NETSCREEN-5

Installer's Guide

Note to Reader: This is a preliminary version of this document.
An updated version will be made available in the very near future.

Version 2.6.0 P/N 093-0041-000 Rev. B

Copyright Notice

NetScreen Technologies, Inc.
350 Oakmead Parkway, Suite 500
Sunnyvale, CA 94085 U.S.A.
www.netscreen.com

FCC Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a light commercial installation. This equipment generates, uses and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Product License Agreement

PLEASE READ THIS LICENSE AGREEMENT ("AGREEMENTS") CAREFULLY BEFORE USING THIS PRODUCT. BY INSTALLING AND OPERATING, YOU INDICATE YOUR ACCEPTANCE OF THE TERMS OF THIS LEGAL AND BINDING AGREEMENT AND ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PART TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT START THE INSTALLATION PROCESS.

1. License Grant. This is a license, not a sales agreement, between you, the end user, and NetScreen Technologies, Inc. ("NetScreen"). The term "Firmware" includes all NetScreen and third party Firmware and software provided to you with the NetScreen product, and includes any accompanying documentation, any updates and enhancements of the Firmware and software provided to you by NetScreen, at its option. NetScreen grants to you a non-transferable (except as provided in section 3 ("Transfer") below, non-exclusive license to use the Firmware and software in accordance with the terms set forth in this License Agreement. The Firmware and software are "in use" on the product when they are loaded into temporary memory (i.e. RAM).

2. Limitation on Use. You may not attempt and if you are a corporation, you will use best efforts to prevent your employees and contractors from attempting to, (a) modify, translate, reverse engineer decompile, disassemble, create, derivative works based on, sublicense, or distribute the Firmware or the accompanying documentation; (b) rent or lease any rights in the Firmware or software or accompanying documentation in any form to any person; or (c) remove any proprietary notice, labels, or marks on the Firmware, software, documentation, and containers.

3. Transfer. You may transfer (not rent or lease) the Firmware or software to the end user on a permanent basis, provided that: (i) the end user receives a copy of this Agreement and agrees in writing to be bound by its terms and conditions, and (ii) you at all times comply with all applicable United States export control laws and regulations.

4. Proprietary Rights. All rights, title, interest, and all copyrights to the Firmware, software, documentation, and any copy made by you remain with NetScreen. You acknowledge that no title to the intellectual property in the Firmware and software is transferred to you and you will not acquire any rights to the Firmware except for the license as expressly set forth herein.

5. Term and Termination. The term of the license is for the duration of NetScreen's copyright in the Firmware and software. NetScreen may terminate this Agreement immediately without notice if you breach or fail to comply with any of the terms and conditions of this Agreement. You agree that, upon such termination, you will either destroy all copies of the documentation or return all materials to NetScreen. The provisions of this Agreement, other than the license granted in Section 1 ("License Grant") shall survive termination.

6. Limited Warranty. For a period of one (1) year after delivery to Customer, NetScreen will repair or replace any defective product shipped to Customer, provided it is returned to NetScreen at Customer's expense within that period. For a period of ninety (90) days after the initial delivery of a particular product, NetScreen warrants to Customer that such product will substantially conform with NetScreen's published specifications for that product if properly used in accordance with the procedures described in documentation supplied by NetScreen. NetScreen's exclusive obligation with respect to non-conforming product shall be, at NetScreen's option, to replace the product or use diligent efforts to provide Customer with a correction of the defect, or to refund to customer the purchase price paid for the unit. Defects in the product will be reported to NetScreen in a form and with supporting information reasonably requested by NetScreen to enable it to verify, diagnose, and correct the defect. For returned product, the customer shall notify NetScreen of any nonconforming product during the warranty period, obtain a return authorization for the nonconforming product, from NetScreen, and return the nonconforming product to NetScreen's factory of origin with a statement describing the nonconformance.

NOTWITHSTANDING ANYTHING HEREIN TO THE CONTRARY, THE FOREGOING IS CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR BREACH OF WARRANTY BY NETSCREEN WITH RESPECT TO THE PRODUCT.

The warranties set forth above shall not apply to any Product or Hardware which has been modified, repaired or altered, except by NetScreen, or which has not been maintained in accordance with any handling or operating instructions supplied by NetScreen, or which has been subjected to unusual physical or electrical stress, misuse, abuse, negligence or accidents.

THE FOREGOING WARRANTIES ARE THE SOLE AND EXCLUSIVE WARRANTIES EXPRESS OR IMPLIED GIVEN BY NETSCREEN IN CONNECTION WITH THE PRODUCT AND HARDWARE, AND NETSCREEN DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. NETSCREEN DOES NOT PROMISE THAT THE PRODUCT IS ERROR-FREE OR WILL OPERATE WITHOUT INTERRUPTION.

7. Limitation of Liability. IN NO EVENT SHALL NETSCREEN OR ITS LICENSORS BE LIABLE UNDER ANY THEORY FOR ANY INDIRECT, INCIDENTAL, COLLATERAL, EXEMPLARY, CONSEQUENTIAL OR SPECIAL DAMAGES OR LOSSES SUFFERED BY YOU OR ANY THIRD PARTY, INCLUDING WITHOUT LIMITATION LOSS OF USE, PROFITS, GOODWILL, SAVINGS, LOSS OF DATA, DATA FILES OR PROGRAMS THAT MAY HAVE BEEN STORED BY ANY USER OF THE FIRMWARE. IN NO EVENT WILL NETSCREEN'S OR ITS LICENSORS' AGGREGATE LIABILITY CLAIM BY YOU, OR ANYONE CLAIMING THROUGH OR ON BEHALF OF YOU, EXCEED THE ACTUAL AMOUNT PAID BY YOU TO NETSCREEN FOR FIRMWARE.

Some jurisdictions do not allow the exclusions and limitations of incidental, consequential or special damages, so the above exclusions and limitations may not apply to you.

8. Export Law Assurance. You understand that the Firmware is subject to export control laws and regulations.

YOU MAY NOT DOWNLOAD OR OTHERWISE EXPORT OR RE-EXPORT THE FIRMWARE OR ANY UNDERLYING INFORMATION OR TECHNOLOGY EXCEPT IN FULL COMPLIANCE WITH ALL UNITED STATES AND OTHER APPLICABLE LAWS AND REGULATIONS.

9. U.S. Government Restricted Rights. If this Product is being acquired by the U.S. Government, the Product and related documentation is commercial computer Product and documentation developed exclusively at private expense, and (a) if acquired by or on behalf of civilian agency, shall be subject to the terms of this computer Firmware, and (b) if acquired by or on behalf of units of the Department of Defense ("DoD") shall be subject to terms of this commercial computer Firmware license Supplement and its successors.

10. Tax Liability. You agree to be responsible for the payment of any sales or use taxes imposed at any time whatsoever on this transaction.

11. General. If any provisions of this Agreement are held invalid, the remainder shall continue in full force and effect. The laws of the State of California, excluding the application of its conflicts of law rules shall govern this License Agreement. This Agreement will not be governed by the United Nations Convention on the Contracts for the International Sale of Goods. This Agreement is the entire agreement between the parties as to the subject matter hereof and supersedes any other Technologies, advertisements, or understandings with respect to the Firmware and documentation. This Agreement may not be modified or altered, except by written amendment, which expressly refers to this Agreement and which, is duly executed by both parties.

You acknowledge that you have read this Agreement, understand it, and agree to be bound by its terms and conditions.

Hardware, including technical data, is subject to U.S. export laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licensed to export, re-export, or import hardware.

Table of Contents

Preface

Note to Reader: *This is a preliminary version of this document. An updated version will be made available in the very near future.*

The NetScreen-5™ is a network security device that protect your Ethernet local area network (LAN) or standalone desktop computer when connecting to the Internet. Using a NetScreen-5 as a firewall, you can configure access policies that control inbound and outbound network and VPN traffic.

MANUAL ORGANIZATION

This manual has 3 chapters and 1 appendix.

Chapter 1, Hardware Description, describes the NetScreen-5 device.

Chapter 2, Connecting the NetScreen-5 to the Network, describes how to connect the NetScreen-5 to a network in single-workstation or multiple-workstation configurations.

Chapter 3, Initial Configuration, describes 3 ways of configuring the device. You can use the Quick Start™ disk provided, use the Web UI, or use the command line interface (CLI).

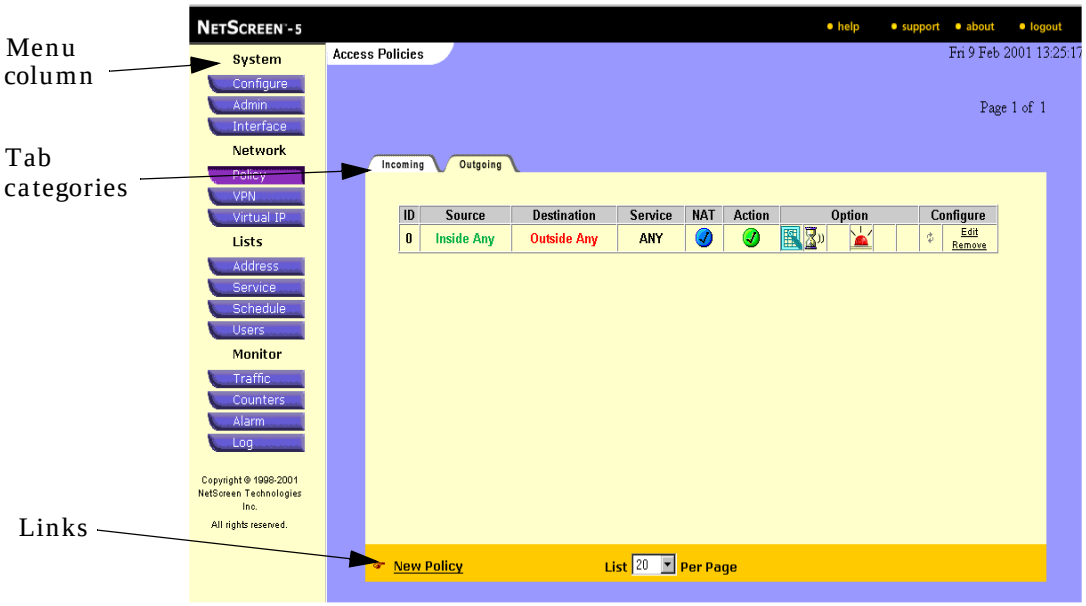
Appendix A, Safety Recommendations and Warnings, provides general site requirements, safety warnings, and explains the cautionary procedures you should observe before installing and operating the NetScreen-5 unit.

GENERAL LAYOUT OF THE NETSCREEN-5 WEB UI

The web user interface (WebUI) consists of two main logical sections: the menu column and the central display area.

- The menu column consists of four main 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 must select a main functional category before choosing the various utilities offered within each sub-category.

- The central display area 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 links such as **New Policy**, **New Manual Key User**, **New Entry**, **Edit** and so forth.



The NetScreen-5 Central Display Area

COMMAND LINE INTERFACE (CLI) SYNTAX

These conventions apply to all NetScreen commands:

- To remove a single character, press BACKSPACE or CTRL+H.
- To remove an entire line, press CTRL+U.
- To traverse up to 16 lines forward in the command history buffer, press CTRL+F or the DOWN ARROW key.

Note: *To use the arrow keys for navigating among commands in a Telnet session on Windows 95, 98, NT, or 2000: On the Terminal menu, click* ***Preferences...****, select the* ***VT100 Arrows*** *check box, and click the* ***OK*** *button.*

- To traverse up to 16 lines backward in the command history buffer, press CTRL+B or the UP ARROW key.
- To see the next available keyword or input, and a brief description of usage, type a question mark (?).
- A parameter inside [ ] (square brackets) is optional.
- A parameter inside { } (braces) is required.
- Anything inside < > is a variable.
- If there is more than one choice for a parameter inside [ ] and { }, they are separated by *a pipe* (|). For example, [auth {md5 | sha-1}] means “choose either MD5 or SHA-1 as your authentication method.”
- IP addresses are represented by <a.b.c.d> and <w.x.y.z>.
- A subnet mask is represented by <A.B.C.D>.
- The console times out and the connection is broken if no keyboard activity is detected for 10 minutes.

Items you enter are into the system are in **bold** text.

RELATED PUBLICATIONS

The following technical publications are shipped with the NetScreen-5 device:

NetScreen-5 Getting Started Guide
(P/N 093-0008-000 Rev C)

The following publications are included on the product CD:

NetScreen CLI Reference Guide
(P/N 093-0011-000 Rev C)

NetScreen WebUI Reference Guide
(P/N 093-0040-000 Rev. B)

NetScreen Concepts and Examples ScreenOS Reference Guide
(P/N 093-0039-000 Rev. B)

Hardware Description 1

This chapter provides illustrations and descriptions of the NetScreen-5 front and back panel.

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

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

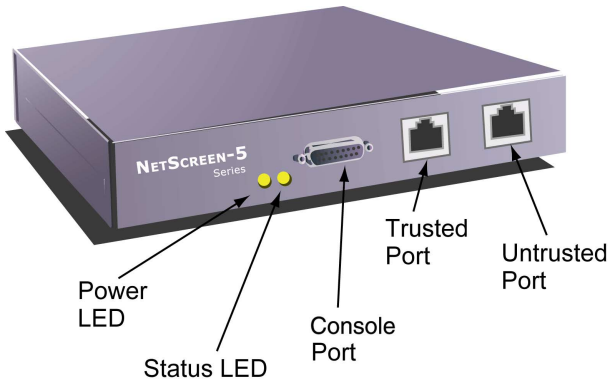


Figure 1-1 Front Panel of the NetScreen-5

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 glows 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. See “Connecting the NetScreen-5 to the Network” on page 2-1 for cabling guidelines.
- **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 1-2. 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

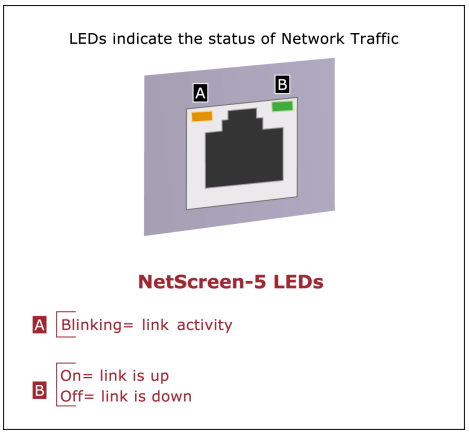


Figure 1-2 The NetScreen-5 Ethernet LEDs

Figure 1-3 on page 1-3 shows the back view of the NetScreen-5.

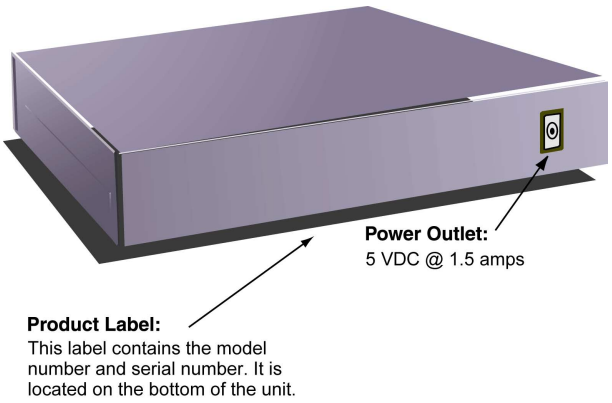


Figure 1-3 Back Panel of the NetScreen-5

Connecting the NetScreen-5 to the Network

2

Follow the instructions in this chapter to connect the NetScreen-5 device to the network.

⚠ Caution *Make sure you have read the Appendix, "Safety Recommendations and Warnings" on page A-1, before you begin.*

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. Connect the universal power supply's DC cable to the power outlet on the NetScreen-5 device, and the AC cable 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.

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

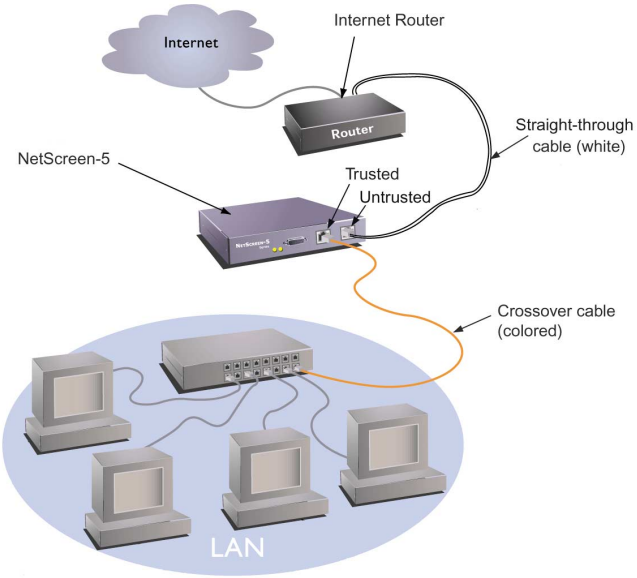


Figure 2-1 Typical Multiple-Workstation Configuration—Router Connected to the Untrusted Port, LAN Connected to the Trusted Port

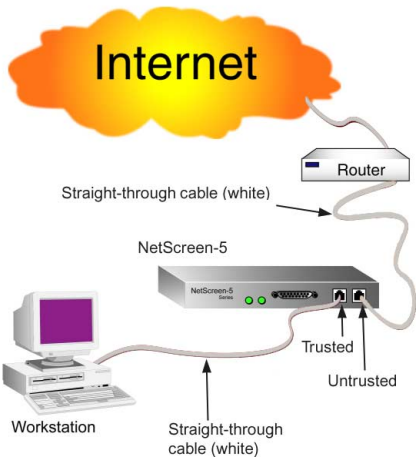


Figure 2-2 Typical Single-Workstation Configuration—Router Connected to the Untrusted Port, Workstation Connected to the Trusted Port

Note: *Because of the wide variety of available routers, hubs, and switches, the cabling configuration presented here might not satisfy your network connection requirements. If the cabling suggested above does not work, try other cable configurations until a link light is established.*

You may have to supply additional cables, depending on your particular configuration. A DTE (Data Terminal Equipment) device requires a crossover cable to connect to a DTE port. A DCE (Data Communications Equipment) device requires a crossover cable to connect to a DCE port.

Table 2-1 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.

3. 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 glows.

Initial Configuration 3

The NetScreen-5 device supports three operational modes: Transparent mode, NAT (Network Address Translation) mode, and Route mode. This section provides an overview of each mode and the required steps to perform an initial configuration.

TRANSPARENT, NAT AND ROUTE MODES

Transparent Mode

In Transparent mode, the NetScreen device inspects packets traversing the firewall without modifying any of the source or destination information in the IP packet header. Because it does not translate addresses, the IP addresses on the protected network must be valid, routable addresses on the Untrusted network[1], 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. The NetScreen device acts as a Layer 2 bridge.

Network Address Translation (NAT) Mode

When in NAT mode, the NetScreen device 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 port[2] of the NetScreen device. Also, it replaces the source port number with another random port number generated by the NetScreen device.

---

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

2. If the outbound traffic is destined for the DMZ, then the source IP address is translated to that of the DMZ port.

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.

For further configuration examples and detail, see the NetScreen Concepts & Examples ScreenOS Reference Guide.

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 3-1 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	Netscape Communicator v4.5 or greater, or Microsoft Internet Explorer v 5.0 Web browser TCP/IP network connection to the NetScreen-5 SSL requires that a certificate be loaded into the NetScreen-5. See the *NetScreen Concepts and Examples ScreenOS Reference Guide* for further information.
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. SSH requires that a key be generated in the NetScreen-5. See the *NetScreen Concepts and Examples ScreenOS Reference Guide* for further information.

Table 3-2 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
Default Policy:	source: inside any destination: outside any service: any action: permit

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 3 1/2 -inch floppy drive of the Windows® 95/98, Windows NT® v4.0 or Win2000 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.**

Note: *If the floppy drive of your computer does not use "a," replace the "a" in the above command with the drive letter it uses.*

The NetScreen Quick Start Welcome window appears as in Figure 3-1 on page 4.

Figure 3-1 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 3-2.

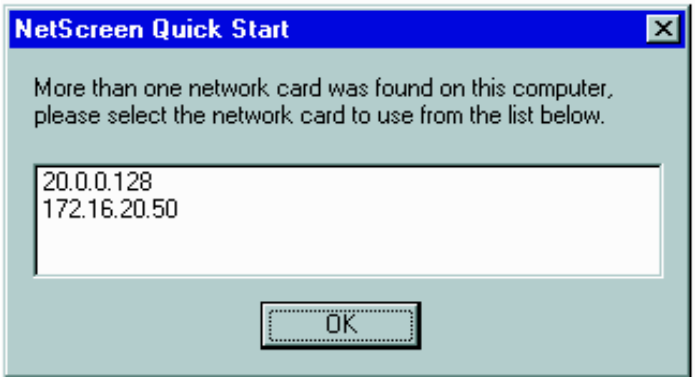


Figure 3-2 Network Card IP Address List

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 3-3, then click the **Next** button. In the event more than one NetScreen device is found, match the serial number of the new device to the one found by the Quick Start program, select it, and click **Next**.

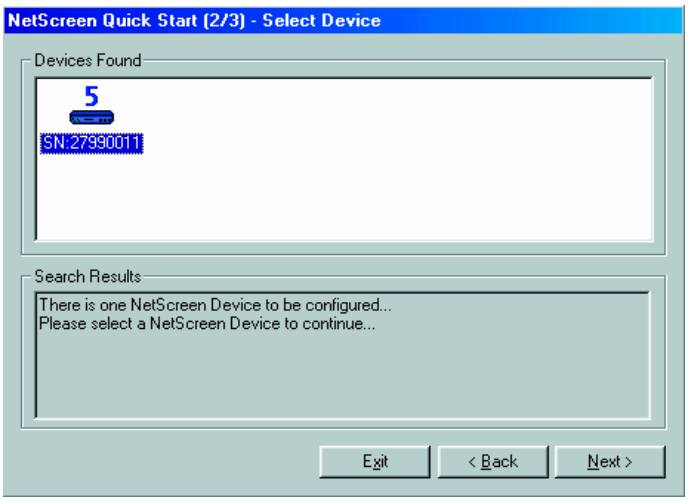


Figure 3-3 NetScreen Quick Start-Select Device

6. Enter the new System IP address for the NetScreen device you are configuring, as shown in Figure 3-4.

Note: *Since connectivity is lost when the IP address is moved to a different subnet, the user must record the IP address.*

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.

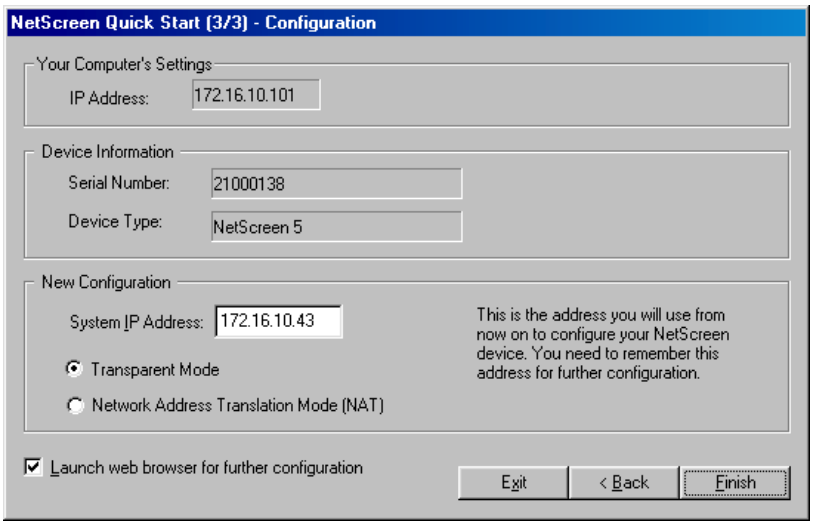


Figure 3-4 NetScreen Quick Start-Configuration Dialog Box

Selecting Transparent Mode

1. To launch your NetScreen-5 in Transparent mode, select **Transparent Mode** as shown in Figure 3-4.
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 3-7 on page 3-9.

   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 or Route Mode

1. To launch your NetScreen-5 in NAT mode, select **Network Address Translation Mode (NAT)** as shown in Figure 3-5.

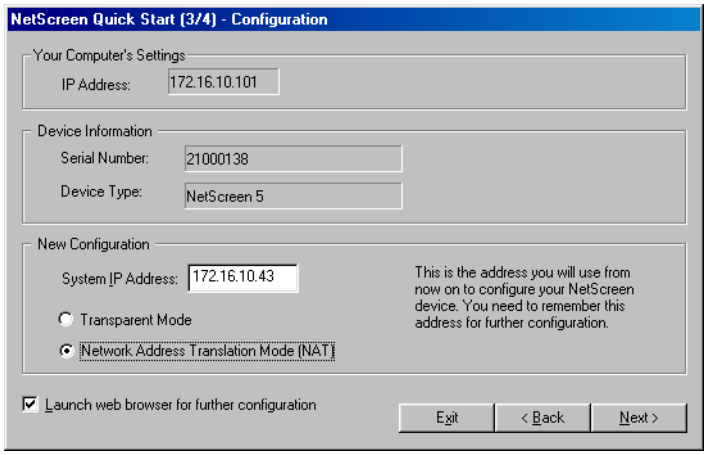


Figure 3-5 NetScreen Quick Start Configuring Screen

2. Click **Next**. The Configuration (NAT) screen appears, as in Figure 3-6.

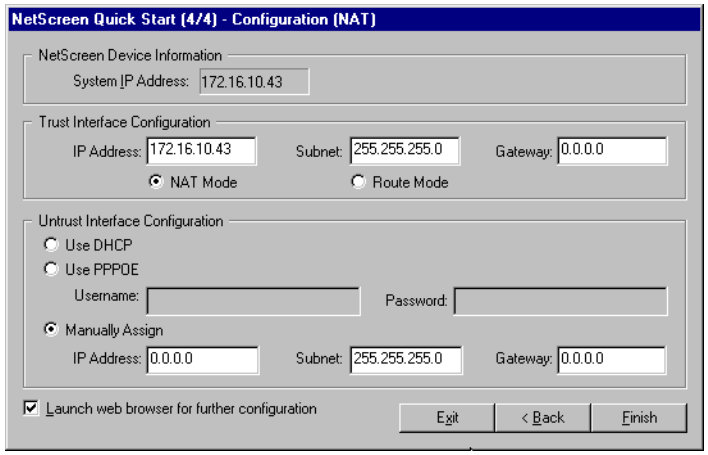


Figure 3-6 NetScreen Quick Start Configuration (NAT) Screen

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 3-7 on page 3-9.

   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 and Setting the System IP Address" on page 3-8.*

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 to Table 3-1 for administration requirements.

Making a Connection

Before you begin, be sure you connected the NetScreen-5 hardware to the network as outlined in "Connecting the NetScreen-5 to the Network" on page 2-1.

Logging on and 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, perform the following procedure:

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 netmask 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 3-7 on page 3-9.

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

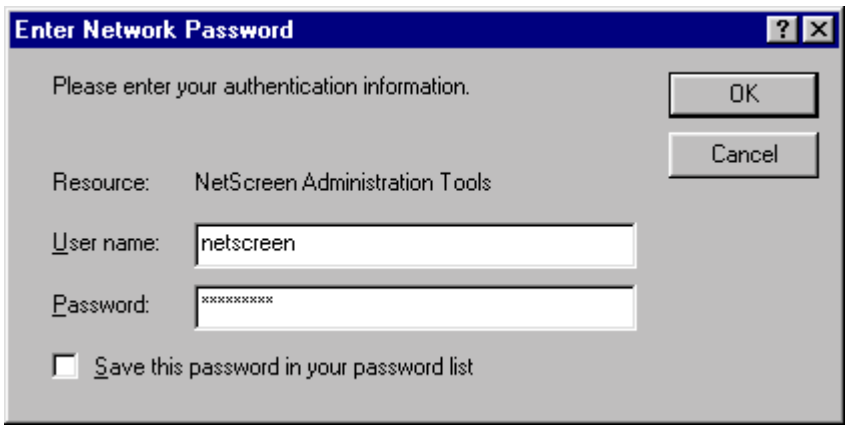


Figure 3-7 Enter Network Password Dialog Box

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 3-18.*

   An IP Address Configuration dialog box, as shown in Figure 3-8 on page 3-10 is displayed for first-time configuration.

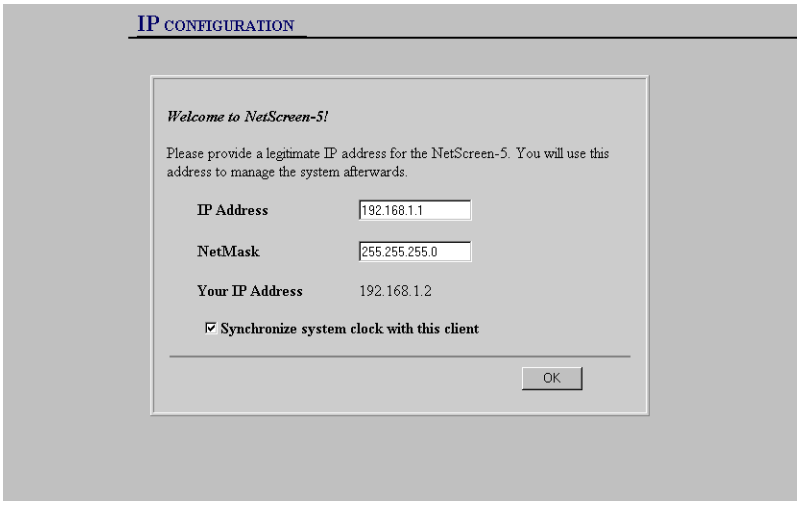


Figure 3-8 Initial IP Address Configuration

6. Enter a new System IP address and netmask 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 3-9.

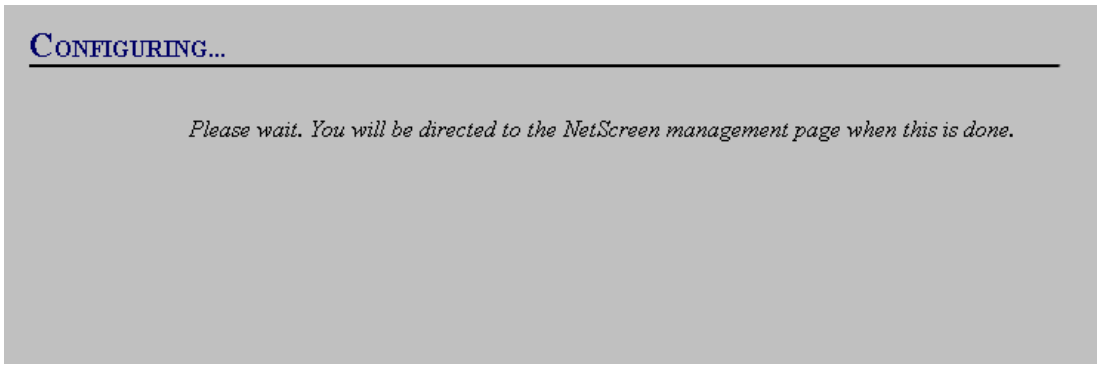


Figure 3-9 Configuring in Progress Screen

7. 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.

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

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

   The User name and Password dialog box displays.

9. In the User name and Password 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.)

   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 3-18 for instructions.

Setting Interface Addresses

Before configuring the interface addresses, decide whether to use NAT or Transparent mode. The following procedure provides information for configuring both modes of operation.

Trusted Interface Configuration

1. Click the **Interface** button in the menu column.

   The Interface pages appear, with the Trusted Interface page displayed.

2. Click **Edit** to open the Trusted Interface Configuration dialog box.

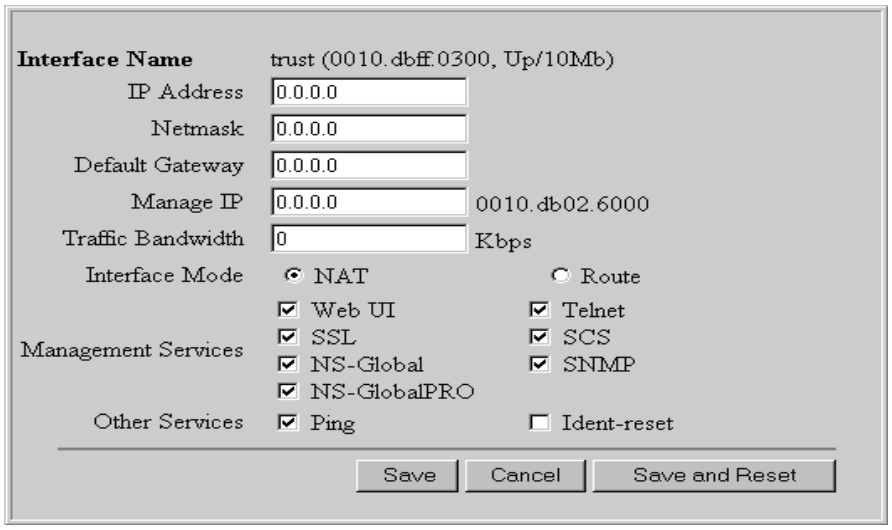


Figure 3-10 Trusted Interface Configuration

3. Enter the following, and then click **Save**:
   - IP Address: Type an IP address for the Trusted interface.
   - Netmask: Type an appropriate netmask.
   - Default Gateway: Type the IP address of the router—if there is one—that exists between the Trusted network and the NetScreen-5.
4. Select either **NAT Mode** or **Route Mode**, and then click **Save**.

Untrusted Interface Configuration

1. Click the Untrusted tab, and then Edit to open the Untrusted Interface Configuration dialog box.

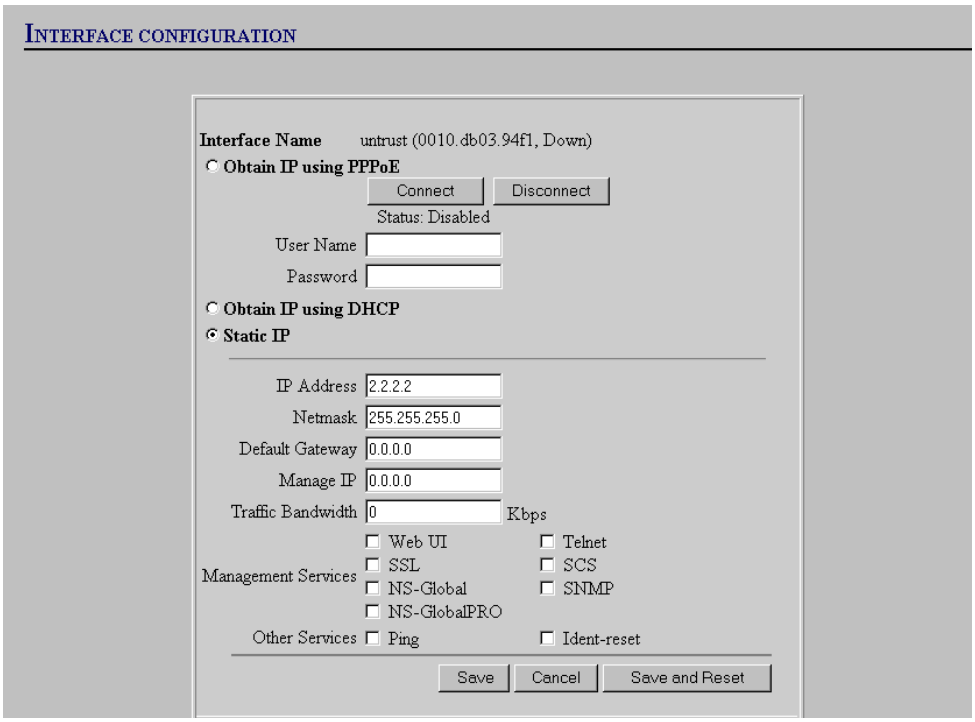


Figure 3-11 Untrusted Interface Configuration

2. For the Untrusted Interface Configuration, select one of the following and click **Save and Reset**:

   Obtain IP using PPPoE (Point-to-Point Protocol over Ethernet), and enter the user name and password.

   Obtain IP using DHCP (Dynamic Host Control Protocol).

Static IP, and enter the following:

- IP Address: Type the ISP-assigned Untrusted IP address.
- Netmask: Type an appropriate netmask.
- Default Gateway: Type the IP address of the external router.

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.

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

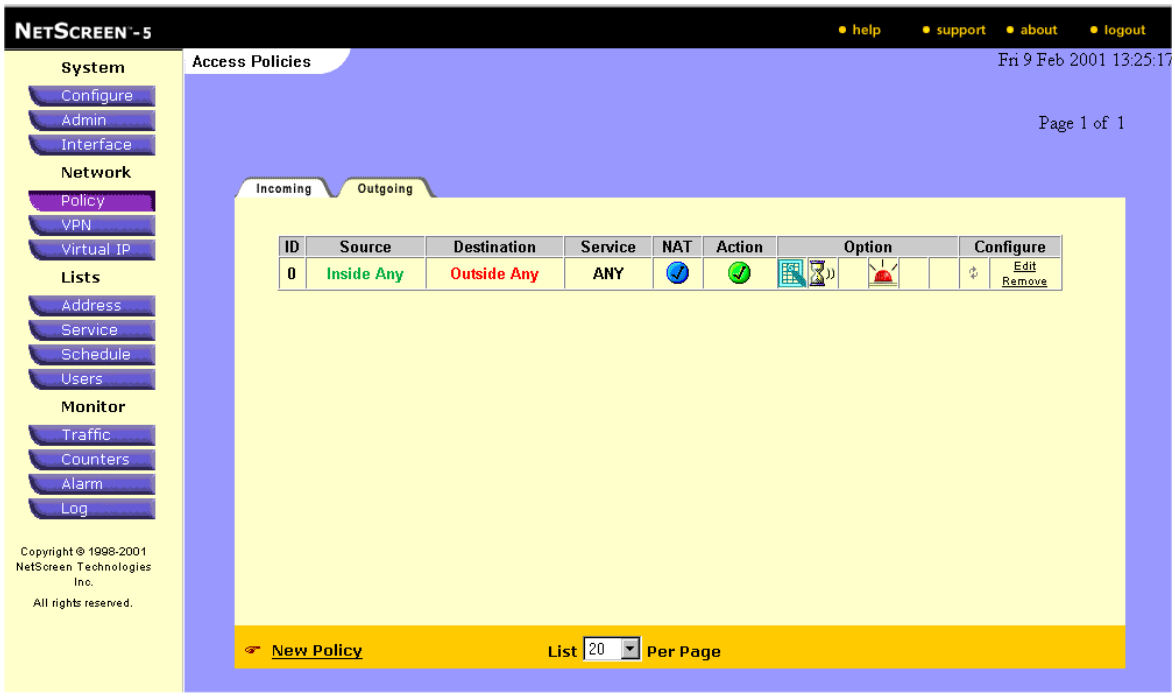


Figure 3-12 Default Outgoing Access Policy

Changing the Administrator Login Name and Password

To change the default administrator login and password:

1. Select the **Admin** button in the menu column to view the **Admin** page.
2. On the Local Administrator Name Click **Edit** under **Options**.
3. The Admin User Configuration screen appears, as in Figure 3-13.

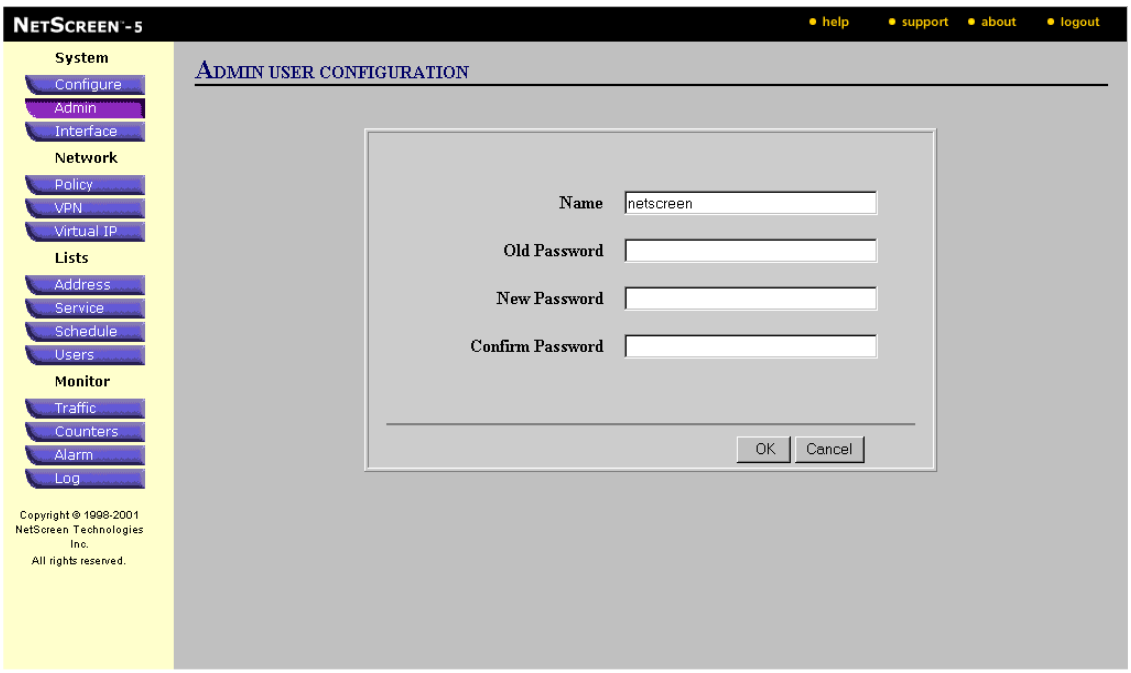


Figure 3-13 The Administration Page

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

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

7. 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.*

8. Leave the other fields at their default entries, and select the **OK** button.

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

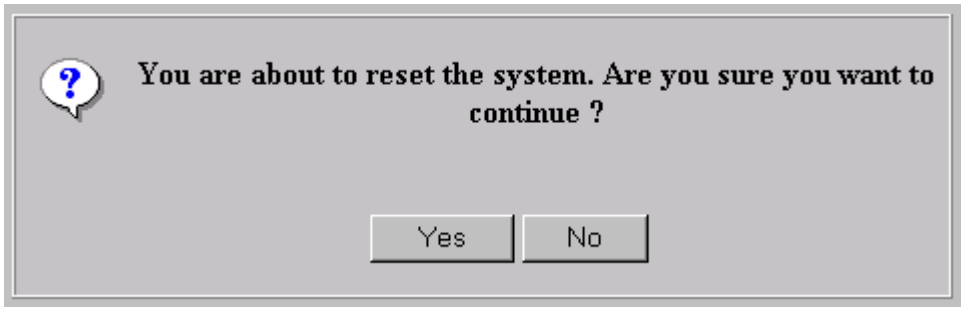


Figure 3-14 System Message Display

9. 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.*

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 glowing.
- The workstation IP and Netmask have the correct settings.
- The workstation gateway points to the router.
- The workstation has a valid DNS entry.

CONFIGURING VIA THE CLI

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

> ***Note:*** *For further information regarding using the command line interface, see the* NetScreen Command Line Interface Reference Guide.

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 3-1 on page 3-2 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 "Connecting the NetScreen-5 to the Network" on page 2-1.

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 and Setting the System IP Address

To manage the NetScreen device over a network connection, you must change the system IP address from its default (192.168.1.1) to one that is appropriate for your network. To log on and change the system IP address, enter the following commands, where <a.b.c.d> is the new system IP address:

1. At the login prompt, type **netscreen**.
2. At the password prompt, type **netscreen**.
3. set admin sys-ip <a.b.c.d>
4. save

The system IP address can be 0.0.0.0, or the same as the trust interface IP address.

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

Setting Interface Addresses

The NetScreen-5 ships with all its interface addresses and netmasks set as 0.0.0.0. If you want to operate the NetScreen-5 in Transparent mode, leave the trusted, untrusted, and tunnel interface addresses as they are.

To operate the NetScreen-5 in NAT mode or Route mode, you must also configure the trusted and untrusted interface addresses.

To set the interface addresses, enter the following commands, where <a.b.c.d> are the interface IP addresses and <A.B.C.D> is the netmask:

1. set interface trust ip <a.b.c.d> <A.B.C.D>
2. set interface untrust ip <a.b.c.d> <A.B.C.D>
3. save

Allowing Outbound Traffic

By default, the NetScreen-5 ships with a default Access Policy allowing all traffic inside the network to access the Internet. You need to create access policies to permit specified kinds of traffic in the direction(s) you want. (You can also create access policies to deny and tunnel traffic.)

The following access policy permits all kinds of outbound traffic from any point on the trusted network to any point on the untrusted network. Of course, your network might require a more restrictive policy. The following is offered to illustrate how an access policy is created; it is not presented as a requirement for an initial configuration:

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

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.*

At the command line enter:

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

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.*

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 glowing.
- The workstation IP and Netmask have the correct settings.
- The workstation gateway points to the router.
- The workstation has a valid DNS entry.

Appendix A: Safety Recommendations and Warnings

When using the NetScreen-5, follow these safety guidelines:

- Make sure that the work area is dry and without excess humidity.
- Keep the chassis area clear and dust-free during and after installation.
- Disconnect all power supply connections before changing the Ethernet or serial port connection.
- Never assume that power is disconnected from a circuit. Always check.

BEFORE SUPPLYING POWER

- Look carefully for possible hazards in the work area, such as moist floors, ungrounded power extension cables, and missing safety grounds.
- Locate the emergency power-off switch for the room where you are working.

Do not perform any action that creates a potential hazard to people or makes the equipment unsafe. Do not stack or balance the equipment on other devices to avoid tipping over, and to allow air circulation. Make sure the installation is securely in place.

Make sure you adhere to all safety warnings.

SAFETY WARNINGS

Make sure that you adhere to the following set of safety warnings.

Installation Warning

⚠ Caution *Read the cabling instructions before connecting the NetScreen-5 to its power source.*

Power Disconnection Warning

⚠ Warning *Before working on a device that has an On/Off switch, turn OFF the power and unplug the power cord.*

No User-Serviceable Parts Warning

⚠ Warning *The NetScreen-5 contains no user-serviceable parts and is housed in a tamper-proof enclosure. Therefore, the chassis should never be opened under any circumstances. Doing so will also void the warranty.*

Circuit Breaker (15A) Warning

⚠ Caution *The NetScreen-5 relies on the building's installation for short-circuit (over-current) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductor (all current-carrying conductors).*

SELV Circuit Warning

⚠ Warning *The Ethernet 10BaseT, 100BaseT, serial, console, and auxiliary ports contain safety extra-low voltage (SELV) circuits. Do not connect the NetScreen-5 to a telephone line or any Telco line (e.g., T-1, T-3, RJ-48 lines).*

Lightning Activity Warning

Danger *Do not work on the device, specifically, connecting or disconnecting cables during periods of lightning activity, as the unit can function as a conduit.*

Lithium Battery Warning

Warning *There is a danger of explosion if the battery is incorrectly replaced. The chassis should never be opened under any circumstances. Doing so will also void the warranty. Return the device to the manufacturer for battery replacement.*

Product Disposal Warning

Warning *Ultimate disposal of this product should be handled according to all national laws and regulations.*

GENERAL SITE REQUIREMENTS

This section describes the requirements your site must meet for the safe installation and operation of your system. Ensure that your site is properly prepared before beginning the hardware installation.

Site Environment

The NetScreen-5 can be placed on a desktop. Equipment placed too close together will cause inadequate ventilation, besides rendering areas of the device inaccessible for system maintenance during any system malfunctions and shutdowns.

When planning your site layout and equipment locations, follow the precautions described in the next section to help avoid equipment failures and reduce the possibility of environmentally caused shutdowns. If you are experiencing shutdowns or unusually high errors with your existing equipment, these precautions may help you isolate the cause of the failures and prevent future problems.

Preventive Site Precautions

The following precautions will help you plan an acceptable operating environment for your NetScreen-5 and will help you avoid environmentally caused equipment failures:

- Electrical equipment generates heat. Natural air temperature might not be sufficient to cool equipment to acceptable operating temperatures without an additional circulation system. Ensure that the room in which you operate your system has adequate air circulation.
- Do not work alone if potentially hazardous conditions exist.
- Never assume that the power supply has been disconnected from a circuit. Always check.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.

Power Supply Considerations

Check the power at your site to ensure that you are receiving “clean” power (free of spikes and noise). Install a power conditioner if necessary.

Environmental Requirements

The NetScreen-5 is intended for use in a normal office environment. For more extreme conditions, verify that temperature, humidity, and power conditions meet the specifications indicated in Table A-1.

Table 3-3 Environmental Requirements

Item	Operating Specification
Temperature	32-122°F, 0- 50°C
Relative humidity	5-90%, non-condensing: for storage
	10-90%, non-condensing: for operation
Voltage	90-264 VAC
Input frequency	47-63 Hz
AC input current	1.5A (120VAC), 1.5A (240VAC)
Altitude	0-12,000 feet, 0-3,660 meters

Index

I

L

M

N

O

P

Q

R

S

T

U

V

W