policies pages appear with the Default Outgoing page displayed, as shown in Figure 3-12 on page 3-26.

Note: For more information on Access Policies, please refer to the NetScreen Concepts and Examples ScreenOS Reference Guide.

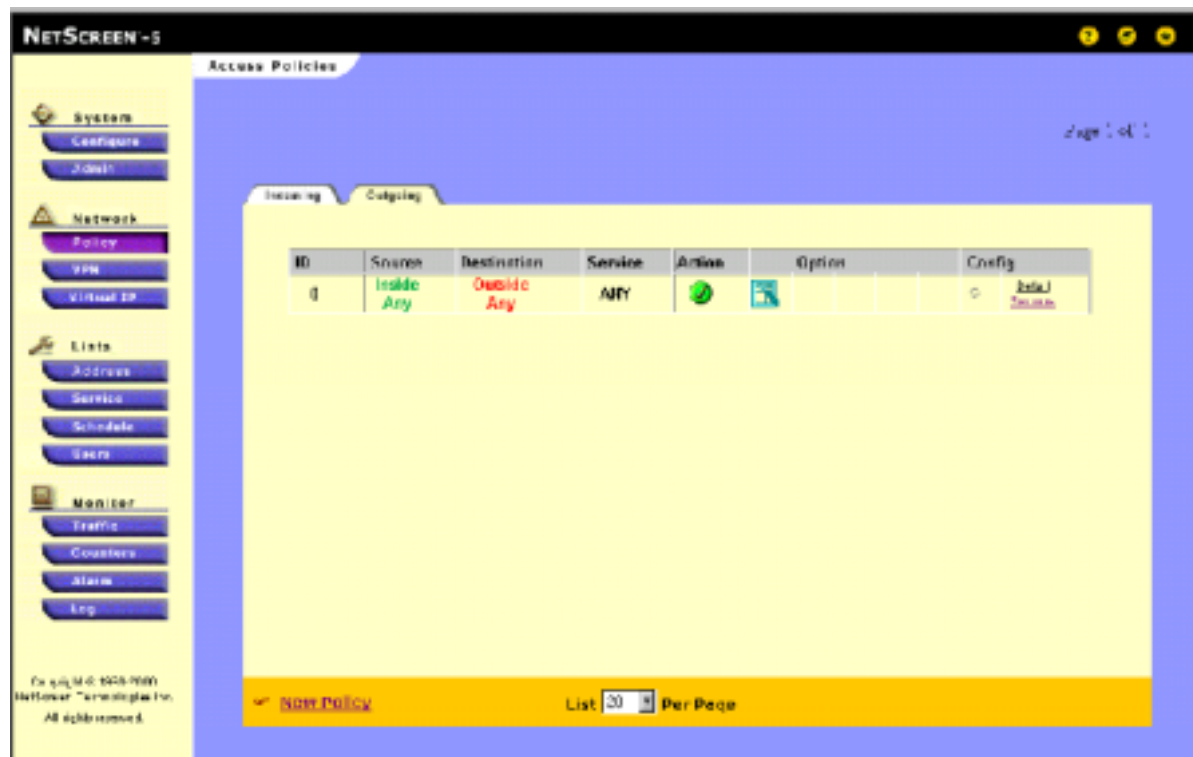


Figure 3-12 Default Outgoing Access Policy

Testing the Configuration

Use a Web browser to access an external Web site (for example, www.netscreen.com). You should be able to locate the site and access the available Web pages.

If you cannot access the Web site, check the following:

- Link lights on the NetScreen-5, workstations, hubs, and the router are illuminated.
- The workstation IP and Netmask have the correct settings.
- The workstation gateway points to the router.
- The workstation has a valid DNS entry.

Note: See the NetScreen Command Line Reference Guide.

Configuring Via the CLI

The following section provides information on how to configure the device using the command line interface (CLI).

Making a Connection

You can access the CLI either by connecting directly via a console (or serial) cable or you can use the network via Telnet. Connection instructions are offered for both methods.

Refer to Table 3-2 on page 3-16 for administration requirements.

Connecting via the Console Port

You need direct access to the NetScreen device you want to configure and the following items before you start:

- An RS-232 male-to-female serial cable
- Microsoft Hyperterminal software on the management workstation (or, if you are using a different operating system, a VT100 terminal emulator)

Follow these steps to connect the NetScreen device to the workstation:

1. Connect the serial cable from the management workstation to the serial port on the NetScreen-5.
2. Start the terminal emulator on the workstation.
3. To create a new connection, type a name, select an icon, and then click **OK**.

The Connect To dialog box appears.

4. Select the serial port to which the serial cable is connected to the workstation, and click **OK**. The COM1 Properties dialog box appears.
5. Configure the port settings as follows, and then click **OK**.
 - Serial communications 9600 bps
 - 8 bit, no parity
 - 1 stop bit
 - no flow control
6. Press **ENTER** to see the login prompt.

Connecting via Telnet

Telnet operates over TCP/IP networks. It allows you to configure the device using the command line interface (CLI).

Before you begin, be sure you connected the NetScreen-5 hardware to the network as outlined in on page 3-13.

1. Establish a Telnet connection to the NetScreen device.
2. For Host name, type: 192.168.1.1.

Note: Select *vt100* for Terminal type.

Logging On

To log on, enter the default administrator name and password.

1. At the login prompt, enter `netscreen.`
2. At the password prompt, enter `netscreen.`

Note: The user name and password are case-sensitive.

After configuring the NetScreen-5 for the first time, change the user name and password. See “Changing the Administrator Login Name and Password” on page 3-30 for instructions.

Setting the System IP Address

You can configure your NetScreen device for either Transparent mode or Network Address Translation (NAT) mode.

Transparent Mode

At the command line enter:

1. `set admin sys-ip <a.b.c.d>`
2. `save`

Note: Substitute your actual system IP address for *<a.b.c.d>*.

Network Address Translation (NAT) Mode

At the command line enter:

1. `set admin sys-ip <a.b.c.d>`
2. `set interface trust ip <a.b.c.d>`
3. `set interface untrust ip <a.b.c.d>`
4. `save`

Allowing Outbound Traffic

To create an outgoing Access Policy that permits any inside traffic to pass through the firewall and access the Internet, enter the following commands:

1. `set policy outgoing "inside any" "outside any" any permit`
2. `save`

Note: Making system-level changes through the CLI does not require restarting the NetScreen-5, whereas making similar changes through the WebUI does.

Testing the Configuration


Use a Web browser to access an external Web site (for example, www.netscreen.com). You should be able to locate the site and access the available Web pages.

See “Testing the Configuration” on page 3-26 for instructions.

Note: See the NetScreen Command Line Reference Guide.

CHANGING THE ADMINISTRATOR LOGIN NAME AND PASSWORD

Because all NetScreen-5 devices come with the same default login name and password, you should change this information immediately after you install the device. You can change the default administrator login and password either through the WebUI or the CLI.

 **Caution** *The information in this guide has been widely published, and failure to change the defaults might expose your system to attack.*

Using the WebUI

To change the default administrator login and password via the WebUI:

1. Select the **Admin** button in the menu column to view the **Admin** page, as shown in Figure 3-13.

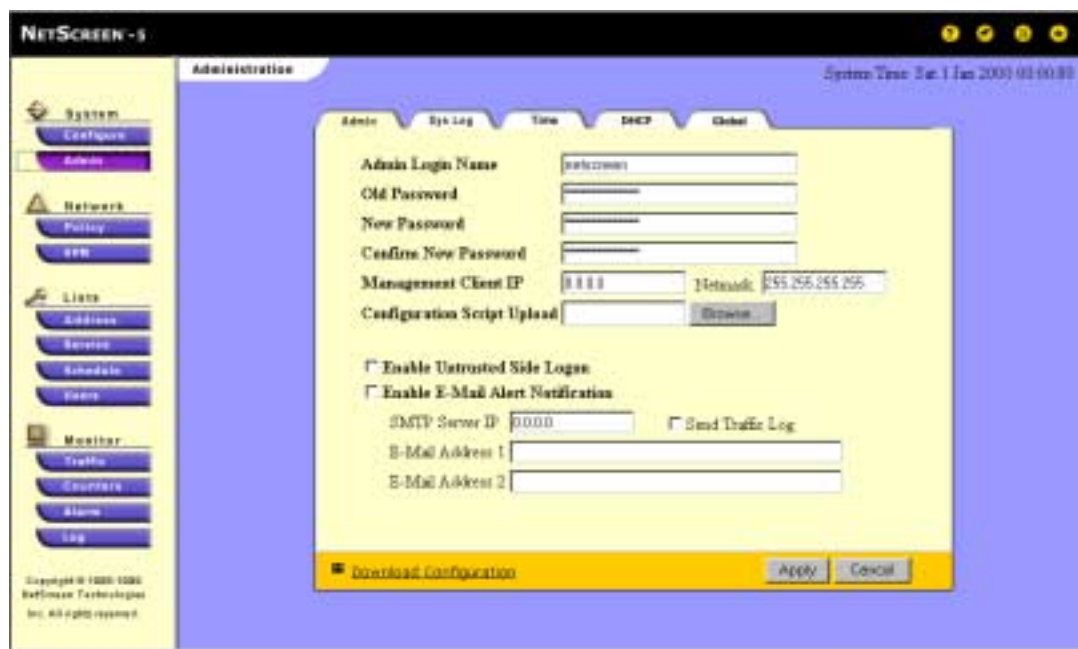


Figure 3-13 The Administration Page

2. Type a new Admin Login Name.

Note: *The login name and password must be alphanumeric. The login username and password are case-sensitive*

3. Type the old password (initially *netscreen*) in the Old Password field. You must enter the old password to change to the new password.
4. Type the new password in the New Password field and the Confirm New Password field.
5. Record the new Administrator Login Name and Password in a secure manner.



Warning

Make sure that you remember your password! If you forget it, you will have to return the unit to the factory for initialization. This feature has been implemented in this manner as an extra security measure.

6. Leave the other fields at their default entries, and select the **Apply** button.

The changes require the NetScreen-5 to reset, which it automatically does at this point. Figure 3-14 on page 32 shows the system message that appears.



Figure 3-14 The System Message Display

7. Click the **Yes** button to confirm your command to reset the system.
The next time you log in, use the new login name and password.

Note: To receive important news on product updates, please visit our web site at www.netscreen.com and register your product.

Using the CLI

At the command line enter:

1. `set admin name <name>`
2. `set admin password <password>`

Record the new Administrator Login Name and Password in a secure manner.



Warning

Make sure that you remember your password! If you forget it, you will have to return the unit to the factory for initialization. This feature has been implemented in this manner as an extra security measure.

NetScreen 10 & 100 Hardware and Software Description 4

This chapter provides illustrations and descriptions of the NetScreen-10/100 front and back panels and an introduction to the Web user interface (WebUI).

Hardware Description

Before you install your NetScreen device, you should unpack it onsite and verify the contents against the packing slip.

A front view of the NetScreen-10/100 is shown below. The label on the left side indicates the model name: NetScreen-10 or NetScreen-100.

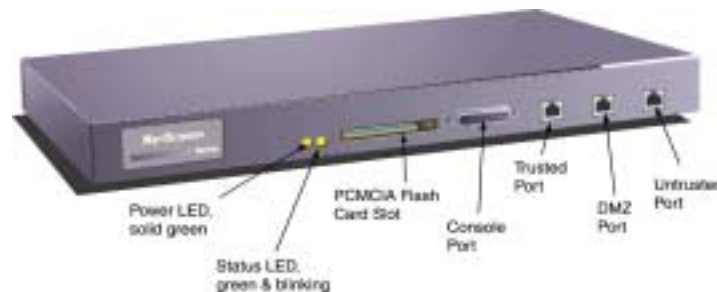


Figure 4-1 Front Panel of the NetScreen-10/100

- **Power LED:** glows solid green when power is supplied to the NetScreen-10/100.
- **Status LED:** glows solid green when the NetScreen-10/100 is first powered up and the unit first performs diagnostics. Then the unit goes into a startup phase, which takes up to one minute to complete. During startup, the LED blinks orange, after which the LED blinks green. If an error is detected, then the LED illuminates red. The LED changes to yellow whenever the unit writes to the internal flash card.
- **PCMCIA Flash Card Slot:** The NetScreen-10/100 supports a removable PCMCIA PC Card ATA compatible Flashdisk. Supported cards include the SanDisk 96-MB and 20-MB Flash card. The NetScreen device automatically detects the presence of a flashcard and records the Event Log to it.

- **Console Port:** DB25 serial port connector for local configuration and administration.
- **Trusted Port:** Connect the NetScreen-10/100 using a twisted pair cable with RJ45 connectors. The trusted port is a data circuit-terminating equipment (DCE) port. See the following chapter for cabling guidelines.
- **DMZ Port:** Connect the NetScreen-10/100 using a twisted pair cable with RJ45 connectors. The DMZ port is a DCE port.
- **Untrusted Port:** Connect the NetScreen-10/100 using a twisted pair cable with RJ45 connectors. The untrusted port is a data terminal equipment (DTE) port. See the following chapter for cabling guidelines.
- **Trusted, DMZ, and Untrusted Ethernet LEDs:** Each Ethernet port has two link lights, or LEDs. The right LED indicates if the link is up (connected to an active device) and the left LED indicates network traffic activity. These LEDs differ for the NetScreen-10 and NetScreen-100. See Figure 4-2.



Figure 4-2 Ethernet LEDs

The back panel of the NetScreen-10/100 is shown in Figure 4-3.



Figure 4-3 Back Panel of the NetScreen-10/100

- **Product Label:** The model number is either NS-10x or NS-100x, where x=a, e, or f.

Table 4-1 NetScreen-10/100 Model Numbers

Model Type	Functionality
a	Firewall & VPN (3DES & DES)
e	Firewall & VPN (DES)
f	Firewall

Note: Certain export restrictions apply to International customers. Check with your sales representative.

- **Power Outlet:** Use the outlet to connect power to the NetScreen-10/100 with the supplied power cable.
- **On/Off Switch:** Turns the power to the NetScreen-10/100 on or off.

GENERAL LAYOUT OF THE NETSCREEN-10/100 ADMINISTRATION TOOLS

The Web Administration Tools page consists of two main logical sections:

- Figure 4-4 shows the NetScreen-10/100 menu column and explains the features found under each button. The menu column consists of four functional categories: System, Network, Lists, and Monitor, each of which contains further sub-functions, represented by tabs on the screen. During configuration, you first select a main functional category, then choose the various utilities offered within each sub-category.



Figure 4-4 The NetScreen-10/100 Menu Column

- A central display area, shown in Figure 4-5, lists the information for each of the menu items above, in either a tabular or graphical format. These displays generally contain links to other related screens through action buttons such as **Apply** and **Reset**, **Apply**, **OK**, **New Entry**, **Edit**, **Remove**, and so forth.

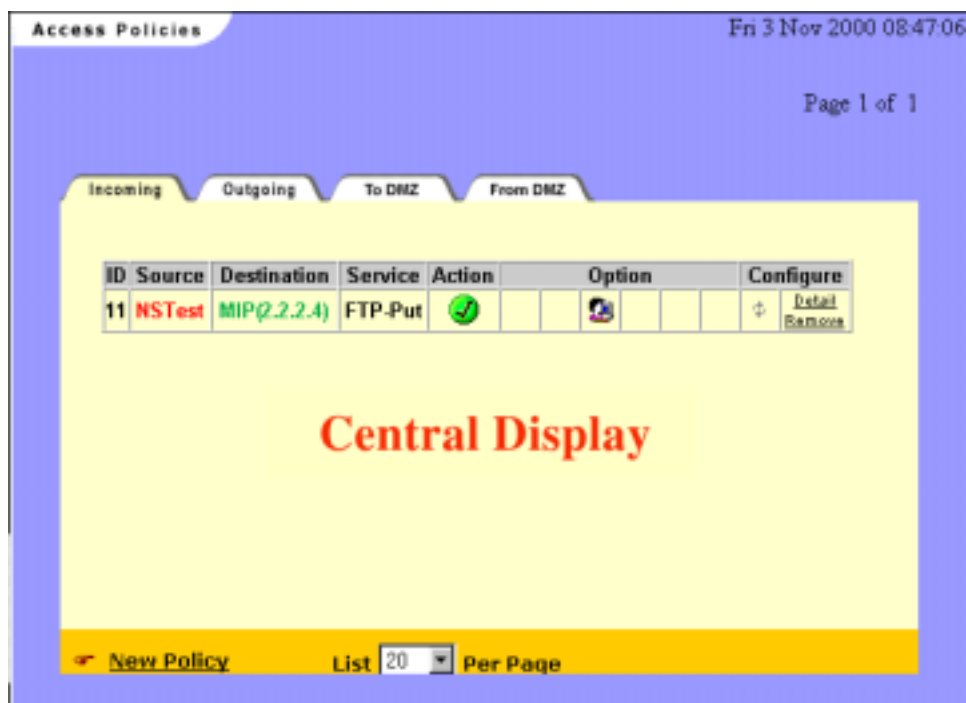


Figure 4-5 Central Display

Connecting the NetScreen10 & 100 5 to the Network

Follow the instructions in this chapter to set up the NetScreen-10/100 hardware and to configure the software for the first time. For further configuration options, see Chapter 2, “System Parameters” in the *NetScreen Concepts & Examples ScreenOS Reference guide*, on the product CD.

This chapter contains the following sections:

- Gathering the Necessary Tools
- Connecting the NetScreen-10/100 to Networks and Devices

GATHERING THE NECESSARY TOOLS

The chassis can be placed on a table top or mounted in a standard 19-inch equipment rack. Table top installation requires no tools. Rack mounting requires a Phillips-head screwdriver, the rack mount bracket kit, and four screws to match the rack. Screws for attaching the mounting brackets to the chassis are provided in the NetScreen-10/100 product package. Users will have to supply screws to match rack thread size.

CONNECTING THE NETSCREEN-10/100 TO NETWORKS AND DEVICES

Note that if you are configuring multiple NetScreen-10/100 devices, you should install and configure them *one* at a time. Otherwise, you will run into IP address conflicts.

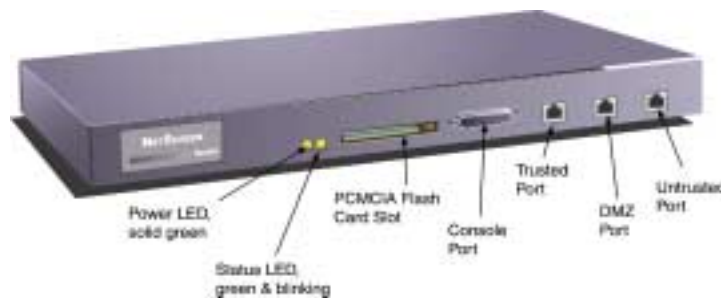


Figure 5-1 Front View of the NetScreen-10/100



Figure 5-2 Back View of the NetScreen-10/100

To set up the NetScreen-10/100 hardware connections, follow these steps.

Note: Check your router, hub, or computer documentation to determine if you must reconfigure the device or if you must switch off the power supply when connecting new equipment to the LAN.

1. Install the NetScreen-10/100 in a rack (optional) or on a level surface.
2. Make sure that the power connection to the NetScreen-10/100 is turned off; that is, that "0" is pressed.
3. Connect the power cable provided in the product package, from the NetScreen-10/100 power outlet to the power supply.
4. Connect the NetScreen-10/100 to the network as shown in one of the examples beginning on page 2-3.

5. Turn on the NetScreen-10/100 and any other network devices that you had turned off.
6. If all cables are connected correctly, the link light for each connection will illuminate.

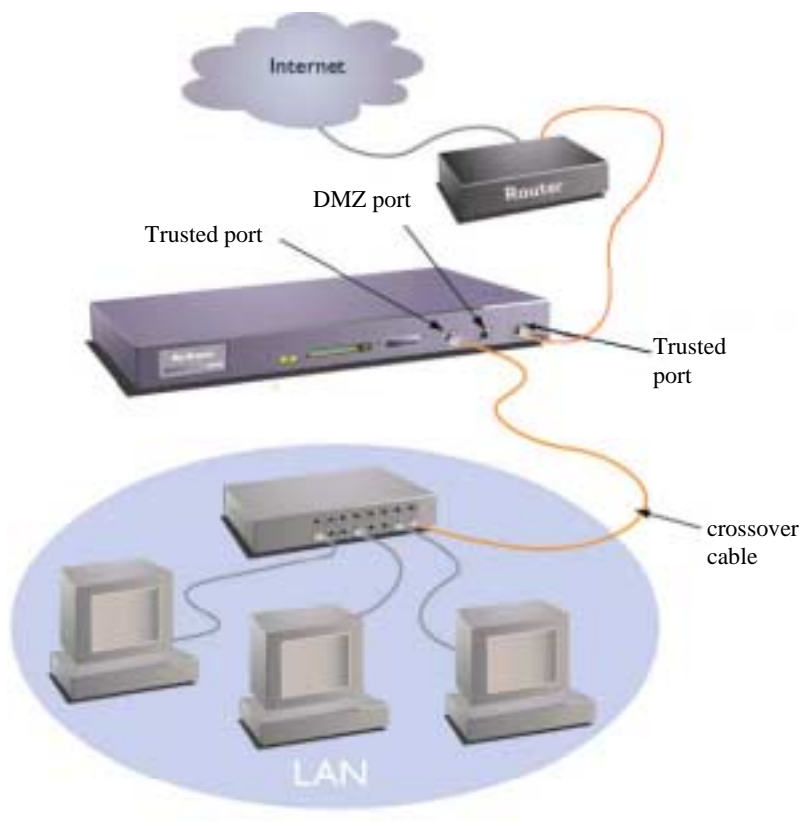


Figure 5-3 Sample Configuration with a Router Connected to the Untrusted Port, Local Area Network (LAN) Connected to the Trusted Port

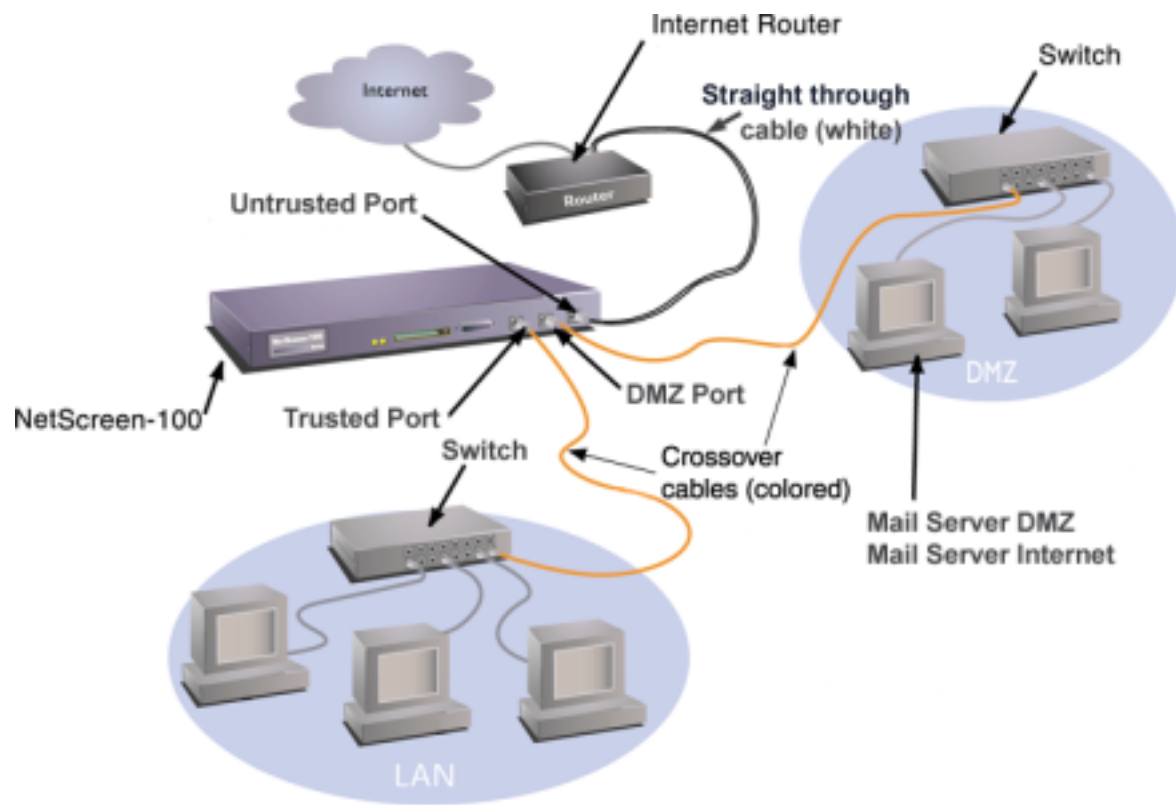


Figure 5-4 Sample Configuration Using DMZ Port

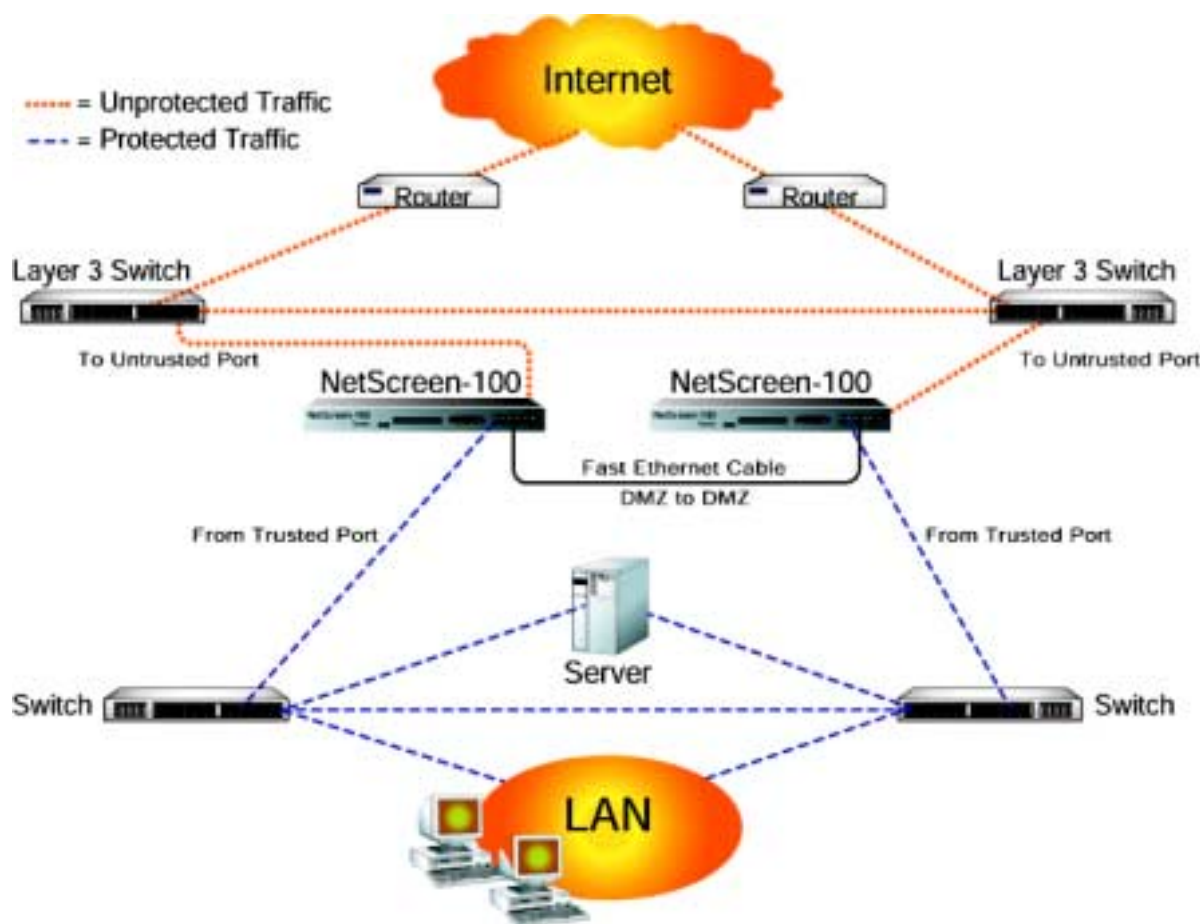


Figure 5-5 Sample Configuration in a redundant group for High Availability (NetScreen-100 only)

Note: You may have to supply additional cables, depending on your particular configuration. A straight-through cable is a 10/BaseT unshielded twisted pair (UTP) and is usually white. A crossover cable is a 10/BaseT UTP and is usually orange.

A DTE (Data Terminal Equipment) device cannot connect to a DTE port without a crossover cable. Conversely, a DCE (Data Communications Equipment) device cannot connect to a DCE port without a crossover cable.

Table 5-1 Typical NetScreen-5 Cable Connections.

For a Device Connected to:	Untrusted Port (DTE)[*]	Trusted Port (DCE)
Workstation (DTE)	crossover	straight-through
Switch/Hub (DCE)	straight-through	crossover
Router [§] (DTE)	crossover	straight-through
[*] An Untrusted Ethernet port is not technically a DTE but for cabling purposes, should be treated as such.		
[§] Routers with uplink ports may behave in reverse.		

If all cables are connected correctly, the link light for each connection illuminates.

Configuring the NetScreen 10 & 100 for the First Time

6

This chapter shows you how to configure your NetScreen-10/100 in Transparent mode and allow internal users to access the Internet while denying internal access from the Internet. You do this by setting the System IP address and creating an Access Policy that permits outgoing traffic.

There are two methods for configuring the NetScreen-10/100 for the first time. Table 6-1 “Administration Requirements” lists the workstation requirements for each method.

Table 6-1 Administration Requirements

Configuration Method	Requirements
WebUI via a Web browser	Netscape [®] Communicator [®] V4.5 or greater, or Microsoft [®] Internet Explorer V5. or greater TCP/IP network connection to the NetScreen-10/100
CLI	Via the console port, using Hilgraeve [®] Hyperterminal [®] or a VT100 terminal emulator on the administrator's workstation and an RS-232 Console cable Via Telnet, using TCP/IP network connection to the NetScreen device.

The installation procedure using a Web browser is explained first, followed by the CLI procedures using the console port and Telnet.

USING THE WEBUI

To perform the initial configuration through a WebUI, you need to change the IP address of the management workstation to the same subnet as the NetScreen-10/100 default system IP address. You can log on through a Web browser and set the system IP address. The following sections details the procedures for administration of the NetScreen-10/100 device from the administrator's workstation.

Refer back to Table 6-1 on page 6-47 for administration requirements.

Making a Connection

Before you begin, be sure you connected the NetScreen-10/100 hardware to the network.

Setting the System IP Address

For remote administration of the NetScreen device over a network connection, you must change the system IP address. The NetScreen-10/100 ships from the factory with a default IP address of 192.168.1.1. To change this to an address on the same subnet as the other network devices to which the NetScreen-10/100 is connected, enter the following command:

1. Record the IP address and subnet mask of your workstation; you must re-enter them later in this process.
2. Change the IP address of the workstation to 192.168.1.2 and the subnet mask to 255.255.255.0. You might have to restart the workstation to enable the changes to take effect. The workstation is now part of the same subnet as the default IP address of the NetScreen-10/100, which is 192.168.1.1.
3. Start your Web browser.
4. In the URL field of the browser, enter the IP address of the NetScreen-10/100: `http://192.168.1.1`.
5. The Enter Network Password dialog box appears, as shown in Figure 6-1 on page 6-49.



Figure 6-1 Enter Network Password Dialog Box

6. In the dialog box, type **netscreen** for both the user name and password, and then click **OK**.

Note: The user name and password are case-sensitive. After configuring the NetScreen device for the first time, you should change the default user name and password as described in “Changing the Administrator Login Name and Password” on page 6-54.

7. For the first-time configuration, you are directed to a special setup page as shown in Figure 6-2.

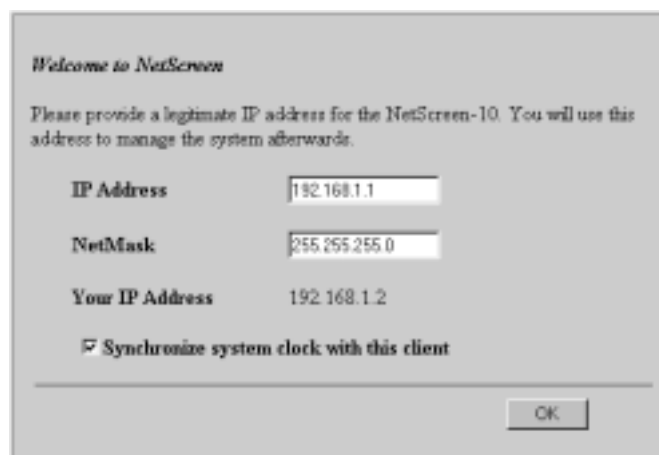


Figure 6-2 Initial IP Address Configuration

8. Enter the IP address and subnet mask for administration of the NetScreen-10/100, and then click **OK**.

Note: Select the Synchronize system clock with this client checkbox to synchronize the NetScreen-10/100 clock with the clock in the administrator's workstation.

The IP address must be a valid and available IP address on your local network and the subnet mask must be an appropriate value for your local network.

The Configuring in Progress screen displays as shown in Figure 6-3.

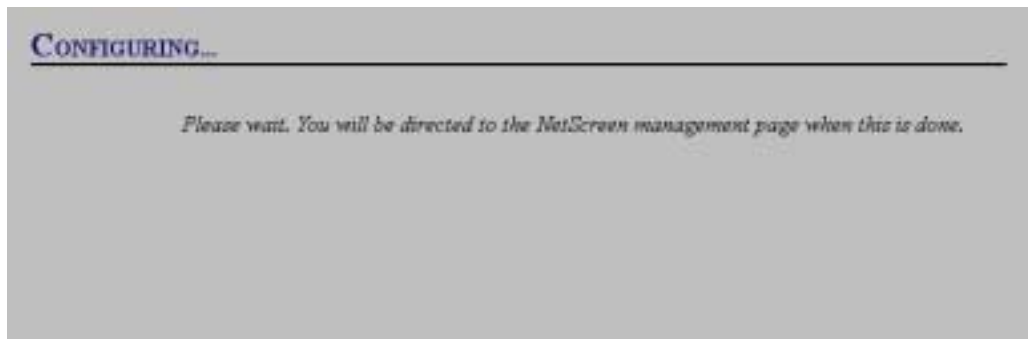


Figure 6-3 Configuring in Progress Screen

9. Reconfigure your administration workstation IP address and subnet mask back to values you recorded in step 1. Depending on the operating system, you might have to restart your workstation.

Logging On

Once the IP configuration is complete, you must again log on.

1. In the URL field of the browser, enter the new IP address for the NetScreen device.

The Enter Network Password dialog box re-appears, shown in Figure 6-4.

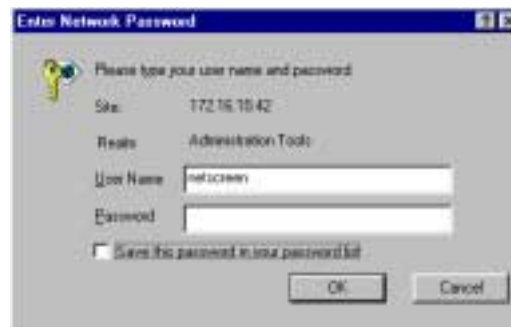


Figure 6-4 Enter Network Password Dialog Box

2. In the dialog box, type **netscreen** for both the user name and password, and then click **OK**. Remember that the user name and password are case-sensitive.

The Access Policies pages appear, with the Outgoing Access Policies page displayed, as shown in Figure 6-5. You are now logged on to the NetScreen-10/100.

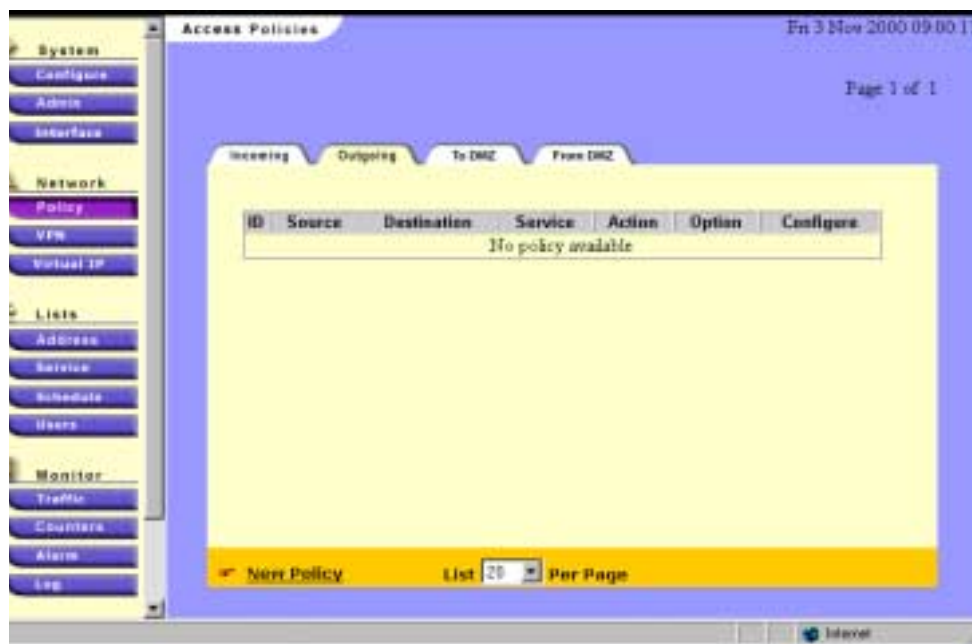


Figure 6-5 Access Policies Pages

Allowing Outbound Traffic

1. Click the **New Policy** option in the lower left corner of the Access Policies page. The Policy Configuration dialog box appears.

POLICY CONFIGURATION

Name (optional)

Source Address

Destination Address

Service

Action

VPN Tunnel

Authentication ☐

Logging ☐ Enable Counting ☐ Enable

Alarm Threshold Bytes/Sec Bytes/Min

Schedule

Traffic Shaping ☒ Off

☐ Guaranteed Bandwidth kbps

☐ Maximum Bandwidth kbps

Traffic Priority

DS Codepoint Marking ☐ Enable

Figure 6-6 New Policy Page

2. Set an Access Policy that allows all inside hosts to access the Internet. Set the options as follows:
 - **Name:** This is optional.
 - **Source Address:** Inside Any (Inside Any is a predefined address for any host on the Trusted network)
 - **Destination Address:** Outside Any (Outside Any is a predefined address for any location on the Untrusted network, Internet)
 - **Service:** Any (Any is a predefined value for any IP service)
 - **Action:** Permit (Allows the traffic defined by the Access Policy)
 - Leave the rest of the options to their default values, and click the **OK** button.

The Outgoing Access Policies page now has one Access Policy that permits any inside traffic to pass through the firewall and access the Internet, as shown in Figure 6-7.

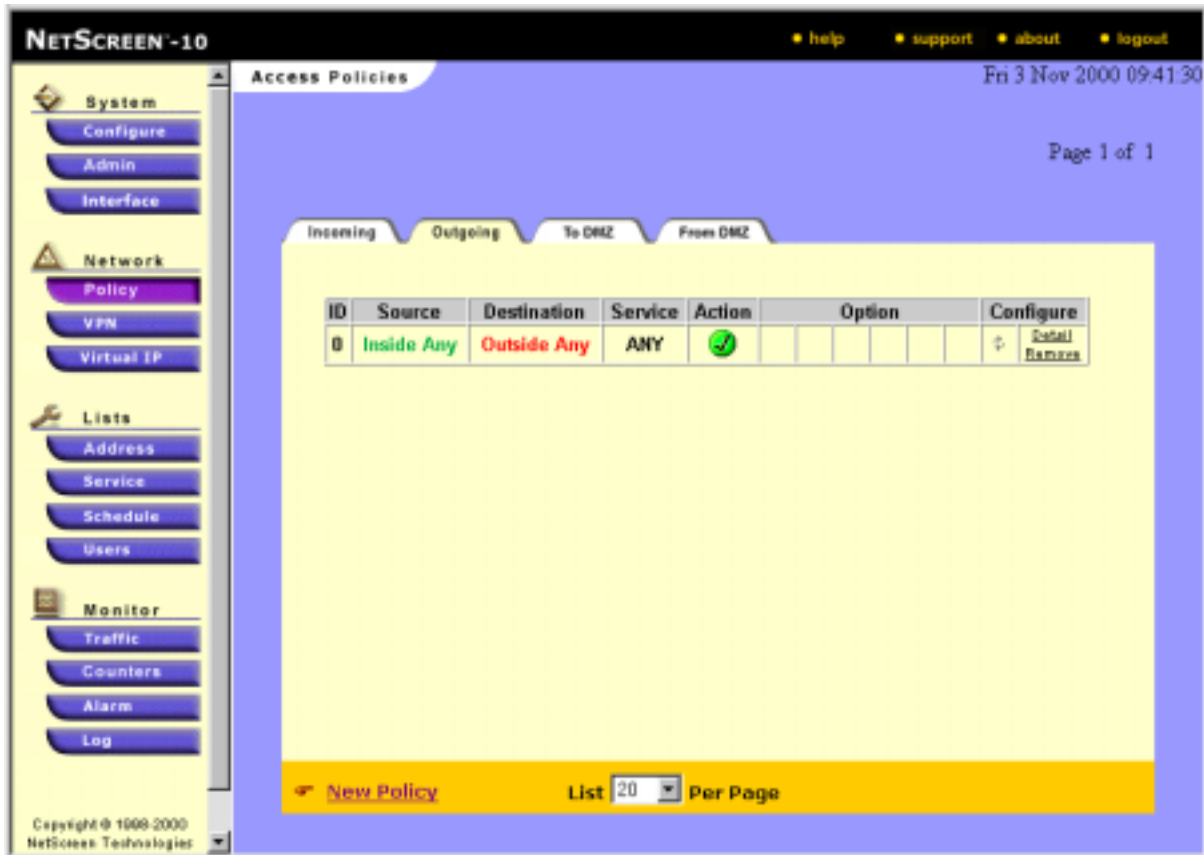


Figure 6-7 Access Policies Page

Because there is no need to configure other interface IP settings, your NetScreen-10/100 configuration for Transparent mode is now complete.

Changing the Administrator Login Name and Password

Because all NetScreen units come with the same default name and password, it is highly recommended that you change the default Admin Login name and Password.

Note: *The information in this guide has been widely published, and failure to change the defaults might expose your system to attack.*

1. Admin >> Admin >> Edit: Enter the following and then click **OK**:

Name: <name>

Old Password: netscreen

New Password: <new password>

Confirm Password: <new password>

The Enter Network Password dialog box appears.

Note: *The login name and password are case-sensitive.*

2. Enter your new user name and password, and then click **OK**.

The next time you log on, you must supply the new login name and password.

3. Record the new Administration name and Password in a secure manner.



Warning

Make sure that you remember your password! If you forget it, you will have to return the unit to the factory for initialization. This feature has been implemented in this manner as an extra security measure.

Testing the Configuration

Use your Web browser to access an external Web site (for example, www.netscreen.com). You should be able to locate the site and access the available Web pages.

If you cannot access the Web site, check the following:

- The power, status and link lights on NetScreen-10/100 are illuminated.
- The LEDs on the host, hubs and router are illuminated.
- The Administrator's workstation IP address and subnet mask are correct.
- The workstation gateway points to the external router.
- The workstation has valid Domain Name Service (DNS) entry.

Note: For more information and examples on other configuration options, please refer to the NetScreen Concepts & Examples ScreenOS Reference Guide.

USING THE CLI

The following section provides information on how to configure the device using the command line interface (CLI).

Making a Connection

You can access the CLI either by connecting directly via a console (or serial) cable or you can use the network via Telnet. Connection instructions are offered for both methods.

Connecting via the Console Port

You need direct access to the NetScreen device you want to configure and the following items before you start:

- An RS-232 male-to-female serial cable
- Microsoft Hyperterminal software on the management workstation (or, if you are using a different operating system, a VT100 terminal emulator)

Follow these steps to connect the NetScreen device to the workstation:

1. Connect the serial cable from the management workstation to the serial port on the NetScreen-10/100.
2. Start the terminal emulator on the workstation.
3. To create a new connection, type a name, select an icon, and then click **OK**.

The Connect To dialog box appears.

4. Select the serial port to which the serial cable is connected to the workstation, and click **OK**. The COM1 Properties dialog box appears.
5. Configure the port settings as follows, and then click **OK**.
 - Serial communications 9600 bps
 - 8 bit, no parity
 - 1 stop bit
 - no flow control
6. Press **ENTER** to see the login prompt.

Connecting via Telnet

Telnet operates over TCP/IP networks. It allows you to configure the device using the command line interface (CLI).

Before you begin, be sure you connected the NetScreen device hardware to the network as outlined in Chapter 2.

1. Establish a Telnet connection to the NetScreen device.
2. For Host name, type: 192.168.1.1.

Note: Select *vt100* for Terminal type.

Logging On

To log on, enter the default administrator login name and password.

1. At the login prompt, enter `netscreen`.
2. At the password prompt, enter `netscreen`.

Setting the System IP Address

To administer the NetScreen device over a network connection, you must change the system IP address. The NetScreen-10/100 ships from the factory with a default IP address of 192.168.1.1. To change this to an address on the same subnet as the other network devices to which the NetScreen-10/100 is connected, enter the following command, substituting your system IP address for the letters:

At the command line enter:

1. `set admin sys-ip <a.b.c.d>`
2. `save`

Changing the Administrator Login Name and Password

Because all NetScreen units come with the same default name and password, it is highly recommended that you change the default Admin Login name and Password.

Note: *The information in this guide has been widely published, and failure to change the defaults might expose your system to attack.*

At the command line enter:

1. set admin name <name>
2. set admin password <password>
3. save

Record the new Administration name and Password in a secure manner.



Warning

Make sure that you remember your password! If you forget it, you will have to return the unit to the factory for initialization. This feature has been implemented in this manner as an extra security measure.

Testing the Configuration

Use a Web browser to access an external Web site (for example, www.netscreen.com). You should be able to locate the site and access the available Web pages.

If you cannot access the Web site, check the following:

- The power, status and link lights on NetScreen-10/100 are illuminated.
- The LEDs on the host, hubs and router are illuminated.
- The Administrator's workstation IP address and subnet mask are correct.
- The workstation gateway points to the external router.
- The workstation has valid Domain Name Service (DNS) entry.

Interfaces and Operational Modes

7

This chapter describes the various physical, logical, and virtual interfaces and the three operational modes supported by NetScreen devices. The chapter is organized into the following sections:

- “Interfaces” on page 7-60
- “Transparent Mode” on page 7-62
- “Network Address Translation Mode” on page 7-71
- “Route Mode” on page 7-83

INTERFACES

All NetScreen devices have a Trusted interface and an Untrusted interface. The NetScreen-10 and -100 also have a DMZ interface. These are physical interfaces used for channeling network user traffic. Additionally, on each of the Virtual Systems supported by the NetScreen-1000 there can be one or more Sub interfaces linking a particular Virtual System to one or more virtual LANs (VLANs).

Other interfaces—some physical, some logical, and some virtual—provide exclusive channels for administrative traffic, or for communication among members in a redundant group.

Trusted Interface

The Trusted interface is a physical interface that leads to the network (usually the intranet or corporate network) protected by the NetScreen device.

Untrusted Interface

The Untrusted interface is a physical interface that leads to the network (usually the Internet) against which the NetScreen device defends. If the NetScreen device is in either NAT or Route mode (see “Interface Settings and Operational Modes” on page 7-62), the address for the Untrusted interface can be fixed (all NetScreen devices) or dynamically assigned (NetScreen-5 and -10) via Dynamic Host Control Protocol (DHCP). For the NetScreen-5, the address can also be provided by an ISP using Point-to-Point Protocol over Ethernet (PPPoE).

DMZ Interface

The DMZ interface is a physical interface that leads to a protected network to which access from the Untrusted side is typically granted. The DMZ, which stands for “demilitarized zone,” offers a separate and secure area on your network for receiving incoming traffic from unknown Untrusted sources—unlike the Trusted side, to which access from the Untrusted side is tightly restricted.

Web Management Interface

The Web Management interface is a logical interface that allows network administrators to manage the NetScreen device through an IP address and port number via a Web browser, such as Internet Explorer and Netscape Navigator.

Management Interface

On the NetScreen-1000, you can also manage the device through a separate physical interface—the Management (MGT) interface—moving administrative traffic outside the regular network user traffic. Separating administrative traffic from network user traffic greatly increases security and assures constant management bandwidth.

Sub Interface

On the NetScreen-1000, a Sub interface leads to a VLAN of a particular Virtual System. Each Virtual System can have its own Untrusted interface¹ and one or more Sub interfaces, each Sub interface leading to a different VLAN. In essence, a Sub interface leading to a VLAN is similar to the Trusted interface leading to a protected LAN only you can have more than one Sub interface.

HA Interface

You can link two or more NetScreen-1000 devices together to form a redundant group, or cluster, through the High Availability (HA) interface. In a redundant group, one unit acts as the Master, performing the network firewall functions, while the other units act as Slaves, basically waiting to take over the firewall functions should the Master unit fail. The HA interface is a physical port used exclusively for HA functions.

Virtual HA Interface

On the NetScreen-100, a Virtual High Availability (HA) interface provides the same functionality as the HA interface on the NetScreen-1000. However, because the NetScreen-100 does not have a separate physical port exclusively used for HA traffic, the Virtual HA interface must be bound to one of the physical ports—Trusted, Untrusted, or DMZ.

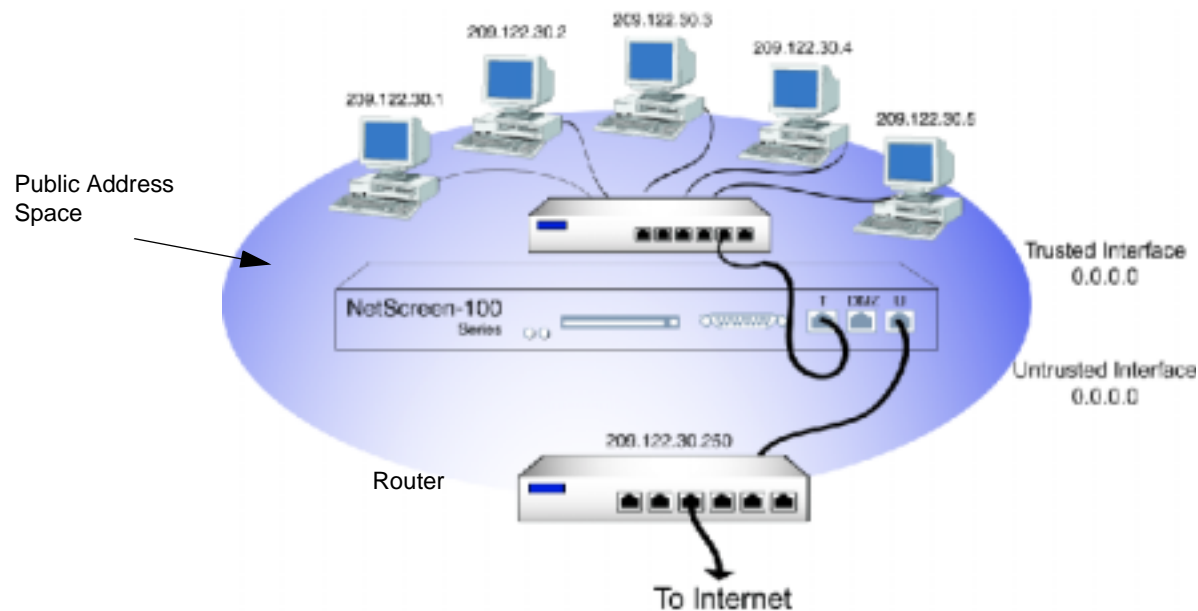
-
1. A Virtual System can have an Untrusted interface if one is defined for it. If an Untrusted interface is not defined for a Virtual System, the Virtual System uses the Untrusted interface at the root level of the NetScreen-1000.

INTERFACE SETTINGS AND OPERATIONAL MODES

The three operational modes are Transparent, Network Address Translation (NAT), and Route. The configuration of the Trusted, Untrusted, and (on the NetScreen-10 and -100) DMZ interfaces of a NetScreen device defines which mode is in operation. Each mode offers distinct advantages.

Transparent Mode

In Transparent mode, the NetScreen device filters packets traversing the firewall without modifying any of the source or destination information in the IP packet header. All interfaces behave as though they are part of the same network, with the NetScreen device acting much like a layer-2 switch or bridge. Because it does not translate addresses, the IP addresses on the protected network must be valid, routable addresses on the Untrusted network², which might be the Internet. In Transparent mode, the IP addresses for the Trusted and Untrusted interfaces are set at 0.0.0.0, making the presence of the NetScreen device invisible, or “transparent,” to users.



-
2. If the router on the Untrusted side performs NAT, then the addresses on the Trusted side can be private IP addresses.

Transparent mode is a convenient means for protecting Web servers, or any other kind of server that mainly receives traffic from Untrusted sources. Using Transparent mode offers the following benefits:

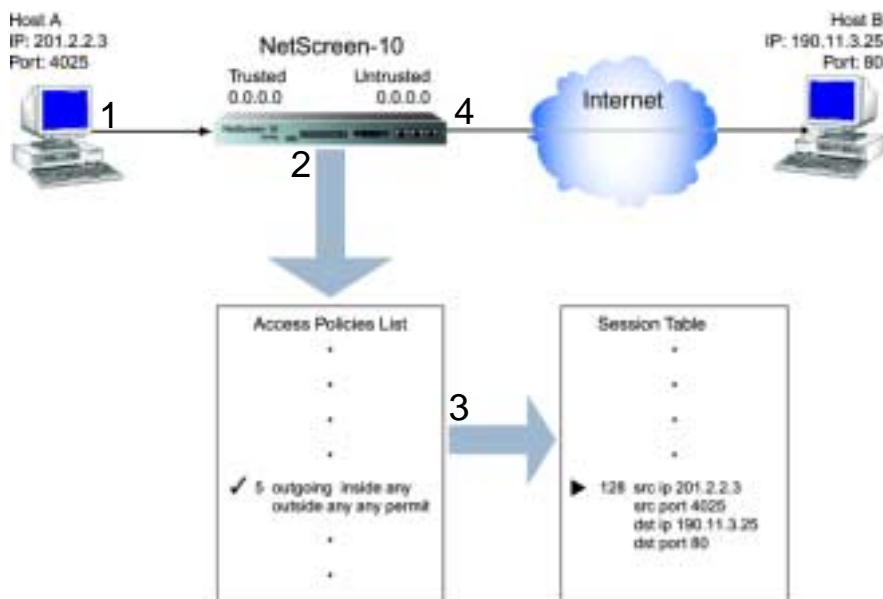
- No need to reconfigure the IP settings of routers or protected servers
- No need to create Mapped or Virtual IP addresses for incoming traffic to reach protected servers
- (NetScreen-100) Because port numbers are not translated when the NetScreen-100 is operating in Transparent mode, there can be twice as many concurrent outgoing sessions (from ~64,000 to ~128,000 sessions) than when it is operating in NAT mode. The maximum number of sessions—outgoing and incoming—remains the same (~128,000) in either mode, but the maximum number of outgoing sessions is not limited to 64,000 in Transparent mode because the limit imposed by port translation is not involved.

Packet Flow Sequence

The packet flow initiating a session from a host on the Trusted side of a NetScreen device in Transparent mode to a host on the Untrusted side progresses as follows:

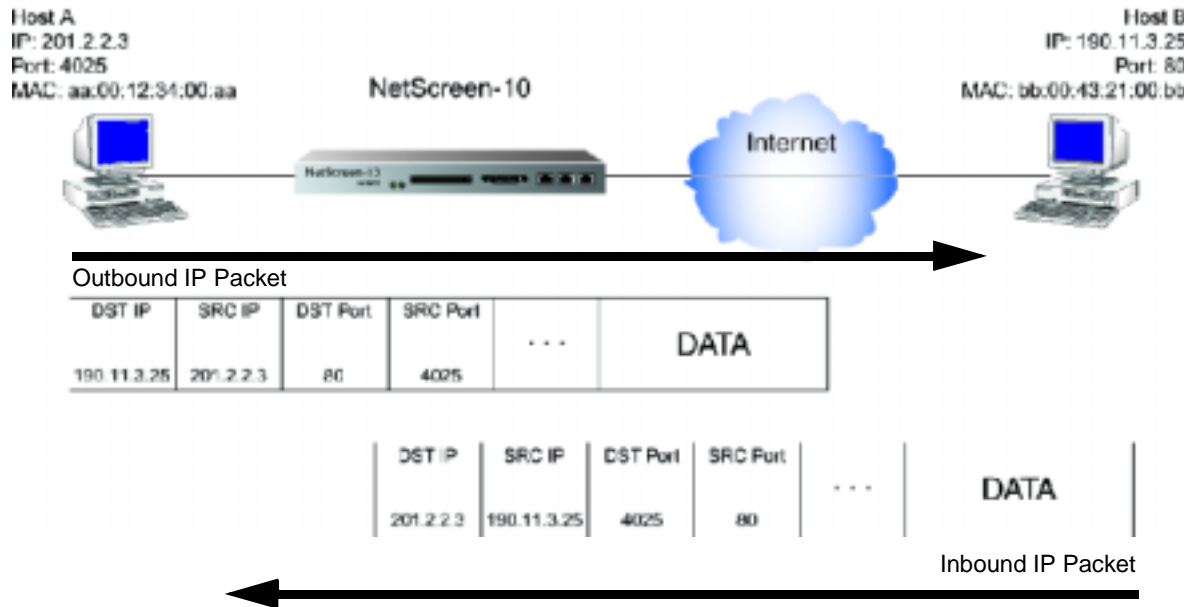
1. Host A, on the Trusted side of the NetScreen device, sends an IP packet to Host B, which is located on the Untrusted side.
2. The NetScreen device receives the IP packet and checks if there is an Access Policy allowing outbound TCP/IP traffic from Host A to Host B of the specified service.
3. If there is an Access Policy, the NetScreen device creates a new session in its session table.

4. The NetScreen device forwards the IP packet.



5. When the NetScreen device receives a responding IP packet from Host B, it inspects the address information in the packet header. If it matches the addressing information stored in the session table, it forwards the packet to Host A.

The connection is established. Host B knows Host A's actual IP address and port number.



Note: The flow sequence for any session requiring a packet to traverse the NetScreen firewall proceeds similarly; that is, when the NetScreen device receives a packet originating from any interface (Trusted, Untrusted, DMZ) and destined for any other interface, it performs the following three actions:

1. Checks the Access Policies list
 2. Finding permission for the passage granted, creates an entry in the session table
 3. Forwards the packet
6. When Hosts A and B close their connection, the NetScreen device removes the entry from its session table. Host B can no longer send traffic to Host A.

Interface Settings

For Transparent mode, define the following interface settings, where <a.b.c.d> and <e.f.g.h> represent numbers in an IP address, <A.B.C.D> represents the numbers in a subnet mask, and <number> represents the bandwidth size in kbps:

Trusted	IP: 0.0.0.0
	Subnet Mask: 0.0.0.0
	Default Gateway: 0.0.0.0
	Manage IP: <a.b.c.d>
	Traffic Bandwidth [*] : <number>
Untrusted	IP: 0.0.0.0
	Subnet Mask: 0.0.0.0
	Default Gateway: 0.0.0.0
	Manage IP: <a.b.c.d>
	Traffic Bandwidth [*] : <number>
DMZ (NetScreen-10 and -100)	IP: 0.0.0.0
	Subnet Mask: 0.0.0.0
	Default Gateway: 0.0.0.0
	Manage IP: <a.b.c.d>
	Traffic Bandwidth [*] : <number>
Web Management	System IP: <a.b.c.d>
	Port: <port_number> [†]
MGT (NetScreen-1000)	IP: <a.b.c.d>
	Subnet Mask: <A.B.C.D>
	Default Gateway: <e.f.g.h>

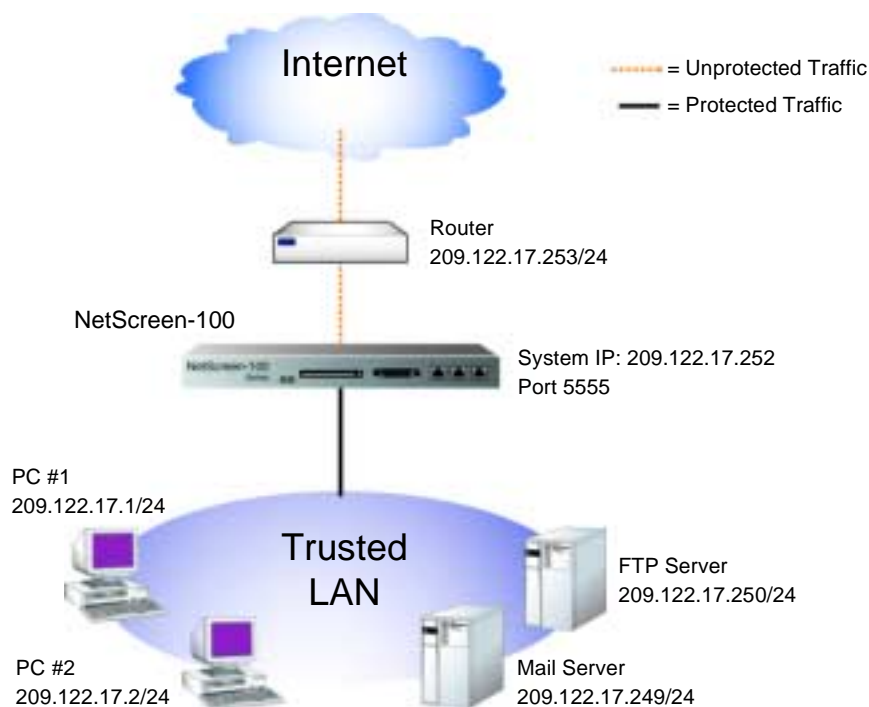
^{*} Optional setting for traffic shaping

[†] The default port number is 80. Changing this to any number between 1024 and 32,767 is advised for discouraging unauthorized access and modifications to the configuration.

Note: For managing the devices, you can use the System IP address, the Manage IP addresses, or the MGT IP address (NetScreen-1000).

Example: Transparent Mode

The following example illustrates a basic configuration for a single LAN protected by a NetScreen-100 in Transparent mode. Access Policies permit outgoing traffic for all four Trusted hosts, incoming mail for the mail server, and incoming FTP for the FTP server. The device is managed through its System IP address.



WebUI

1. Admin >> Settings: Enter the following, and then click **Apply**:
System IP Address: 209.122.17.252
2. Admin >> Web: Enter the following, and then click **Apply**:
Port: 5555³

3. When logging in to manage the device later, enter the following in the URL field of your Web browser: <http://172.16.10.40:5555>.

3. Interface >> Trusted >> Edit: Enter the following, and then click **Save**:
 - Inside IP: 0.0.0.0
 - Netmask: 0.0.0.0
 - Default Gateway: 0.0.0.0
 - Manage IP: 0.0.0.0
 - Traffic Bandwidth: 0
4. Interface >> Untrusted >> Edit: Enter the following, and then click **Save and Reset**:⁴
 - IP Address: 0.0.0.0
 - Netmask: 0.0.0.0
 - Default Gateway: 209.122.17.253
 - Manage IP: 0.0.0.0
 - Traffic Bandwidth: 0
5. (NetScreen-10 and -100) Interface >> DMZ >> Edit: Enter the following, and then click **Save**:
 - Inside IP: 0.0.0.0
 - Netmask: 0.0.0.0
 - Default Gateway: 0.0.0.0
 - Manage IP: 0.0.0.0
 - Traffic Bandwidth: 0
6. (NetScreen-1000) Interface >> MGT >> Edit: Enter the following, and then click **OK**:
 - MGT IP (NetScreen-1000): 0.0.0.0
 - Netmask: 0.0.0.0
 - Traffic Bandwidth: 0
7. Address >> Trusted >> New Address: Enter the following and then click **OK**:
 - Address Name: Mail Server
 - IP Address/Domain Name: 209.122.17.249
 - Netmask: 255.255.255.255

-
4. Through the CLI, you can schedule the NetScreen-5, -10, and -100 to reset at a time that is convenient for maintaining uninterrupted network operation: **set timer <mm>|<dd>|<yyyy> <hh:mm> action reset.**

8. Address >> Trusted >> New Address: Enter the following and then click **OK**:
 - Address Name: FTP Server
 - IP Address/Domain Name: 209.122.17.250
 - Netmask: 255.255.255.255
9. Policy >> Outgoing >> New Policy: Enter the following and then click **OK**:
 - Source Address: Inside Any
 - Destination Address: Outside Any
 - Service: Any
 - Action: Permit
10. Policy >> Incoming >> New Policy: Enter the following and then click **OK**:
 - Source Address: Outside Any
 - Destination Address: Mail Server
 - Service: Mail
 - Action: Permit
11. Policy >> Incoming >> New Policy: Enter the following and then click **OK**:
 - Source Address: Outside Any
 - Destination Address: FTP Server
 - Service: FTP
 - Action: Permit

Note: Because PC #1 and PC #2 are not specified in an Access Policy, they do not need to be added to the Trusted Address Book. The term "Inside Any" applies to any device connected to the Trusted interface.

CLI

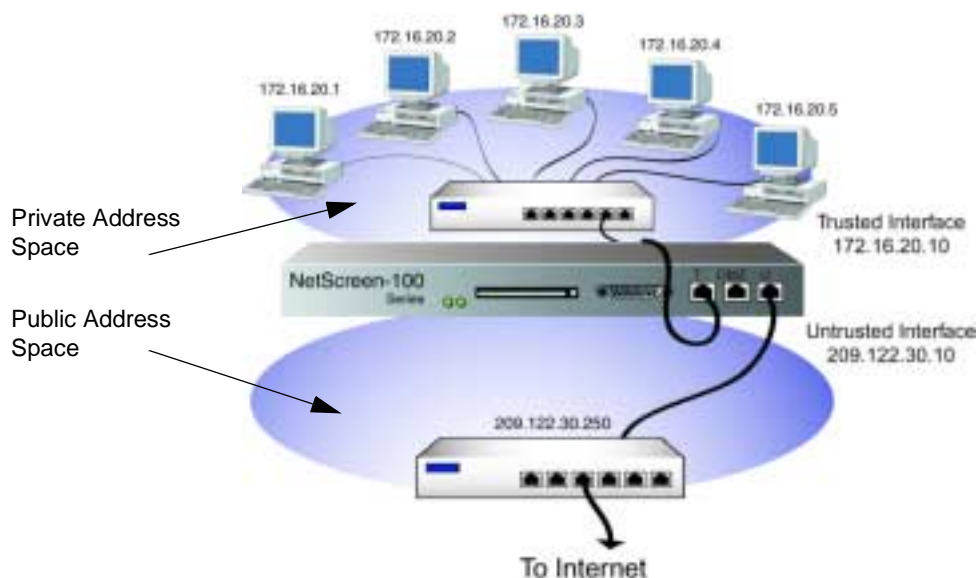
1. set admin sys-ip 209.122.17.252
2. set admin port 5555⁵
3. set interface trust ip 0.0.0.0 0.0.0.0
4. set interface trust gateway 0.0.0.0

-
5. When logging in to manage the device later, enter the following in the URL field of your Web browser: `http://172.16.10.40:5555`.

5. set interface untrust ip 0.0.0.0 0.0.0.0
6. set interface untrust gateway 209.122.17.253
7. (NetScreen-1000) set interface mgt ip 0.0.0.0 0.0.0.0
8. set address trust Mail_Server 209.122.17.249 255.255.255.255
9. set address trust FTP_Server 209.122.17.250 255.255.255.255
10. set policy outgoing "inside any" "outside any" any permit
11. set policy incoming "outside any" 209.122.17.250 255.255.255.255 mail
permit
12. set policy incoming "outside any" 209.122.17.249 255.255.255.255 ftp permit
13. save

Network Address Translation Mode

When in Network Address Translation (NAT) mode, the NetScreen device, acting like a layer-3 switch (or router), translates two components in the header of an outgoing IP packet traversing the firewall from the Trusted side: its source IP address and source port number. The NetScreen device replaces the source IP address of the host that sent the packet with the IP address of the Untrusted port⁶ of the NetScreen device. Also, it replaces the source port number with another random port number generated by the NetScreen device.



When the reply packet arrives at the NetScreen device, the device translates two components in the IP header of the incoming packet: the destination address and port number, which are translated back to the original numbers. The packet is then forwarded to its destination.

NAT adds a level of security not provided in Transparent mode: The addresses of hosts connected to the Trusted port are never exposed to the Untrusted or DMZ network.

-
6. If the outbound traffic is destined for the DMZ (on the NetScreen-10 and -100), then the source IP address is translated to that of the DMZ port.

Also, NAT preserves the use of Internet-routable IP addresses. With only one public, Internet-routable IP address—that of the Untrusted interface—the Trusted LAN can have a vast number of hosts with private IP addresses. The following IP address ranges are reserved for private IP networks and must not get routed on the Internet:

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

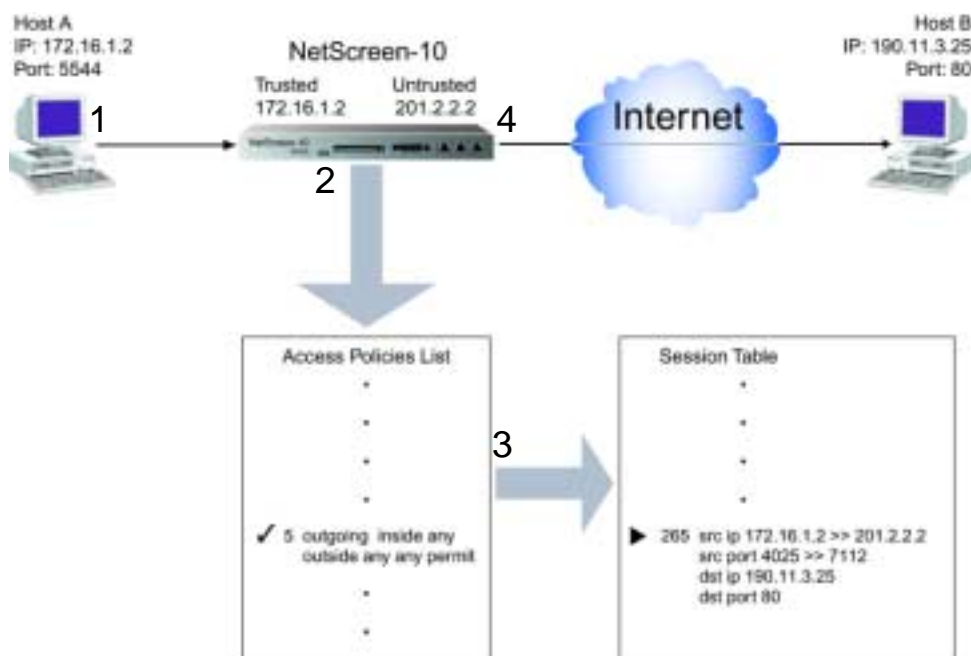
A host on the Trusted LAN can initiate traffic to the Internet, if an Access Policy allows it Internet access, but it cannot receive traffic initiated outside the firewall unless a Mapped IP or Virtual IP is set up for it.

Packet Flow Sequence: Trusted >> Untrusted

The packet flow initiating a session from a host on the Trusted side of a NetScreen device in NAT mode to a host on the Untrusted side progresses as follows:

1. Host A, on the Trusted side of the NetScreen device, sends an IP packet to Host B, which is located on the Untrusted side.
2. The NetScreen device receives the IP packet and checks if there is an Access Policy allowing outbound TCP/IP traffic from Host A to Host B with the specified service.
3. If there is such an Access Policy, the NetScreen device creates a new session in its session table and changes the source IP address and source port number on the outbound IP packet.

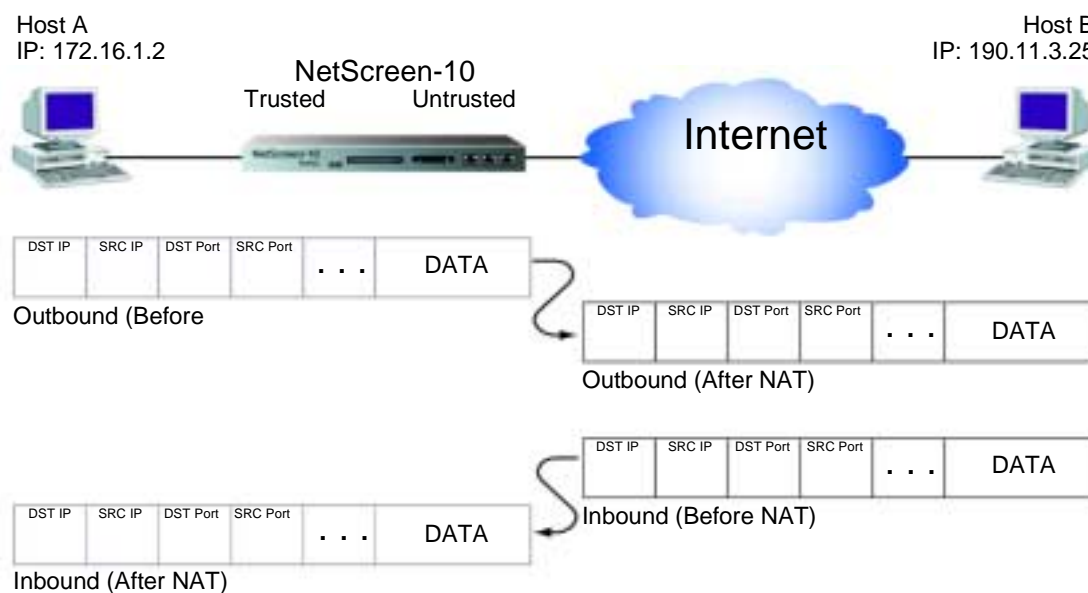
4. The NetScreen device forwards the modified IP packet, its true source IP address and port number unexposed.



5. When the NetScreen device receives a responding IP packet from Host B, it inspects the address information in the packet header. If it matches the information stored in the session table, it forwards the packet to Host A, converting the translated IP address and port number back to the originals. (This packet filtering method is called “stateful inspection.”)

Note: The source port number of an outbound packet is the key to successfully directing an inbound packet to its destination. Because the source IP address for an outbound IP packet is translated to the IP address of the Untrusted interface, the distinguishing factor in the header of an inbound IP packet is its destination port number, which is unique to each inbound IP packet.

The connection is established. Host B does not know Host A's actual IP address or port number.



Note: The NetScreen-10 and -100 can also perform NAT on traffic going from the Trusted interface to the DMZ.

Packet Flow Sequence: Untrusted >> Trusted

For traffic initiated on the Untrusted side of a NetScreen device in NAT mode to reach the Trusted side, you must first create one of the following:

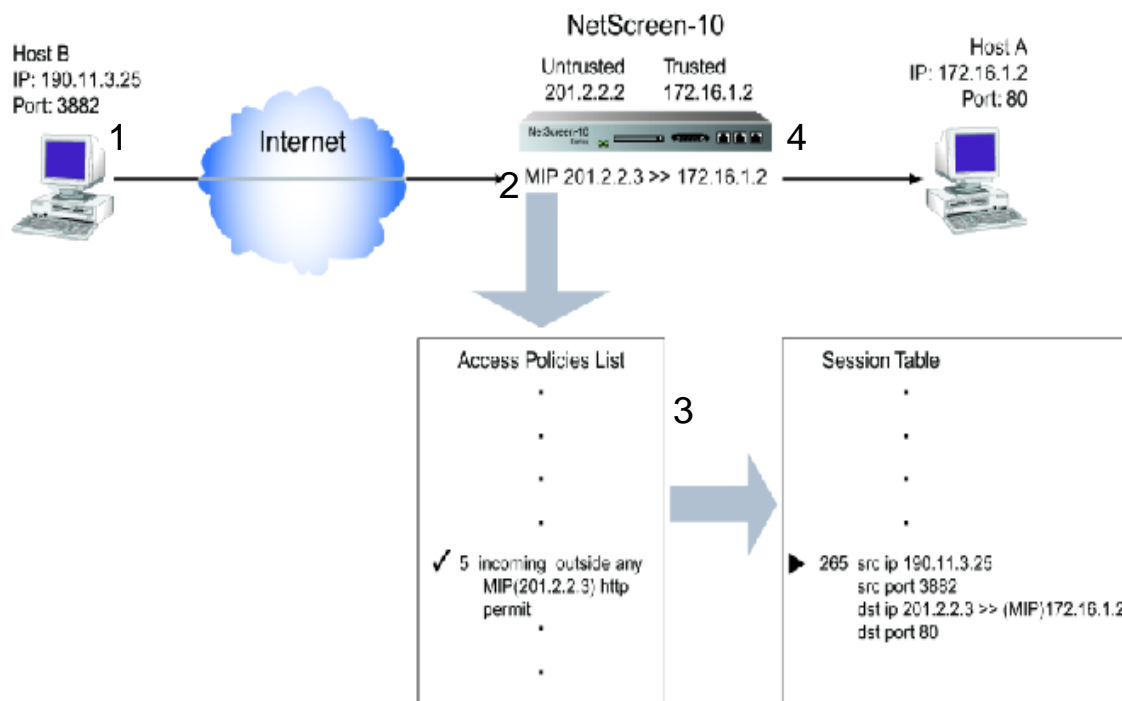
- A Mapped IP (MIP), mapping inbound traffic from a public IP address to a private IP address
- A Virtual IP (VIP), mapping inbound traffic from a public IP address via the port number of the incoming service to one of several possible private IP addresses
- A VPN tunnel

Mapped IP

The packet flow for a session initiating on the Untrusted side of a NetScreen device in NAT mode to a host on the Trusted side using an MIP progresses as follows:

1. Host B, on the Untrusted side of the NetScreen device, sends an IP packet to the public IP address that is mapped to the private IP address for Host A, which is located on the Trusted side.
2. The NetScreen device receives the inbound packet and checks if there is an Access Policy allowing inbound TCP/IP traffic to the MIP.
3. If there is an Access Policy, the NetScreen device creates a new session in its session table and changes the destination IP address on the inbound packet, mapping it to the private address.
4. The NetScreen device forwards the packet to Host A.

The connection is established. Host B does not know Host A's actual IP address.

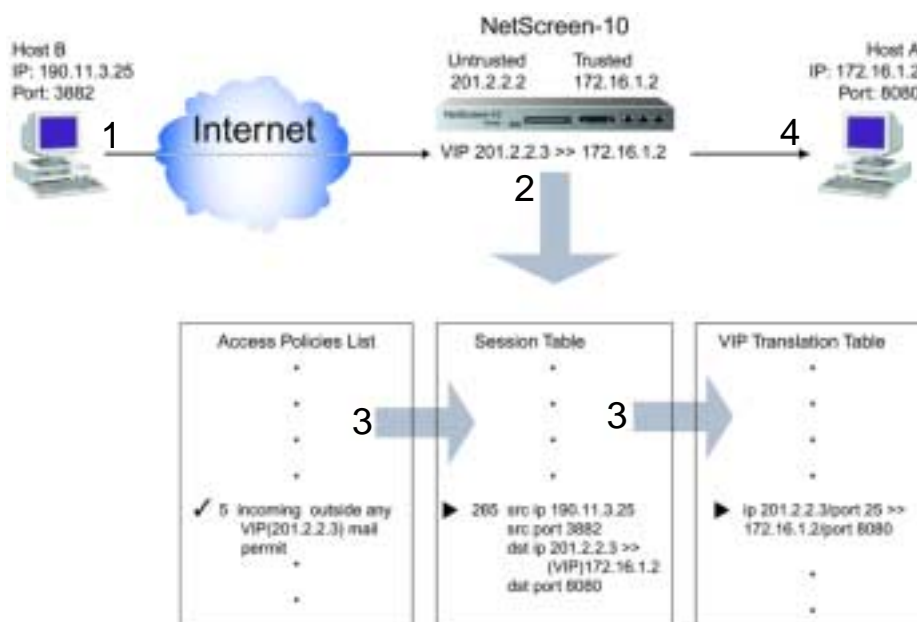


Virtual IP

The packet flow for a session initiating on the Untrusted side of a NetScreen device in NAT mode to a host on the Trusted side using a VIP progresses as follows:

1. Host B, on the Untrusted side of the NetScreen device, sends an IP packet to a public IP address in the same subnet as the Untrusted interface. (That address has been configured to route traffic to any one of several IP addresses on the Trusted side, depending on the port number carried by the incoming packet.)
2. The NetScreen device receives the inbound packet and checks if there is an Access Policy allowing inbound traffic to the VIP.
3. If there is an Access Policy, the NetScreen device creates a new session in its session table and, referring to its VIP translation table, changes the destination IP address and destination port number on the inbound packet to map it to the private IP address and port number.
4. The NetScreen device forwards the packet to Host A.

The connection is established. Host B does not know Host A's actual IP address or port number.



Interface Settings

For NAT mode, define the following interface settings, where <a.b.c.d>, <e.f.g.h>, and <i.j.k.l> represent numbers in an IP address, <A.B.C.D> represents the numbers in a subnet mask, and <number> represents the bandwidth size in kbps:

Trusted	IP: <a.b.c.d> Subnet Mask: <A.B.C.D> Default Gateway: <e.f.g.h> Manage IP: <i.j.k.l> Traffic Bandwidth [*] : <number> NAT: (select) [†]
Untrusted	IP: <a.b.c.d> Subnet Mask: <A.B.C.D> Default Gateway: <e.f.g.h> Manage IP: <i.j.k.l> Traffic Bandwidth [*] : <number>
DMZ (NetScreen-10 and -100)	IP: <a.b.c.d> Subnet Mask: <A.B.C.D> Default Gateway: <e.f.g.h> Manage IP: <i.j.k.l> Traffic Bandwidth [*] : <number>
Web Management	System IP: <a.b.c.d> Port: <port_number> [‡]
MGT (NetScreen-1000)	IP: <a.b.c.d> Subnet Mask: <A.B.C.D> Default Gateway: <e.f.g.h> Traffic Bandwidth [*] : <number>

^{*} Optional setting for traffic shaping

[†] Selecting **NAT** for the Trusted interface defines the mode as NAT. Selecting **Route** defines the mode as Route.

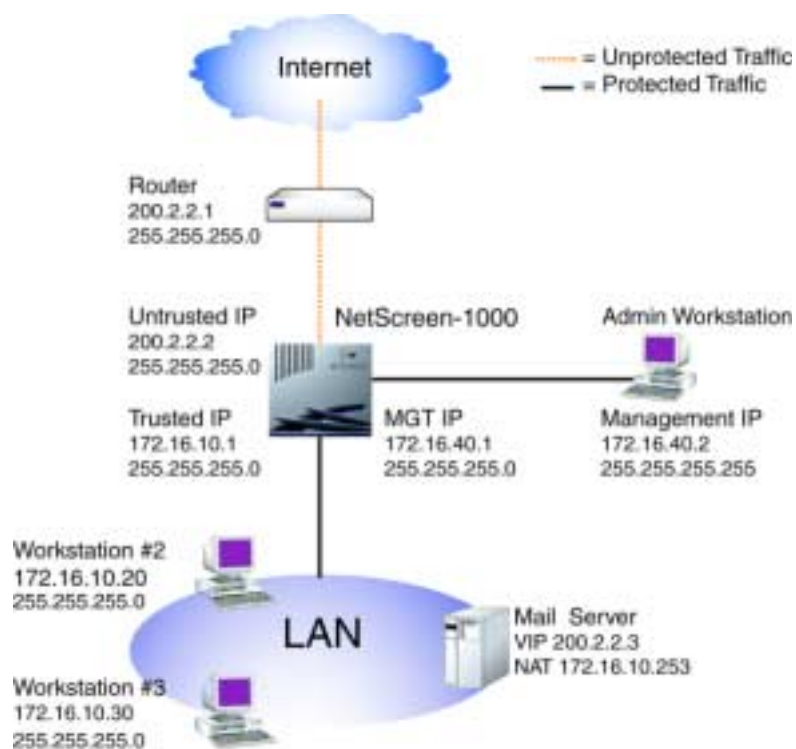
[‡] The default port number is 80. Changing this to any number between 1024 and 32,767 is advised for discouraging unauthorized access and modifications to the configuration.

Note: In NAT mode, you can manage a NetScreen device from any interface—and from multiple interfaces—using the System IP address, interface IP addresses, Manage IP addresses, or the MGT IP address (NetScreen-1000).

Example: NAT Mode

The following example illustrates a simple configuration for a LAN with a single Trusted subnet. The LAN is protected by a NetScreen-1000 in NAT mode. Access Policies permit outgoing traffic for all three Trusted hosts and incoming mail for the mail server. The incoming mail is routed to the mail server through a Virtual IP address. The device is managed through its MGT IP address.

Note: Compare this example with that for Route mode on page 7-85.



WebUI

1. Interface >> Trusted >> Edit: Enter the following, and then click **Save**:

IP Address: 172.16.10.1
 Netmask: 255.255.255.0
 Default Gateway: 0.0.0.0
 Manage IP: 0.0.0.0

Traffic Bandwidth: 0

NAT:⁷ (select)

2. Interface >> Untrusted >> Edit: Enter the following, and then click **Save**:

IP Address:⁸ 200.2.2.2

Netmask: 255.255.255.0

Default Gateway: 200.2.2.1

Manage IP: 0.0.0.0

Traffic Bandwidth: 0

3. (NetScreen-10/100) Interface >> DMZ >> Edit: Enter the following, and then click **Save and Reset**:⁹

DMZ IP (NetScreen-10/100): 0.0.0.0

Netmask: 0.0.0.0

Default Gateway: 0.0.0.0

Manage IP: 0.0.0.0

Traffic Bandwidth: 0

4. (NetScreen-1000) Interface >> MGT >> Edit: Enter the following, and then click **OK**:

IP Address: 172.16.40.1

Netmask: 255.255.255.0

Traffic Bandwidth: 0

5. Admin >> Admin >> New Management Client IP: Enter the following, and then click **OK**:

IP Address: 172.16.40.2

Netmask: 255.255.255.255

-
7. Selecting **NAT** determines that the NetScreen device performs NAT on traffic to and from the Trusted side.
8. If the Untrusted IP address on the NetScreen-5 and -10 is dynamically assigned by an ISP, leave the IP address and subnet mask fields empty and select DHCP. For the NetScreen-5, if the ISP is using Point-to-Point Protocol over Ethernet, select PPPoE and enter the name and password.
9. Through the CLI, you can schedule the NetScreen-5, -10, and -100 to reset at a time that is convenient for maintaining uninterrupted network operation: **set timer <mm>|<dd>|<yyyy>**
<hh:mm> action reset.

6. Virtual IP >> Virtual IP 1 >> [Click here to configure](#): Enter the following, and then click **OK**:

Virtual IP Address: 200.2.2.3

7. Virtual IP >> New Services: Enter the following, and then click **OK**:

Virtual Port: 25

Service: Mail

Map to IP: 172.16.10.253

8. Policy >> Outgoing >> New Policy: Enter the following, and then click **OK**:

Source Address: Inside Any

Destination Address: Outside Any

Service: Any

Action: Permit

9. Policy >> Incoming >> New Policy: Enter the following and then click **OK**:

Source Address: Outside Any

Destination Address: VIP(200.2.2.3)

Service: Mail

Action: Permit

CLI

1. set admin sys-ip 0.0.0.0
2. set interface trust ip 172.16.10.1 255.255.255.0
3. set interface trust NAT
4. set interface trust gateway 0.0.0.0
5. set interface untrust ip 200.2.2.2 255.255.255.0
6. set interface untrust gateway 200.2.2.1

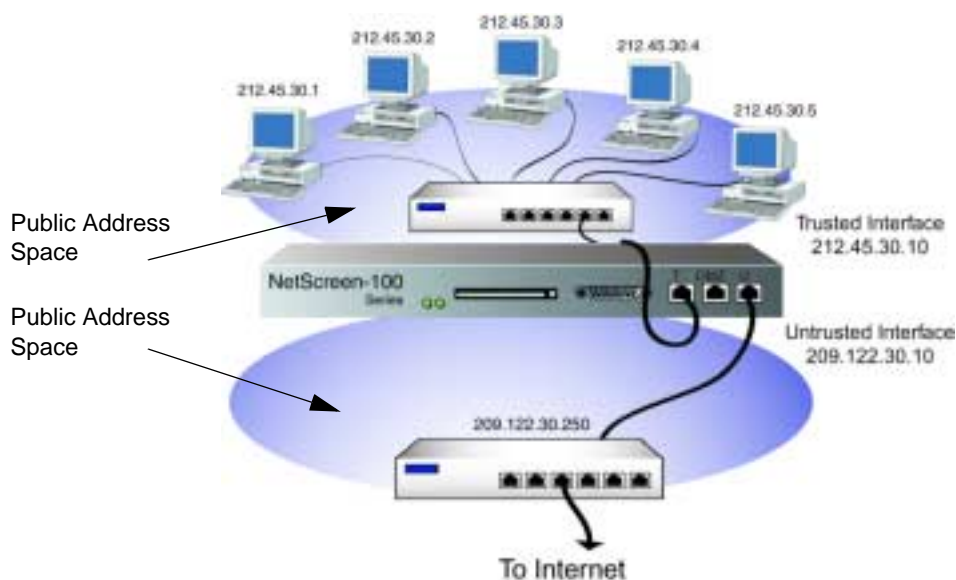
DHCP Note: For the NetScreen-5 and -10, if the ISP dynamically assigns the Untrusted IP address, use the following command: **set interface untrust dhcp**

PPPoE Note: For the NetScreen-5, if the ISP uses PPPoE, use the **set pppoe** and **exec pppoe** commands. For more information, see the NetScreen CLI Reference Guide.

7. (NetScreen-10/100) set interface dmz ip 0.0.0.0 0.0.0.0
8. (NetScreen-1000) set interface mgt ip 172.16.40.1 255.255.255.0
9. set admin mng-ip 172.16.40.2 255.255.255.255
10. set vip 200.2.2.3 25 mail 172.16.10.253
11. set policy outgoing "inside any" "outside any" any permit
12. set policy incoming "outside any" "vip 200.2.2.3" mail permit
13. save

Route Mode

In Route mode, the NetScreen device routes traffic between different interfaces without performing NAT; that is, the source address and port number in the IP packet header remain unchanged as it traverses the NetScreen device. Unlike NAT, the hosts on the Trusted side must have public IP addresses, and you do not need to establish Mapped and Virtual IP addresses to allow sessions initiated on the Untrusted side to reach hosts on the Trusted side. Unlike Transparent mode, the Trusted and Untrusted interfaces are on different subnets.



With the NetScreen-10 or -100 operating in Route mode (or Transparent mode), you do not need to set up Virtual or Mapped IPs for servers in the DMZ; the servers only require Internet-routable IP addresses. Using Route mode for the Trusted side likewise eliminates the need to create Virtual or Mapped IPs.

Interface Settings

For Route mode, define the following interface settings, where <a.b.c.d> and <e.f.g.h> represents numbers in an IP address, <A.B.C.D> represents the numbers in a subnet mask, and <number> represents the bandwidth size in kbps:

Trusted	IP: <a.b.c.d> Subnet Mask: <A.B.C.D> Default Gateway: <e.f.g.h> Manage IP: <i.j.k.l> Traffic Bandwidth [*] : <number> Route: (select) [†]
Untrusted	IP: <a.b.c.d> Subnet Mask: <A.B.C.D> Default Gateway: <e.f.g.h> Manage IP: <i.j.k.l> Traffic Bandwidth [*] : <number>
DMZ (NetScreen-10 and -100)	IP: <a.b.c.d> Subnet Mask: <A.B.C.D> Default Gateway: <e.f.g.h> Manage IP: <i.j.k.l> Traffic Bandwidth [*] : <number>
Web Management	System IP: <a.b.c.d> Port: <port_number> [‡]
MGT (NetScreen-1000)	IP: <a.b.c.d> Subnet Mask: <A.B.C.D> Default Gateway: <e.f.g.h> Traffic Bandwidth [†] : <number>

^{*} Optional setting for traffic shaping

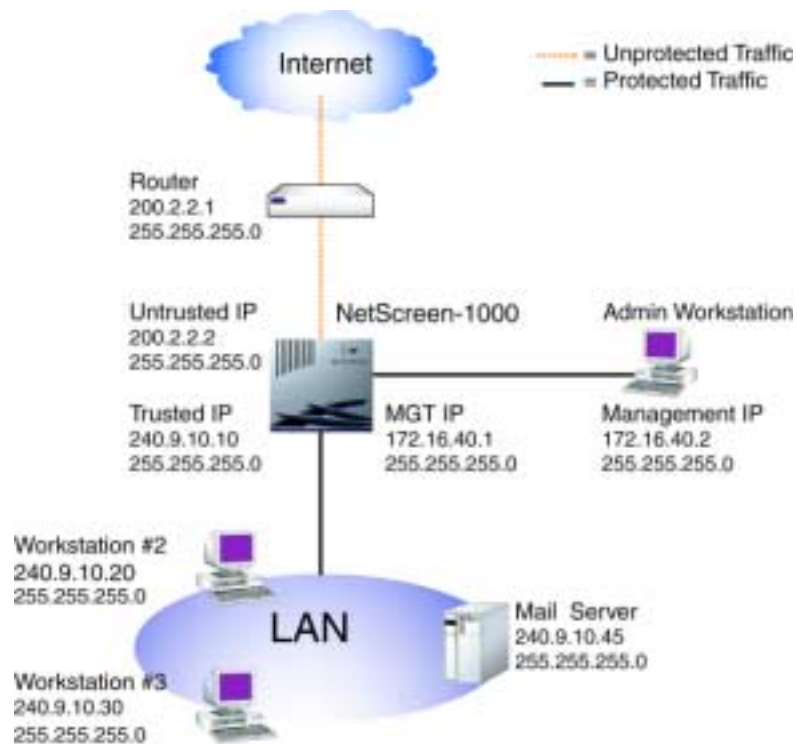
[†] Selecting **Route** for the Trusted interface defines the mode as Route. Selecting **NAT** defines the mode as NAT.

[‡] The default port number is 80. Changing this to any number between 1024 and 32,767 is advised for discouraging unauthorized access and modifications to the configuration.

Note: In Route mode, you can manage a NetScreen device from any interface—and from multiple interfaces—using the System IP address, Manage IP addresses, or interface IP addresses.

Example: Route Mode

In the previous example for NAT mode on page 7-79, the hosts on the protected LAN have private IP addresses and a Mapped IP for the mail server. In the following example of the same network protected by a NetScreen-1000 operating in Route mode, note that the hosts have public IP addresses and that a MIP is unnecessary for the mail server. The device is managed through its MGT IP address.



WebUI

1. Interface >> Trusted >> Edit: Enter the following, and then click **Save**:

IP Address: 240.9.10.10
Netmask: 255.255.255.0
Default Gateway: 0.0.0.0
Manage IP: 0.0.0.0
Traffic Bandwidth: 0
Route:¹⁰ (select)

2. Interface >> Untrusted >> Edit: Enter the following, and then click **Save**:

IP Address:¹¹ 200.2.2.2
Netmask: 255.255.255.0
Default Gateway: 200.2.2.1
Manage IP: 0.0.0.0
Traffic Bandwidth: 0

3. Interface >> DMZ (NetScreen-10/100) >> Edit: Enter the following, and then click **Save**:

DMZ IP: 0.0.0.0
Netmask: 0.0.0.0
Default Gateway: 0.0.0.0
Manage IP: 0.0.0.0
Traffic Bandwidth: 0

4. (NetScreen-1000) Interface >> MGT >> Edit: Enter the following, and then click **Save and Reset**:

MGT IP: 172.16.40.1
Netmask 255.255.255.0

-
10. Selecting **Route** determines that the NetScreen device operates in Route mode, without performing NAT on traffic to or from the Trusted side.
 11. If the Untrusted IP address on the NetScreen-5 and -10 is dynamically assigned by an ISP, leave the IP address and subnet mask fields empty and select DHCP. For the NetScreen-5, if the ISP is using Point-to-Point Protocol over Ethernet, select PPPoE and enter the name and password.

5. Admin >> Admin: Enter the following, and then click **Apply**:
 - Management Client IP: 172.16.40.2
 - Netmask: 255.255.255.255
6. Address >> Trusted >> New Address: Enter the following and then click **OK**:
 - Address Name: Mail Server
 - IP Address/Domain Name: 240.9.10.45
 - Netmask: 255.255.255.255
7. Policy >> Outgoing >> New Policy: Enter the following and then click **OK**:
 - Source Address: Inside Any
 - Destination Address: Outside Any
 - Service: Any
 - Action: Permit
8. Policy >> Incoming >> New Policy: Enter the following and then click **OK**:
 - Source Address: Outside Any
 - Destination Address: Mail Server
 - Service: Mail
 - Action: Permit

CLI

1. set admin sys-ip 0.0.0.0
2. set interface trust ip 240.9.10.10 255.255.255.0
3. unset interface trust NAT¹²
4. set interface trust gateway 0.0.0.0
5. set interface untrust ip 200.2.2.2 255.255.255.0
6. set interface untrust gateway 200.2.2.1
7. (NetScreen-10/100) set interface dmz ip 0.0.0.0 0.0.0.0
8. (NetScreen-1000) set interface mgt ip 172.16.40.1 255.255.255.0
9. set admin mng-ip 172.16.40.2 255.255.255.255
10. set address trust mail_server 240.9.10.45 255.255.255.0
11. set policy outgoing "inside any" "outside any" any permit
12. set policy incoming "outside any" mail_server mail permit

12. The **unset interface trust NAT** command determines that the NetScreen device operates in Route mode.

System Parameters

8

This chapter focusses on the concepts involved in establishing system parameters affecting the following areas of a NetScreen security appliance:

- “Firewall Protection” on page 8-90
- “Route Table Configuration” on page 8-99
- “Domain Name System Support” on page 8-104
- “DHCP” on page 8-107 (NetScreen-5 and -10)
- “PPPoE” on page 8-113 (NetScreen-5)
- “URL Filtering Configuration” on page 8-117
- “Downloading/Uploading Settings and Software” on page 8-119

FIREWALL PROTECTION

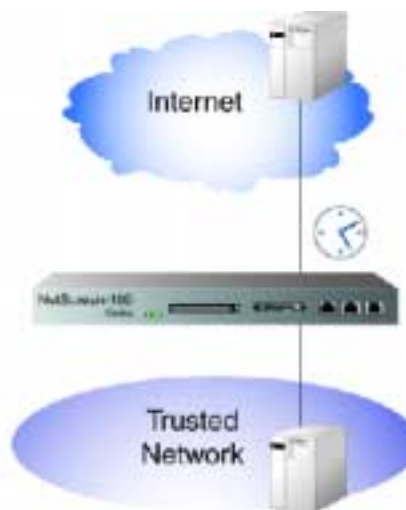
NetScreen firewalls secure a network by inspecting, and then allowing or denying, all connection attempts that require crossing the Untrusted, Trusted, and DMZ (NetScreen-10 and -100) interfaces.

By default, a NetScreen firewall denies all traffic in all directions.¹ Through the creation of Access Policies, you can then control the traffic flow across an interface by defining the kinds of traffic permitted to pass from specified sources to specified destinations at scheduled times. At the broadest level, you can allow all kinds of traffic from any Trusted source to any Untrusted destination without any scheduling restrictions. At the narrowest level, you can create an Access Policy that allows only one kind of traffic between a specified server on the Trusted side and a specified client on the Untrusted side during a scheduled period of time. In the first case, the firewall keeps all Internet traffic out of the protected network while providing all Trusted hosts access to the Internet. In the second case, you completely separate the two sides of the firewall except for a single hole connecting a point on the Trusted side to another point on the Untrusted side.

Broadly defined Internet Access: Any service from any point on the Trusted side to any point on the Untrusted side at any time



Narrowly defined Internet Access: SMTP service from a mail server on the Trusted side to a mail server on the Untrusted side from 5:00 AM to 7:00 PM



-
1. The NetScreen-5 default Access Policy denies all inbound traffic but allows all outbound traffic.

To secure all connection attempts originating from Trusted hosts, NetScreen devices use a dynamic packet filtering method known as stateful inspection. Using this method, the NetScreen device notes various components in an outgoing TCP packet header— source and destination IP addresses, source and destination port numbers, and packet sequence numbers—and maintains the state of each TCP session traversing the firewall. (The NetScreen device also modifies session states based on changing elements such as dynamic port changes or session termination.) When a responding TCP packet arrives, the NetScreen device compares the information reported in its header with the state of its associated session stored in the inspection table. If they match, the incoming packet is allowed to pass the firewall. If the two do not match, the packet is dropped.

To protect against attacks from the Untrusted interface, you can enable defense mechanisms that can detect and deflect over a dozen common network attacks:

- **SYN Flood:** A SYN flood attack occurs when a network becomes so overwhelmed by SYN packets initiating uncompletable connection requests that it can no longer process legitimate connection requests, resulting in a denial of service (DoS).
- **ICMP Flood:** An ICMP flood occurs when ICMP pings overload a system with so many echo requests that the system expends all its resources responding until it can no longer process valid network traffic. After enabling the ICMP flood protection feature, you can set a threshold that once exceeded invokes the ICMP flood attack protection feature. (The default threshold value is 1000 packets per second.) If the threshold is exceeded, the NetScreen device ignores further ICMP echo requests for the remainder of that second.
- **UDP Flood:** Similar to the ICMP flood, UDP flooding occurs when UDP packets are sent with the purpose of slowing down the system to the point that it can no longer handle valid connections. After enabling the UDP flood protection feature, you can set a threshold that once exceeded invokes the UDP flood attack protection feature. (The default threshold value is 1000 packets per second.) If the threshold is exceeded, the NetScreen device ignores further UDP packets for the remainder of that second.
- **Ping of Death:** The TCP/IP specification requires a specific packet size for datagram transmission. Many ping implementations allow the user to specify a larger packet size if desired. A grossly oversized ICMP packet can trigger a range of adverse system reactions such as denial of service (DoS), crashing, freezing, and rebooting. If you enable the NetScreen device to do so, it can detect and reject such oversized and irregular packet sizes.

- **IP Spoofing:** Spoofing attacks occur when an attacker attempts to bypass the firewall security by imitating a valid client IP address. When IP Spoofing defense is enabled, the NetScreen device guards against this attack by analyzing the IP addresses with its own route table. If the IP address is not in the route table, traffic from that source is not allowed to communicate through the NetScreen device and any packets from that source are dropped.
- **Port Scan Attack:** Port scan attacks occur when packets are sent with different port numbers with the purpose of scanning the available services in hopes that one port will respond. The NetScreen device internally logs the number of different ports scanned from one remote source. If a remote host scans 10 ports in 0.3 seconds, NetScreen flags this as a port scan attack, and drops the connection.
- **Land Attack:** Combining a SYN attack with IP spoofing, a Land attack occurs when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address. The receiving system responds by sending the SYN-ACK packet to itself, creating an empty connection that lasts until the idle timeout value is reached. Flooding a system with such empty connections can overwhelm the system, causing a DoS. By combining elements of the SYN flood defense and IP Spoofing protection, the NetScreen device blocks any attempts of this nature.
- **Tear Drop Attack:** Tear Drop attacks exploit the reassembly of fragmented IP packets. In the IP header, one of the options is offset. When the sum of the offset and size of one fragmented packet differ from that of the next fragmented packet, the packets overlap, and the server attempting to reassemble the packet can crash. If the NetScreen sees this discrepancy in a fragmented packet, it drops it.
- **Filter IP Source Route Option:** IP header information has an option to contain routing information that may specify a different source than the header source. Enable this option to block all IP traffic that employs the Source Route Option. Source Route Option can allow an attacker to enter a network with a false IP address and have data sent back to his real address.
- **Address Sweep Attack:** Similar to a port scan attack, an address sweep attack occurs when an attacker sends ICMP echo requests (or pings) to different destination addresses hoping that one will reply, thus uncovering an address to target. The NetScreen device internally logs the number of different addresses being pinged from one remote source. If a remote host pings 10 addresses in 0.3 seconds, NetScreen flags this as an address sweep attack, and drops the connection.

- **Block Java/ActiveX/ZIP/EXE Component:** Malicious Java or ActiveX components can be hidden in Web pages. When downloaded, these applets install a Trojan horse² on your computer. Similarly, Trojan horses can be hidden in compressed files such as .zip, .gzip, and .tar, and executable (.exe) files. Enabling this feature blocks all embedded Java and ActiveX applets from Web pages and strips attached .zip, .gzip, .tar and .exe files from e-mail.
- **Winnuke Attack:** WinNuke is a pervasive application, whose sole intent is to cause any computer on the Internet running Windows to crash. WinNuke sends out-of-band (OOB) data—usually to NetBIOS port 139—to a host with an established connection, and introduces a NetBIOS fragment overlap, which causes many machines to crash. After rebooting, the following message appears, indicating that an attack has occurred:

An exception OE has occurred at 0028:[address] in VxD MSTCP(01) + 000041AE. This was called from 0028:[address] in VxD NDIS(01) + 00008660. It may be possible to continue normally.

- Press any key to attempt to continue.
- Press CTRL+ALT+DEL to restart your computer. You will lose any unsaved information in all applications.
- Press any key to continue.

If you enable the WinNuke attack defense mechanism on a NetScreen device, it scans any incoming Microsoft NetBIOS Session Service (port139) packets. If the NetScreen device observes that TCP URG code bit is set on one of those packets, it inspects the offset, removes the fragmented overlap, and corrects the offset as necessary to prevent an OOB error. The modified packet is then passed, and a WinNuke attack log entry is created in the Alarm Event log.

To enable the firewall features designed to counter the network attacks listed above, do either of the following:

WebUI

Configure >> General: Select the features you want enabled (and set threshold values for SYN Attack, ICMP Flood, and UDP Flood), and then click **Apply**:

Detect SYN Attack (and threshold value)

Detect ICMP Flood (and threshold value)

2. A Trojan horse is a program that when surreptitiously installed on a computer provides direct control of the computer to an outside party.

Detect UDP Flood (and threshold value)
Detect Ping of Death Attack
Detect IP Spoofing Attack
Detect Port Scan Attack
Detect Land Attack
Default Packet Deny
Detect Tear Drop Attack
Filter IP Source Route Option
Detect Address Sweep Attack
Block Java/ActiveX/ZIP/EXE Component

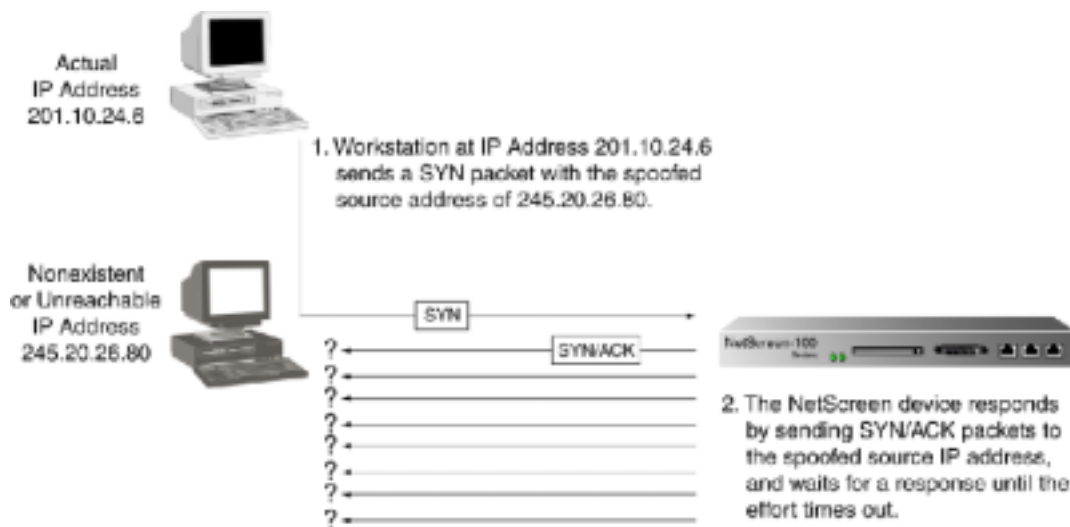
CLI

```
set firewall {applet | bypass-others-ipsec | default-deny | icmp-flood [threshold  
<number>] | ip-spoofing | ip-sweep [threshold <microseconds>] | land | log-self |  
ping-of-death | port-scan [threshold <number>] | src-route | syn-flood  
[alarm-threshold <number> | queue-size <number> | timeout <number>] |  
tear-drop | udp-flood [threshold <number>] | winnuke}
```

Note: See the *NetScreen CLI Reference Guide* for an explanation of the **set firewall** arguments, plus examples and related commands.

Example: SYN Flood Attack

A TCP connection is established with a triple exchange of packets known as a three-way handshake: A sends a SYN packet to B; B responds with a SYN/ACK packet; and A responds with an ACK packet. A SYN Flood attack inundates a site with SYN packets containing forged (“spoofed”) IP source addresses with nonexistent or unreachable addresses. The firewall responds with SYN/ACK packets to these addresses and then waits for responding ACK packets. Because the SYN/ACK packets are sent to nonexistent or unreachable IP addresses, they never elicit responses and eventually time out.



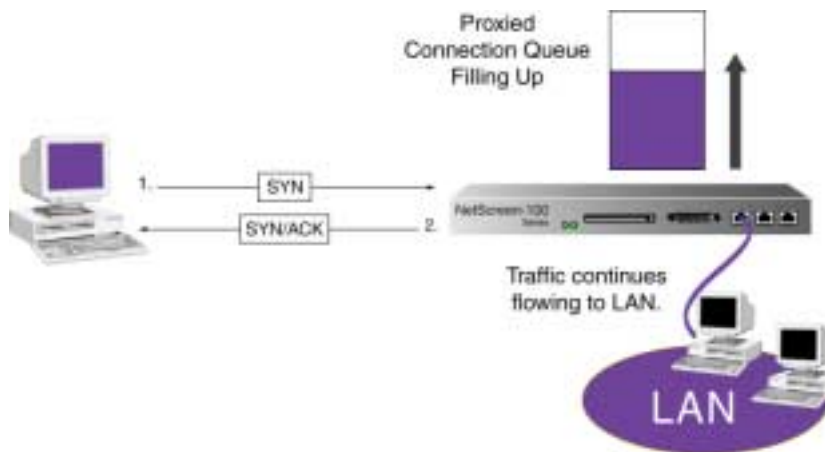
By flooding a server or host with uncompletable connections, the attacker eventually fills the host's memory buffer. Once this buffer is full, no further connections can be made and the host's operating system might be damaged. Either way, the attack disables the host and its normal operations. A SYN Flood attack is classified as a denial-of-service (DoS) attack.

SYN Flood Attack Protection

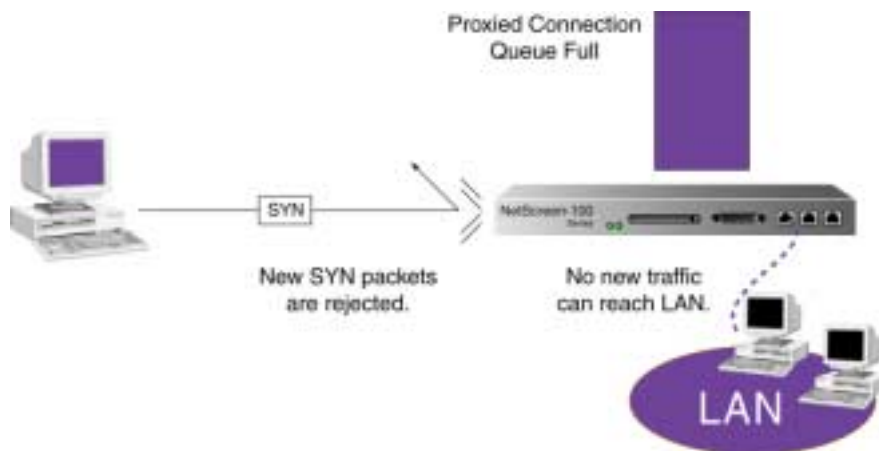
NetScreen devices can impose a limit on the number of SYN packets per second permitted to pass through the firewall. When that threshold is reached, the NetScreen device starts proxying incoming SYN packets, sending out SYN/ACK responses for the host and storing the incomplete connections in a connection queue.³ The incomplete connections remain in the queue until the connection is completed or the request times out.

3. Because the NetScreen-1000 proxies all incoming SYN packets, setting a threshold is unnecessary.

In the following illustration, the SYN threshold has been passed and the NetScreen device has begun proxying SYN packets.



In the next illustration, the proxied connection queue has completely filled up, and new incoming SYN packets are being rejected.



This action attempts to shield hosts on the protected network from the bombardment of incomplete three-way handshakes.

Note: The procedure of proxying incomplete SYN connections above a set threshold pertains only to traffic permitted by existing Access Policies. Any traffic for which an Access Policy does not exist is automatically dropped.

WebUI: Enabling SYN Flood Attack Protection

1. **Configure >> General:** Enter the following settings, and then click **Apply**:

Detect SYN Attack check box: Select

SYN Attack Threshold (NetScreen-5/10/100):
20,000/Sec.

Note: The NetScreen-1000 proxies all sessions; therefore, there is no threshold to set. On the NetScreen-5/10/100, proxying is enabled when SYN Attack detection is enabled.

Through the WebUI, you can set the threshold at which the NetScreen-5, -10, and -100 begin proxying sessions. Through the CLI, you can also set the queue length, timeout value, and alarm threshold.

CLI: Enabling SYN Flood Attack Protection and Defining Parameters

1. Enable SYN Flood attack protection.

```
set firewall syn-attack
```

You can set the following four parameters for proxying uncompleted SYN connections:

2. **Threshold:** The number of SYN packets per second required to activate the SYN proxying mechanism. Although you can set the threshold at any number, you need to know the normal traffic patterns at your site to set an appropriate threshold for it. For example, if it is an e-business site that normally gets 20,000 SYN packets per second, you might want to set the threshold at 30,000/second. If a smaller site normally gets 20 SYN packets/second, you might consider setting the threshold at 40.

```
set syn-threshold <number>
```

3. **Queue size:** The number of proxied connection requests held in the proxied connection queue before the system starts rejecting new connection requests. The longer the queue size, the longer the NetScreen device needs to scan the queue to match a valid ACK response to a proxied connection request. This can slightly slow the initial connection establishment; however, because the time to begin data transfer is normally far greater than any minor delays in initial connection setup, users would not see a noticeable difference. The queue size can be from 0–2000 for the NetScreen-10, and 0–20,000 for both the NetScreen-100 and -100p.

```
set syn-qsize <number>
```

4. **Timeout:** The maximum length of time before a half-completed connection is dropped from the queue. The default is 20 seconds, and you can set the timeout from 0–50 seconds on the NetScreen-10, -100, and -100p. You might try decreasing the timeout value to a shorter length until you begin to see any dropped connections during normal traffic conditions. 20 seconds is a very conservative timeout for a three-way-handshake ACK response.

```
set syn-timeout <number>
```

5. **Alarm:** The number of proxied, half-complete connections per second at which an alarm is entered in the Event Alarm log. The value you set for an alarm threshold triggers an alarm when the number of proxied, half-completed connections per second exceeds that value. For example, if the SYN threshold is set at 2000 SYN packets per second and the alarm at 1000, then a total of 3001 SYN packets per second are required to trigger an alarm entry in the log. More precisely:

1. The firewall passes the first 2000 SYN packets per second that meet Access Policy requirements.
2. The firewall proxies the next 1000 SYN packets in the same second.
3. The 1001st proxied connection (or 3001st connection request in that second) triggers the alarm.

If an attack persists, the Event Alarm log enters an alarm for each second of the attack until the attack stops and the queue empties.

```
set syn-alarm <number>
```

ROUTE TABLE CONFIGURATION

The route table provides information that helps the NetScreen device direct traffic to different interfaces⁴ and subnets. You need to define static routes for conditions such as the following:

- If the Trusted interface is on a subnet with more than one router leading to other subnets, you must define static routes that specify which router to use when forwarding traffic destined for those subnets.
- If the Untrusted interface is on a subnet with more than one router leading to multiple Internet connections, you must define static routes that specify which router to use for forwarding traffic to specific ISPs.
- You *must* define static routes that direct management traffic originating from the device itself (as opposed to user traffic traversing the firewall). For example, you need to define static routes directing syslog, SNMP, OneSecure, and WebTrends messages to the administrator's address, authentication requests to the RADIUS, SecurID, and LDAP servers, and URL checks to the Websense server.

Note: When the NetScreen device is in Transparent mode, you must define a static route for management traffic from the device even if the destination is on the same subnet as the device. This route is necessary to define the interface through which to send traffic.

-
4. When you set the interface IP addresses for a NetScreen device in NAT mode, the route table automatically creates static routes for traffic traversing the interfaces.

Example

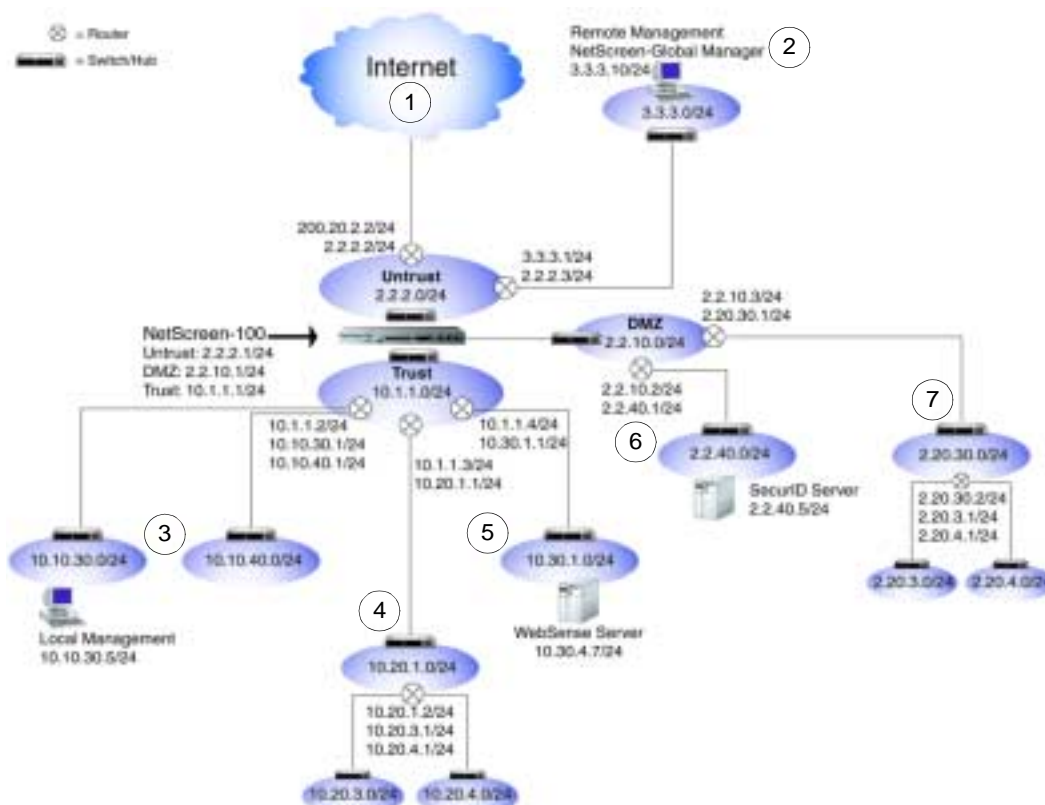
In the following example, a NetScreen-100 operating in NAT mode protects a multilevel network. There is both local and remote management (via NetScreen-Global Manager and Global Pro). SNMP traps and syslog reports are sent to the local administrator, located on the Trusted network, while NetScreen-Global PRO reports are sent to the remote administrator, located on the Untrusted network. A SecurID server on the DMZ is used to authenticate users, and a Websense server on the Trusted side performs URL blocking.

There must be statements in the NetScreen-100 route table specifying the destination network address and subnet mask, and the gateway IP address and interface⁵ through which the NetScreen-100 directs traffic to the following destinations:

1. Default gateway to the Internet
2. Remote administrator in the 3.3.3.0/24 subnet
3. The Trusted 10.10.0.0/16 subnet
4. The Trusted 10.20.0.0/16 subnet
5. The Trusted 10.30.1.0/24 subnet
6. The DMZ 2.2.40.0/24 subnet
7. The DMZ 2.20.0.0/16 subnet

Note: The following example assumes that you have already configured the Untrusted, DMZ, and Trusted interfaces as 2.2.2.1/24, 2.2.10.1/24, and 10.1.1.1/24 respectively.

-
5. For each route table entry, there is also metric statement of either 0 or 1. This parameter specifies the priority of the route; that is, when there are multiple route entries for the same subnet in the route table, the NetScreen device uses the one with the lowest metric value. When using the WebUI, all route table entries that are automatically created when you define the Trusted, Untrusted, or DMZ interface have a value of 0, and any user-defined routes have a metric value of 1. Although you cannot redefine this value through the WebUI, the CLI does allow you to set it.



WebUI

1. Interface >> Untrusted >> Edit: Enter the following to create the Untrusted default gateway, and then click **Save and Reset**:

Default Gateway: 2.2.2.2

2. Configure >> Route Table >> New Entry: Enter the following to direct system reports generated by the NetScreen-100 to remote management, and then click **Apply**:

Network Address: 3.3.3.0

Netmask: 255.255.255.0

Gateway IP Address: 2.2.2.3

Interface: Untrusted

3. Configure >> Route Table >> New Entry: Enter the following, and then click **Apply**:

Network Address: 10.10.0.0

Netmask: 255.255.0.0

Gateway IP Address: 10.1.1.2

Interface: Trusted

4. Configure >> Route Table >> New Entry: Enter the following, and then click **Apply**:

Network Address: 10.20.0.0

Netmask: 255.255.0.0

Gateway IP Address: 10.1.1.3

Interface: Trusted

5. Configure >> Route Table >> New Entry: Enter the following, and then click **Apply**:

Network Address: 10.30.1.0

Netmask: 255.255.255.0

Gateway IP Address: 10.1.1.4

Interface: Trusted

6. Configure >> Route Table >> New Entry: Enter the following, and then click **Apply**:

Network Address: 2.2.40.0

Netmask: 255.255.255.0

Gateway IP Address: 2.2.10.2

Interface: DMZ

7. Configure >> Route Table >> New Entry: Enter the following, and then click **Apply**:

Network Address: 2.20.0.0

Netmask: 255.255.0.0

Gateway IP Address: 2.2.10.3

Interface: DMZ

Note: To modify a route table entry, click **Edit** under the Configure section for the entry you want to modify. The Route Table Configuration dialog box for that entry opens. Make your changes and click **Apply**.

To remove an entry, click **Remove**. A System Message appears prompting you to confirm the removal. Click **Yes** to proceed, or **No** to cancel the action.

CLI

1. set interface untrust gateway 2.2.2.2
2. set route 3.3.3.0 255.255.255.0 interface untrust gateway 2.2.2.3
3. set route 10.10.0.0 255.255.0.0 interface trust gateway 10.1.1.2
4. set route 10.20.0.0 255.255.0.0 interface trust gateway 10.1.1.3
5. set route 10.30.1.0 255.255.255.0 interface trust gateway 10.1.1.4
6. set route 2.2.40.0 255.255.255.0 interface dmz gateway 2.2.10.2
7. set route 2.20.0.0 255.255.0.0 interface dmz gateway 2.2.10.3
8. save

DOMAIN NAME SYSTEM SUPPORT

The NetScreen device incorporates Domain Name System (DNS) support allowing you to use domain names as well as IP addresses for identifying locations. A DNS server keeps a table of the IP addresses associated with domain names. Using DNS makes it possible to reference locations by domain name (such as `www.netscreen.com`) in addition to using the routable IP address, which for `www.netscreen.com` is `209.125.148.135`. DNS translation is supported in all the following programs:

- Address Book
- Syslog
- E-mail
- WebTrends®
- Websense®
- LDAP
- SecurID®
- RADIUS
- NetScreen Global-Manager

Before you can use DNS for domain name/address resolution, you must enter the addresses for DNS servers (the primary and secondary DNS servers) in the NetScreen device.

Note: When enabling the NetScreen-5 or -10 as a Dynamic Host Control Protocol server (see “DHCP” on page 8-107), you must also enter the IP addresses for DNS servers in the DHCP page on the WebUI or through the **set dhcp** command in the CLI.

DNS Lookup

When the NetScreen device connects to the DNS server to resolve a domain name/IP address mapping, it stores that entry in its DNS status table. Some details involved in a DNS lookup follow:

- In the WebUI, the DNS lookup is performed as soon as you press **Apply** or **OK** on a page that supports DNS. In the CLI, the DNS lookup occurs when you enter a command that supports DNS.
- When a DNS lookup returns multiple entries, the address book accepts all entries. The other programs listed above accept only the first one.

- The NetScreen device reinstalls all Access Policies if it finds that anything in the domain name table has changed when you refresh a lookup using the **Refresh Now** button in the WebUI or enter the **exec dns refresh** CLI command.
- If a DNS server fails, the NetScreen device looks up everything again.
- If a lookup fails, the NetScreen device removes it from the cache table.
- If the domain name lookup fails when adding addresses to the address book, the NetScreen device displays an error message and prompts you to choose to continue adding the entry to the address book or not.

The NetScreen device must do a new lookup once a day, which you can schedule the NetScreen device to do at a specified time:

WebUI

Configure >> DNS: Enter the following, and then click **Apply**:

Lookup DNS every day at: Select check box
and enter time <hh:mm>

CLI

1. set dns host schedule <hh:mm>
2. save

The DNS Status Table

The DNS status table reports all the domain names looked up, their corresponding IP addresses, whether the lookup was successful, and when the domain name/IP address was last resolved. The report format looks like the example below:

Domain Name	Corresponding IPs	Status	Last Resolved
www.yahoo.com	204.71.200.74 204.71.200.75 204.71.200.67 204.71.200.68	Success	8/13/2000 16:45:33
www.hotbot.com	209.185.151.28 209.185.151.210 216.32.228.18	Success	8/13/2000 16:45:38

Example: Defining DNS Server Addresses and Scheduling Lookups

To implement DNS functionality, the IP addresses for the DNS servers at 24.0.0.3 and 24.1.64.38 are entered in the NetScreen-5, protecting a single host in a home office. The NetScreen-5 is scheduled to refresh the DNS settings stored in its DNS status table everyday at 11:00 P.M.



WebUI

Configure >> DNS: Enter the following, and then click **Apply**:

Primary DNS Server: 24.0.0.3

Secondary DNS Server: 24.1.64.38

Lookup DNS every day at: 23:00

CLI

1. set dns host dns1 24.0.0.3
2. set dns host dns2 24.1.64.38
3. set dns host schedule 23:00
4. save

DHCP

Dynamic Host Control Protocol (DHCP) was designed to reduce the demands on network administrators by automatically assigning the TCP/IP settings for the hosts on a network. Instead of requiring administrators to assign, configure, track, and change (when necessary) all the TCP/IP settings for every machine on a network, DHCP does it all automatically. Furthermore, DHCP ensures that duplicate addresses are not used, reassigns unused addresses, and automatically assigns IP addresses appropriate for the subnet on which a host is connected.

Both the NetScreen-5 and -10 can act as a DHCP client, receiving a dynamically assigned IP address for the Untrusted interface from an ISP. The NetScreen-5 and -10 can also act as a DHCP server, allocating dynamic IP addresses to hosts, acting as DHCP clients, on the Trusted network.

Note: While using DHCP to assign addresses to hosts on the Trusted network such as workstations and printers, you can still use fixed IP addresses for other machines such as mail servers and WINS servers.

DHCP consists of two components: a protocol for delivering host-specific TCP/IP configuration settings and a mechanism for allocating IP addresses. The NetScreen device provides the following TCP/IP settings to each host when that host boots up:

- Default gateway IP address of the router—if there is one—that connects to the Trusted interface.
- The IP addresses of the following servers:
 - WINS servers (2):⁶ A Windows Internet Naming Service (WINS) server maps a NetBIOS name used in a Windows NT network environment to an IP address used on an IP-based network.
 - DNS servers (3): A Domain Name System (DNS) server maps a uniform resource locator (URL) to an IP address.
 - SMTP server (1): A Simple Mail Transfer Protocol (SMTP) server delivers SMTP messages to a mail server, such as a POP3 server, which stores the incoming mail.

6. The number in parentheses indicates the number of servers supported.

- POP3 server (1): A Post Office Protocol version 3 (POP3) server stores incoming mail. A POP3 server must work conjointly with an SMTP server.
- News server (1): A news server receives and stores postings for news groups.

Note: *If a DHCP client to which the NetScreen device is passing the above parameters has a specified IP address, that address overrides all the dynamic information received from the DHCP server.*

When using DHCP, a NetScreen device allocates IP addresses and subnet masks in two modes:

- In Dynamic mode, the NetScreen device, acting as a DHCP server, assigns (or “leases”) an IP address from an address pool⁷ to a host, acting as a DHCP client. The IP address is leased for a determined period of time or until the client relinquishes the address. (To define an unlimited lease period, enter 0.)
- In Reserved mode, the NetScreen device assigns a designated IP address from an address pool exclusively to a specific client every time that client goes online.

Note: *The NetScreen device saves every IP address assigned through DHCP in flash memory. Consequently, rebooting the NetScreen device does not affect address assignments.*

7. An address pool is a defined range of IP addresses within the same subnet from which the NetScreen device can draw DHCP address assignments. You can group up to 255 IP addresses in up to 64 address pools.

Example: NetScreen-10 as DHCP Server

Using DHCP, the Trusted network behind a NetScreen-10 is sectioned into three IP address pools. All IP addresses are assigned dynamically, except for two workstations that have reserved IP addresses, and four servers that have static IP addresses. The NetScreen-10 is operating in NAT mode. The domain name is dynamic.com.



WebUI

1. Address >> Trust >> New Address: Enter the following, and then click **OK**:
 - Address Name: DNS#1
 - IP Address/Domain Name: 172.16.10.240
 - Netmask: 255.255.255.255
 - Comment: Primary DNS Server
 - Trust: (select)
2. Address >> Trust >> New Address: Enter the following, and then click **OK**:
 - Address Name: DNS#2
 - IP Address/Domain Name: 172.16.10.241
 - Netmask: 255.255.255.255
 - Comment: Secondary DNS Server
 - Trust: (select)

3. Address >> Trust >> New Address: Enter the following, and then click **OK**:

Address Name: SMTP

IP Address/Domain Name: 172.16.10.25

Netmask: 255.255.255.255

Comment: SMTP Server

Trust: (select)

4. Address >> Trust >> New Address: Enter the following, and then click **OK**:

Address Name: POP3

IP Address/Domain Name: 172.16.10.110

Netmask: 255.255.255.255

Comment: POP3 Server

Trust: (select)

5. Admin >> DHCP >> Enter the following information and click **Apply**:

Enable DHCP Server: (select)

Lease: Unlimited (select)

Gateway: 0.0.0.0

Netmask: 255.255.255.0

Domain Name: dynamic.com

WINS#1: 0.0.0.0

WINS#2: 0.0.0.0

DNS#1: 172.16.10.240

DNS#2: 172.16.10.241

DNS#3: 0.0.0.0

SMTP: 172.16.10.25

POP3: 172.16.10.110

NEWS: 0.0.0.0

6. Admin >> DHCP >> New Address: Enter the following, and then click **OK**:

Dynamic: (select)

IP Address Start: 172.16.10.10

IP Address End: 172.16.10.19

7. Admin >> DHCP >> New Address: Enter the following, and then click **OK**:

Dynamic: (select)

IP Address Start: 172.16.10.120

IP Address End: 172.16.10.129

8. Admin >> DHCP >> New Address: Enter the following, and then click **OK**:
Dynamic: (select)
IP Address Start: 172.16.10.210
IP Address End: 172.16.10.219
9. Admin >> DHCP >> New Address: Enter the following, and then click **OK**:
Reserved: (select)
IP Address: 172.16.10.21
Ethernet Address: 1234 abcd 5678
10. Admin >> DHCP >> New Address: Enter the following, and then click **OK**:
Reserved: (select)
IP Address: 172.16.10.112
Ethernet Address: abcd 1234 efgh

CLI

1. set address trust dns#1 172.16.10.240 255.255.255.255 "primary dns server"
2. set address trust dns#2 172.16.10.241 255.255.255.255 "secondary dns server"
3. set address trust snmp 172.16.10.25 255.255.255.255 "snmp server"
4. set address trust pop3 172.16.10.110 255.255.255.255 "pop3 server"
5. set dhcp server service
6. set dhcp server option domainname dynamic.com
7. set dhcp server option lease 0
8. set dhcp server option netmask 255.255.255.0
9. set dhcp server option dns1 172.16.10.240
10. set dhcp server option dns2 172.16.10.241
11. set dhcp server option smtp 172.16.10.25
12. set dhcp server option pop3 172.16.10.110
13. set dhcp server ip 172.16.10.10 to 172.16.10.19
14. set dhcp server ip 172.16.10.120 to 172.16.10.129
15. set dhcp server ip 172.16.10.210 to 172.16.10.219
16. set dhcp server ip 172.16.10.11 mac 1234abcd5678
17. set dhcp server ip 172.16.10.112 mac abcd1234efgh
18. save

Example: NetScreen-5 as DHCP Client

The Untrusted interface of the NetScreen-5 has a dynamically assigned IP address. When the NetScreen-5 requests its IP address from its ISP, it receives its IP address, subnet mask, gateway IP address, and the length of its lease on the address. The IP address of the DHCP server is 222.33.44.55.



Note: Before setting up a site for DHCP service, you must have the following:

- Digital subscriber line (DSL) modem and line
- Account with ISP

WebUI

Interface >> Untrust >> Edit: Select **Obtain IP using DHCP**, and then click **Save and Reset**.⁸

-
8. You cannot specify the IP address of the DHCP server through the WebUI; however, you can do so through the CLI. Also, through the CLI, you can schedule the NetScreen-5, -10, and -100 to reset at a time that is convenient for maintaining uninterrupted network operation: **set timer <mm | dd | yyyy> <hh:mm> action reset**.

CLI

1. set interface untrust dhcp
2. set dhcp client server 222.33.44.55
3. save

PPPoE

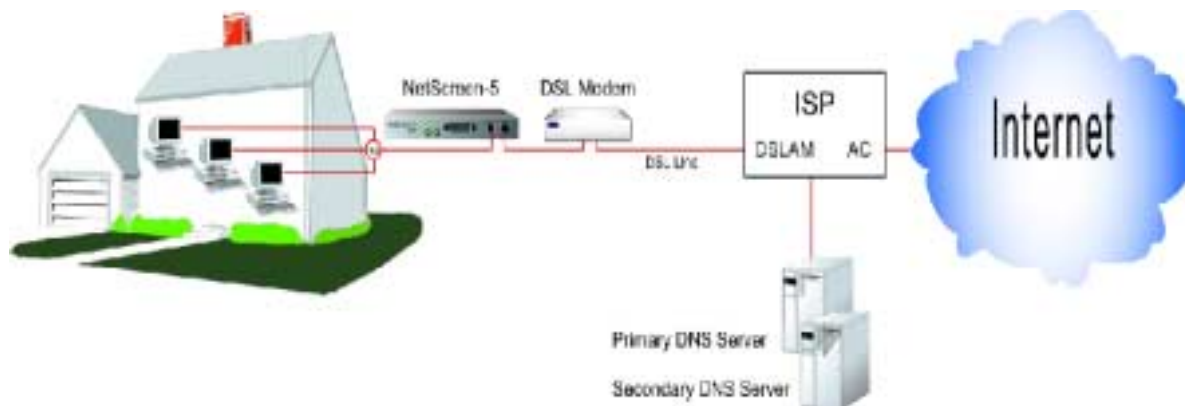
Point-to-Point Protocol over Ethernet (PPPoE) is a protocol that allows the members of an Ethernet LAN to make individual PPP connections with their ISP by encapsulating the IP packet within the PPP payload, which is encapsulated inside the PPPoE payload.

The NetScreen-5 supports PPPoE, allowing it to operate compatibly on DSL, Ethernet Direct, and cable networks run by ISPs using PPPoE for their clients' Internet access.

Example: Setting Up PPPoE

The following example illustrates how to define the Untrusted interface of the NetScreen-5 for PPPoE connections, and how to initiate PPPoE service.

In this example, the NetScreen-5 receives a dynamically assigned IP address for its Untrusted interface from the ISP, and the NetScreen-5 also dynamically assigns IP addresses for the three hosts on its Trusted side. In this case, the NetScreen-5 acts both as a PPPoE client and DHCP server. The NetScreen-5 must be in either NAT mode or Route mode.



Before setting up the site in this example for PPPoE service, you must have the following:

- Digital subscriber line (DSL) modem and line
- Account with ISP
- User name and password (obtained from the ISP)

WebUI

1. Interface >> Trusted >> Edit: Enter the following, and then click **Save**:
Address: 172.16.30.10
Subnet Mask: 255.255.255.0
2. Interface >> Untrusted >> Edit: Enter the following:
Obtain IP using PPPoE (select)
User Name: <name>
Password: <password>
3. Interface >> Untrusted >> Edit: To test your PPPoE connection, click **Connect**.

Note: When you initiate a PPPoE connection, your ISP automatically provides the IP addresses for the Untrusted interface and the IP addresses for the Domain Name Service (DNS) servers.

If you use a static IP address for the Untrusted interface, you must obtain the DNS servers' IP addresses and then manually enter them on the NetScreen-5 and on the Trusted hosts.

4. Admin >> DHCP: Enter the following, and then click **Apply**:

Enable DHCP Server (select)

Lease: 1 hour

Gateway: 0.0.0.0

Netmask: 0.0.0.0

Domain Name: (leave blank)

DNS#1: 0.0.0.0

DNS#2: 0.0.0.0

5. Admin >> DHCP >> New Address: Enter the following, and then click **OK**:

Dynamic: (select)

IP Address Start: 172.16.30.2

IP Address End: 172.16.30.5

6. Turn off the power to the DSL modem, the NetScreen-5, and the three workstations.

7. Turn on the DSL modem.

8. Turn on the NetScreen-5.

The NetScreen-5 makes a PPPoE connection to the ISP and, through the ISP, gets the IP addresses for the DNS servers.

9. Turn on the workstations.

The workstations automatically receive the IP addresses for the DNS servers. They get an IP address for themselves when they attempt a TCP/IP connection.

Note: When you use DHCP to assign IP addresses to hosts on the Trusted side, the NetScreen-5 automatically forwards the IP addresses of the DNS servers that it receives from the ISP to the Trusted hosts.

If the IP addresses for the hosts are not dynamically assigned through DHCP, you must manually enter the IP addresses for the DNS servers on each host.

Every TCP/IP connection that a Trusted host makes to the Untrusted side, automatically goes through the PPPoE encapsulation process.

CLI

1. set interface trust ip 172.16.30.10 255.255.255.0
2. set pppoe interface untrust
3. set pppoe username <name> password <password>
4. To test your PPPoE connection:
 exec pppoe connect
 get pppoe
5. set dhcp server service
6. set dhcp server ip 172.16.30.2 to 172.16.30.5
7. set dhcp server option lease 60
8. save
9. Turn off the power to the DSL modem, the NetScreen-5, and the three workstations.
10. Turn on the DSL modem.
11. Turn on the NetScreen-5.
12. Turn on the workstations.

The workstations automatically receive the IP addresses for the DNS servers. They get an IP address for themselves when they attempt a TCP/IP connection.

Every TCP/IP connection that a Trusted host makes to the Untrusted side, automatically goes through the PPPoE encapsulation process.

URL FILTERING CONFIGURATION

NetScreen URL filtering features the Websense Enterprise Engine, which enables you to block or permit access to different sites based on their URLs, domain names, and IP addresses. With the Websense API built directly into the NetScreen firewall, the NetScreen device creates a direct link to a Websense URL-blocking server, running on either Microsoft Windows NT 4.0 or Solaris 2.5 or 2.6.

Using Websense manager, the NetScreen administrator can do the following:

- Alter the URL-blocking database to block or allow access to any sites they choose
- Schedule different URL filtering profiles for different times of the day
- Download Websense Reporter logs of blocked or viewed URLs

Note: For additional information about Websense, visit www.websense.com.

To specify URL filtering options:

WebUI

Configure >> URL Filtering: Enter the following information, and then click **Apply**:

Enable URL Filtering via Websense Server:
(select)

Websense Server Name: The IP address of the computer running the Websense server.

Websense Server Port: The default port for Websense is 15868. If you have changed the default port on the Websense server you must also change it on the NetScreen device. Please see your Websense documentation for full details.

Communication Timeout: The time interval, in seconds, that the NetScreen device waits for a response from the Websense filter. If Websense does not respond within the time interval, the NetScreen device will ultimately block the request.

Current Server Status: The NetScreen device reports the status of the Websense server.

URL Block Return Message: This is the message the NetScreen device returns to the user after blocking the site. You can use the message sent from the Websense server, or create a message (up to 220 characters) to be sent from the NetScreen device.

CLI

set url config {enable | disable}

set url message <string>

set url msg-type {0 | 1}

set url server {<domain_name> | <a.b.c.d>} <port_number> <timeout_value>

Note: See the *NetScreen CLI Reference Guide* for an explanation of the **set url** arguments, plus examples and related commands.

DOWNLOADING/UPLOADING SETTINGS AND SOFTWARE

You can upload and download configuration settings and software to and from a NetScreen device. The kinds of location that you upload from and download to depend on whether you use the WebUI or the CLI to perform the operation. Using the WebUI and Web browser support, you can upload and download configuration settings and upload ScreenOS software from any local directory. Through the CLI, you can upload and download settings and software from and to a TFTP server or PCMCIA card.

Saving and Importing Settings

It is good practice to backup your settings after every significant change you make. Through the WebUI, you can download the configuration to any local directory as a backup precaution. Through the CLI, you can download the configuration to a TFTP server or PCMCIA card (NetScreen-10, -100, and -1000). Should you need the saved backup configuration, you can then simply upload it to the NetScreen device.

The ability to download and upload a configuration also provides the means for mass distribution of configuration templates.

To download a configuration:

WebUI

1. Admin >> Settings: Click **Download Configuration**.
2. Browse to the location where you want to keep the configuration file, and then click **Save**.

CLI

save config to {tftp <a.b.c.d> | slot} <filename>

Note: On the NetScreen-1000, you must specify slot 1 or slot 2.

To upload a configuration:

WebUI

Admin >> Settings: Specify the file name and location, and then click **Apply**:

Configure Script Upload: Type the configuration file location.

Or

Click **Browse** and navigate to the file location, select the file, and then click **Open**.

CLI

save config from {tftp <a.b.c.d> | slot} <filename>

Note: On the NetScreen-1000, you must specify slot 1 or slot 2.

Uploading and Downloading Software

When the NetScreen ScreenOS operating system is updated, a customer can purchase and upload it to their NetScreen device. Through the WebUI, you can upload software from a local directory. Through the CLI, you can upload the software from a TFTP server or PCMCIA card (NetScreen-10, -100, and -1000), and you can download software to a TFTP server.

Note: After the software is upgraded, the NetScreen device reboots. This process takes a few minutes.

WebUI

Configure >> General: Specify the file name and location, and then click **Apply**:

Software Update: Type the software file location.

Or

Click **Browse** and navigate to the file location, select the file, and then click **Open**.

CLI

save software from {tftp <a.b.c.d> | slot} <filename>

Note: On the NetScreen-1000, you must specify slot 1 or slot 2.

Through the CLI, you can also download software to a TFTP server, using the **save** command:

save software from flash to tftp <a.b.c.d> <filename>

Software Keys

The software key feature allows you to expand the capabilities of your NetScreen device without having to upgrade to a different device or system image. You can purchase a key that unlocks specified features already loaded in the software, such as the following:

- VPN tunnels
- User capacity
- Virtual Systems

Each NetScreen device ships with a standard set of features enabled and might support the activation of optional features or the increased capacity of existing features. For information regarding which features are currently available for upgrading, refer to the latest marketing literature from NetScreen.

Example: Expanding User Capacity

A small company using a single NetScreen-5 with a license for 10 users has grown to the point where it now needs an unrestricted user license. The NetScreen administrator expands the capabilities of the NetScreen-5 by obtaining a software key for an unrestricted number of users.

1. Contact the value-added reseller (VAR) who sold you the NetScreen device or contact NetScreen Technologies directly.
2. Provide the serial number of your device and state the feature option you want—an unrestricted user license, in this example.

A combination of the serial number, the feature keyword (vpn, capacity, vsys), and the feature option keyword (<number> or “unlimited” tunnels, users, users) is used to generate the software key (for example, 7e58e876ca050192). The key is then sent to you via e-mail.

3. Enter the key through either the WebUI or CLI:

WebUI

Admin >> Software Key: Specify the path and file name, and then click **Apply and Reset**.⁹

Software Update: Type the software key file location.

Or

Click **Browse** and navigate to the software key file location, select the file, and then click **Open**.

CLI

```
set software-key {vpn | capacity | vsys} <key_value>
```

```
reset
```

9. Through the CLI, you can schedule the NetScreen-5, -10, and -100 to reset at a time that is convenient for maintaining uninterrupted network operation: **set timer <mm | dd | yyyy> <hh:mm> action reset.**

Administration

9

This chapter describes various management methods and tools, ways to secure administrative traffic, and the administrative privilege levels that you can assign to admin users:

- “Management Methods and Tools” on page 9-125
- “Levels of Administration” on page 9-135
- “Securing Administrative Traffic” on page 9-138

MANAGEMENT METHODS AND TOOLS

The management methods and the tools with which to apply each method are presented in the following sections:

- “Web User Interface” on page 9-126
 - HTTP
 - HTTPS using Secure Sockets Layer (SSL)
- “Command Line Interface” on page 9-129
 - Telnet
 - SSH[®] Secure Shell[™]
 - Serial console
- “Central Administration” on page 9-132
 - NetScreen-Global Manager
 - NetScreen-Global PRO

Web User Interface

For administrative ease and convenience, you can use the Web user interface (WebUI). NetScreen devices use Web technology that provides a Web-server interface to configure and manage the software.

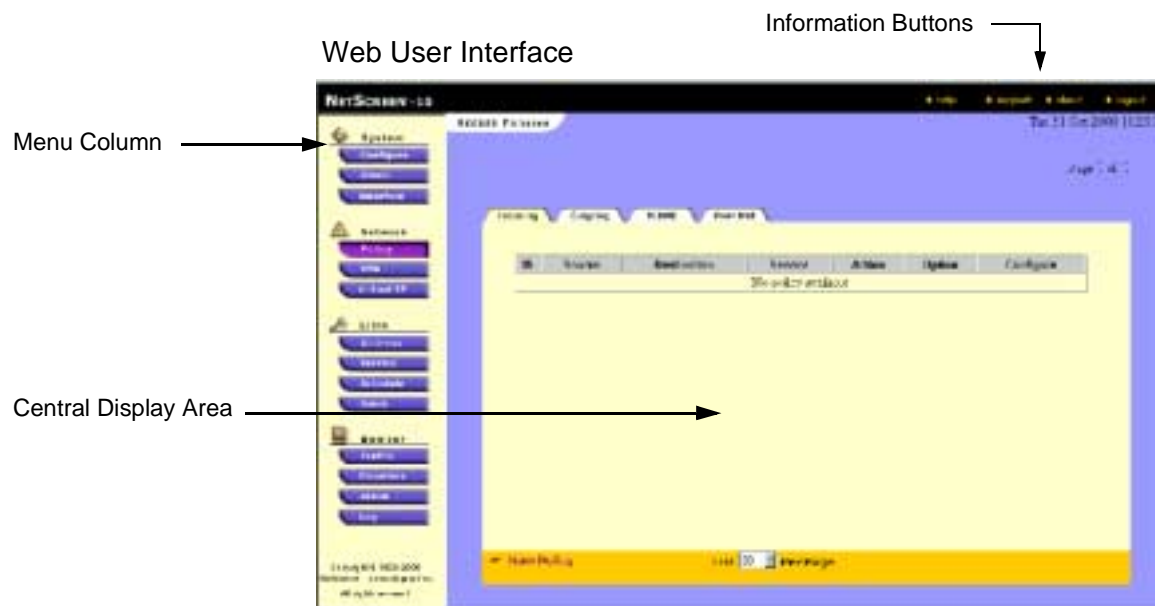
To use the WebUI, you must have the following:

- Netscape® Communicator® (version 4.5 or later) or Microsoft® Internet Explorer (version 5 or later)
- TCP/IP network connection to the NetScreen device

Note: For a complete description of WebUI, refer to the NetScreen WebUI Reference Guide.

HTTP

With a standard Web browser you can access, monitor, and control your network security configurations remotely using the Hypertext Transfer Protocol (HTTP).



You can secure HTTP traffic by either encapsulating it in a virtual private network (VPN) tunnel or through the Secure Sockets Layer (SSL) protocol. You can also secure it by completely separating management traffic from network user traffic. You can run all administrative traffic through the MGT interface (NetScreen-1000) or devote an interface such as the DMZ (NetScreen-10 and -100) entirely to administrative traffic.

Note: For more information, see “Virtual Private Networks” on page 9-147, “Secure Sockets Layer” (below), and “Manage IP” on page 9-143.

Secure Sockets Layer

Secure Sockets Layer (SSL) is a set of protocols that can provide a secure connection between a Web client and server communicating over a TCP/IP network. NetScreen ScreenOS provides:

- Web SSL support
- SSL version 3 compatibility
- Netscape Navigator 4.7x and Internet Explorer 5.x compatibility¹
- Public Key Infrastructure (PKI) key management integration

SSL is not a single protocol, but consists of the SSL Handshake Protocol (SSLHP), which allows the server and client to authenticate each other and negotiate an encryption method, and the SSL Record Protocol, which provides basic security services to higher-level protocols such as HTTP.

-
1. Check your Web browser to see how strong the ciphers can be and which ones your browser supports. (Both the NetScreen device and your Web browser must support the same kind and size of ciphers you use for SSL.) In Internet Explorer 5x, click **Help, About Internet Explorer**, and read “Cipher Strength.” To obtain the advanced security package, click the **Update Information** link. In Netscape Navigator, click **Help, About Communicator**, and read the section about RSA[®]. To change the SSL configuration settings, click **Security, Navigator, Configure SSL v3**.

Independent of application protocol, SSL uses TCP to provide secure service. SSL uses certificates to authenticate first the server or both the client and the server, and then encrypt the traffic sent during the session. Before using SSL, you must first create a public/private key pair and then load a certificate. Because SSL is integrated with PKI key/certificate management, you can select the SSL certificate from one of the certificates in the certificate list. You can also use the same certificate for a VPN.

NetScreen supports the following encryption algorithms for SSL:

- RC4 with 40-bit and 56-bit keys
- DES: Data Encryption Standard
- 3DES: Triple DES

NetScreen supports the same authentication algorithms for SSL as for VPNs—Message Digest version 5 (MD5) and Secure Hash Algorithm version 1 (SHA-1). The RC4 algorithms are always paired with MD5; DES and 3DES with SHA-1.

When you type the IP address for managing the NetScreen device in your browser's URL field, change "http" to "https", and follow the IP address with a colon and the HTTPS (SSL) port number (for example, `https://123.45.67.89:1443`).

Command Line Interface

Advanced administrators can attain finer control by using the command line interface (CLI). To configure a NetScreen device with the CLI, you can use any software that emulates a VT100 terminal. With a terminal emulator, you can configure the NetScreen device using a console from any Windows®, UNIX™, or Macintosh® operating system. For remote administration through the CLI, you can use Telnet or Secure Command Shell (SCS). With a direct connection through the console port, you can use Hyperterminal®.

Note: For a complete listing of the CLI commands for the NetScreen devices, refer to the NetScreen CLI Reference Guide.

Telnet

Telnet is a login and terminal emulation protocol that uses a client/server relationship to connect to and remotely configure network devices over a TCP/IP network. The administrator launches a Telnet client program on the administration workstation and creates a connection with the Telnet server program on the NetScreen device. After logging in, the administrator can issue CLI commands, which are sent to the Telnet program on the NetScreen device, effectively configuring the device as if operating through a direct connection. Using Telnet to manage NetScreen devices requires the following:

- Telnet software on the administrative workstation
- An Ethernet connection to the NetScreen device

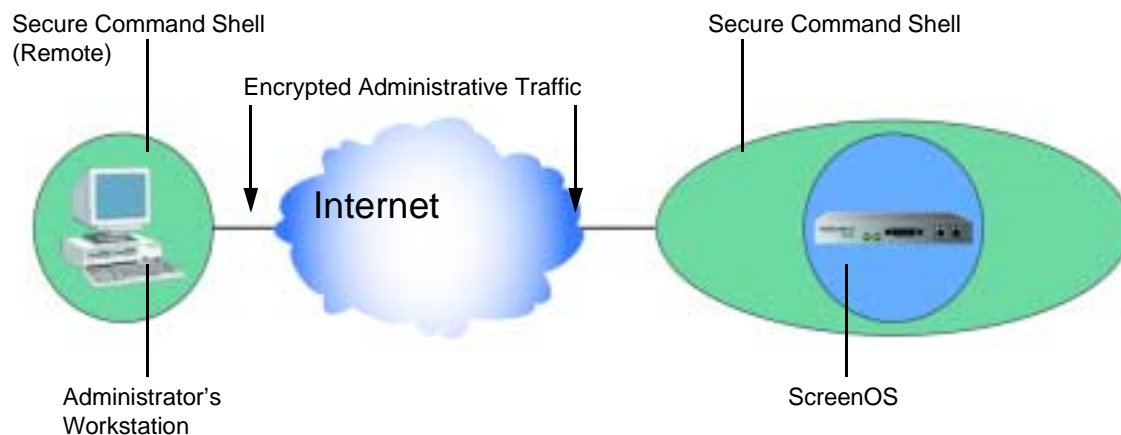
You can secure Telnet traffic by encapsulating it in a virtual private network (VPN) tunnel or by completely separating it from network user traffic. You can run all administrative traffic through the MGT interface (NetScreen-1000) or devote an interface such as the DMZ (NetScreen-10 and -100) entirely to administrative traffic.

Note: For more information, see “Virtual Private Networks” on page 9-147, “Secure Sockets Layer” on page 9-127, and “Manage IP” on page 9-143.

Secure Shell

You can use secure shell (SSH[™]) for secure CLI access over unsecure channels. SSH allows you to open a remote command shell² securely, execute commands, and copy files to or from the remote device. Secure Command Shell (SCS) is a SSH-compatible utility that allows you to remotely manage your NetScreen device without establishing a VPN.

Using SCS, you can administer NetScreen devices from an Ethernet connection or a dial-in modem. The built-in SCS server on the NetScreen device allows the SSH client, installed on the administrator's workstation, to open an instance of the NetScreen device console, which makes secure configuration and management possible.



-
2. A command shell is an operating system's outer layer, providing an environment in which you can launch and operate programs running within the operating system's inner layer, or kernel.

Serial Console

You can manage a NetScreen device through a direct serial connection from the administrator's workstation to the NetScreen device via the Console port (Diagnostics port on the NetScreen-5). Although a direct connection is not always possible, this is surely the most secure method for managing the device.

You need the following items to create a serial connection:

- A DB-9 female to DB-25 male serial cable (NetScreen-10 and -100)
- A DB-9 female to DB-9 male serial cable (NetScreen-5)
- A MiniDIN-8 to DB-9 female serial cable (NetScreen-1000)
- Hyperterminal software (or another kind of VT100 terminal emulator) on the management workstation, with the Hyperterminal port settings configured as follows:
 - Serial communications 9600 bps
 - 8 bit, no parity
 - 1 stop bit
 - no flow control

Note: For more details on using Hyperterminal, see the "Getting Started" chapter in the NetScreen CLI Reference Guide.

Central Administration

If you manage large or dispersed systems, you can use either NetScreen-Global Manager independently or in conjunction with NetScreen-Global PRO to manage and configure all of your NetScreen devices from a central location.

NetScreen-Global Manager

NetScreen-Global Manager allows you to deploy and control up to 1000 NetScreen devices over multiple local-area networks (LANs) or a wide-area network (WAN) from a central location. NetScreen-Global Manager runs on Windows NT and requires network access to each device.

Note: For more information, refer to the NetScreen-Global Manager User's Guide.

NetScreen-Global PRO

The NetScreen-Global PRO system allows you to control up to 10,000 NetScreen devices from a central location. NetScreen-Global PRO contains the following components:

- The database, which collects reports and statistics
- The master controller, which communicates with the database to retrieve management information and update tables
- The data collector, which collects performance- and fault-related data from the NetScreen devices

These additional components work with the NetScreen-Global PRO system:

- NetScreen devices, which provide data to the data collector
- The administration tool, which allows you to administer the system
- NetScreen-Global Manager™ Report Viewer, which displays the Global PRO reports

NetScreen-Global PRO runs on a UNIX® (Solaris™) platform.

Note: For more information, refer to the NetScreen-Global PRO User's Guide.

Administrative Interface Options

You can configure the NetScreen-5, -10, -100, and -1000 to allow administration of the device through one or more interfaces. For example, you might have local management access the device through the Trusted interface and remote management through the Untrusted interface. With a NetScreen-10 or -100, you might use the DMZ interface exclusively for administration, separating management traffic completely from network user traffic for the Trusted and Untrusted interfaces.

To enable an interface to allow various methods of administration to traverse it through the WebUI and the CLI, do the following:

WebUI

Interface >> Trusted | Untrusted | DMZ: Select the following management service options, and then click **Save and Reset**³:

WebUI: Selecting this option allows the interface to receive HTTP traffic to manage the NetScreen device via the Web user interface (WebUI).

SSL: Selecting this option allows the interface to receive HTTPS traffic for secure management of the NetScreen device via the Web user interface (WebUI).

NS-Global: NetScreen offers two applications for central management of multisite networks—NetScreen-Global Manager and NetScreen-Global PRO. Selecting this option allows the interface to receive management traffic from NetScreen-Global Manager.

-
3. Through the CLI, you can schedule the NetScreen-5, -10, and -100 to reset at a time that is convenient for maintaining uninterrupted network operation: **set timer <mm | dd | yyyy> <hh:mm> action reset.**

NS-GlobalPRO: NetScreen offers two applications for central management of multisite networks—NetScreen-Global Manager and NetScreen-Global PRO. Selecting this option allows the interface to receive management traffic from NetScreen-Global PRO⁴.

Telnet: A terminal emulation program for TCP/IP networks such as the Internet. Telnet is a common way to remotely control network devices. Selecting this option enables Telnet manageability.

SCS: You can administer the NetScreen device from an Ethernet connection or a dial-in modem using Secure Command Shell (SCS), which is SSH-compatible. You must have a SSH client that is compatible with Version 1.5 of the SSH protocol. These clients are available for Windows 95, Windows 98, Windows NT, Linux, and UNIX. The NetScreen device communicates with the SSH client through its built-in SCS server, which provides device configuration and management services. Selecting this option enables SCS manageability.

SNMP: The NetScreen device supports the Simple Network Management Protocol version 1.5 (SNMPv1), described in RFC-1157, and all relevant Management Information Base II (MIB II) groups, as defined in RFC-1213. Selecting this option enables SNMP manageability.

CLI

```
set interface {trust | untrust | dmz | mgt} manage {global | global-pro | ping |  
scs | snmp | ssl | telnet | web}
```

4. NetScreen-Global PRO requires the use of NetScreen-Global Manager, so if you want to enable this option, you also need to select the **NetScreen-Global Manager** option.

LEVELS OF ADMINISTRATION

NetScreen devices support multiple administrative users. The privileges on the NetScreen-1000 differ somewhat from those on the other NetScreen devices because of the administration of virtual systems. Therefore, the administration privileges are treated separately in the following sections.

NetScreen-5, -10, and -100 Administrators

The NetScreen-5 and -10 support up to four admin users, and the NetScreen-100 supports up to ten. (For the NetScreen-1000, see “NetScreen-1000 Administrators” on page 9-136.)

On the NetScreen-5, -10, and -100, there are three administrative levels with the following privileges:

- **Level 1: Root Administrator**

The Root Administrator has complete administrative privileges.

- **Level 2: Super Administrator**

The Super Administrator has the same privileges as the Root Administrator, but cannot create, modify, or remove other admin users.

- **Level 3: Sub Administrator**

The Sub Administrator has viewing privileges only for the WebUI, and can only issue the get and ping CLI commands.

For any configuration changes that an administrator makes, the following information is logged:

- Name of the administrator making the change
- IP address from which the change was made
- Time of the change

NetScreen-1000 Administrators

There are four levels of administrative privilege possible for the NetScreen-1000:

- Level 1: Root Administrator
- Level 2: Super Administrator
- Level 3: Sub Administrator
- Level 4: Virtual System Administrator

Root Administrator

The Root Administrator has the following privileges:

- Manages the root system of the NetScreen device
- Adds and manages all other administrators
- Establishes and manages Virtual Systems

Super Administrator

The Super Administrator, who has root level access (similar to “root privilege” in UNIX), has the following privileges:

- Manages the root system of the NetScreen device
- Creates Virtual Systems and assigns a Virtual System administrator for each one
- Monitors any Virtual System
- Tracks statistics (a privilege that cannot be delegated to a Virtual System administrator)

Sub Administrator

The Sub Administrator has the following privileges:

- Read-only privileges in the root system, using the following four commands: **enter**, **exit**, **get**, and **ping**
- Read-only privileges in Virtual Systems

Virtual System Administrator

You can configure the NetScreen-1000 with up to 100 subsystems called virtual systems. Virtual systems are unique security domains that can be managed by their own administrators (Virtual System Administrators).

Virtual System Administrators independently manage their own virtual systems, either through CLI or the WebUI. On each virtual system, the Virtual System Administrator has the following privileges:

- Creates and edits users
- Creates and edits services
- Creates and edits Access Policies
- Creates and edits addresses
- Creates and edits VPNs
- Creates his or her login password

If necessary, a Virtual System Administrator can set up a VPN tunnel for managing a virtual system securely from a remote location, and for remote users to secure their connections to the virtual system.

Adding Admin Users

The Root Administrator is the only one who can create, modify, and remove admin users. In the following example, the one performing the procedure must be a Root Administrator.

Example: Adding a Sub Administrator

The Root Administrator is adding a new Sub Administrator named Roger with the password 2bd21wG7 to the NetScreen-100.

WebUI

Admin >> Admin >> New Admin: Enter the following, and then click **OK**:

Name: Roger

New Password: 2bd21wG7⁵

Confirm Password: 2bd21wG7

CLI

set admin user Roger password 2bd21wG7 privilege read-only

-
5. The password can be up to 31 characters long. It must be alphanumeric, without any spaces or special characters.

SECURING ADMINISTRATIVE TRAFFIC

To secure the NetScreen device during setup, perform these four steps:

1. On the Web interface, change the administrative port.
See “Changing the System IP Port Number” on page 9-139.
2. Turn off any unnecessary interface management service options.
See “Administrative Interface Options” on page 9-133.
3. Disable the ping and ident-reset service options on the interfaces, both of which respond to requests initiated by unknown parties and can reveal information about your network:

WebUI

Interface >> Trusted | Untrusted | DMZ: Clear the following service options, and then click **OK**:

Ping: A utility that enables you to determine whether a specific IP address is accessible. Selecting this option allows people to ping the IP address of the NetScreen device through the Trusted, Untrusted, or DMZ interface.

Ident-reset: Services like Mail and FTP send identification requests. If they receive no acknowledgement, they send the request again. While the request is processing, there is no user access. By enabling the Ident-reset option, the NetScreen device sends a TCP reset announcement in response to an IDENT request to port 113 and restores access that has been blocked by an unacknowledged identification request.

CLI

```
unset interface {trust | untrust | dmz | mgt} manage ping
unset interface {trust | untrust | dmz | mgt} ident-reset
```

4. Change the user name and password for administration access.
5. Define the management client IP addresses for the admin users.

See “Restricting Administrative Access” on page 9-142.

Changing the System IP Port Number

Changing the port number to which the NetScreen device listens for HTTP management traffic improves security. The default setting is port 80, the standard port number for HTTP traffic. After you change the port number, you must then type the new port number in the URL field in your Web browser when you next attempt to contact the NetScreen device. (In the following example, the administrator needs to enter `http://188.30.12.2:15522`.)

Example: Changing the Port Number

In this example, the System IP is 188.30.12.2 with the standard port number 80. You change the port number from 80 to 15522.

WebUI

1. Admin >> Web >> Port: 15522
2. Click **Apply and Reset**⁶.

CLI

1. set admin port 15522
2. save

-
6. Through the CLI, you can schedule the NetScreen-5, -10, and -100 to reset at a time that is convenient for maintaining uninterrupted network operation: **set timer <mm|dd|yyyy> <hh:mm> action reset.**

Changing the Admin Login Name and Password

By default, the initial login name for NetScreen devices is *netscreen*. The initial password is also *netscreen*. Because these have been widely published, you should change the login name and password immediately. The login name and password are both case-sensitive. Each must be one word, alphanumeric, with no symbols. Record the new admin login name and password in a secure manner.



Warning

Be sure to record your new password! If you forget it, you cannot reset or gain access to the device. It must then be returned to the factory for resetting.

Administrative users for the NetScreen device can be authenticated using the internal database and an external RADIUS server⁷. When the admin user logs in to the NetScreen device, it first checks the local internal database for authentication. If there is no entry present, it then uses RADIUS to authenticate. The purpose of this feature is to extend the authentication schemes to the management of administrative users.

-
7. Remote Authentication Dial-In User Service (RADIUS) is a protocol for authenticating and authorizing dial-up users. The NetScreen device can act as a client of a RADIUS server.

Example: Changing an Admin User Login Name and Password

The Root Administrator has decided to change a Super Administrator's login name from John to Smith and his password from xL7s62a1 to 3MAb99j2.

Note: For information on the different levels of administrators, see “Click the Save button.” on page 9-151.

WebUI

Admin >> Admin >> (John) Edit: Enter the following, and then click **OK**:

Name: Smith

New Password: 3MAb99j2

Confirm Password: 3MAb99j2

CLI

1. unset admin user John
2. set admin user Smith password 3MAb99j2 privilege all
3. save

Example: An Admin User Changing Her Own Password

Non-root users can change their own administrator password, but not their login name. In this example, a Super Administrator with the login name “starling” is changing her password from 3MAb99j2 to ru494Vq5.

WebUI

Admin >> Admin >> (starling) Edit: Enter the following, and then click **OK**:

Name: starling

Old Password: 3MAb99j2

New Password: ru494Vq5


Confirm Password: ru494Vq5

CLI

1. set admin password ru494Vq5
2. save

Restricting Administrative Access

You can administer NetScreen devices from one or multiple addresses of a subnet. By default, any host on the Trusted interface can administer a NetScreen device. To restrict this ability to specific workstations, you must configure Management Client IP addresses.

 **Caution** *The assignment of a management client IP address takes effect immediately. If you are managing the device via a network connection and your workstation is not included in the assignment, the NetScreen device will immediately terminate your current session and you will no longer be able to manage the device from that workstation.*

Example: Restricting Administration to a Single Workstation

In this example, the administrator at the workstation with the IP address 172.16.40.42 is the only administrator specified to manage the NetScreen-10.

WebUI

Admin >> Admin >> New Management Client IP: Enter the following, and then click **OK**:

IP Address: 172.16.40.42
Netmask: 255.255.255.255

CLI

1. set admin manage-ip 172.16.40.42 255.255.255.255
2. save

Example: Restricting Administration to a Subnet

In this example, the group of administrators with workstations in the 172.16.40.0/24 subnet are specified to manage the NetScreen-10.

WebUI

Admin >> Admin >> New Management Client IP: Enter the following, and then click **OK**:

IP Address: 172.16.40.0
Netmask: 255.255.255.0

CLI

1. set admin manage-ip 172.16.40.0 255.255.255.0
2. save

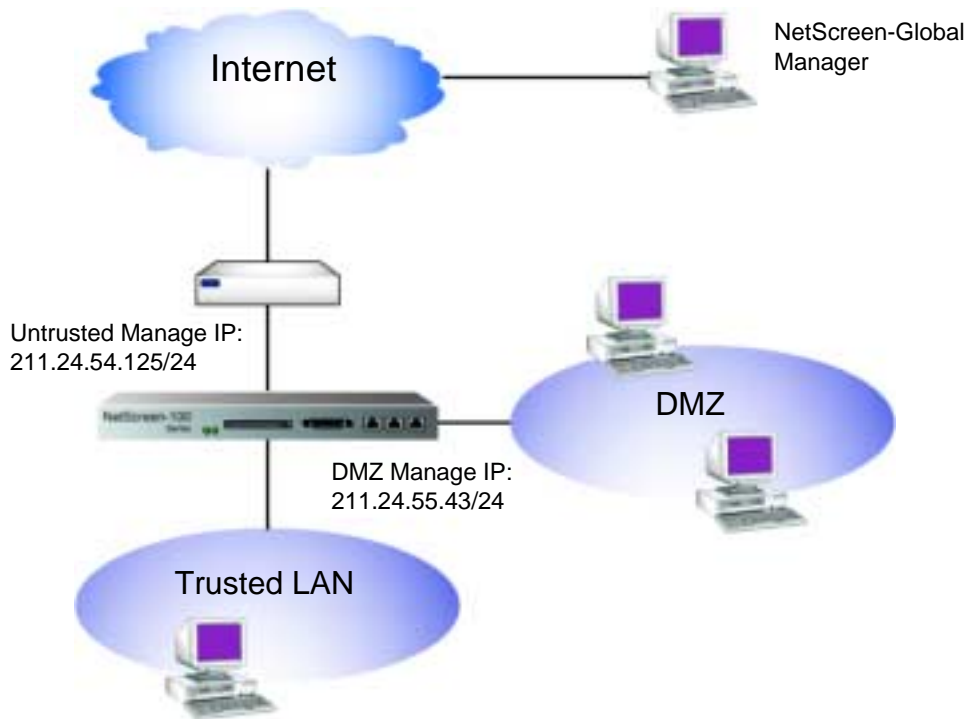
Manage IP

The Trusted, Untrusted, and DMZ (NetScreen-10 and -100) interfaces can have two IP addresses: an interface IP address that corresponds with the physical port through which that interface connects to a network, and a Manage IP address that can be used to receive administrative traffic.

You can specify a Manage IP address for managing a NetScreen device through every available interface. Also, when a NetScreen-100 or -1000 is a slave unit in a redundant group for High Availability, you can access and configure the unit through its Manage IP address (or addresses).

Example: Setting Manage IPs for Multiple Interfaces

In this example, a small group of local administrators in the DMZ use the DMZ interface exclusively for HTTP, SNMP, and Telnet traffic. The Untrusted interface must also be able to support administrative traffic from a remote administrator using NetScreen-Global Manager. Manage IP addresses are set for both the DMZ and Untrusted interfaces to allow administrative access from both of those directions.



WebUI

1. Interface >> DMZ >> Edit: Enter the following, and then click **Save**:

IP Address: 211.24.55.144

Netmask: 255.255.255.0

Default Gateway: 0.0.0.0

Manage IP: 211.24.55.43

Traffic Bandwidth: 0

WebUI: (select)

Telnet: (select)

SNMP: (select)

2. Interface >> Untrusted >> Edit: Enter the following, and then click **Save and Reset**:

IP Address: 211.24.54.10
 Netmask: 255.255.255.0
 Default Gateway: 0.0.0.0
 Manage IP: 211.24.54.125
 Traffic Bandwidth: 0
 NS-Global: (select)
 NS-GlobalPRO: (select)

CLI

1. set interface dmz ip 211.24.55.144 255.255.255.0
2. set interface dmz manage-ip 211.24.55.43
3. set interface dmz manage web
4. set interface dmz manage telnet
5. set interface dmz manage web
6. set interface untrust ip 211.24.54.10 255.255.255.0
7. set interface untrust manage-ip 211.24.54.125
8. set interface untrust manage global
9. set interface untrust manage global-pro
10. save

Management Interface

The Management (MGT) interface allows you to manage the NetScreen-1000 through a separate interface, moving administrative traffic outside the regular network user traffic. Separating administrative traffic from network user traffic greatly increases administrative security and assures constant management bandwidth.

On the NetScreen-1000, the Management (MGT) interface provides a dedicated connection for management traffic. Connect one end of a Cat-5 serial cable to the MGT interface and the other end to your management network or workstation.

With this arrangement, you can use a Web browser to manage through the WebUI (see “Web User Interface” on page 9-126) or use Telnet (see “Telnet” on page 9-129) to manage through the CLI. You can also manage through the MGT interface by connecting a workstation directly to the console port or modem port and accessing the device through its MGT IP address.

Example: Administration Through the MGT Interface

You can configure the NetScreen-1000 to allow administration through one or more of the Trusted, Untrusted, or Management (MGT) interfaces. To maintain the highest level of security, NetScreen recommends that you limit administrative traffic exclusively to the MGT interface and user traffic to the Trusted and Untrusted interfaces. This prohibits administrative access from Trusted and Untrusted workstations that are connected to your network and assures bandwidth availability for administrative traffic.

In this example, the IP address of the MGT interface is 192.168.20.2/24, and the MGT interface is enabled to receive Telnet and Web administrative traffic.

WebUI

Interface >> Management >> Edit: Enter the following, and then click **Save and Reset**:

IP Address: 192.168.20.2

Netmask: 255.255.255.0

Default Gateway: 0.0.0.0.

Traffic Bandwidth: 0

Enable Manageability: WebUI (select),
Telnet (select)

CLI

1. set interface mgt ip 192.168.20.2 255.255.255.0
2. set interface mgt manage web
3. set interface mgt manage telnet
4. save

Virtual Private Networks

You can use a Virtual Private Network (VPN) to secure remote management and monitoring of a NetScreen device from either a dynamically assigned or fixed Untrusted IP address. Using a VPN, you can protect any kind of traffic, such as HTTP, Telnet, or SNMP.

NetScreen supports three methods for creating a VPN tunnel:

- *Manual Key*: You manually set the three elements that define a Security Association (SA) at both ends of the tunnel: a Security Parameters Index (SPI), an encryption key, and an authentication key. To change any element in the SA, you must manually enter it at both ends of the tunnel.
- *AutoKey IKE with Preshared Key*: One or two preshared secrets—one for authentication and one for encryption—function as seed values. Using them, the IKE protocol generates a set of symmetrical keys at both ends of the tunnel; that is, the same key is used to encrypt and decrypt. At predetermined intervals, these keys are automatically regenerated.
- *AutoKey IKE with Certificates*: Using the Public Key Infrastructure (PKI), the participants at both ends of the tunnel use a digital certificate (for authentication) and an RSA public/private key pair (for encryption). The encryption is asymmetrical; that is, one key in a pair is used to encrypt and the other to decrypt.

By default, NetScreen VPN tunnels use the Untrusted interface IP address (in NAT mode) or the System IP address (in Transparent mode) as the tunnel endpoint. Optionally, you can designate the Trusted interface as the endpoint when directing management traffic through a VPN tunnel to an address on the Untrusted side. This allows you to create an Access Policy encrypting management traffic, such as SNMP or syslog, originating within the NetScreen device (with the source address being the Trusted interface) and destined for a remote server on the Untrusted side. To enable this, do the following:

WebUI

Select one or more of the following check boxes, and then click **OK**:

Admin >> Syslog: Enable Syslog VPN encryption: (select)

Admin >> Syslog: Enable WebTrends VPN encryption: (select)

Admin >> SNMP: Enable SNMP VPN encryption: (select)

Admin >> NS Global: Enable Global Manager/PRO VPN encryption: (select)

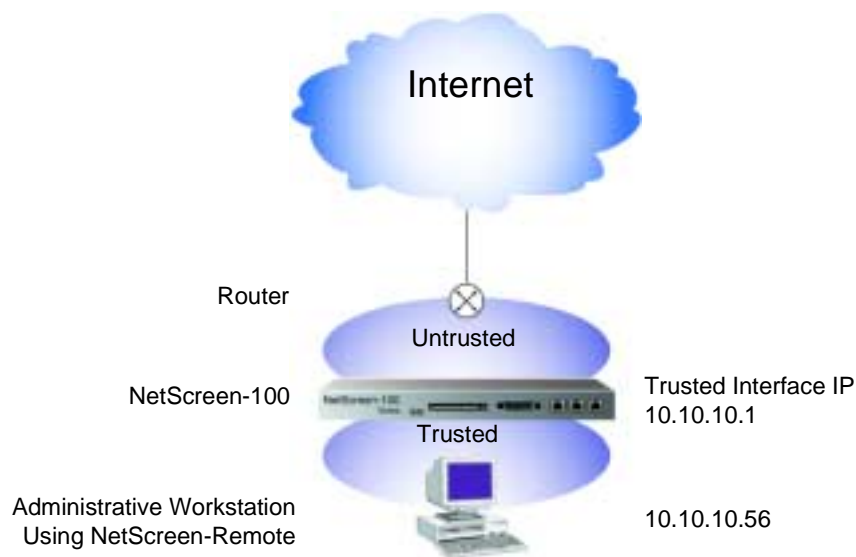
CLI

```
set {global | snmp | syslog | webtrends} vpn
```

Note: You also need to define the VPN tunnel and create an Access Policy.

Example: Administration through a VPN Tunnel on the Trusted Side

In this example, the network security administrator uses a VPN to keep security separate from general network administration. She creates a Manual Key VPN tunnel from her workstation at 10.10.11.56/24 to 10.10.10.1/24, the IP address of the Trusted interface. She has NetScreen-Remote 5.0 installed on her workstation.



WebUI

NetScreen-100

1. Address >> Trusted: New Address: Enter the following, and then click **OK**:
Name: Trusted Interface

Address: 10.10.10.1

Netmask: 255.255.255.255

2. Address >> Untrusted: New Address: Enter the following, and then click **OK**:

Name: Admin 1

Address: 10.10.10.56

Netmask: 255.255.255.255

Comment: For VPN Admin

3. VPN >> Manual Key >> New Manual Key Entry: Enter the following, and then click **OK**:

Name: Admin Tunnel

Gateway IP: 10.10.10.56

Security Index: 4567 (Local) 5555 (Remote)

ESP-CBC: (select)

Encryption Algorithm: DES-CBC

Generate Key by Password⁸: netscreen1

Authentication Algorithm: MD5

Generate Key by Password: netscreen2

Tunnel to Trusted Interface: (select)

Note: By default, a VPN tunnel to a NetScreen device terminates at the Untrusted interface. After you select the **Tunnel to Trusted Interface** option, you cannot clear it. To modify the tunnel to terminate at the Untrusted interface, you must first remove the existing tunnel, and then create a new one.

If the NetScreen device is in Transparent mode, then the tunnel from the Trusted side terminates at the system IP address.

4. Policy >> Outgoing >> New Policy: Enter the following, and then click **OK**:

Name: Admin VPN Policy

8. Because NetScreen-Remote processes passwords into keys differently than other NetScreen products do, after you configure the tunnel do the following: (1) Return to the Manual Key Configuration dialog box (click **Edit** in the Configure column for "Admin Tunnel"); (2) copy the generated hexadecimal key; and (3) use that hexadecimal key when configuring the NetScreen-Remote end of the tunnel.

Source Address: Trusted Interface

Destination Address: Admin 1

Service: Any

Action: Tunnel

VPN Tunnel: Admin VPN

CLI

1. set address trust "Trusted Interface" 10.10.10.1 255.255.255.255
2. set address untrust "Admin 1" 10.10.11.56 255.255.255.255
3. set vpn trust manual 4567 5555 "Admin tunnel" gateway 10.10.10.56 esp des password netscreen1 auth md5 password netscreen2
4. set policy outgoing "Trusted Interface" "Admin 1" any tunnel vpn "Admin tunnel"

NetScreen-Remote Security Policy Editor

1. Click **Options** >> **Secure** >> **Specified Connections**.
2. Click the **Add a new connection** button, and type **ns100** next to the new connection icon that appears.
3. Configure the connection options:

Connection Security: Secure
Remote Party ID Type: IP Address
IP Address: 10.10.10.1
4. Click the **PLUS** symbol, located to the left of the new connection icon, to expand the connection policy.
5. ns100 >> Security Policy: Use Manual Keys: (select)
6. Click the **PLUS** symbol, located to the left of the Security Policy icon, and then the **PLUS** symbol to the left of Key Exchange (Phase 2) to expand the policy further.
7. Key Exchange (Phase 2) >> Proposal 1: Select the following IPSec Protocols:

Encapsulation Protocol (ESP): (select)
Encrypt Alg: DES
Hash Alg: MD5
Encapsulation: Tunnel
8. Proposal 1 >> Inbound Keys: In the Security Parameters Index field, type 5555, and then click **Enter Key**.

9. Inbound Keys >> Enter Key: Enter the following⁹, and then click **OK**:
 - Choose key format: Binary
 - ESP Encryption Key: dccbee96c7e546bc
 - ESP Authentication Key:
dccbe9e6c7e546bcb0b667794ab7290c
10. Proposal 1 >> Outbound Keys: In the Security Parameters Index field, type 4567, and then click **Enter Key**.
11. Outbound Keys >> Enter Key: Enter the following, and then click **OK**:
 - Choose key format: Binary
 - ESP Encryption Key: dccbee96c7e546bc
 - ESP Authentication Key: dccbe9e6c7e546bcb0b667794ab7290c
12. ESP Authentication Key: dccbe9e6c7e546bcb0b667794ab7290c
13. Click the **Save** button.

9. These are the two generated keys that you copied after configuring the NetScreen device.

Building Blocks for Access Policies and VPNs 10

This chapter discusses the concepts common to Access Policies and Virtual Private Networks (VPNs). The specific topics discussed are:

- “Addresses” on page 10-153
- “Virtual IP” on page 10-161
- “Mapped IP” on page 10-166
- “Users” on page 10-168
- “Dialup User Groups” on page 10-173
- “Services” on page 10-177
- “Service Groups” on page 10-180
- “Schedules” on page 10-184

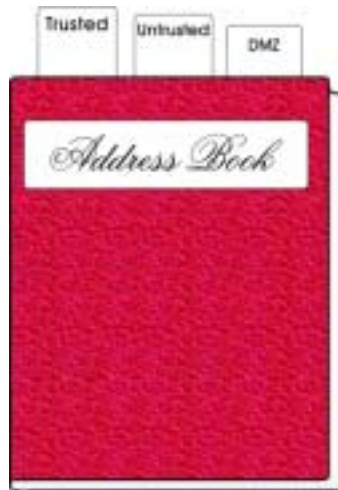
ADDRESSES

The NetScreen ScreenOS classifies the addresses of all other devices by location and netmask. Trusted addresses are located behind the Trusted interface and appear as green in the WebUI. Untrusted addresses are located behind the Untrusted interface and appear as red. DMZ addresses are located behind the DMZ interface (NetScreen-10 and -100) and appear as brown.

Individual hosts have only a single IP address defined and are represented by a single computer icon in the WebUI. Individual hosts must have a netmask setting of 255.255.255.255 (which masks out all but this host).

Subnets have an IP address and a netmask (for example, 255.255.255.0 or 255.255.0.0) and are represented by multiple computer icons in the WebUI.

Before you can configure Access Policies to permit, deny, or tunnel traffic to and from individual hosts and subnets, you must make entries for them in the Trusted, Untrusted, and DMZ (NetScreen-10 and -100) sections of the NetScreen address book.



Note: You do not have to make address book entries for “Inside Any,” “Outside Any,” or “DMZ Any.” These terms automatically apply to all devices physically located beyond these respective interfaces.

Address Book Entries

Before you can set up many of the NetScreen firewall, VPN, and traffic shaping features, you need to define addresses in the address book. The address book contains the IP addresses or domain names¹ of hosts or subnets whose traffic is either allowed, blocked, encrypted, or user-authenticated.

-
1. Before you can use domain names for address book entries, you must configure the NetScreen device for Domain Name System (DNS) services.

Example: Adding Addresses

In this example, you add the subnet “Santa Clara Eng” with the IP address 192.10.10.0/24 as a Trusted address, and the address www.firenet.com as an Untrusted address.

WebUI

1. Address >> Trusted >> New Address: Enter the following information, and then click **OK**:

Address Name: Santa Clara Eng
IP Address/Domain Name: 192.10.10.0
Netmask: 255.255.255.0
Trust: (select)

2. Address >> Untrusted >> New Address: Enter the following information, and then click **OK**:

Address Name: FireNet
IP Address/Domain Name: www.firenet.com
Netmask: 255.255.255.255
Untrust: (select)

CLI

1. set address trust “Santa Clara Eng” 192.10.10.0 255.255.255.0
2. set address untrust www.firenet.com 255.255.255.255
3. save

Example: Modifying Addresses

In this example, you change the address entry for the host “Santa Clara Eng” to reflect that this host has moved to Dallas and reassigned an IP address of 192.10.40.0/24.

WebUI

Address >> Trusted >> Edit (for Santa Clara Eng): Change the name and IP address to the following, and then click **OK**:

Address Name: Dallas Eng

IP Address/Domain Name: 192.10.40.0

CLI

1. unset address trust “Santa Clara Eng”
2. set address trust “Dallas Eng” 192.10.40.0 255.255.255.0
3. save

Note: After you define an address—or an address group—and associate it with an Access Policy, you cannot change the address location to another interface (such as from Trusted to Untrusted). To change its location, you must first disassociate it from the underlying Access Policy.

Example: Deleting Addresses

In this example, you remove the address entry for the subnet “Dallas Eng.”

WebUI

Address >> Trusted: Click **Remove** in the Configure column for Dallas Eng.

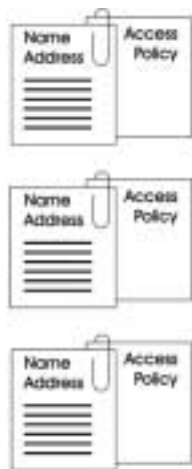
CLI

1. unset address trust “Dallas Eng”
2. save

Address Groups

The previous section explained how you create, modify, and delete address book entries for individual hosts and subnets. As you add addresses to the address book, it becomes difficult to manage how Access Policies affect each address entry. NetScreen allows you to create groups of addresses. Rather than manage a large number of address book entries, you can manage a small number of groups. Changes you make to the group are applied to each address entry in the group.

1 Access Policy per Address



1 Access Policy per Address Group



The Address Group option has the following features:

- You can create address groups on the Trusted, Untrusted, or DMZ sides.
- You can create address groups with existing users, or you can create empty address groups and then fill them with users.
- Address group entries can be used like individual address book entries.
- NetScreen applies Access Policies to each member of the group by creating individual Access Policies for each group member. While you only have to create one Access Policy for a group, NetScreen actually creates an Access Policy for each member in the group (as well as for each service configured for each user).²
- When an individual address book entry is deleted from the address book, it is also removed from all groups in which it was referenced.

The following constraints apply:

- Address groups can only contain addresses for one type of interface (Trusted, Untrusted, or DMZ).
- Address names cannot be the same as group names. If the name “Paris” is used for an individual address entry, it cannot be used for a group name.
- If an address group is referenced in an Access Policy, the group cannot be removed. It can, however, be edited.
- When a single Access Policy is assigned to an address group, it is applied to each group member individually, and the NetScreen device makes an entry for each member in the access control list (ACL). If you are not vigilant, it is possible to exceed the number of available Access Policy resources, especially if both the source and destination are address groups
- You cannot add the predefined addresses: “Outside Any,” “Inside Any,” “DMZ Any,” “All Virtual IPs,” and “Dial-Up VPN” to groups.
- The following table lists the group size limits for each platform.

Hardware Platform	Number of Groups	Members per Group
NetScreen-5	16	16
NetScreen-10	32	32
NetScreen-100	64	64
NetScreen-1000	256 (Root); 8 (Virtual System)	256 (Root); 16 (Virtual System)

-
2. The automatic nature by which NetScreen applies Access Policies to address group members, saves you from having to create them one by one for each address. Furthermore, NetScreen writes these Access Policies to ASIC which makes lookups run very fast.

Example: Creating an Address Group

In the following example, you create a group named “HQ 2nd Floor” that includes “Santa Clara Eng” and “Tech Pubs,” two Trusted addresses that you have already entered in the address book.

WebUI

1. Address >> Trusted >> New Group: Enter the following group name, move the following addresses, and then click **OK**:

Group Name: HQ 2nd Floor

Group Members << Available Members:

Santa Clara Eng

Tech Pubs

CLI

1. set group address trust “HQ 2nd Floor” add “Santa Clara Eng”
2. set group address trust “HQ 2nd Floor” add “Tech Pubs”
3. save

Example: Editing a Group Address Entry

In this example, you add Support (an address that you have already entered in the address book) to the HQ 2nd Floor address group.

WebUI

1. Address >> Trusted >> Edit (for HQ 2nd Floor): Move the following address, and then click **OK**:

Group Members << Available Members:

Support

CLI

1. set group address trust “HQ 2nd Floor” add Support
2. save

Example: Removing an Address Group Member and a Group

In this example, you remove the member Support from the HQ 2nd Floor address group, and how to delete Sales, an address group that you had previously created.

WebUI

1. Address >> Trusted >> HQ 2nd Floor >> Edit: Move the following address, and then click **OK**:

Group Members >> Available Members:
Sales

2. Address >> Trusted: Click **Remove** in the Configure column for Sales.

CLI

1. unset group address trust "HQ 2nd Floor" remove Support
2. unset group address trust Sales
3. save

Note: The NetScreen device does not automatically delete a group from which you have removed all names.

VIRTUAL IP

The Virtual IP (VIP) feature provides network flexibility and security. In a Network Address Translation (NAT) environment, host computers use non-routable IP addresses inside the firewall while maintaining full Internet connection and functionality. This feature gives network administrators flexibility to expand their networks without being constrained by the scarcity of legal IP addresses. In addition, NAT also provides better network security by hiding internal network topology and host information from the outside world.

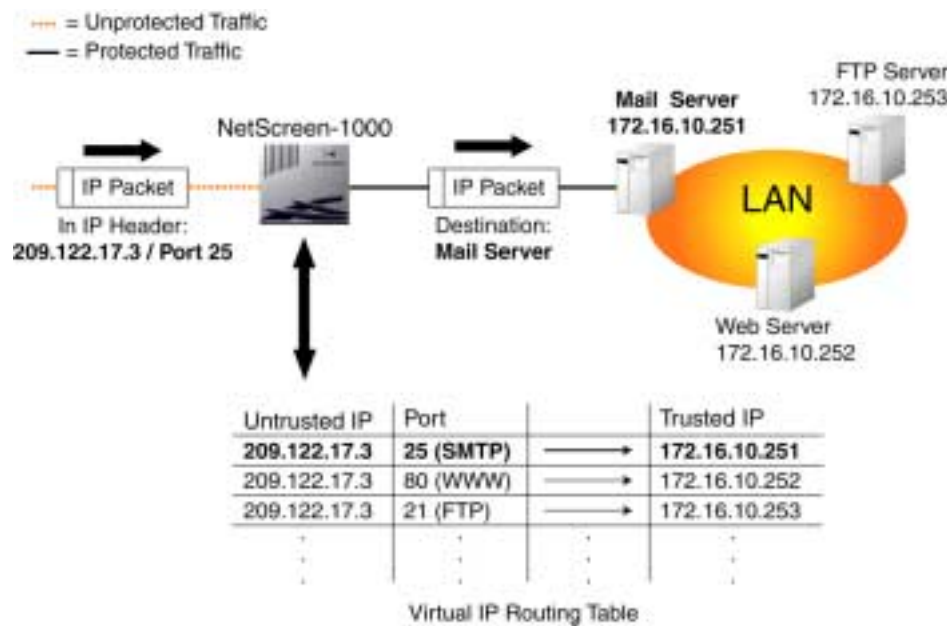
However, to maintain some Internet services (for example, e-mail, POP3, FTP), a server with a legal IP address must be present to service the requests. VIP allows you to map routable IP addresses to internal servers, thereby providing transparent connections for a NAT network to the Internet. Other benefits of using VIP include:

Scalability: As Internet service demand increases, companies need to improve servers' performance in order to maintain the quality of their services. While upgrading the server to a larger, faster machine generally relieves the short-term pressures, the disruption to services and the prohibitive cost of upgrading quickly make this solution undesirable.

Redundancy: With Virtual IP, servers can be assigned to the same IP address and mirrored to provide High Availability (HA) for network services. Individual servers can also be taken off-line for maintenance without disruption to network traffic.

Reduction in capital cost: Multiple domains and Web servers can be mapped to the same physical server, thus reducing the cost of computer equipment as well as the associated administration tasks.

Flexibility in assigning ports: By setting up Virtual IP (VIP) addresses, you can configure your NetScreen device to route traffic destined for many different IP addresses on the subnet of the Untrusted interface to specific addresses on the Trusted network.



The maximum number of VIPs, and the maximum number of services per VIP that are supported by each NetScreen device are as follows:

	VIPs	Services/VIP
NetScreen-5	1	64
NetScreen-10	2	64
NetScreen-100	4	8
NetScreen-1000	6	8

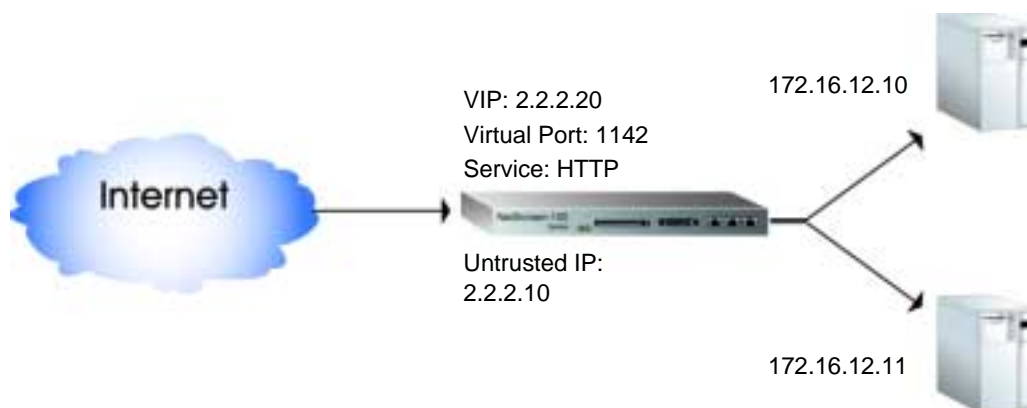
Required Information

You need the following information to define a Virtual IP:

- The IP address for the VIP, which must be in the same subnet as the Untrusted interface and can even be the same address as the Untrusted interface³
- The port number for communication between the Trusted server and the Untrusted interface on the NetScreen device
- The IP address for the server on the Trusted interface that processes the requests

Example: Configuring Virtual IP Servers

In this example, you configure a VIP at 2.2.2.20 to route inbound HTTP traffic to a pool of two Web servers at 172.16.12.10 and 172.16.12.11. (The Untrusted IP address of the NetScreen-100 is 2.2.2.10/24.) The port number for HTTP is translated from 80 (the standard protocol ID number) to 1142.



3. On the NetScreen-5, the Untrusted interface can receive its Untrusted IP address dynamically via DHCP or PPPoE. If you want to use a VIP in such a situation, do either of the following: In the WebUI (Virtual IP >> Virtual Server IP >> Click here to configure), select the **Same as the Untrusted IP address** option when setting up the VIP; in the CLI, use the **set vip untrust-ip** command.

WebUI

1. Virtual IP >> Virtual IP1 >> Virtual Server IP: Enter the following address, and then click **OK**:

Virtual IP Address: 2.2.2.20

2. New Service: Enter the following, and then click **OK**:

Virtual Port: 1142⁴

Service: HTTP⁵

(NetScreen-100) Load Balance: None

1 Server IP: 172.16.12.10

(NetScreen-100) Server Weight: 1

2 Server IP: 172.16.12.11

(NetScreen-100) Server Weight: 1

CLI

1. set vip 2.2.2.20 1142 http none 172.16.12.10/1
2. set vip 2.2.2.20 1142 http none 172.16.12.11/1
3. save

-
4. Using non-standard port numbers adds another layer of security, thwarting attacks that check for services at standard port numbers.
 5. When initially configuring a VIP, you can only map one service at a time. For example, if you are mapping six services to a Virtual IP, you must enter each one individually.

Example: Editing a VIP Configuration

In this example, you modify the Virtual IP server configuration you just created. In this case, you add an additional server 172.16.12.12.

WebUI

Virtual IP >> Virtual IP1 >> Edit (in the HTTP row): Enter the following, and then click **OK**:

3 Server IP: 172.16.12.12
(NetScreen-100) Server Weight: 1

CLI

1. set vip 2.2.2.20 1142 http none 172.16.12.12/1
2. save

Example: Removing a VIP Configuration

In this example, you delete the VIP configuration that you just created and modified.

WebUI

Virtual IP >> Virtual IP1 >> Virtual Server IP 2.2.2.20: Click **Clear**.

CLI

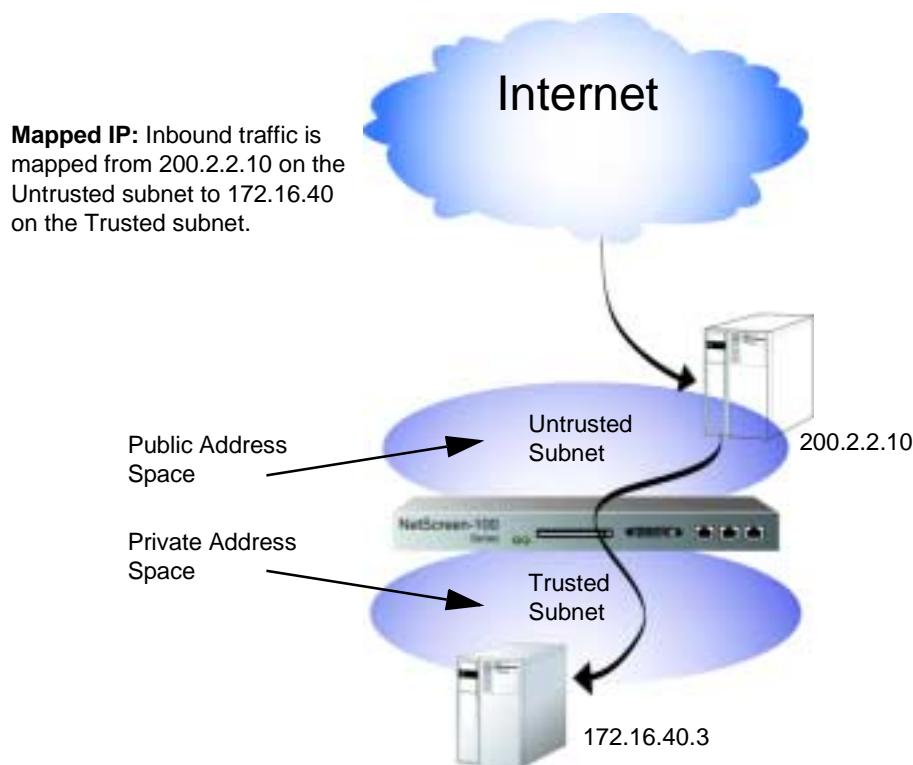
1. unset vip 2.2.2.20
2. save

Note: You cannot edit or remove a Virtual IP entry when existing Access Policies are still associated with it.

MAPPED IP

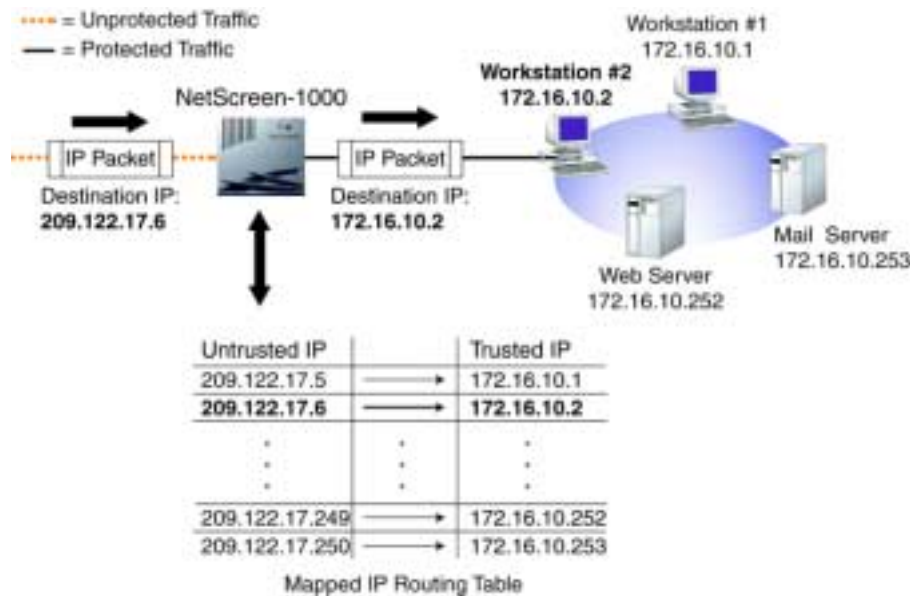
Mapped IP (MIP) is a direct one-to-one mapping of traffic destined for one IP address to another IP address, and is based solely on IP addresses. When the NetScreen device is operating in NAT mode, an MIP provides a means for incoming traffic to reach a private address on the Trusted network. You can configure an MIP address to route traffic destined for an address on the Untrusted subnet to a different address on the Trusted subnet, regardless of the service and corresponding port number involved.

By setting up MIP addresses, you can configure the NetScreen device to route traffic destined for many different IP addresses on the subnet of the Untrusted interface to specific addresses on the Trusted network.



Example: Creating a Mapped IP Address

This example explains how to map incoming traffic destined to the Untrusted IP address 209.122.17.6 to the Trusted IP address 172.16.17.6.



WebUI

Virtual IP >> Mapped IP >> New Entry: Enter the following and then click **OK**:

Untrusted IP Address: 209.122.17.6

Netmask: 255.255.255.255

Map to IP Address: 172.16.10.2

CLI

1. set mip 209.122.17.6 host 172.16.10.2 255.255.255.255
2. save

Note: You must define an Access Policy allowing the mapped IP address to be accessed. No address book entry is required for a Mapped IP.

You can map an address-to-address or subnet-to-subnet relationship. When a subnet-to-subnet mapped IP configuration is defined, the netmask is applied to both the mapped IP subnet and the original IP subnet.

USERS

NetScreen supports three kinds of users:

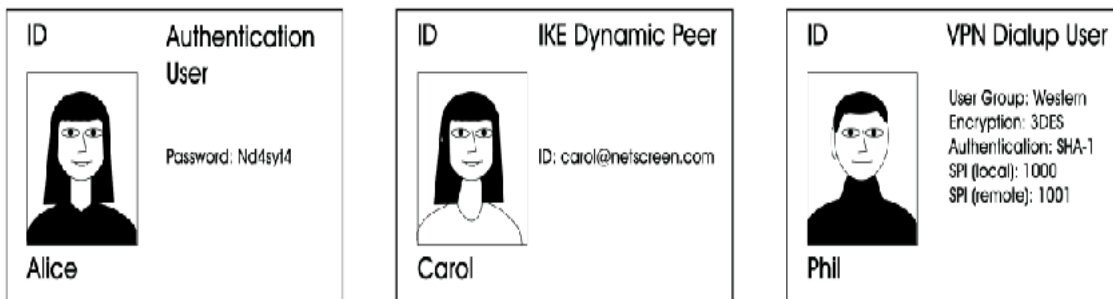
- **Authentication User** – A network user who must provide a user name and password for authentication when initiating a connection across the firewall.
- **IKE Dynamic Peer** – A VPN user with a dynamically assigned IP address. The user provides his or her identity using an e-mail address, an IP address, or a domain name. The VPN can use either AutoKey IKE with a preshared key or AutoKey IKE with a certificate.
- **VPN Dialup User** – A VPN user with a dynamically assigned IP address. The VPN uses the manual key method for encryption and/or authentication.

Before traffic from an authentication user can traverse the firewall, and before a VPN user participate in a VPN, you must create a configuration profile for each one.

Example: Creating Three New Users

In this example, you create the following users:

- An authentication user named Alice with the password “Nd4syt4.”
- An IKE dynamic peer named Carol with the ID carol@netscreen.com
- A VPN dialup user named Phil, who is assigned to the dialup user group “Western” and uses 3DES encryption with SHA-1 authentication.



WebUI

1. Users >> Users >> New User: Enter the following, and then click **OK**:
 - User Name: Alice
 - Authentication User: (select)
 - Authentication Password: Nd4syt4
 - Confirm Password: Nd4syt4
 - Status: Enable (select)
2. Users >> Users >> New User: Enter the following, and then click **OK**:
 - User Name: Carol
 - VIKE Dynamic Peer: (select)
 - User Group: None
 - Identity: carol@netscreen.com
3. Users >> Users >> New User: Enter the following, and then click **OK**:
 - User Name: Phil
 - VPN Dialup User - Manual Key Only: (select)
 - User Group: Western
 - Security Index: 1000 (Local); 1001 (Remote)
 - ESP: (select)
 - ESP-Encryption-Algorithm: 3DES CBC

Generate Key by Password: 12345678

Authentication Algorithm: SHA-1

Generate Key by Password: 99999999

CLI

1. set user Alice password Nd4syt4
2. set user Carol ike-id carol@netscreen.com
3. set user Carol enable
4. set user Phil dialup 1000 1001 esp 3des pass 12345678 auth sha-1 pass 99999999
5. save

User Authentication

There are a number of different protocols that your NetScreen device can use to verify that a user is who they say they are. These different techniques are discussed in this section.

Internal Database

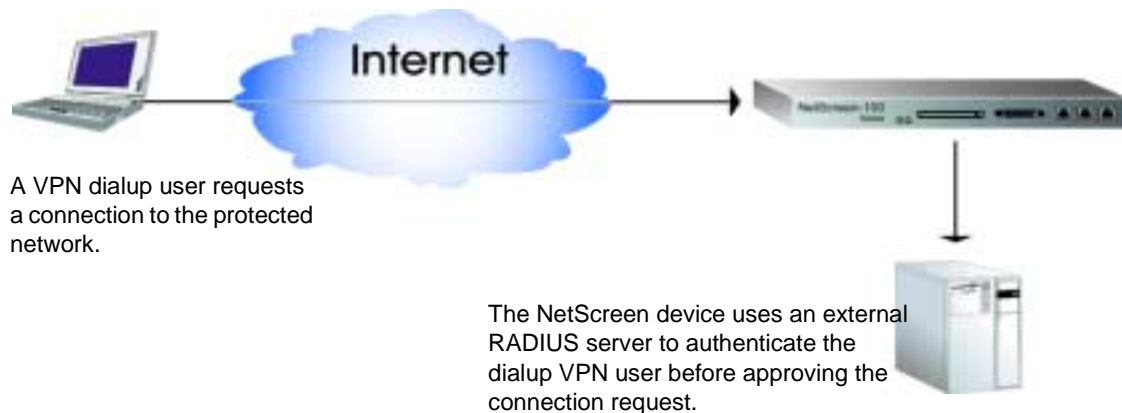


All NetScreen devices support a built-in user database for authentication. The maximum number of entries supported by each device are:

Platform	Total Number of Entries
NetScreen-5	100
NetScreen-10	500
NetScreen-100	1500
NetScreen-1000	2000

After entering the user name and password in the database, you must create an Access Policy that requires a user to authenticate him or herself when initiating a specified connection (for example, outbound or inbound HTTP, or Telnet traffic). When the user attempts to initiate traffic for which the Access Policy applies, he or she is prompted to enter his or her name and password. Before granting permission, the NetScreen device validates the user name and password by checking them against those stored in the database.

RADIUS



The Remote Authentication Dial-In User Service (RADIUS) is a protocol for an authentication server which can be modified to run on different kinds of networks, and makes it easy and efficient to manage large modem pools. The focus for RADIUS is the remote user who needs to dial into the network.

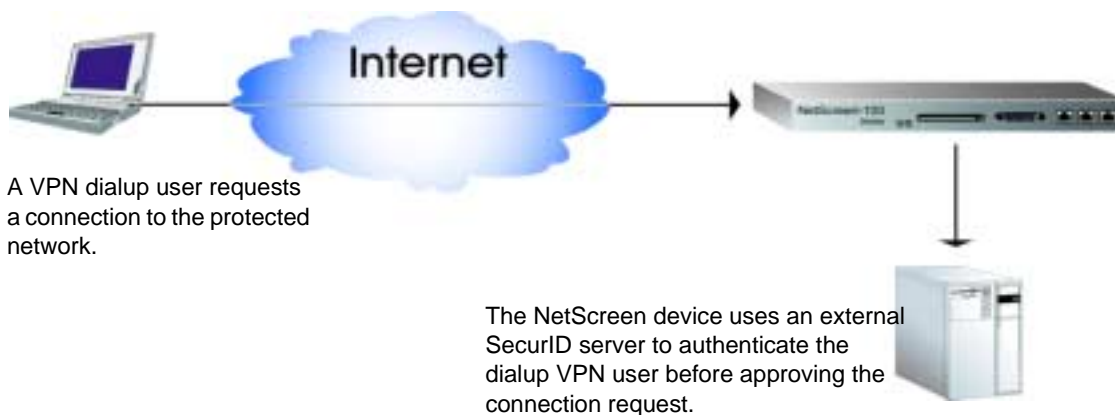
RADIUS uses an authentication server to solve the security problems associated with remote computing. Distributed security separates user authentication and authorization from the communications process and creates a single, central location for user authentication data.

One RADIUS server can support up to tens of thousands of users, making it a very practical service for rapidly growing networks.

The RADIUS client (that is, the NetScreen device) authenticates users through a series of communications between the client and the server. Basically, RADIUS asks the person logging on to enter his or her user name and password. It then compares these values to those in its database, and once a user is authenticated, the client provides the user with access to the appropriate network services.

SecurID

The relationship of NetScreen device and a Security Dynamics Technologies® SecurID® ACE™ server is similar to that of a NetScreen device and a RADIUS server; that is, the NetScreen device acts as a client, forwarding authentication requests to the external server for approval. SecurID differs from RADIUS in that the user password involves a continually changing string of numbers.

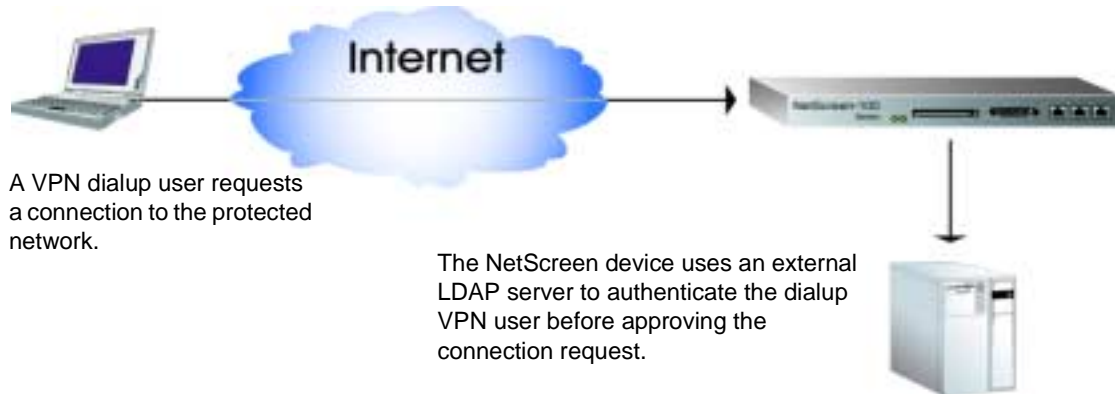


SecurID issues a credit card sized device with an LCD window that displays a randomly generated string of numbers that changes every minute. There is no other information on the card besides the number in the LCD display.



Security Dynamics issues a card and a personal ID number (PIN) to a registered user and maintains the user profile in their database. When the user is prompted to authenticate himself, he enters his name and password, which is his PIN followed by the string of numbers currently displayed on his card. The numbers displayed on the card change every minute. The values that display are generated by an algorithm known only by Security Dynamics. This value is saved to the Security Dynamics database entry for this PIN. When the user to be authenticated enters his PIN and the number on his card, Security Dynamics compares these values to those in the database. If they match, the user is authenticated.

Lightweight Directory Access Protocol



Lightweight Directory Access Protocol (LDAP) is a directory server standard developed by Netscape® to help in authenticating users attempting to connect to networks controlled by directory servers.

LDAP is a client-server protocol for accessing a directory service. It can be used as a front-end to X.500, as a stand-alone protocol, or as a directory server.

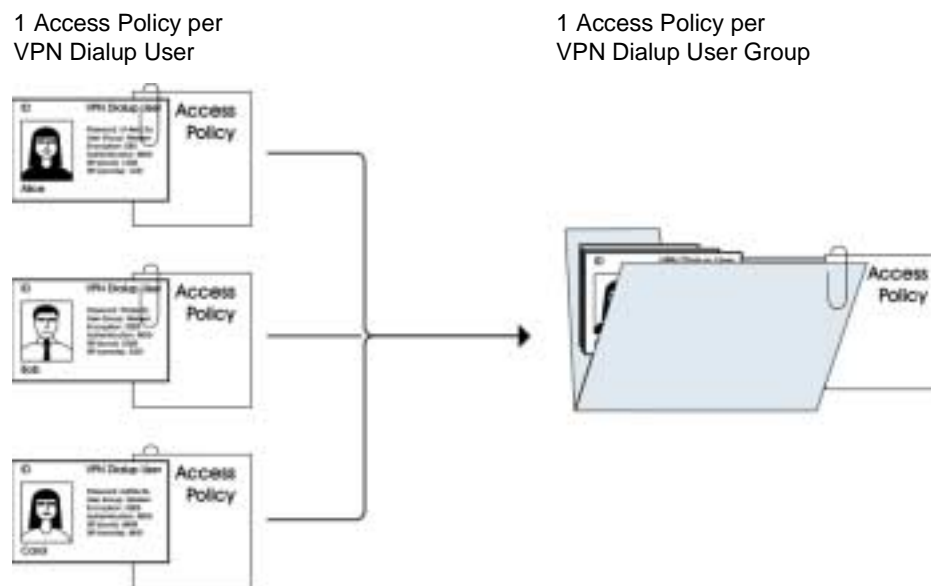
LDAP does not require the upper layers OSI stack, it is a simpler protocol to implement (especially in clients), and LDAP is under IETF change control and so can more easily evolve to meet Internet requirements.

The LDAP information model is based on the entry, which contains information about some object (for example, a person). Entries are composed of attributes, which have a type and one or more values. Each attribute has a syntax that determines what kind of values are allowed in the attribute and how those values behave during directory operations.

Examples of attribute syntaxes are for IA5 (ASCII) strings, JPEG photographs, u-law encoded sounds, URLs, and Pretty Good Privacy (PGP) keys.

Dialup User Groups

One of the main reasons organizations use VPNs is to allow remote dialup users to be able to traverse the firewall from anywhere in the world and access their data in a secure environment. The VPN tunnel connection from them to the corporate site assures security as well as access.



To manage a number of remote dialup users, NetScreen enables you to create dialup user groups. Rather than manage each user individually, you can aggregate users into a group. Changes you make to the group are then propagated to each group member. The examples that follow illustrate how to create new dialup user groups and then add users to it. Other examples show how to remove members from a group and move members from one group to another.

Example: Defining a New Dialup User Group

In this example, you define a new dialup user group named Tahoe.

WebUI

Users >> Dialup Group >> New Group: Enter the following, and then click **OK**:

Dialup Group Name: Tahoe

CLI

1. set dialup-group tahoe
2. save

Example: Adding a Member to a Dialup User Group

In this example, you add a user named Fred to the dialup user group Tahoe.

WebUI

Users >> Users >> Edit (for the user named Fred): Select the following, and then click **OK**:

VPN Dialup User: (select)

User Group: Tahoe

CLI

1. set dialup-group tahoe + Fred
2. save

Example: Removing an Existing Group Member

In this example, you delete Phil from the Tahoe dialup user group.

WebUI

Users >> Users: Click **Remove** (for Phil).

CLI

1. set dialup-group Tahoe - Phil
2. save

Example: Moving a Group Member to Another Group

In this example, you move Phil from the dialup user group Tahoe to the group Santa Cruz.

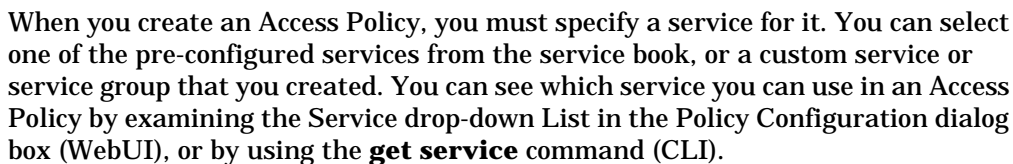
WebUI

1. Users >> Users >> Edit (for Phil): Enter the following, and then click **OK**:
VPN Dialup User: Select
User Group: Santa Cruz

CLI

1. set dialup-group Tahoe - Phil
2. set dialup-group "Santa Cruz" + Phil
3. save

The illustration below shows the services supported in ScreenOS 2.5. For information on each service, hold your cursor over the service icon. In this illustration, the mouseover information block is displayed for X-Windows.



10-177

Example: Viewing the Service Book

In this example, you view the predefined and custom services in the service book.

WebUI

1. Service >> Pre-defined
2. Service >> Custom

CLI

get service

The output from the CLI is similar to that shown below.

transport	src port(low/high)	dst port(low/high)	ack/reverse
Name:ANY(Group:other/5, Id#0, Flag:128)			
0	0/65535	0/65535	0/0
Name:AOL(Group:remote/1, Id#1, Flag:128)			
tcp	1/65535	5190/5194	0/0
Name:DNS(Group:info seeking/3, Id#2, Flag:128)			
udp	0/65535	53/53	0/0
tcp	1024/65535	53/53	0/0

Example: Adding a Custom Service

To add a custom service to the service book, you need the following information:

- A name for the service, in this example “Corporate”
- A range of source port numbers valid for the service. For example, 1500-10000.
- A range of destination port numbers to receive the service request; for example, 15000-25000.
- Whether the service uses TCP or UDP protocol, or some other protocol as defined by the Internet specifications. In this example, the protocol is TCP

WebUI

Service >> Custom >> New Service: Enter the following, and then click **OK**:

Service Name: Corporate
Source Port Low: 1500
Source Port High: 10000
Destination Port Low: 15000
Destination Port High: 25000
Transport: TCP

CLI

1. set service Corporate + protocol tcp src-port 1500-10000 dst-port 15000-25000
2. set service Corporate + timeout 30
3. save

Example: Modifying a Custom Service

In this example, you change a custom service. In this case, the Transport is UDP, and the Source Port range changes to 1 through 1000.

Use the **set service <name> clear** command to remove the definition of a custom service without removing the service from the service book:

WebUI

1. Service >> Custom: Enter the following and then click **OK**:
 - Service Name: Corporate
 - Source Port Low: 1
 - Source Port High: 1000
 - Destination Port Low: 15000
 - Destination Port High: 25000
 - Transport: UDP

CLI

1. set service Corporate clear
2. set service Corporate + protocol udp src-port 1-1000 dst-port 15000-25000
3. save

Example: Removing a Custom Entry

In this example, you remove the custom service “Corporate.”

WebUI

Service >> Custom: Click **Remove** in the Configure column for “Corporate.”

CLI

1. unset service Corporate
2. save

Service Groups

A service group is a set of services that you have gathered together under one name. After you create a group containing several services, you can then apply services at the group level to Access Policies, thus simplifying administration.

The NetScreen service group option has the following features:

- Each service book entry can be referenced by one or more service groups.
- Each service group can contain pre-defined and user-defined service book entries.
- Each service group can be referenced by other service groups, providing that a group referencing other groups does not include itself in the reference list.

Service groups are subject to the following limitations:

- Service groups cannot have the same names as services; therefore, if you have a service named “FTP,” you cannot have a service group named “FTP.”
- If a service group is referenced in an Access Policy, you can edit the group but you cannot remove it until you have first removed the reference to it in the Access Policy.
- If a custom service book entry is deleted from the service book, the entry is also removed from all the groups in which it was referenced.
- The all-inclusive service term “ANY” cannot be added to groups.
- The following table lists the number of service groups supported by platform.

Hardware Platform	Number of Groups	Number of Members
NetScreen-5	16	16
NetScreen-10	32	32
NetScreen-100	64	64
NetScreen-1000	256 (Root); 8 (Virtual System)	64 (Root); 16 (Virtual System)

Example: Creating a Service Group

This example illustrates how you create a custom service named Wiget that supports IKE, FTP, and LDAP services.

WebUI

1. Service >> Custom >> New Group: Enter the following, move the following services, and then click **OK**:

Group Name: Wiget

Group Members << Available Members:

IKE

FTP

LDAP

CLI

1. set group service Wiget
2. set group service Wiget add ike
3. set group service Wiget add ftp
4. set group service Wiget add ldap
5. save

Note: If you attempt to add a service to a service group that does not exist, the NetScreen device creates the group. Also, ensure that groups referencing other groups do not include themselves in the reference list.

Example: Modifying a Service Group

Although you cannot modify any of the pre-defined NetScreen services, you can modify existing user-defined custom services and service groups.

In this example, you change the existing user-defined services from IKE, FTP, and LDAP to HTTP, FINGER, IMAP, and H.323 protocols.

WebUI

Service >> Custom >> Edit (for Wiget): Move the following services, and then click **OK**:

Group Members >> Available Members:

IKE

FTP

LDAP

Group Members << Available Members:

HTTP

FINGER

IMAP

H.323

CLI

1. clear group service Wiget
2. set group service Wiget add http
3. set group service Wiget add finger
4. set group service Wiget add imap
5. set group service Wiget add h.323
6. save

Example: Deleting a Service

Although you cannot remove any of the pre-defined NetScreen services, you can remove existing user-defined custom services and service groups.

In this example, you delete HTTP from the service group Widget.

WebUI

Service >> Custom >> Edit (for Widget): Move the following service, and then click **OK**:

Group Members >> Available Members:
HTTP

CLI

1. unset group service Widget remove http
2. get service Widget
3. save

Example: Deleting a Service Group

In this example, you delete the service group Widget.

WebUI

Service >> Custom: Click **Remove** (for Widget).

CLI

1. unset group service Widget
2. save

Note: The NetScreen device does not automatically delete a group from which you have removed all members.

SCHEDULES

A schedule is a configurable object that you can associate with one or more Access Policies to define when they are in effect. Through the application of schedules, you can control network traffic flow and enforce network security.

When you define a schedule, enter values for the following parameters:

Schedule Name: The name that appears in the Schedule drop-down list in the Policy Configuration dialog box. Choose a descriptive name to help you identify the schedule. The name must be unique and is limited to 19 characters.

Comment: Any additional information that you want to add.

Recurring: Enable this when you want the schedule to repeat on a weekly basis.

Start and End Times: You must configure both a start time and an end time. You can specify up to two time periods within the same day.

Once: Enable this when you want the schedule to start and end only once.

mm/dd/yyyy hh:mm: You must enter both start and stop dates and times.

Example: Recurring Schedule

In this example, there is a short-term employee named Tom who is using the company's Internet access for personal pursuits after work. You create a schedule for non-business hours that you can then associate with an Access Policy to deny outbound TCP/IP traffic from that worker's computer (10.10.4.5/24) outside of regular business hours.

WebUI

1. Schedule >> New Schedule: Enter the following, and then click **OK**:

Schedule Name: After Hours

Comment: For non-business hours

Recurring: (select)

Period 1:

Week Day	Start Time	End Time
Sunday	00:00	23:59
Monday	00:00	06:00
Tuesday	00:00	06:00
Wednesday	00:00	06:00
Thursday	00:00	06:00
Friday	00:00	06:00
Saturday	00:00	23:59

Period 2:

Week Day	Start Time	End Time
Sunday	17:00	23:59
Monday	17:00	23:59
Tuesday	17:00	23:59
Wednesday	17:00	23:59
Thursday	17:00	23:59
Friday	17:00	23:59
Saturday	17:00	23:59

2. Address >> Trusted >> New Address: Enter the following, and then click **OK**:

Address Name: Tom

IP Address/Domain Name: 10.10.4.5

Netmask: 255.255.255.255

Comment: Temp

Location: Trust

3. Policy >> Outgoing: New Policy: Enter the following, and then click **OK**:

Name: No Net

Source Address: Tom

Destination Address: Outside Any

Service: HTTP

Action: Deny

Schedule: After Hours

CLI

1. set schedule "after hours" recurrent sunday start 00:00 stop 23:59
2. set schedule "after hours" recurrent monday start 00:00 stop 06:00 start 17:00 stop 23:59
3. set schedule "after hours" recurrent tuesday start 00:00 stop 06:00 start 17:00 stop 23:59
4. set schedule "after hours" recurrent wednesday start 00:00 stop 06:00 start 17:00 stop 23:59
5. set schedule "after hours" recurrent thursday start 00:00 stop 06:00 start 17:00 stop 23:59
6. set schedule "after hours" recurrent friday start 00:00 stop 06:00 start 17:00 stop 23:59
7. set schedule "after hours" recurrent saturday start 00:00 stop 23:59 comment "for non-business hours"
8. set address trust tom 10.10.4.5 255.255.255.0 "temp"
9. set policy outgoing tom outside-any http deny schedule "after hours"
10. save

Access Policies

11

This chapter describes what Access Policies do and how the various elements that comprise an Access Policy are related. It is divided into the following two main sections:

- “Access Policies Defined” on page 11-187
- “Access Policies Applied” on page 11-192

ACCESS POLICIES DEFINED

A firewall provides a network boundary with a single point of entry and exit—a choke point. Because all incoming and outgoing traffic must pass through the choke point, you can screen and direct all that traffic through the implementation of a set of Access Policies—the Access Control List (ACL).

Access Policies allow you to permit, deny, encrypt, authenticate, prioritize, schedule, and monitor the traffic attempting to cross your firewall, whether incoming, outgoing, to the DMZ (NetScreen-10 and -100), or from the DMZ. You decide which users and what information can enter and leave, and when and where they can go..

Note: Access Policies set in the root system of the NetScreen-1000 do not affect Access Policies set in Virtual Systems.

Anatomy of a Policy

An Access Policy must contain the following elements:

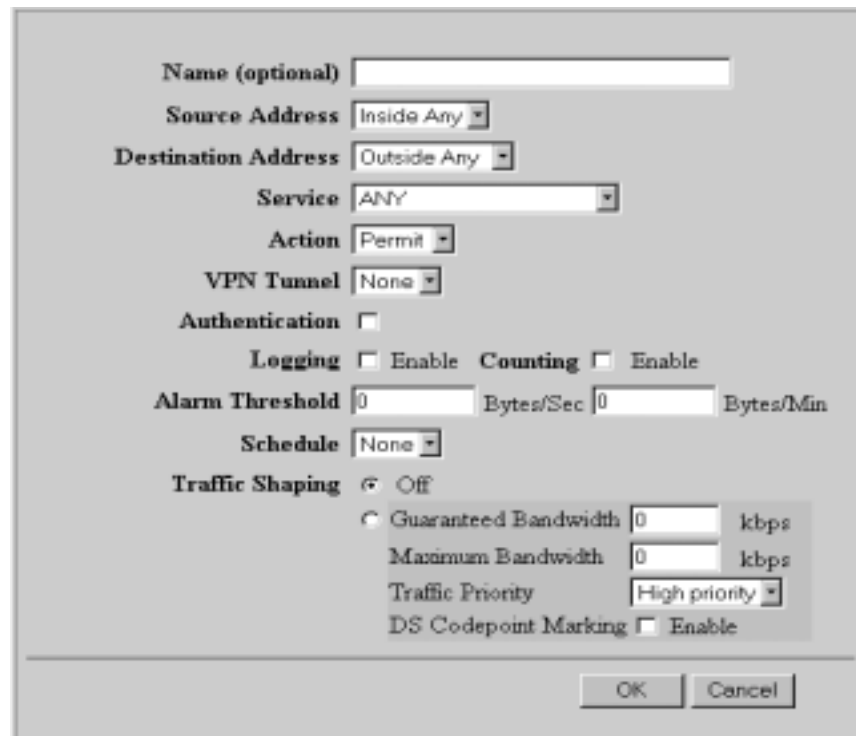
- Addresses (source and destination)
- Service
- Action (permit, deny, tunnel)

An Access Policy can also contain the following elements:

- VPN tunneling
- Authentication
- Logging
- Counting
- Traffic alarm settings
- Scheduling
- Traffic shaping

The remainder of this section examines each of the above elements in turn.

Policy Configuration Dialog
Box



The image shows a 'Policy Configuration Dialog Box' with various settings for an access policy. The fields are as follows:

- Name (optional):** A text input field.
- Source Address:** A dropdown menu with 'Inside Any' selected.
- Destination Address:** A dropdown menu with 'Outside Any' selected.
- Service:** A dropdown menu with 'ANY' selected.
- Action:** A dropdown menu with 'Permit' selected.
- VPN Tunnel:** A dropdown menu with 'None' selected.
- Authentication:** A checkbox, currently unchecked.
- Logging:** A checkbox with 'Enable' text next to it, currently unchecked.
- Counting:** A checkbox with 'Enable' text next to it, currently unchecked.
- Alarm Threshold:** Two input fields. The first is '0' followed by 'Bytes/Sec'. The second is '0' followed by 'Bytes/Min'.
- Schedule:** A dropdown menu with 'None' selected.
- Traffic Shaping:** A radio button group with 'Off' selected.
- Guaranteed Bandwidth:** A radio button, currently unselected, followed by an input field '0' and 'kbps'.
- Maximum Bandwidth:** An input field '0' followed by 'kbps'.
- Traffic Priority:** A dropdown menu with 'High priority' selected.
- DS Codepoint Marking:** A checkbox with 'Enable' text next to it, currently unchecked.

At the bottom right are 'OK' and 'Cancel' buttons.

Addresses

Addresses are objects that identify network devices such as hosts and networks by their location in relation to the firewall—on the Trusted side, the Untrusted side, or in the DMZ (NetScreen-10 and -100). Individual hosts are specified using the mask 255.255.255.255, indicating that all 4 bytes of the address are significant. Networks are specified using their subnet mask to indicate which bytes are significant. To create an Access Policy for specific addresses, you must first create entries for the relevant hosts and networks in the address book.

You can also create address groups and apply Access Policies to them as you would to other address book entries.

When using address groups as elements of Access Policies, be aware that because the NetScreen device applies the Access Policy to each address in the group, the number of available Access Policies can become depleted more quickly than expected. This is a danger especially when you use address groups for both the source and destination.

Services

Services are objects that identify application protocols using layer 4 information such as standard and accepted TCP and UDP port numbers for application services like Telnet, FTP, SMTP, and HTTP. NetScreen includes predefined core Internet services. Additionally, the administrator can define custom services. You can define Access Policies that specify which services are permitted, denied, encrypted, authenticated, logged, or counted, and which trigger an alarm.

Actions

Actions are objects that describe what the firewall does to the traffic it receives.

- **Permit** allows the packet to pass the firewall.
- **Deny** blocks the packet from traversing the firewall.
- **Tunnel** encrypts and authenticates data using IPSec. After selecting Tunnel, specify which VPN tunnel to use.

The NetScreen device applies the specified action on traffic that matches the first two criteria: addresses (source and destination) and service.

VPN Tunnel

You can apply a single Access Policy or multiple Access Policies to any VPN tunnel that you have configured. In the WebUI, the VPN Tunnel option provides a drop-down list of all such tunnels. In the CLI, you can see all available tunnels with the **get vpn** command.

Authentication

Selecting this option requires the user at the source address to authenticate his/her identity by supplying a user name and password before traffic is allowed to traverse the firewall or enter the VPN tunnel. The NetScreen device can use the internal user database or an external RADIUS, SecurID, or LDAP server to perform the authentication check.

Schedules

By associating a schedule to an Access Policy, you can determine when the Access Policy is in effect. You can configure schedules on a recurring basis and as a one-time event. Schedules provide a powerful tool in controlling the flow of network traffic and in enforcing network security. For an example of the latter, if you were concerned about employees transmitting important data outside the company, you might set an Access Policy that blocked outbound FTP-Put and MAIL traffic after normal business hours.

In the WebUI, define schedules in the Schedule section. In the CLI, use the `set schedule` command. For more information on setting schedules, see.

Note: In the WebUI, scheduled Access Policies appear in green to indicate that the current time is not within the defined schedule. When a scheduled Access Policy becomes active, it appears in red.

Logging

When you enable logging in an Access Policy, the NetScreen device logs all connections to which that particular Access Policy applies. You can view the logs through either the WebUI or CLI, and the graphs in the Monitor section of the WebUI.

Counting

When you enable counting in an Access Policy, the NetScreen device counts the total number of bytes of traffic to which this Access Policy applies and records the information in historical graphs.

Alarm Threshold

You can set a threshold that triggers an alarm when the traffic permitted by the Access Policy exceeds a specified number of bytes per second, bytes per minute, or both. Because the traffic alarm requires the NetScreen device to monitor the total number of bytes, you must also enable the counting feature.

Traffic Shaping

You can set parameters for the control and shaping of traffic for each Access Policy. The traffic shaping parameters include:

Guaranteed Bandwidth: Guaranteed throughput in kilobits per second (kbps). Traffic below this threshold passes with the highest priority without being subject to any traffic management or shaping mechanism.

Maximum Bandwidth: Secured bandwidth available to the type of connection being specified in kilobits per second (kbps). Traffic beyond this threshold will be throttled and dropped.

***Note:** It is advised that you do not use rates less than 10 kbps. Rates below this threshold lead to dropped packets and excessive retries that defeat the purpose of traffic management.*

Traffic Priority: When traffic bandwidth falls between the guaranteed and maximum settings, the NetScreen device passes higher priority traffic first, and lower priority traffic only if there is no other higher priority traffic. There are eight priority levels.

DS Codepoint Marking: Differentiated Services (DiffServ) is a system for tagging (or “marking”) traffic at a position within a hierarchy of priority. The eight NetScreen priority levels can be mapped to the DiffServ system. By default, the highest priority (priority 0) maps to the first three bits (111) in the DS field (see RFC 2472) or the IP precedence field in the TOS byte (see RFC 1349) in the IP packet header. The lowest priority (priority 8) in the NetScreen system maps to 000 in the DiffServ system.

To change the mapping between the NetScreen priority levels and the DS system, use the following CLI command:

```
set traffic-shaping ip_precedence <number for priority 0 (highest priority)>  
<number for priority 1> <number for priority 2> <number for priority 3>  
<number for priority 4> <number for priority 5> <number for priority 6>  
<number for priority 7>
```

ACCESS POLICIES APPLIED










This section describes the management of Access Policies: viewing, creating, ordering and reordering, modifying, and removing Access Policies.


Viewing Access Policies

To view Access Policies through the WebUI, click **Policy >> Incoming | Outgoing | To DMZ | From DMZ**. In the CLI, use the **get policy** command.

Access Policy Icons

When viewing a list of Access Policies, the WebUI uses icons to provide you a graphical summary of policy components. The table below defines the different icons used in the Access Policies page.

Icon	Function	Description
	Permit	All traffic meeting the criteria is passed.
	Deny	All traffic meeting the criteria is denied.
	Encrypt enabled	All traffic meeting the criteria is encrypted.
	Encrypt disabled	There is a VPN configuration error (Action: Tunnel; VPN Tunnel: None), so no encryption is applied.
	Authenticate	The user must authenticate himself/herself when initiating a connection.
	Log	All traffic is logged and made available for syslog and e-mail, if enabled.
	Count	The amount of traffic is counted in bytes per second.
	Alarm	Indicates that you have set alarm thresholds.
	Traffic Shaping	Bandwidth shaping is active.

Icon	Function	Description
	Schedule	An Access Policy is only active during the time defined by the chosen schedule.

Creating Access Policies

Access Policies define the security of your network. You can set Access Policies to accept, deny, encrypt, and authenticate the network traffic travelling through the Netscreen device.

Note: The default policy for the NetScreen-10, -100, and 1000 is to deny all access. The NetScreen-5 default Access Policy denies all inbound traffic but allows all outbound traffic.

Access Policy Location

You assign an Access Policy for one of four directions, based on the intended source and destination addresses: Incoming, Outgoing, To DMZ, or From DMZ.

The differences are categorized as follows:

TRAFFIC	Outgoing	Incoming	To DMZ	From DMZ
Source	Trusted	Untrusted	Trusted Untrusted	DMZ
Destination	Untrusted	Trusted MIP VIP	DMZ	Trusted Untrusted

Example: Typical ACL for a Small-to-Medium Enterprise

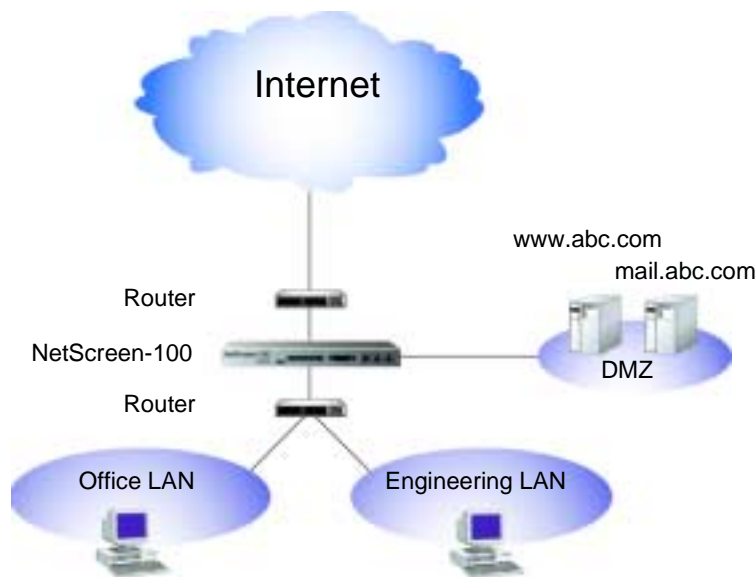
A small software firm, ABC Design, has divided its Trusted network into two subnets:

- Engineering (with the defined address “Engineering”)
- The rest of the company (with the defined address “Office”).

It also has a DMZ for its Web and mail servers.

The following example presents a typical set of Access Policies for the following users:

- Engineering is permitted to use all the services for outbound traffic except FTP-Put, IMAP, MAIL, and POP3.
- Office is permitted to use e-mail and access the Internet, provided they authenticate themselves.
- The entire company can access the company Web and mail servers on the DMZ.
- There is also a group of system administrators (with the defined address “Sys-admins”), who have complete user and administrative access to the servers on the DMZ.



Outgoing

Source	Destination	Service	Action
Inside Any	Outside Any	Com (service group: FTP-Put, IMAP, MAIL, POP3)	Deny
Engineering	Outside Any	Any	Permit
Office	Outside Any	Internet (service group: FTP-Get, HTTP, HTTPS)	Permit (+ Authentication)

Incoming (Default Access Policy)

Source	Destination	Service	Action
Outside Any	Inside Any	Any	Deny

To DMZ

Source	Destination	Service	Action
Outside Any	mail.abc.com	MAIL	Permit
Outside Any	www.abc.com	Web (service group: HTTP, HTTPS)	Permit
Inside Any	mail.abc.com	e-mail (service group: IMAP, MAIL, POP3)	Permit
Inside Any	www.abc.com	Internet	Permit

From DMZ

Source	Destination	Service	Action
mail.abc.com	Outside Any	MAIL	Permit

WebUI

1. Policy >> Outgoing >> New Policy: Enter the following, and then click **OK**:

Source Address: Inside Any

Destination Address: Outside Any

Service: Com¹

Action: Deny

2. Policy >> Outgoing >> New Policy: Enter the following, and then click **OK**:

Source Address: Engineering

Destination Address: Outside Any

Service: ANY

Action: Permit

3. Policy >> Outgoing >> New Policy: Enter the following, and then click **OK**:

Source Address: Office

Destination Address: Outside Any

Service: Internet²

Action: Permit

Authentication: (select)

Note: For incoming traffic, use the default Access Policy to deny everything.

4. Policy >> To DMZ >> New Policy: Enter the following, and then click **OK**:

Source Address: Outside Any

Destination Address: mail.abc.com

Service: MAIL

Action: Permit

-
1. "Com" is a service group with the following members: FTP-Put, MAIL, IMAP, and POP3.
 2. "Internet" is a service group with the following members: FTP-Get, HTTP, and HTTPS.

5. Policy >> To DMZ >> New Policy: Enter the following, and then click **OK**:
 - Source Address: Outside Any
 - Destination Address: www.abc.com
 - Service: Web³
 - Action: Permit
6. Policy >> To DMZ >> New Policy: Enter the following, and then click **OK**:
 - Source Address: Inside Any
 - Destination Address: mail.abc.com
 - Service: e-mail⁴
 - Action: Permit
7. Policy >> To DMZ >> New Policy: Enter the following, and then click **OK**:
 - Source Address: Inside Any
 - Destination Address: www.abc.com
 - Service: Internet
 - Action: Permit
8. Policy >> To DMZ >> New Policy: Enter the following, and then click **OK**:
 - Source Address: Sys-admins
 - Destination Address: DMZ Any
 - Service: Any
 - Action: Permit
9. Policy >> From DMZ >> New Policy: Enter the following, and then click **OK**:
 - Source Address: mail.abc.com
 - Destination Address: Outside Any
 - Service: MAIL
 - Action: Permit

-
3. “Web” is a service group with the following members: HTTP and HTTPS.
 4. “e-mail” is a service group with the following members: MAIL, IMAP, and POP3.

CLI

1. set policy outgoing “inside any” “outside any” com deny
2. set policy outgoing engineering “outside any” any permit
3. set policy outgoing office “outside any” internet permit auth
4. set policy todmz “outside any” mail.abc.com mail permit
5. set policy todmz “outside any” www.abc.com web permit
6. set policy todmz “inside any” mail.abc.com e-mail permit
7. set policy todmz “inside any” www.abc.com internet permit
8. set policy todmz sys-admins “dmz any” any permit
9. set policy fromdmz mail.abc.com “outside any” mail permit
10. save

Modifying Access Policies

After you create an Access Policy, you can always return to it to make modifications. In the WebUI, you click the **Edit** link in the Configure column for the Access Policy that you want to change. In the Policy Configuration dialog box that appears for that Access Policy, make your changes and then click **OK**. In the CLI, you use the **set policy** command.

Example: Disabling an Access Policy through the Schedule Feature

NetScreen does not provide a specific method for enabling and disabling Access Policies. After you create an Access Policy, it is automatically enabled. However, you can use the schedule feature to effectively accomplish the same enabling and disabling function.

You must first, create a schedule for a one-time event that started and stopped in the past and name it “disable.” Then you apply that schedule to whatever Access Policy you want to disable. When you want to enable it again, change the schedule back to None (or to another schedule).

WebUI

Policy >> Incoming | Outgoing | To DMZ | From DMZ >> Edit: In the Schedule drop-down list, select **disable**, and then click **OK**.

CLI

1. set policy {incoming | outgoing | todmz | fromdmz} <source address>
<destination address> <service> <action> schedule disable
2. save

Reordering Access Policies

The NetScreen device checks all attempts to traverse the firewall against Access Policies, beginning with the first one listed in the ACL for the appropriate direction (outgoing, incoming, to DMZ, from DMZ) and moving through the list. Because action applies to the first matching Access Policy, you must arrange them from the most specific to the most general. (Whereas a specific Access Policy does not preclude the application of a more general Access Policy located down the list, a general Access Policy appearing before a specific one does.)

To move an Access Policy to a different position in the ACL, do the following:

WebUI

1. Policy >> Incoming | Outgoing | To DMZ | From DMZ: Click the circular arrows in the Configure column to display the Move Policy Micro dialog box:



2. Change the order of the Access Policy to fit your needs, and then click the **OK** button.

The Access Policies page reappears with the Access Policy you moved in its new position.

CLI

1. set policy move <id number> {before | after} <number>
2. save

Example: Reordering Home-to-Office Access Policies

By setting priority levels and guaranteed bandwidth levels for outbound traffic, you can ensure that important traffic always has enough bandwidth. At home, you might want to set up the following three Access Policies on your NetScreen-5 to ensure that you can still reach your office through your home-to-office VPN even when your children are playing games on the Internet. (These Access Policies also ensure that you have enough bandwidth to play games on the Internet when your children are doing the same thing.)

Outgoing Access Policies

ID	Source	Destination	Service	Action	Guaranteed and Maximum Bandwidth*	Priority
0	Inside Any	Outside Any	Any	Permit	0 Kbps	Low priority
1	Mom/Dad	corp-net	Any	Tunnel (VPN Tunnel: home-corp)	3500 Kbps	High priority
2	Mom/Dad	Outside Any	Any	Permit	1500 Kbps	2nd priority

* The bandwidth for the Trusted and Untrusted interface is set at 5 Mbps per interface.

Note that if the three Access Policies are ordered as shown above, the NetScreen device only applies the first Access Policy to outgoing traffic. You must move the Access Policy #0 to the bottom of the list.

WebUI

1. Policy >> Outgoing: Click the circular arrows in the Configure column for Access Policy ID #0.
2. In the Move Policy Micro dialog box that appears, enter the following, and then click **OK**:

After: (select)

ID: 2

CLI

1. set policy move 0 after 2
2. save

Removing an Access Policy

In addition to modifying an Access Policy, you can also delete it from the ACL. In the WebUI, you click **Remove** in the Configure column for the Access Policy that you want to remove. When the system message prompts for confirmation to proceed with the removal, click **Yes**. In the CLI, use the **unset policy <number>** command.