NETSCREEN-10/100
Installer’s Guide

Version 2.5.0    P/N 093-0042-000    Rev. A
Copyright Notice

Copyright © 2000-2001 NetScreen Technologies, Inc. All rights reserved. Printed in USA.

NetScreen, the NetScreen logo, NetScreen-5, NetScreen-10, and NetScreen-100 are registered trademarks or trademarks of NetScreen Technologies, Inc.

Netscape Communicator is a registered trademark of Netscape in the United States and/or other countries. Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation in the U.S.A. and/or other countries. Hyperterminal is a registered trademark of Hilgeave Corporation. All other brands and their products mentioned in this document are trademarks or registered trademarks of their respective owners.

The specifications regarding the products in this manual are subject to change without notice. All statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of any products. This document may only be used or copied in accordance with the terms of such license.

NetScreen Technologies, Inc.
350 Oakmead Parkway
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 to 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 notices, 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 and the Firmware or return them 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 replacement of a product, NetScreen will notify Customer 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, CONSEQUENTIAL, EXEMPLARY, 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 controls 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

Who Should Read this Manual? ................................................................. vii

Manual Organization .............................................................................. vii

Related Publications .............................................................................. viii

Chapter 1 Hardware and Software Description ........................................ 1-1

Hardware Description ........................................................................... 1-1

General Layout of the NetScreen-10/100 Administration Tools .................. 1-5

Chapter 2 Connecting the NetScreen-10/100 to the Network ......................... 2-1

Gathering the Necessary Tools ............................................................... 2-1

Connecting the NetScreen-10/100 to Networks and Devices ....................... 2-2

Chapter 3 Configuring the NetScreen-10/100 for the First Time ..................... 3-1

Using the WebUI .................................................................................. 3-2

Making a Connection ........................................................................... 3-2

Setting the System IP Address .............................................................. 3-2

Logging On .......................................................................................... 3-4

Allowing Outbound Traffic ................................................................. 3-6

Changing the Administrator Login Name and Password ......................... 3-8

Testing the Configuration .................................................................... 3-9

Using the CLI ...................................................................................... 3-10

Making a Connection .......................................................................... 3-10

Connecting via the Console Port ......................................................... 3-10

Connecting via Telnet ......................................................................... 3-10

Logging On ......................................................................................... 3-11

Setting the System IP Address .............................................................. 3-11

Changing the Administrator Login Name and Password ....................... 3-12

Testing the Configuration .................................................................... 3-12

Interface Settings and Operational Modes .............................................. 3-13

Transparent Mode .............................................................................. 3-13

Interface Settings ............................................................................. 3-14

Network Address Translation Mode .................................................... 3-15

Interface Settings ............................................................................. 3-16

Route Mode ....................................................................................... 3-17

Interface Settings ............................................................................. 3-17

Appendix A Safety Recommendations and Warnings .................................. A-1

Safety Warnings .................................................................................. A-1
Preface

The NetScreen-10™ and NetScreen-100™ are network security devices that protect your Ethernet local area network (LAN) when connecting to the Internet. Using a NetScreen-10/100 firewall, you can configure access policies that control inbound and outbound network and VPN traffic.

MANUAL ORGANIZATION

This manual has 3 chapters and one appendix.

Chapter 1, "Hardware and Software Description", describes the NetScreen® device. It explains the functions of the status LEDs, identifies the device interface ports, and provides a key to the layout of the NetScreen Administrative Web user interface (WebUI).

Chapter 2, "Connecting the NetScreen-10/100 to the Network", explains how to connect the NetScreen-10/100 device to a network. It includes diagrams that show the typical placement of the NetScreen device between your network and the Internet, and a summary of the tools and information you need before connecting the device.

Chapter 3, "Configuring the NetScreen-10/100 for the First Time" explains how to configure the basic functions of the NetScreen-10/100, and details the method for ensuring that your device is working correctly on the network.

“Appendix A: Safety Recommendations and Warnings” provides general site requirements as well as safety warnings and general cautions when using the NetScreen-10/100 device.

RELATED PUBLICATIONS

The following technical publication ships with the NetScreen-100 device:

NetScreen-100 Getting Started Guide
(P/N 093-0019-000 Rev B)

The following publication ships with the NetScreen-10 device:

NetScreen-10 Getting Started Guide
(P/N 093-0018-000 Rev B)

The following publications are included on the product CD for both devices:
NetScreen CLI Reference Guide (P/N 093-0011-000, Revision C)
NetScreen WebUI Reference Guide (P/N 093-0040-000, Revision A)
NetScreen Concepts & Examples ScreenOS Reference Guide (P/N 093-0039-000, Revision A)
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).

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.

![NetScreen-10/100 Front Panel](image)

**Figure 1-1** 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 flash card. Supported cards include the SanDisk 96-MB and 20-MB CompactFlash. The NetScreen device automatically detects the presence of a flash card 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 RJ 45 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 RJ 45 connectors. The DMZ port is a DCE port. See Chapter 2 for cabling guidelines.

• **Untrusted Port:** Connect the NetScreen-10/100 using a twisted pair cable with RJ 45 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 1-2.

![LEDs indicate the status of Network Traffic](image)

**Figure 1-2 Ethernet LEDs**
The back panel of the NetScreen-10/100 is shown in Figure 1-3.

![Back Panel of the NetScreen-10/100](image)

**Figure 1-3** 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 1-1** NetScreen-10/100 Model Numbers

<table>
<thead>
<tr>
<th>Model Type</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Firewall &amp; VPN (3DES &amp; DES)</td>
</tr>
<tr>
<td>e</td>
<td>Firewall &amp; VPN (DES)</td>
</tr>
<tr>
<td>f</td>
<td>Firewall</td>
</tr>
</tbody>
</table>

**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.

⚠️ **Caution**: Make sure you have read “Appendix A: Safety Recommendations and Warnings” before you begin installation.
**General Layout of the NetScreen-10/100 Administration Tools**

The Web Administration Tools page consists of two main sections: the menu column and the central display area:

- Figure 1-4 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 1-4 The NetScreen-10/100 Menu Column](image)
A central display area, shown in Figure 1-5, 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 links such as **New Entry**, **New Policy**, **New Manual Key User**, and so forth.

**Figure 1-5** Central Display Area
Follow the instructions in this chapter to connect the NetScreen-10/100 device to the network and to configure the software for the first time. For further configuration options, see the NetScreen Concepts & Examples ScreenOS Reference guide, on the product CD.

⚠️ Caution Make sure you have read “Appendix A: Safety Recommendations and Warnings”, before you begin this chapter.

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. Users will have to supply screws to match rack thread size.

**Table 2-1 Typical NetScreen-10/100 Cable Connections.**

<table>
<thead>
<tr>
<th>For a Device Connected to:</th>
<th>Untrusted Port (DTE)</th>
<th>Trusted Port (DCE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstation (DTE)</td>
<td>crossover</td>
<td>straight-through</td>
</tr>
<tr>
<td>Switch/Hub (DCE)</td>
<td>straight-through</td>
<td>crossover</td>
</tr>
<tr>
<td>Router² (DTE)</td>
<td>crossover</td>
<td>straight-through</td>
</tr>
</tbody>
</table>

² An Untrusted Ethernet port is not technically a DTE but for cabling purposes, should be treated as such.

³ Routers with uplink ports may behave in reverse.

If all cables are connected correctly, the link light for each connection illuminates.
Chapter 2 Connecting the NetScreen-10/100 to the Network

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, because they all share the same default IP address (192.168.1.1), you might run into IP address conflicts.

Figure 2-1 Front View of the NetScreen-10/100

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

To set up the NetScreen-10/100 network connections, follow these steps:

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 2-3.¹

¹. 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.
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 illuminates.

Figure 2-3 Sample Configuration with a Router Connected to the Untrusted Port, Local Area Network (LAN) Connected to the Trusted Port

7. To use the DMZ interface, use a crossover cable to connect the DMZ port on the NetScreen-10/100 to the switch linking the machines using the DMZ interface. See Figure 2-4 “Sample Configuration Using DMZ Port” on page 2-4 for an example of this configuration.
Figure 2-4 Sample Configuration Using DMZ Port
**Figure 2-5** 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.
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. Incoming traffic is denied by default; therefore, you do not need to set an incoming Access Policy expressly to deny it.

There are two methods for configuring the NetScreen-10/100 for the first time: via the Web use interface (WebUI) and via the command line interface (CLI). Table 3-1 “Administration Requirements” lists the workstation requirements for each method.

<table>
<thead>
<tr>
<th>Configuration Method</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| WebUI                | Netscape® Communicator® V4.5 or greater, or Microsoft® Internet Explorer V5 web browser.  
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.
To perform the initial configuration through the 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, which is 192.168.1.1. You can then log on through a Web browser and set the system IP address. The following sections detail the procedures for administration of the NetScreen-10/100 device from the administrator’s workstation.

Refer to Table 3-1 for administration requirements.

Making a Connection

Before you begin, be sure you connected the NetScreen-10/100 hardware to the network as outlined in Chapter 2, “Connecting the NetScreen-10/100 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, perform the following procedure:

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 netmask 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.

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.
The Enter Network Password dialog box appears, as shown in Figure 3-1.

![Enter Network Password Dialog Box](Image)

**Figure 3-1 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, you should change the default user name and password as described in “Changing the Administrator Login Name and Password” on page 3-8.

For the first-time configuration, you are directed to a special setup page as shown in Figure 3-2.

![Initial IP Address Configuration](Image)

**Figure 3-2 Initial IP Address Configuration**
6. Enter the IP address and netmask 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 netmask must be an appropriate value for your local network.

The Configuring in Progress screen appears, as shown in Figure 3-3 “Configuring in Progress Screen”.

![Configuring in Progress Screen](image)

**Figure 3-3** Configuring in Progress Screen

7. Reconfigure your administration workstation IP address and netmask back to the 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 3-4.
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 3-5 “Access Policies Pages”. You are now logged on to the NetScreen-10/100.

---

**Figure 3-4** Enter Network Password Dialog Box

**Figure 3-5** Access Policies Pages
Allowing Outbound Traffic

By default, the NetScreen-10/100 does not allow inbound or outbound traffic. You need to create an outgoing Access Policy to permit outbound traffic to traverse the firewall.

1. Click the **New Policy** link in the lower left corner of the page.

   The Policy Configuration dialog box appears, as shown in Figure 3-6 “Policy Configuration Dialog Box” on page 3-6.

![Policy Configuration Dialog Box](image)

**Figure 3-6** Policy Configuration Dialog Box

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 all hosts on the Trusted network.)
   - **Destination Address**: Outside Any (Outside Any is a predefined address for all locations on the Untrusted network, usually the Internet.)
   - **Service**: Any (Any is a predefined value for any IP service.)
- **Action:** Permit (Allows the traffic defined by the Access Policy to traverse the firewall.)

- Leave the rest of the options at 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 3-7 “Access Policies Page”.

**Figure 3-7** 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 can expose your system to attack.

1. At the command line, enter the following:
   a. name: <name>
   b. old password: <password>
   c. new password: <new password>
   d. save
2. 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 reinitialization. This feature has been implemented in this manner as an extra security measure.

If you want to configure the NetScreen device for Transparent mode, you do not have to define IP addresses for the Trusted, Untrusted and DMZ interfaces. Initial configuration is complete.

To configure the NetScreen-10/100 device for Network Address Translation (NAT) mode or Route mode, you must configure the Trusted, Untrusted and DMZ interfaces.

**Testing the Configuration**

From a workstation on the trusted side of the NetScreen-10/100, 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(s) are illuminated.
- The administrator’s workstation IP address and netmask are correct.
- The workstation gateway points to the external router.
- The workstation has a valid Domain Name Service (DNS) entry.
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 to the NS-10/100 console port or you can make a connection 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 console 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 the **ENTER** key to see the login prompt.

**Note:** For more information and examples on other configuration options, please refer to the NetScreen Concepts & Examples ScreenOS Reference Guide.
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, the NetScreen-10/100 default IP address.

**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:

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

Allowing Outbound Traffic

If you want to configure the NetScreen device for Transparent mode, you do not have to define IP addresses for the Trusted, Untrusted and DMZ interfaces. Initial configuration is complete.

To configure the NetScreen-10/100 device for Network Address Translation (NAT) mode or Route mode, you must configure the Trusted, Untrusted and DMZ interfaces.

```
  a.set policy outgoing "inside any" "outside any" any permit
  b.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 can expose your system to attack.

1. At the command line enter the following:
   a. `set admin name <name>`
   b. `set admin password <password>`
   c. `save`

2. 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.

If you want to configure the NetScreen device for Transparent mode, you do not have to define IP addresses for the Trusted, Untrusted and DMZ interfaces. Initial configuration is complete.

To configure the NetScreen-10/100 device for Network Address Translation (NAT) mode or Route mode, you must configure the Trusted, Untrusted and DMZ interfaces.

Testing the Configuration

From a workstation on the trusted side of the NetScreen-10/100, 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(s) are illuminated.
- The administrator’s workstation IP address and netmask are correct.
- The workstation gateway points to the external router.
- The workstation has a valid Domain Name Service (DNS) entry.
Interface Settings and Operational Modes

The NetScreen-10/100 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.

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

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. Because it does not translate addresses, the IP addresses on the protected network must be valid, routable addresses on the Untrusted network, 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.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>IP:</th>
<th>Subnet Mask:</th>
<th>Default Gateway:</th>
<th>Manage IP:</th>
<th>Traffic Bandwidth*:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trusted</strong></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td><code>&lt;a.b.c.d&gt;</code></td>
<td><code>&lt;number&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Untrusted</strong></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td><code>&lt;a.b.c.d&gt;</code></td>
<td><code>&lt;number&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DMZ</strong></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td><code>&lt;a.b.c.d&gt;</code></td>
<td><code>&lt;number&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Tunnel</strong></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

a. Optional setting for traffic shaping

**Note:** For managing the devices, you can use the System IP address or the Manage IP addresses.
Network Address Translation Mode

When in Network Address Translation (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\(^1\) 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.

1. If the outbound traffic is destined for the DMZ, then the source IP address is translated to that of the DMZ port.
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 \(<\text{number}>\) represents the bandwidth size in kbps:

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP:</th>
<th>Subnet Mask:</th>
<th>Default Gateway:</th>
<th>Manage IP:</th>
<th>Traffic Bandwidth(^a):</th>
<th>NAT: (select)(^b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted</td>
<td>&lt;a.b.c.d&gt;</td>
<td>&lt;A.B.C.D&gt;</td>
<td>&lt;e.f.g.h&gt;</td>
<td>&lt;i.j.k.l&gt;</td>
<td>&lt;\text{number}&gt;</td>
<td>(select)</td>
</tr>
<tr>
<td>Untrusted</td>
<td>&lt;a.b.c.d&gt;</td>
<td>&lt;A.B.C.D&gt;</td>
<td>&lt;e.f.g.h&gt;</td>
<td>&lt;i.j.k.l&gt;</td>
<td>&lt;\text{number}&gt;</td>
<td></td>
</tr>
<tr>
<td>DMZ</td>
<td>&lt;a.b.c.d&gt;</td>
<td>&lt;A.B.C.D&gt;</td>
<td>&lt;e.f.g.h&gt;</td>
<td>&lt;i.j.k.l&gt;</td>
<td>&lt;\text{number}&gt;</td>
<td></td>
</tr>
<tr>
<td>Tunnel</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(^a\) Optional setting for traffic shaping  
\(^b\) Selecting **NAT** for the **Trusted** interface defines the mode as NAT. Selecting **Route** defines the mode as Route.

**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, or Manage IP addresses.
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 device 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:

<table>
<thead>
<tr>
<th></th>
<th>IP:</th>
<th>Subnet Mask:</th>
<th>Default Gateway:</th>
<th>Manage IP:</th>
<th>Traffic Bandwidth:</th>
<th>Route: (select)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trusted</strong></td>
<td></td>
<td>&lt;a.b.c.d&gt;</td>
<td>&lt;A.B.C.D&gt;</td>
<td>&lt;e.f.g.h&gt;</td>
<td>&lt;number&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt;i.j.k.l&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Untrusted</strong></td>
<td></td>
<td>&lt;a.b.c.d&gt;</td>
<td>&lt;A.B.C.D&gt;</td>
<td>&lt;e.f.g.h&gt;</td>
<td>&lt;number&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt;i.j.k.l&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DMZ</strong></td>
<td></td>
<td>&lt;a.b.c.d&gt;</td>
<td>&lt;A.B.C.D&gt;</td>
<td>&lt;e.f.g.h&gt;</td>
<td>&lt;number&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt;i.j.k.l&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web Management</strong></td>
<td>System IP:</td>
<td>&lt;a.b.c.d&gt;</td>
<td></td>
<td></td>
<td></td>
<td>Port: &lt;port_number&gt;</td>
</tr>
</tbody>
</table>

### Virtual MGT (NetScreen-100)

<table>
<thead>
<tr>
<th>IP:</th>
<th>&lt;a.b.c.d.&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netmask:</td>
<td>&lt;A.B.C.D.&gt;</td>
</tr>
<tr>
<td>Default Gateway:</td>
<td>&lt;e.f.g.h.&gt;</td>
</tr>
<tr>
<td>Bind to Port:</td>
<td>&lt;Trusted, Untrusted, DMZ&gt;</td>
</tr>
</tbody>
</table>

- a. Optional setting for traffic shaping
- b. Selecting **Route** for the Trusted interface defines the mode as Route. Selecting **NAT** defines the mode as NAT.
- c. 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.
Appendix A: Safety Recommendations and Warnings

Before supplying power to the NetScreen-10/100, follow these safety guidelines:

- 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 area where you are working.

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

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-10/100 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-10/100 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-10/100 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-10/100 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

For the safe installation and operation of your NetScreen device, ensure that your site is properly prepared before beginning the hardware installation.

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Operating Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>32-122°F, 0-50°C: for storage</td>
</tr>
<tr>
<td></td>
<td>50-104°F, 10-40°C: for operation</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>5-90%, non-condensing: for storage</td>
</tr>
<tr>
<td></td>
<td>10-90%, non-condensing: for operation</td>
</tr>
<tr>
<td>Nominal Voltage</td>
<td>120 +/-15%, 220 +/-15%</td>
</tr>
<tr>
<td>Voltage Range</td>
<td>102-253 Auto Sensing</td>
</tr>
<tr>
<td>Input frequency</td>
<td>47-63 Hz</td>
</tr>
<tr>
<td>AC input current</td>
<td>1A (120VAC), 0.5A (220VAC)</td>
</tr>
<tr>
<td>Altitude</td>
<td>0-12,000 feet, 0-3,660 meters</td>
</tr>
</tbody>
</table>

Onsite Precautions

You can place the NetScreen-10/100 on a desktop or mounted in a rack. The location of the chassis and the layout of your equipment rack or wiring room are extremely important for proper system operation. 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 below 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.

- 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.

**Equipment Rack Mounting Guidelines**

The following information will help you plan an acceptable equipment rack configuration.

- Enclosed racks must have adequate ventilation. Ensure that the rack is not overly congested because each unit generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.
- When mounting a chassis in an open rack, ensure that the rack frame does not block the intake or the exhaust ports. If the chassis is installed on slides, check the position of the chassis when it is seated all the way into the rack.
- In an enclosed rack with a ventilation fan in the top, excessive heat generated by equipment near the bottom of the rack can be drawn upward and into the intake ports of the equipment above it in the rack. Ensure that you provide adequate ventilation for equipment at the bottom of the rack.
- Baffles can help to isolate exhaust air from intake air, which also helps to draw cooling air through the chassis. The best placement of the baffles depends on the airflow patterns in the rack, which can be found by experimenting with different arrangements.
## Compliance Specifications

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Certification</td>
<td>UL, CUL</td>
</tr>
<tr>
<td>EMI/RFI</td>
<td>FCC Part 15, Class A</td>
</tr>
<tr>
<td>Standards Compliance</td>
<td>IEEE 802.3, Ethernet</td>
</tr>
<tr>
<td></td>
<td>IPSec Compliance:</td>
</tr>
<tr>
<td></td>
<td>RFC 2401 (Security Architecture for the Internet Protocol)</td>
</tr>
<tr>
<td></td>
<td>RFC 2402 (IP Authentication Header)</td>
</tr>
<tr>
<td></td>
<td>RFC 2403 (The Use of HMAC-MD5-96 within ESP and AH)</td>
</tr>
<tr>
<td></td>
<td>RFC 2404 (The Use of HMAC-SHA-1-96 within ESP and AH)</td>
</tr>
<tr>
<td></td>
<td>RFC 2405 (The ESP DES-CBC Cipher Algorithm With Explicit IV)</td>
</tr>
<tr>
<td></td>
<td>RFC 2406 (IP Encapsulating Payload)</td>
</tr>
<tr>
<td></td>
<td>RFC 2409 (The Internet Key Exchange, IKE)</td>
</tr>
<tr>
<td></td>
<td>RFC 2410 (The NULL Encryption Algorithm and Its Use With IPSec)</td>
</tr>
<tr>
<td></td>
<td>RFC 1851 (The ESP-Triple DES Transform)</td>
</tr>
</tbody>
</table>
Index

A
Access Policies
   outgoing  3-1, 3-5
Admin name  3-8
Administration requirements  3-1

B
Back panel  1-1, 1-4, 2-2

C
Cables
   connections  2-3, 2-6
crossover  2-6
DCE  2-5
DTE  2-5
power  2-2
RJ45 connectors  1-2
RS-232 console  3-1
serial  3-10
twisted pair  1-2
unshielded twisted pair (UTP)  2-5
Central display area  1-6
CLI  3-1, 3-11
Command line interface
   See CLI
Configuration
   DMZ port  2-4
   initial  2-1
   methods  3-1
   multiple devices  2-2
   testing  3-9, 3-12
Connection examples  2-2
Console port  1-2, 3-10

D
Data circuit-terminating equipment
   See DCE
Data Communications Equipment
   See DCE
Data Terminal Equipment
   See DTE
DB25 serial port connector  1-2
DCE  1-2, 2-5
Diagnostics  1-1
DMZ  1-2, 2-4
DMZ port  2-4
DNS  3-9, 3-12
Domain name service
   See DNS
DTE  1-2, 2-5

E
Ethernet
   LEDs  1-3
   port connection  A-2

F
Flashdisk  1-1
Front panel  1-1, 2-2

G
General layout  1-5

H
HA  2-5
Hardware connections  2-2
High availability
   See HA

I
Internal flash card  1-1
IP address 3-4
  change 3-2
  conflicts 2-2
  default 3-2
  management 3-2
  management workstation 3-2
  system 3-1, 3-2, 3-11

L
LAN 1-vii, 2-2
LEDs 1-2, 2-2, 2-6
  DMZ 1-2
  Ethernet 1-3
  power 1-1
  status 1-vii, 1-1
  Trusted 1-2
  Untrusted ethernet 1-2
Link lights 1-2, 2-3, 2-6
  See also LEDs
Logging on 3-11
Login name
  case-sensitive 3-8
  changing 3-8, 3-12

M
Main functional categories 1-5
Management system IP address 3-2
Menu column 1-5
Multiple devices 2-2

N
NAT mode 3-2, 3-11
NetScreen-10/100 connecting 2-2
Network address translation mode
  See NAT mode

O
Operating specification A-3

Outgoing access policies 3-5

P
Password
  changing 3-8, 3-12
  forgetting 3-8
  initial use 3-3
PCMCIA flash card slot 1-1
PCMCIA PC card 1-1
Ports
  console 1-2
  DMZ 1-2, 2-4
  ethernet 1-2
  serial 1-2
  Trusted 1-2
  Untrusted 1-2
  uplink 2-6
Power 2-2, A-3
  on/off switch 1-4
  supply 2-2

R
Rack 2-2, A-3, A-4
  configuration A-4
  mounting 2-1, A-4
  tools needed 2-1
Requirements
  administration 3-1
  general site A-3
  workstation 3-1
Router 2-6, 3-9, 3-12

S
Safety
  guidelines A-1
  recommendations A-1
Sample configuration 2-3, 2-4
Site requirements A-3
Specifications A-5
Index

T
TCP/IP 1-vii, 3-1
Telnet 3-10
Terminal emulator 3-1
Transparent mode 3-1, 3-7
Trusted port 1-2, 2-6

U
Untrusted port 1-2
User name
  initial use 3-3

V
Ventilation A-3, A-4

W
Warnings A-1
Web administration tools 1-5
Web browser 1-vii
  requirements 3-1
Web user interface
  See WebUI
WebUI 1-vii, 1-1, 3-1, 3-2
Workstation requirements 3-1