

NetScreen WebUI

Reference 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 093-0040-000
Rev. A

Copyright Notice

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

NetScreen, the NetScreen logo, NetScreen device, and NetScreen device0 are U.S. registered trademarks or trademarks of NetScreen Technologies, Inc.

Macintosh is a registered trademark of Apple Computer, Inc., registered in the United States and other countries. Netscape and Netscape Communicator are registered trademarks of Netscape Communications Corporation and may be registered outside the U.S. SecurID is a registered trademark of Security Dynamics Technologies, Inc. SSH and Secure Shell are trademarks or registered trademarks of SSH Communications Security, Inc. All rights reserved. Solaris is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries. SunNet Manager is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries. UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd. Websense is a registered trademark of Websense, Inc. and Websense's product names are either trademarks, trade names, service marks or registered trademarks of Websense. WebTrends is a registered trademark of WebTrends. Windows 95, Windows 98, Windows NT, and NetMeeting are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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 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.

Contents

Preface	XV
Chapter 1 System	1-1
Configure >> General	1-2
System Information	1-2
Firewall Settings	1-3
Synchronize system clock with this client	1-5
Configure >> Authen	1-7
Enable New Connection Idle Timeout	1-7
Authentication Method Settings	1-8
Configure >> DNS	1-11
Domain Name System Support	1-11
Configuring DNS Servers	1-12
Domain Name Server Settings	1-12
DNS Refresh Settings	1-12
DNS Lookup Table	1-13
Apply and Cancel	1-13
Configure >> URL Filtering	1-14
URL Filtering	1-14
Configure >> Route Table	1-16
Static Route Table	1-16
Configure >> Route Table >> New Entry	1-18
Route Table Configuration Dialog Box	1-18
Configure >> High Availability (NetScreen 100 and -1000)	1-20
To Implement High Availability:	1-20
To Configure High Availability:	1-21
Configure >> HA >> New Path	1-23
Create A New Path	1-23
Configure >> HA >> Status	1-25
IP Packet Status	1-25
Configure >> DHCP	1-27
Dynamic Host Configuration Protocol	1-27
Configure >> DHCP >> Options	1-29
DHCP Options	1-29

Configure >> DHCP >> New Address	1-31
New DHCP Address.....	1-31
Configure >> DHCP >> Status Report	1-32
DHCP Status Report.....	1-32
Configure >> Software Key	1-34
License File Update	1-34
Admin >> Admin Menu	1-36
Administration Menus	1-36
Administration User Authentication	1-36
Creating Administrators	1-37
Setting Management Client IP Addresses.....	1-37
Modifying and Removing Administration Users.....	1-37
Modifying and Removing Management Client IP Addresses	1-37
Admin >> New Local Administrator	1-39
Local Administrator User Configuration.....	1-39
Creating an Administrator User.....	1-40
Admin >> New Management Client IP	1-41
Management Client IP Configuration.....	1-41
Admin >> Settings	1-43
Downloading and Uploading System Configuration	1-43
GMT Time Offset.....	1-44
Enabling Network Time Protocol	1-44
To enable Network Time Protocol (NTP):.....	1-44
Enabling Daylight Saving Time	1-44
E-Mail Alert Notification.....	1-44
Admin >> Syslog	1-46
Syslog Configuration	1-46
Admin >> SNMP	1-49
Simple Network Management Protocol (SNMP)	1-49
Admin >> SNMP >> New Community	1-51
Community Configuration Dialog Box	1-51
Admin >> NS Global	1-53
NS Global Manager	1-53
Enable Global Manager/PRO VPN Encryption	1-53
Enabling NetScreen-Global Manager.....	1-54
Enabling NetScreen Global PRO	1-55
Admin >> Web	1-57
Web Management IP	1-57
SSL Settings	1-58

Interface >> Trusted	1-59
Trusted Interface.....	1-59
Interface >> Trusted >> Edit	1-61
Interface Configuration Dialog Box	1-61
Interface >> Trusted >> Dynamic IP	1-65
Dynamic IP Menu	1-65
Interface >> Trusted >> New Dynamic IP Configuration	1-67
New Dynamic IP Configuration	1-67
Interface >> Untrusted	1-68
Untrusted Interface Menu	1-68
Interface >> Untrusted >> Edit	1-70
Interface Configuration Dialog Box	1-70
Interface >> Untrusted >> Mapped IP	1-73
Mapped IP Menu	1-73
Interface >> Untrusted >> Dynamic IP	1-74
Dynamic IP Menu	1-74
Interface >> Untrusted >> New Dynamic IP Configuration	1-75
New Dynamic IP Configuration	1-75
Interface >> DMZ	1-76
DMZ Interface.....	1-76
Interface >> DMZ >> Edit	1-78
Interface Configuration Dialog Box	1-78
Interface >> Management (NetScreen-1000)	1-81
Management (MGT) Interface.....	1-81
Interface >> Management >> Edit	1-83
Interface Configuration Dialog Box	1-83
Interface >> Tunnel	1-86
Tunnel Interface.....	1-86
Interface >> Tunnel >> New Entry	1-87
New Tunnel Menu	1-87
Interface >> Tunnel >> Mapped IP	1-88
Mapped IP Menu	1-88
Interface >> Tunnel >> New Mapped IP	1-89
New Mapped IP Configuration.....	1-89
Interface >> Tunnel >> Dynamic IP	1-90
Dynamic IP Menu	1-90

Interface >> Tunnel >> New Dynamic IP	1-91
New Dynamic IP Configuration	1-91
Chapter 2 Network.....	2-1
Policy >> Incoming	2-2
Incoming Access Policies	2-2
Categorizing Access Policies.....	2-3
Viewing Access Policies.....	2-3
Route Mode.....	2-5
Policy >> Incoming >> New Policy	2-7
Creating a New Access Policy	2-7
Policy >> Incoming >> Edit	2-10
Viewing and Changing Access Policies	2-10
Policy >> Incoming >> Remove	2-11
Removing an Access Policy	2-11
Policy >> Incoming >> Move	2-12
Reordering Access Policies.....	2-12
Policy >> Outgoing	2-14
What Access Policies Are	2-14
Categorizing Access Policies.....	2-15
Viewing Access Policies.....	2-15
Policy >> Outgoing >> Edit	2-17
Viewing and Changing Access Policies	2-17
Policy >> Outgoing >> Remove	2-18
Removing an Access Policy	2-18
Policy >> Outgoing >> Move	2-19
Reordering Access Policies.....	2-19
Policy >> Outgoing >> New Policy	2-21
Creating a New Access Policy	2-21
Policy >> To DMZ (NetScreen-5 and 10 only)	2-24
What Access Policies Are	2-24
Categorizing Access Policies.....	2-25
Viewing Access Policies.....	2-25
Policy >> To DMZ >> Edit	2-27
Viewing and Changing Access Policies	2-27
Policy >> To DMZ >> Remove	2-28
Removing an Access Policy	2-28

Policy >> To DMZ >> Move	2-29
Reordering Access Policies.....	2-29
Policy >> To DMZ >> New Policy	2-30
Creating a New Access Policy	2-30
Policy >> From DMZ	2-33
What Access Policies Are	2-33
Categorizing Access Policies.....	2-34
Viewing Access Policies.....	2-34
Policy >> From DMZ >> Edit	2-36
Viewing and Changing Access Policies	2-36
Policy >> From DMZ >> Remove Policy	2-37
Removing an Access Policy	2-37
Policy >> From DMZ >> Move	2-38
Reordering Access Policies.....	2-38
Policy >> From DMZ >> New Policy	2-39
Creating a New Access Policy	2-39
VPN >> Manual Key	2-42
Manual Key VPN Tunnel.....	2-42
VPN >> Manual Key >> New Manual Key Entry	2-44
Manual Key Configuration	2-44
To create a manual key:	2-44
ESP-CBC.....	2-45
AH.....	2-46
VPN >> Manual Key >> Create VPN Entry	2-48
Create VPN Entry	2-48
To create a manual key:	2-48
ESP-CBC.....	2-49
AH.....	2-51
VPN >> AutoKey IKE	2-52
Viewing an Autokey IKE	2-52
VPN >> New AutoKey IKE Entry	2-54
Autokey IKE VPN Configuration	2-54
To create an Autokey IKE VPN:	2-54
VPN >> Gateway	2-56
Gateway Definition.....	2-56
VPN >> New Remote Gateway	2-58
New Remote Gateway	2-58
To create a gateway:.....	2-58

VPN >> Edit Remote Gateway	2-61
Remote Gateway Tunnel Configuration	2-61
To edit a gateway:	2-61
VPN >> P1 Proposal	2-64
Creating a P1 Proposal	2-64
VPN >> P1 Proposal >>Edit	2-66
Phase 1 Proposal Edit	2-66
VPN >> New Phase 1 Proposal	2-68
Phase 1 Proposal Configuration	2-68
VPN >> P2 Proposal	2-70
Phase 2 Proposal	2-70
VPN >> P2 Proposal >> New Phase 2 Proposal	2-72
To create a new P2 Proposal:	2-72
VPN >> Certificates	2-74
Viewing a VPN Certificate	2-74
VPN >> Certificates >> Certificate Request	2-76
Generating Keys and Completing a Certificate Request	2-76
VPN >> Certificates or CRL >> Load	2-78
Loading Your Signed Certificates or CRL	2-78
Loading the CRL	2-79
VPN >> Certificates >> Default LDAP Server Settings	2-80
Configuring LDAP Default Server Settings	2-80
VPN >> Certificate >> Key Pair	2-81
Generating a Key Pair Using Existing Information	2-81
VPN >> L2TP Tunnel	2-82
Default L2TP Settings	2-82
L2TP Table	2-83
VPN >> New L2TP Tunnel	2-84
L2TP Tunnel Configuration	2-84
VPN >> IP Pool	2-85
IP Pool Addresses	2-85
VPN >> New IP Pool	2-86
New IP Pool Range	2-86

Network >> Virtual IP >> Virtual IP 1 (NetScreen-100 and -1000 only)	2-87
Virtual IP 1	2-87
Setting up the Configurations	2-88
Load Balancing (For NetScreen-100 Only)	2-89
New Service Menu.....	2-90
Virtual IP >> Virtual IP1 >> Edit Virtual Server IP	2-93
Edit Virtual Server Address.....	2-93
Virtual IP >> Edit Virtual IP1	2-94
Virtual IP Service Menu	2-94
Virtual IP >> Virtual IP2 (NetScreen-100 and NetScreen-1000)	2-96
Virtual IP 2	2-96
Virtual IP >> Virtual IP3 (NetScreen-100 and NetScreen-1000)	2-99
Virtual IP 3	2-99
Virtual IP >> Virtual IP4 (NetScreen-100 and NetScreen-1000)	2-102
Virtual IP 4	2-102
Chapter 3 Lists	3-1
Address >> Trusted Untrusted DMZ	3-2
Viewing the Address Book.....	3-2
Address >> Edit Group	3-4
Modify Address Group.....	3-4
Address >> Removing Address Entries	3-6
Remove Address Entry	3-6
Address >> Creating Address Groups	3-7
Create Address Group	3-7
Address >> Trusted Untrusted DMZ >> New Address	3-9
Adding to the Address Book	3-9
Service >> Pre-defined	3-11
Viewing Pre-defined Services	3-11
Service >> Custom	3-13
Custom Services	3-13
Service >> Custom >> New	3-14
Adding a Custom Service.....	3-14

Service >> Custom >> Edit	3-16
Modifying a Custom Service	3-16
Service >> Custom >> Remove	3-18
Removing a Custom Entry	3-18
Service >> Custom >> New Group	3-19
Adding a Service Group:.....	3-19
Service >> New Service	3-21
Adding a Custom Service:.....	3-21
Service >> New Group	3-23
Configure a New Group	3-23
Schedule	3-25
Viewing Schedule Detail.....	3-25
Viewing the Schedule Book	3-25
Schedule >> Edit	3-26
Modifying a Schedule	3-26
Schedule >> Remove	3-27
Removing a Schedule	3-27
Schedule >> New Schedule	3-28
Adding a Schedule	3-28
Users >> User List	3-30
Viewing User Details.....	3-30
Users >> Edit >> Auth/IKE/L2TP User Configuration	3-32
Modifying User Authentication	3-32
Users >> Edit >> Manual Key User Configuration	3-34
Modifying User Authentication	3-34
Users >> Dialup Group	3-37
Creating, Viewing, and Removing Dialup Groups.....	3-37
Users >> Dialup Group >> New Group	3-38
To Create a New Dialup Group	3-38
Users >> Dialup Group >> Add Members	3-39
Adding Members to a Group:	3-39
Users >> Remove Dialup Group	3-40
Remove a Dialup Group	3-40
Users >> Remove User	3-41
Remove a Dialup Group User	3-41

Chapter 4 Monitor	4-1
Traffic >> Policy	4-2
Viewing Traffic Allocation	4-2
Traffic >> Policy >> Graph	4-4
Viewing Traffic Graph	4-4
Traffic >> Interface	4-6
Viewing Interface Traffic Assignment	4-6
Counters	4-7
Viewing Counter Table	4-7
Counters >> View Count Details	4-9
Counter Details Reported	4-9
Alarm >> Traffic Alarm	4-10
Viewing Traffic Alarm	4-10
Alarm >> Event Alarm	4-12
Viewing Event Alarm	4-12
Log >> Traffic Log	4-13
Viewing Traffic Log.....	4-13
Log >> Traffic Log >> View Log Entries	4-15
Viewing Log Entries	4-15
Log >> Event Log	4-16
Viewing Event Log	4-16
Log >> Self Log	4-17
Viewing Self Log	4-17

Preface

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

This manual provides NetScreen WebUI users with a guide to operate their NetScreen network security devices.

Who Should Read This Manual?

System Administrators with a background in network installation and maintenance who want to install and operate NetScreen security devices should read this manual.

Manual Organization

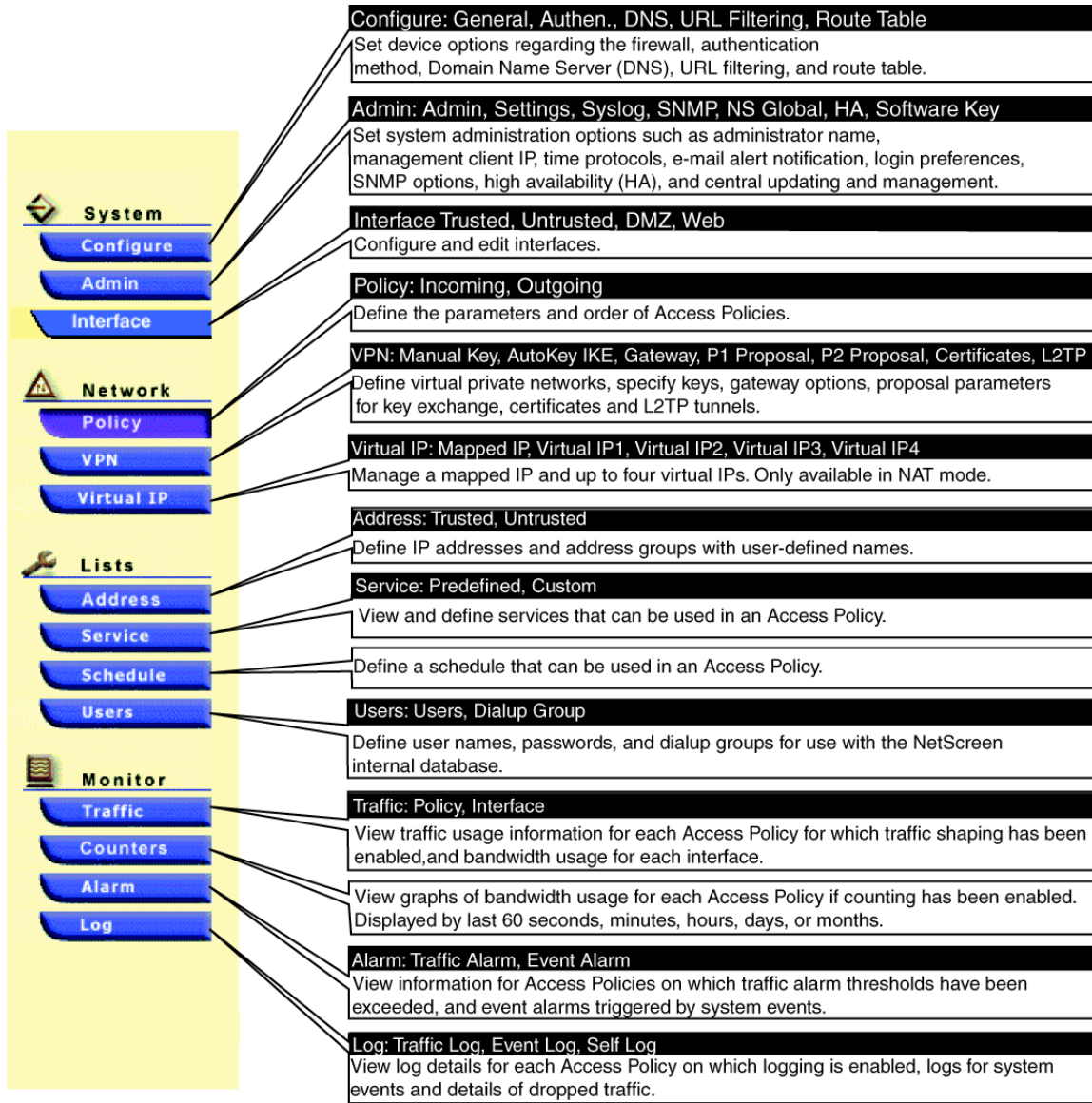
This section will contain a brief description of the contents of each chapter in the manual, and the WebUI pages described in the chapter.

Chapter 1, “System” on page 1-1 describes the WebUI pages grouped under System in the menu column: Configure, Administration and Interface.

Chapter 2, “Network” on page 2-1 describes the WebUI pages grouped under Network in the menu column: Policy, VPN and Virtual IP.

Chapter 3, “Lists” on page 3-1 describes the WebUI pages grouped under Lists in the menu column: Address, Service, Schedule and Users.

Chapter 4, “Monitor” on page 4-1 describes the WebUI pages grouped under Monitor in the menu column: Traffic, Counters, Alarm and Log.



System

1

This chapter describes the WebUI pages grouped under System in the menu column. The main sections and their subsections are as follows:

- **Configure**
 - General
 - Authentication
 - DNS
 - URL Filtering
 - Route Table
 - HA
 - DHCP
 - Software Key
- **Administration**
 - Administration
 - Settings
 - Syslog
 - SNMP
 - NS Global
 - Web
- **Interface**
 - Trusted
 - Untrusted
 - DMZ and Tunnel (NetScreen-10 and -100 devices)
 - Management and Tunnel (NetScreen-1000 device)

CONFIGURE >> GENERAL

NETSCREEN-100 • help • support • about • logout Mon 12 Feb 2001 08:32:56

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

Configuration

General Authen. DNS URL Filtering Route Table HA DHCP Software Key

Operation Mode Network Address Translation (NAT)

Software Version 2.6.0de (SN: 03000191, Firewall+VPN)

Software Update Browse...

Host Name NS100 **Domain** netscreen.com

Firewall Settings

☒ Detect SYN Attack SYN Attack Threshold packets per second.

☒ Detect ICMP Flood ICMP Flood Threshold packets per second.

☒ Detect UDP Flood UDP Flood Threshold packets per second.

☒ Detect Ping of Death Attack

☒ Detect WinNuke Attack

☒ Detect Port Scan Attack

☒ Detect Land Attack

☒ Default Packet Deny

☒ Detect Tear Drop Attack

☒ Filter IP Source Route Option

☒ Detect Address Sweep Attack

☒ Block Java/ActiveX/ZIP/EXE Component

☒ Detect IP Spoofing Attack

Sync Synchronize system clock with this client Apply Cancel

Figure 1-1 Configuration >> General

System Information

The information provided here relates to the operational mode and identity of the NetScreen software and hardware that you are managing.

System Fields	Description
Operation Mode	<i>(Read only)</i> This field reports the mode of operation for the NetScreen device. The three modes are Transparent, Network Address Translation (NAT), and Route.
Software Version	<i>(Read only)</i> This field displays the serial number of your NetScreen device and the software version number running on the device.
Software Update	You can update the NetScreen ScreenOS by using your Web browser to download the latest software release from the NetScreen Web site.
Host Name	The name for the physical NetScreen device.

Domain

The name of the domain in which the NetScreen device is located. You must fill this in if you want to use Domain Name System (DNS) name/address resolution.

Firewall Settings

The firewall security options are available on all NetScreen devices except the SYN Attack threshold option, which appears only on the NetScreen-5, -10, and -100 platforms.¹

Firewall Option	Description
Detect SYN Attack	A SYN attack occurs when a network becomes so overwhelmed by SYN packets initiating uncompletable connection requests that it can no longer process legitimate connection requests, resulting in a denial of service (DoS).
Detect ICMP Flood	An ICMP flood occurs when ICMP pings overload a system with so many echo requests that the system expends all its resources responding until it can no longer process valid network traffic.
Detect UDP Flood	A UDP flood occurs when UDP packets are sent with the purpose of slowing down the system to the point that it can no longer handle valid connections.
Detect Ping of Death Attack	The TCP/IP specification requires a specific packet size for datagrams being transmitted. Many ping implementations allow the user to specify a larger packet size if desired, which can trigger a range of adverse system reactions including crashing, freezing, and rebooting. The device can be configured to detect and reject such oversized and irregular packet sizes.
Detect IP Spoofing Attack	Spoofing attacks occur when unauthorized agents attempt to bypass the firewall security by imitating valid client IP addresses. When this feature is enabled, the device invalidates these false IP address connections.

-
1. Because the NetScreen-100 proxies all SYN packets, it does not need to reach a threshold before activating the proxying mechanism.

Detect Port Scan Attack

Port Scan attacks occur when packets are sent with different port numbers with the purpose of scanning the available services in hopes that one port will respond. Enable this feature to detect and prevent Port Scan attacks.

Detect Land Attack

A Land attack occurs when spoofed packets are sent with SYN flag set to a system with any port that is listening. If the packets contain the same source and destination IP address as the sending host, the receiving system hangs or reboots. Enable this feature to prevent Land attacks.

Default Packet Deny

Denies all traffic not specifically allowed by an Access Policy. The default is to have this option checked. Disabling this would allow all traffic that is not specifically denied. This could be useful for other non-network TCP protocols that may be required for other services.

SYN Attack Threshold

The number of SYN packets per second required to activate the SYN proxying mechanism.

ICMP Flood Threshold

The number of ICMP packets per second required to trigger the ICMP flood attack protection feature. If the threshold is exceeded, the NetScreen device ignores further ICMP echo requests for the remainder of that second.

UDP Flood Threshold

UDP Attack has a threshold that once exceeded, invokes the UDP Attack detection if it is enabled. The default threshold is 1000 UDP packets per second.

Detect Tear Drop Attack

Tear Drop attacks occur when TCP packets overlap, rendering Windows 95 machines dead. The device intercepts these illegal connection requests, shielding valuable corporate computing resources on the internal network. Enable this feature to prevent Tear Drop attacks.

Filter IP Source Route Option

IP header information has an option to contain routing information that may specify a different source than the header source. Enable this option to block all IP traffic that uses Source Route Option. Source Route Option can allow an attacker to enter a network with a fraudulent IP address and have data sent back to his real address.

**Detect
Address
Sweep
Attack**

An Address Sweep attack occurs when ICMP ping packets are sent with different destination addresses in hopes that one of them will reply, thus uncovering the vulnerable hosts. Enable this feature to prevent this type of attack.

**Block
Java/ActiveX
/ZIP/EXE
Components**

Malicious Java or ActiveX components can be hidden in Web pages. When downloaded, these applets install a Trojan horse on your computer. Similarly, Trojan horses can be hidden in compressed files such as .zip, .gzip, and .tar, and executable (.exe) files. Enable this feature to block all embedded Java and ActiveX applets from Web pages and to strip attached .zip, .gzip, .tar, and .exe files from e-mail.

**Detect
Winnuke
Attack**

Enable this feature to detect attacks on Windows NetBIOS communications.

Synchronize system clock with this client

You can synchronize the NetScreen device system clock with one of two clocks—the clock on the administrator's computer or a clock on a Network Time Protocol (NTP) server.

Note: For information on synchronizing the system clock with an NTP server, see "Admin >> Settings" on page 1-43.

To set the system clock of the NetScreen device to the clock on the administrator's computer, click the **Sync** button.

Note: If you are managing remotely across time zones, the time of the NetScreen device will be the same as the administration computer, not the local time.

Apply and Reset

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

Notes

NETSCREEN-100 help support about logout Mon 12 Feb 2001 08:52:56

System
Configure Admin Interface
Network
Policy VPN Virtual IP
Lists
Address Service Schedule Users
Monitor
Traffic Counters Alarm Log

Copyright © 1998-2001
NetScreen Technologies
Inc.
All rights reserved.

Configuration
General Authen. DNS URL Filtering Route Table HA DHCP Software Key

Operation Mode Network Address Translation (NAT)
Software Version 2.6.0de (SN: 03000191, Firewall+VPN)
Software Update Browse...
Host Name NS100 **Domain** netscreen.com

Firewall Settings

<input checked="" type="checkbox"/> Detect SYN Attack	SYN Attack Threshold <input type="text" value="200"/> packets per second
<input checked="" type="checkbox"/> Detect ICMP Flood	ICMP Flood Threshold <input type="text" value="1000"/> packets per second
<input checked="" type="checkbox"/> Detect UDP Flood	UDP Flood Threshold <input type="text" value="1000"/> packets per second
<input checked="" type="checkbox"/> Detect Ping of Death Attack	<input checked="" type="checkbox"/> Detect Tear Drop Attack
<input checked="" type="checkbox"/> Detect WinNuke Attack	<input checked="" type="checkbox"/> Filter IP Source Route Option
<input checked="" type="checkbox"/> Detect Port Scan Attack	<input checked="" type="checkbox"/> Detect Address Sweep Attack
<input checked="" type="checkbox"/> Detect Land Attack	<input checked="" type="checkbox"/> Block Java/ActiveX/ZIP/EXE Component
<input checked="" type="checkbox"/> Default Packet Deny	<input checked="" type="checkbox"/> Detect IP Spoofing Attack

Sync Synchronize system clock with this client Apply Cancel

There is no SYN Attack Threshold on the NetScreen device-1000.

CONFIGURE >> AUTHEN

NETSCREEN-10 • help • support • about • logout Mon 12 Feb 2001 08:39:54

System
 Configure
 Admin
 Interface
Network
 Policy
 VPN
 Virtual IP
Lists
 Address
 Service
 Schedule
 Users
Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

Configuration

General **Authen** DNS URL Filtering Route Table DHCP Software Key

☐ Enable New Connection Idle Timeout Minutes

Authentication Method Settings

☒ Built-in User Database

☐ RADIUS Server
 Server Name
 Shared Secret

☐ SecurID Server
 Master Server Name Client Retries
 Slave Server Name Client Timeout seconds
 Authentication Port
 Encryption Type ☒ DES ☐ SDI Use Duress ☐ Yes ☒ No

☐ LDAP Server
 LDAP Server Name/Port Common Name Identifier
 Distinguished Name (dn)

Apply Cancel

Figure 1-2 Configuration >> Authen

Access Policies can support user authentication before network access is allowed. The NetScreen product supports a built-in user database or can be linked to a RADIUS, SecurID, or LDAP Server.

Enable New Connection Idle Timeout

The amount of idle time in minutes that must elapse before the NetScreen disengages a session. The value can be from 0 to 255 minutes. A value of zero specifies that the NetScreen never terminates a session. The default of 10 minutes is highly recommended because shorter time intervals may be bothersome to normal usage and longer intervals might leave the network open to unwanted access.

Authentication Method Settings

The authentication options are the Built-in User Database, a RADIUS Server, a SecurID Server, or an LDAP Server.

Setting Option	Definition
Built-in User Database	Use the NetScreen Built-in User Database if your needs do not require an external RADIUS, SecurID, or LDAP server. The internal user database can support up to 1,500 entries, which are entered using the Users section
RADIUS Server	The NetScreen device can link to a Remote Authentication Dial-In User Service (RADIUS) server to authenticate users. You need to specify the IP address of the RADIUS server and define a shared secret; that is, a password used for generating a key to encrypt traffic between the devices. A single RADIUS server can support up to tens of thousands of users.
Server Name	The IP address of the RADIUS server.
Shared Secret	The password shared between the NetScreen device and the RADIUS server that is used to encrypt all transactions between them.
SecurID Server	The NetScreen device can link to a Security Dynamics SecurID (ACE) server to authenticate users. Using a credit card-sized device (provided by Security Dynamics Incorporated) that displays a string of randomly derived numbers that automatically changes at regular intervals, the user enters that number with their personal ID (PIN) number to authenticate themselves.
Master Server Name	The IP address of the primary SecurID server.
Slave Server Name	The IP address of the secondary (backup) SecurID server.
Authentication Port	The port number on the SecurID server to which the NetScreen device sends authentication requests. The default port number is 5500.

Setting Option	Definition
Encryption Type	The algorithm used for encrypting communication between the NetScreen device and the SecurID server: DES or SDI.
Client Retries	The number of times that the NetScreen device tries to establish communication with the SecurID server.
Client Timeout	The length of idle time in minutes that the NetScreen device waits before terminating authentication status.
Use Duress	This option allows users to use a different PIN when logging in to indicate to the SecurID server that they are doing so against their will; that is, while under duress. The SecurID server permits access that one time, and then it denies access to any further login attempts by that user until he or she contacts the SecurID administrator. Duress mode is available if the SecurID Server supports this option.
LDAP Server	The NetScreen device can link to a Lightweight Directory Access Protocol (LDAP) server, which uses the LDAP hierarchical syntax to identify each user uniquely.
LDAP Server Name/Port	The IP address and port number of the Lightweight Directory Access Protocol (LDAP) server.
Common Name Identifier	The identifier that the LDAP server uses to locate entries at the end of the path indicated by the Distinguished Name. (For example, uid--for user ID. Refer to the term used on the LDAP server.)
Distinguished Name	The path from which the LDAP server progresses before using the Common Name Identifier to search for a specific entry. (For example, c=us, o=netscreen, in which c stands for "country", and o for "organization".)

Note: *If an Access Policy requiring authentication is for a subnet of IP addresses (for example, inside any), each IP address in the subnet needs to authenticate. If one of the hosts supports multiple user accounts (for example, Unix host running Telnet), then once one user authenticates, all users from that host can pass through the device without authentication because the NetScreen device records the IP address only.*

Note: *As most Web browsers cache the username and password, it will authenticate the user again with the NetScreen device and re-initiate the timeout value.*

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

CONFIGURE >> DNS

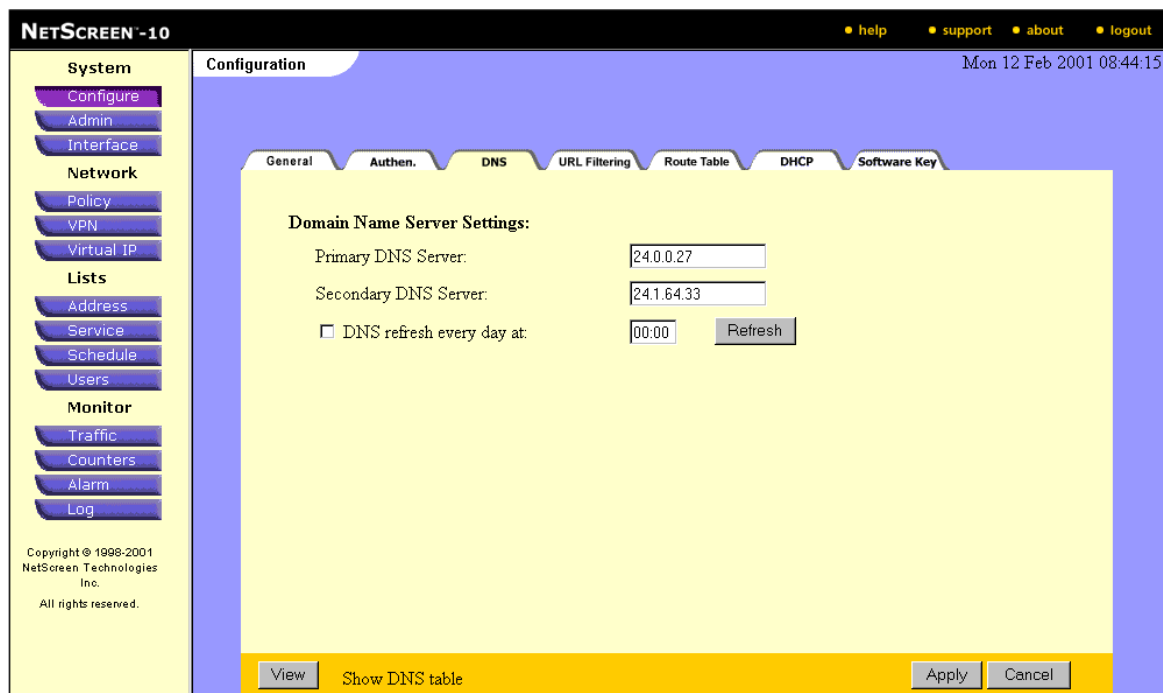


Figure 1-3 Configure >> DNS

Domain Name System Support

The NetScreen device incorporates Domain Name System (DNS) support, allowing you to use domain names as well as IP addresses for identifying locations. The services supported in DNS translation are:

- Address book
- Syslog
- E-mail
- WebTrends
- Websense
- LDAP
- SecurID
- RADIUS
- URL
- NetScreen-Global Manager

- NetScreen-GlobalPRO

Note: The server name/IP address field for each service above must also accept domain names.

Configuring DNS Servers

A Domain Name Server (DNS) keeps a table of the IP addresses associated with domain names. Using DNS makes it possible to reference locations by domain name (such as www.netscreen.com) instead of using the routable IP address, which is 209.125.148.135 for www.netscreen.com.

Before you can use DNS names with the services described above, you must configure DNS servers. Complete the following fields:

Domain Name Server Settings

DNS Server	Detail
Primary DNS Server	Enter the IP address the NetScreen device first checks for addresses.
Secondary DNS Server	Enter the IP address the NetScreen device next checks for addresses.

DNS Refresh Settings

Refresh Setting	Detail
DNS Refresh Every Day At: <hhmmss>	Allows you to specify a daily time (in 24 hour format) at which the NetScreen product resolves DNS settings.
Refresh Now	Forces the NetScreen product to do a DNS lookup. For more information on the functions of the Refresh Now button, see "Lookup".

DNS Lookup Table

Show DNS Status: Clicking the **View** button causes the NetScreen device to display a report of all the DNS names looked up. The report is formatted like the example shown below in the DNS status table.

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

NetScreen Device Lookup

For further information regarding the Lookup feature, consult the NetScreen Concepts & Examples ScreenOS Reference Guide.

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

CONFIGURE >> URL FILTERING

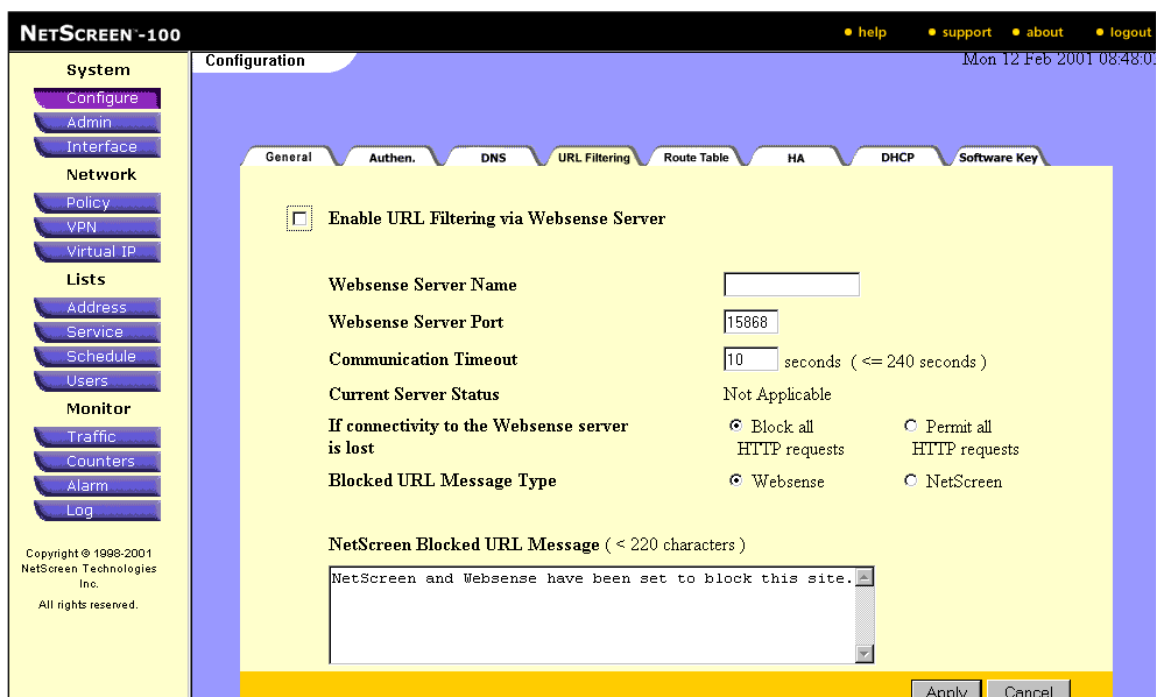


Figure 1-4 Configure >> URL Filtering

URL Filtering

This option enables the NetScreen device to block or permit access to different sites based upon their URLs, domain names, and IP addresses. To specify URL filtering options, select the **Enable URL Filtering via Websense Server** check box to enable this feature, and supply the following information to configure this option:

Configuration Setting	Description
Websense Server Name	The IP address of the Websense server.
Websense Server Port	The default port for Websense is 15868. If you change the default port on the Websense server, you need to change it on the NetScreen device also. Please see your Websense documentation for full details.

Configuration Setting	Description
Communication Timeout	The time interval, in seconds, that the NetScreen device waits for a response from the Websense filter. If Websense does not respond within the time interval, the NetScreen device can block or permit the request, depending on the “If connectivity to the Websense server is lost” setting.
Current Server Status	The NetScreen device reports the status of the Websense server.
If connectivity to the Websense server is lost	Block or permit all HTTP requests.
Blocked URL Message Type	Selects whether NetScreen’s message is displayed after access to a site is blocked or whether Websense’s message is used.
NetScreen Blocked URL Message	This is the message the NetScreen device returns to the user after blocking the site. This message can be customized up to a maximum of 219 characters.

Note: Websense requires that its service be stopped and restarted before any changes in options take effect. For more information regarding Websense, please refer to the Websense documentation.

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

CONFIGURE >> ROUTE TABLE

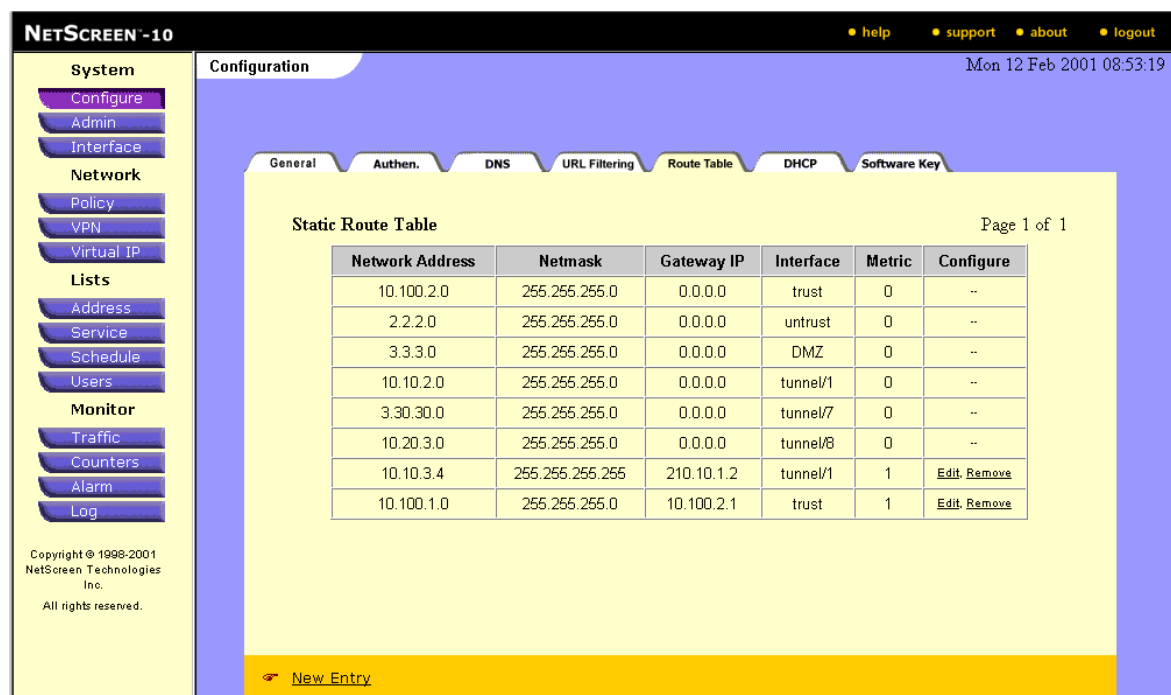


Figure 1-5 Configure >> Route Table

Static Route Table

The Route Table is used to provide the NetScreen device with information that helps it direct data to different subnets. This allows the NetScreen device to support complex networks. Defined routes are required when multiple Internet connections are installed and if multiple subnets are used on the Trusted network.

Static routes

For further information regarding static routes, see the NetScreen Concepts & Examples ScreenOS Reference Guide.

The route table displays information in the following columns:

Route Table Field	Description
Network Address:	The IP address of the target subnet

Route Table Field	Description
Netmask:	The subnet mask of the target subnet
Gateway IP Address:	IP address of the router to which the NetScreen device forwards traffic destined for the target subnet
Interface:	The interface (Trusted, Untrusted, or DMZ) across which traffic must be sent to reach the target subnet
Metric:	A definable parameter that defines the priority of the route. All route table entries that are automatically created when you define an interface (in NAT or Route mode) receive a value of 0, and any user-defined routes can be entered from 1 to 225.
Configure:	Click Edit to modify a route table entry. Click Remove to remove an entry. See below for more details.

To add, modify or remove route table entries:

Route Table Action	Detail
To add a new route table entry	Click New Entry . The Route Table Configuration dialog box appears. Complete the required fields, and then click OK .
To modify an existing route table entry	On the static Route Table page, click Edit under the Configure section for the entry that you want to modify. The Route Table configuration page appears. Type the new information in the fields. To save the changes, click OK .
To remove an existing route table entry:	On the static Route Table page, click Remove under the Configure section for the entry that you want to delete. A System Message window appears prompting you to confirm the removal. Click Yes to proceed, or No to cancel the action.

CONFIGURE >> ROUTE TABLE >> NEW ENTRY

NETSCREEN -100 help support about logout

System

- Configure
- Admin
- Interface

Network

- Policy
- VPN
- Virtual IP

Lists

- Address
- Service
- Schedule
- Users

Monitor

- Traffic
- Counters
- Alarm
- Log

Copyright © 1998-2001
NetScreen Technologies
Inc.
All rights reserved.

ROUTE TABLE CONFIGURATION

Network Address: 0.0.0.0

Netmask: 255.255.255.0

Gateway IP Address: 0.0.0.0

Interface: untrust

Metric: 1

OK Cancel

Figure 1-6 Configure >> Route Table >> New Entry**Route Table Configuration Dialog Box**

To complete the Route Table Configuration dialog box:

1. Enter the following information in the fields.

Route Table Field	Description
Network Address:	The IP address of the target subnet (for example, 123.45.67.0)
Network NetMask:	The subnet mask of the target subnet (for example, 255.255.255.0)
Gateway IP Address:	IP address of the router to which the NetScreen device forwards traffic destined for the target subnet
Interface:	The interface (Trusted, Untrusted, or Tunnel) across which traffic must be sent to reach the target subnet

Route Table Field	Description
Metric:	A definable parameter that defines the priority of the route. All route table entries that are automatically created when you define an interface (in NAT or Route mode) receive a value of 0, and any user-defined routes can be entered from 1 to 225.

2. Click **OK** to add the new configuration to the route table.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

CONFIGURE >> HIGH AVAILABILITY (NETSCREEN 100 AND -1000)

NETSCREEN -100

help support about logout

Wed 14 Mar 2001 08:03:03

System Configuration

Configure Admin Interface

Network Policy VPN Virtual IP

Lists Address Service Schedule Users

Monitor Traffic Counters Alarm Log

Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.

General Authen. DNS URL Filtering Route Table HA DHCP Software Key

HA(Master): 1.2.1

HA Port: DMZ Group ID: 4 Priority: 1

☒ HA Authentication Password:

☐ HA Encryption Password:

Sync All Files

Track IP ☐ off ☒ on Threshold: 255

Track IP	Interval (sec)	Threshold	Interface	Weight	Method	Status
10.100.2.123	1	3	auto	1	ping	Edit Remove
10.100.2.122	1	3	auto	1	ping	Edit Remove
10.100.2.124	1	3	trust	1	ping	Edit Remove
10.100.2.121	1	3	untrust	1	ping	Edit Remove

New Path Apply Cancel

Figure 1-7 Configure >> High Availability

You can configure the NetScreen device (NetScreen-100 and NetScreen-1000) in a redundant group for High Availability (HA). If a Master unit detects a Slave unit failure, it generates a system alarm. If the Master unit fails, the remaining Slave units select a new Master unit.

The High Availability configuration requires 2 NetScreen device units to be cabled together using the DMZ port connectors, two hubs or switches to interconnect the Trusted and Untrusted ports, synchronous system configuration, and an assigned system priority.

Additionally, if you choose, all communication between master and all slaves can be authenticated and encrypted.

To Implement High Availability:

1. Cable the NetScreen device units together correctly.
(For cabling instructions, see Chapter 8, "High Availability" in the NetScreen Concepts & Examples ScreenOS Reference Guide.)
2. Create Redundant Groups
3. Select System Priority (optional)

4. If desired, specify passwords for authenticating and encrypting communication between members of a Redundant Group
5. Synchronize configurations

To Configure High Availability:

HA Field	Description
HA Port	Enter the interface to which you wish to assign the unit. The NetScreen device can actually accommodate the High Availability connection on any one of its interfaces without effecting the normal traffic passing over that interface. You can designate any of the three interfaces, Trusted, Untrusted, or DMZ.
Group ID	Enter the High Availability group to which you want to assign the NetScreen device. The group numbers can be from 1 to 65535. A value of 0 disables High Availability and shuts down the High Availability port.
Priority	<p>Systems in a High Availability configuration require both Master and Slave units. You can either designate one system Master and the others Slaves, or you can let the system itself assign the priority. You can select a number between 1 and 255. The system to which you assign the lower priority becomes the Master.</p> <p>Note: The priority numbers are not synchronized between systems. If two units receive the same priority number, the unit with the lower MAC address becomes the Master.</p>
HA Authentication Password	All masters and slaves in a redundant group must use the same authentication password.
HA Encryption Password	All masters and slaves in a redundant group must use the same encryption password.

Click the **Sync** button to copy configuration to additional units in the redundant group. Following this, the slave device must be reset manually. If the manage-ip, priority or software key has been reconfigured in the master, it must be changed in the slave device as well.

Note: After synchronizing configurations, the units will remain synchronized unless one of the NetScreen device units fails.

Note: *Master and Slave units can be remotely and separately managed. System management information is not synchronized between Master and Slave units.*

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

CONFIGURE >> HA >> NEW PATH

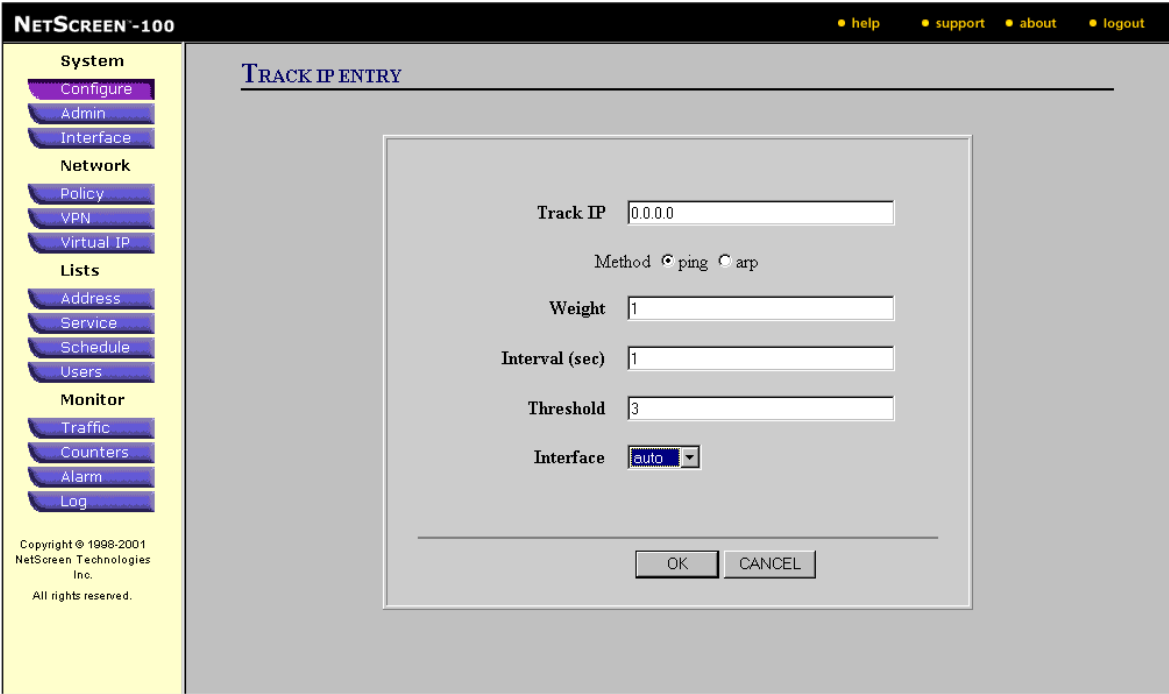


Figure 1-8 Configure >> HA >> New Path

Create A New Path

To create a new path, the Track IP Entry screen is modified:

Path Tracking Field	Description
Track IP	The IP address of the target to be pinged.
Method	Ping: NetScreen device pings the target at periodic intervals. ARP: Alerts target of its presence.
Weight	Number used to determine priority of path traffic.
Interval(s)	The interval between ping requests. You can set an interval between 1 and 200 seconds.
Threshold	The number of consecutive unanswered ping attempts required to trigger an event alarm. You can set the threshold between 1 and 200 failures.

Path Tracking Field	Description
Interface	The interface from which the ping request is sent. Use “Auto” to send a ping request from all available interfaces until a response is received.

OK, Reset and Back

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Reset** to undo any changes that you have made but have not yet applied. Click **Back** to return to the previous screen without putting your changes into effect.

CONFIGURE >> HA >> STATUS

The screenshot shows the NetScreen-100 web interface. On the left is a navigation menu with categories: System (Configure, Admin, Interface), Network (Policy, VPN, Virtual IP), Lists (Address, Service, Schedule, Users), and Monitor (Traffic, Counters, Alarm, Log). The main content area is titled 'TRACK IP STATUS' and contains a table with the following data:

Track IP	Interval (sec)	Threshold	Interface	Weight	Method	Fail Count	Success Rate
10.100.2.123	1	3	auto	1	ping	26997	0
10.100.2.122	1	3	auto	1	ping	0	2
10.100.2.124	1	3	trust	1	ping	26997	0
10.100.2.121	1	3	untrust	1	ping	26997	0

Below the table is a 'CANCEL' button. The footer of the interface includes copyright information: Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.

Figure 1-9 Configure >> HA >> Status

IP Packet Status

The path of an IP packet can be tracked through the Track IP Status table.

Path Tracking Field	Description
Track IP	Displays the IP address of the pinged target.
Interval (sec)	Displays the interval (in seconds) between ping requests.
Threshold	Displays the number of consecutive unanswered ping attempts required to trigger an event alarm.
Interface	Displays the interface from which the ping request is sent. "Auto" indicates that the ping request is sent from all available interfaces until a response is received.
Fail Count	Displays how many times the ping has failed to invoke a response since the last success.

Path Tracking Field	Description
Success Rate	Displays the percent of successes in the last 30 attempts to ping the target.

OK, Reset and Back

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Reset** to undo any changes that you have made but have not yet applied. Click **Back** to return to the previous screen without putting your changes into effect.

CONFIGURE >> DHCP

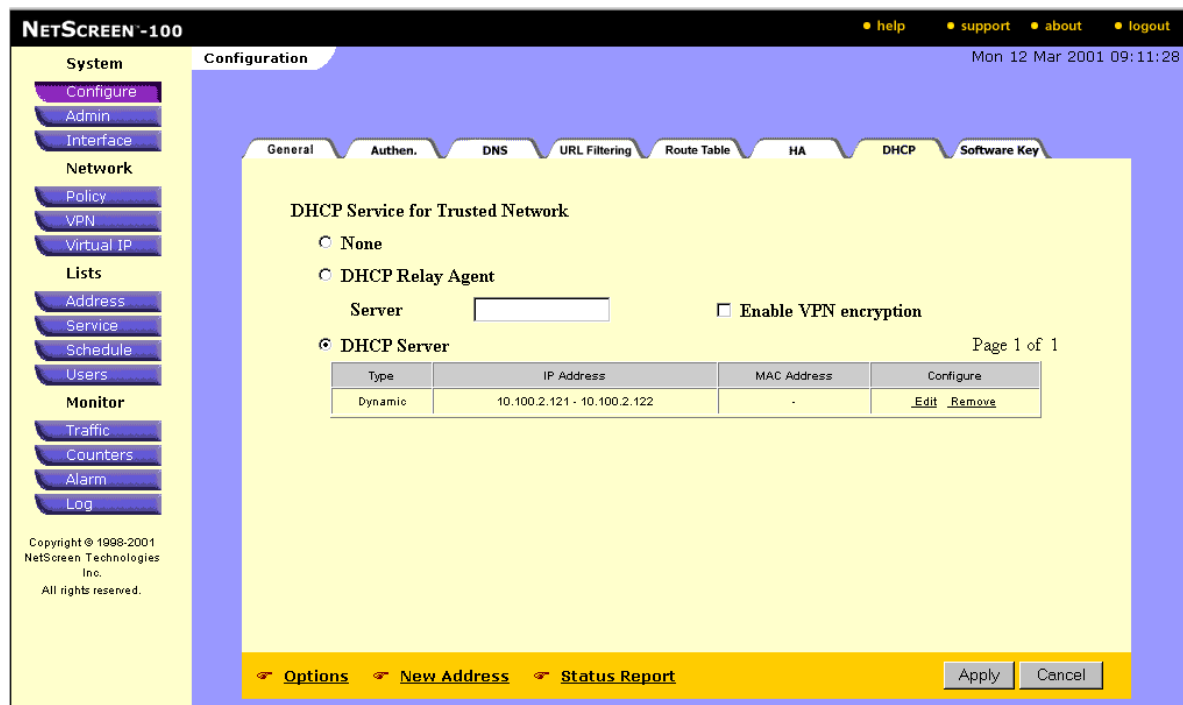


Figure 1-10 Configure >> DHCP

Dynamic Host Configuration Protocol

The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on an IP network.

DHCP works in two modes: Standard Server, where DHCP assigns IP addresses to hosts using either an automatic mechanism, whereby DHCP assigns a reserved IP address to a client, and dynamic mechanism, where DHCP assigns an IP address to a client for a limited period of time.

DHCP can also work in Relay Agent mode, where DHCP relays the DHCP messages between the actual DHCP server and hosts.

DHCP Entry	Description
Enable DHCP Server	Click to enable the DHCP Server.
DHCP Relay Agent	Click to enable and edit DHCP Relay Agent.
Server	Enter DHCP Relay Agent Server IP Address here.

DHCP Entry	Description
Enable VPN Encryption	Click to enable VPN Encryption.
DHCP Server	Click to edit DHCP Server configuration information.

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

CONFIGURE >> DHCP >> OPTIONS

NetScreen-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

DHCP SERVER OPTION CONFIGURATION

Lease ☒ Unlimited
☐ 1 days 0 hours 0 minutes

Gateway 0.0.0.0 Netmask 0.0.0.0

WINS#1 0.0.0.0 WINS#2 0.0.0.0

DNS#1 0.0.0.0 DNS#2 0.0.0.0 DNS#3 0.0.0.0

SMTP 0.0.0.0 POP3 0.0.0.0 NEWS 0.0.0.0

NetInfo Server#1 0.0.0.0 NetInfo Server#2 0.0.0.0

NetInfo Tag

Domain Name

OK Cancel

Figure 1-11 Configure >> DHCP >> Options

DHCP Options

To edit the DHCP Server configuration, click on **Options** on the main Configuration menu, and revise the below fields:

DHCP Server Field	Description
Lease	The period of time (unlimited or fixed by days, hours and minutes) that the IP address will be valid.
Gateway	Router used by clients (<i>read-only</i>).
Netmask	Subnet of IP addresses (<i>read-only</i>).
WINS (#1, #2)	WINS server of Microsoft Network.
DNS (#1-#3)	DHCP allows up to three DNS servers.
SMTP	SMTP server for email.
POP3	DNS server for email.

DHCP Server Field	Description
NEWS	DNS server for the news group.
NetInfo Server #1 and #2	IP address for NetInfo server.
NetInfo Tag	An added piece of information that indicates membership in a particular DHCP Server configuration.
Domain Name	Registered domain name of the network (up to 80 characters).

Apply and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

CONFIGURE >> DHCP >> NEW ADDRESS

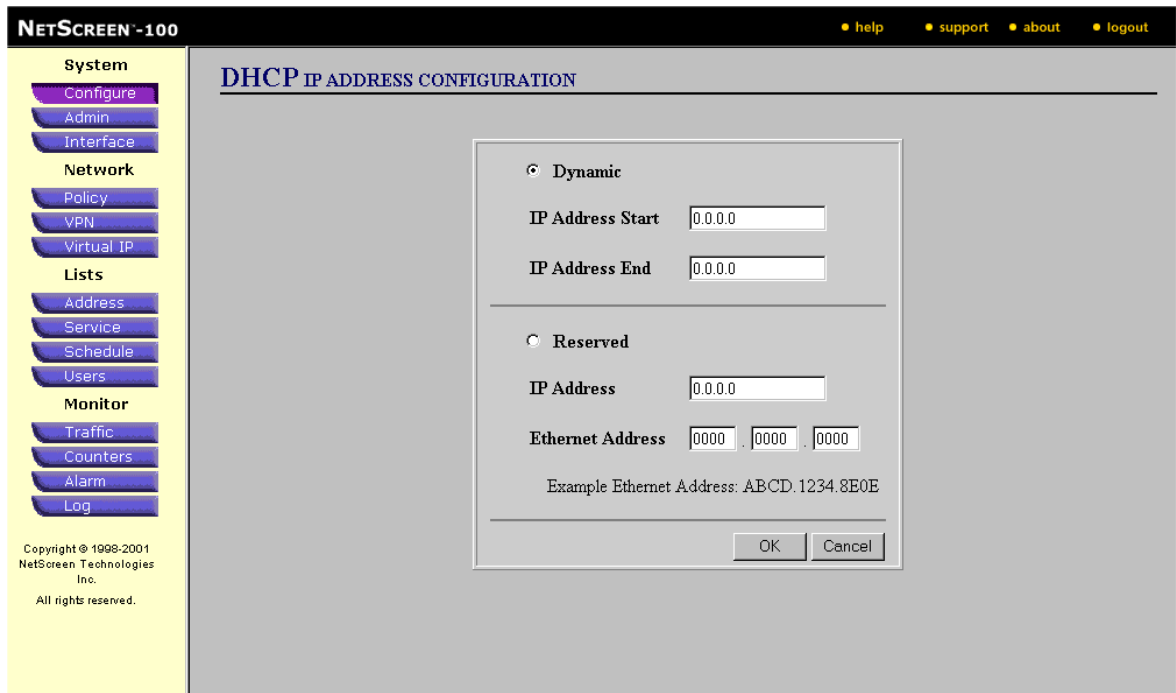


Figure 1-12 Configure >> DHCP >> New Address

New DHCP Address

To enter a new DHCP address, click on the **New Address** button of the DHCP menu, and complete the following entries.

IP Address Configuration Field	Description
Dynamic	Click to make the DHCP IP Address a range.
IP Address Start	Enter the starting value of the DHCP IP Address range.
IP Address End	Enter the ending value of the DHCP IP Address range.
Reserved	Click to reserve the DHCP IP Address
IP Address	Enter the IP Address of the DHCP Reserved IP Address.
Ethernet Address	Enter the Ethernet address for the Reserved DHCP IP Address. <i>Example: ABCD.1234.8E0E.</i>

CONFIGURE >> DHCP >> STATUS REPORT

NetScreen-100 help support about logout

System DHCP Status Mon 12 Mar 2001 09:39:28

Configure Admin Interface

Network Policy VPN Virtual IP

Lists Address Service Schedule Users

Monitor Traffic Counters Alarm Log

Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.

DHCP IP Address Binding Status: Page 1 of 1

IP Address	MAC Address	Lease Time	Action...
10.100.2.121	00a0cc285ee7	unlimited	Release
10.100.2.122	0010db075ea1	unlimited	Release

[Return](#)

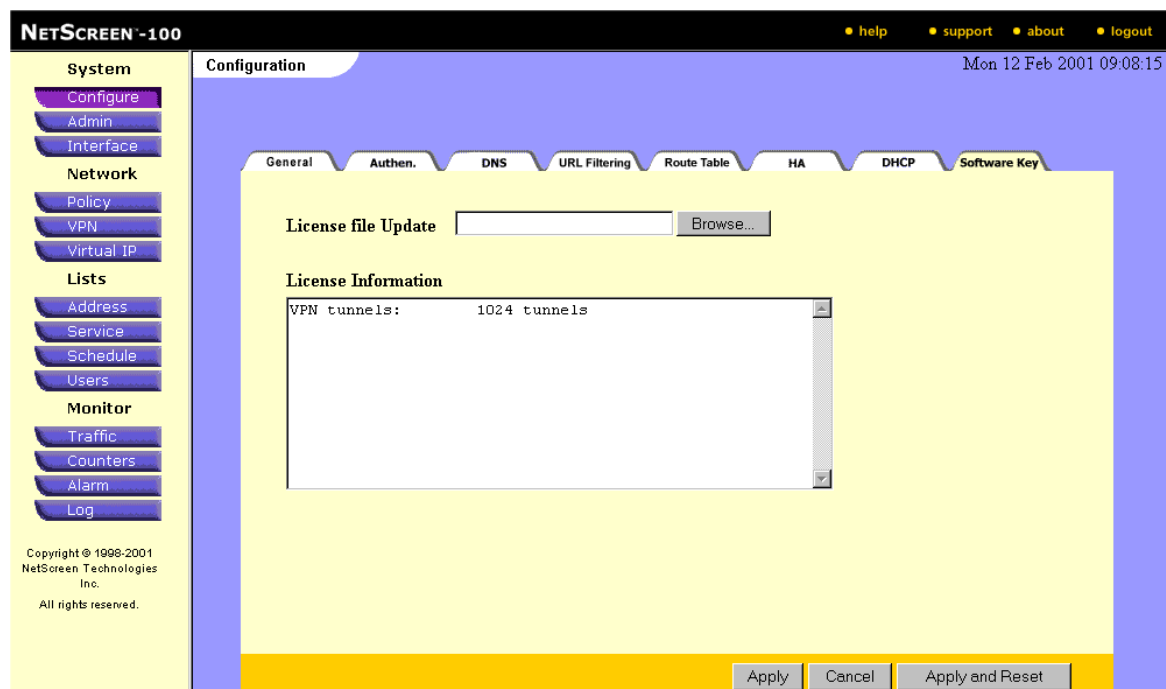
Figure 1-13 Configure >> DHCP >> Status Report

DHCP Status Report

To view a status report on the DHCP IP Address Binding, click on **Status** on the DHCP menu.

DHCP Address Field	Description
IP Address	Assigned IP Address.
MAC Address	Client MAC Address
Lease Time	Time remaining in lease.
Action	<i>Idle:</i> IP available for assignment; default state of all configured IP addresses.
	<i>Offered:</i> IP is temporarily assigned, and awaiting confirmation from the client.
	<i>Committed:</i> IP assigned to client, with time remaining on the IP lease.
	<i>Declined:</i> IP marked as unavailable because of an address conflict, pending manual reset.
	<i>Released:</i> Allocated IP address to be released.

CONFIGURE >> SOFTWARE KEY

**Figure 1-14** Configure >> Software Key

License File Update

The software key feature allows you to expand the capabilities of the NetScreen device without having to upgrade to a different device or system image. You can purchase a key that expands the standard VPN license of 1024 tunnels to an unlimited number of tunnels; that is, to a number limited only by the computing capacity of the NetScreen device and is dependent on factors such as concurrent session activity and the kinds of traffic being processed.

To update the number of VPN tunnels:

1. Contact the value-added reseller (VAR) who sold you the NetScreen device, or contact NetScreen Technologies directly.
2. Provide the serial number, the feature keyword ("vpn"), and the feature option keyword ("unlimited tunnels").

Using the information you provided, a 16-byte MD5 hash is generated. The first 8 bytes (formatted to 16 ASCII characters) is used for the software key. The key is sent to you via e-mail.

3. In the License File Update field, type the path and filename for the file you received, or use the Browse option to navigate to and select the file.

4. Click **Apply and Reset** to put your changes into effect and reset the system immediately, click **Apply** and reset the NetScreen device later or **Cancel** to undo any changes.

When you next view the License Information window, the expanded license appears listed.

Apply, Cancel and Apply and Reset

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied. Click **Apply and Reset** to put the changes into effect immediately and reset the system.

ADMIN >> ADMIN MENU

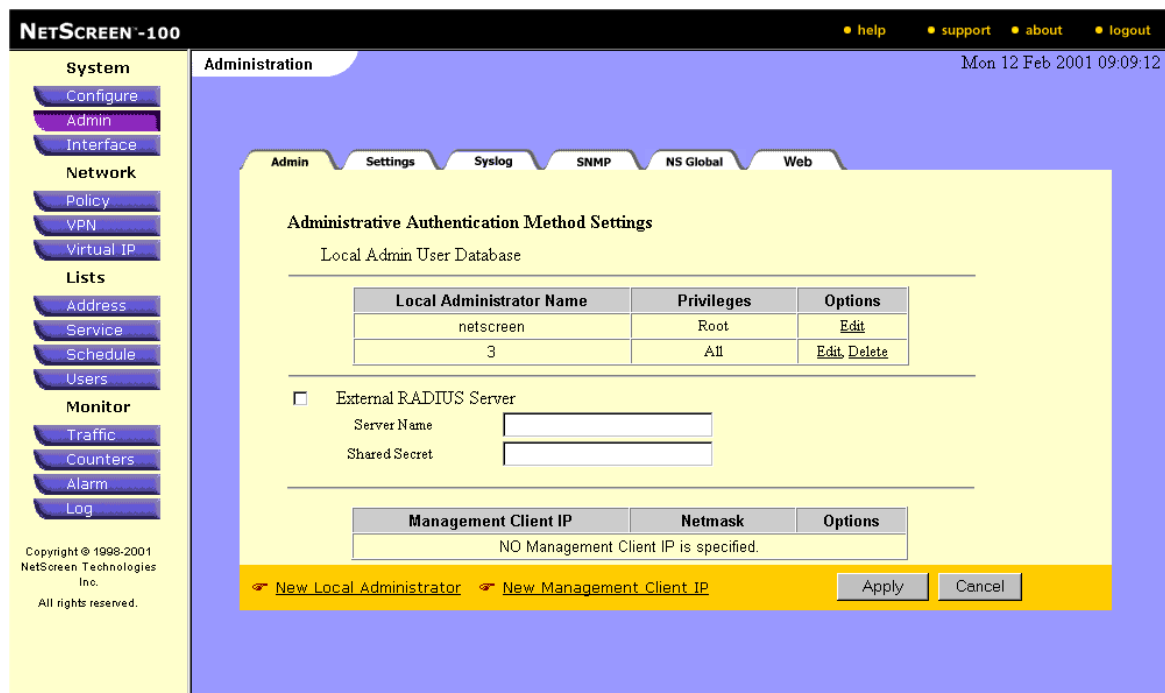


Figure 1-15 Admin >> Admin Menu

Administration Menus

You can set a number of options to restrict user access to the administration of the NetScreen device, as described in the following sections:

- Administration User Authentication
- Creating Administrators
- Setting Management Client IP Addresses
- Modifying and Removing Administration Users
- Modifying and Removing Management Client IP Addresses

Administration User Authentication

By default, you can authenticate administration users via the built-in user database in the NetScreen device. You can also specify a RADIUS database on an external server. If you use RADIUS, you must specify the server name (that is, the IP address of the RADIUS server) and a shared secret (that is, the password shared between the NetScreen device and the RADIUS server that is used to encrypt all transactions between them).

Creating Administrators

In addition to the Root Administrator, you can create up to 20 Sub Administrators. Click the **New Local Administrator** option and fill in the Local Administration User Configuration dialog box. You can determine whether you want each Sub Administrator to have all privileges (that is, the ability to configure and monitor the device) or read-only privileges (that is, the ability to monitor and perform basic troubleshooting such as pinging).

Setting Management Client IP Addresses

You can restrict administration to one or more IP addresses or subnets. If you do not specify an IP address for management, administrators can manage the NetScreen device from any IP address. To create a new management client IP address, do the following:

1. Click the **New Management Client IP** option.
The Management Client IP Configuration dialog box appears.
2. Enter the IP address and the subnet mask, and then click **OK**.

Modifying and Removing Administration Users

You can modify all administrators--Root and Sub Administrators--and you can remove all Sub Administrators.

Do the following to modify an administrator:

1. In the Options column of the Local Administration Name listing, click **Edit**.
The Local Administration User Configuration dialog box appears.
2. Modify the settings, and then click **OK**.

Do the following to remove a Sub Administrator:

1. In the Options column of the Local Administration Name listing, click **Remove**.
A system message appears, prompting you to confirm the removal.
2. Click **Yes** to continue, or **No** to cancel the action.

Modifying and Removing Management Client IP Addresses

You can modify and remove all management client IP addresses.

Do the following to modify an address:

1. In the Options column of the Management Client IP listing, click **Edit**.
The Management Client IP Configuration dialog box appears.
2. Modify the settings, and then click **OK**.

Do the following to remove an address:

1. In the Options column of the Management Client IP listing, click **Remove**.
A system message appears, prompting you to confirm the removal.

2. Click **Yes** to continue, or **No** to cancel the action.

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

ADMIN >> NEW LOCAL ADMINISTRATOR

The screenshot shows the NetScreen-100 web interface. On the left is a navigation menu with categories: System (Configure, Admin, Interface), Network (Policy, VPN, Virtual IP), Lists (Address, Service, Schedule, Users), and Monitor (Traffic, Counters, Alarm, Log). The main content area is titled 'LOCAL ADMIN USER CONFIGURATION'. Inside this area is a configuration dialog box with the following fields and options:

- Name:** A text input field.
- New Password:** A text input field.
- Confirm Password:** A text input field.
- Privileges:** Two radio buttons, ☒ ALL and ☐ READ_ONLY.
- Buttons:** OK and Cancel buttons at the bottom right of the dialog.

At the bottom left of the interface, there is a copyright notice: Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.

Figure 1-16 Administration >> New Local Administrator

Local Administrator User Configuration

Administrator Login Name and Password

To change the user name and password (initially netscreen, netscreen) for NetScreen device the Root Administrator, do the following:

1. Type the new name in the Name field.
You can now use the new user name with the old password.
2. To change the password as well, type the current password (netscreen) in the Old Password field.

Note: Passwords must be 1 to 31 characters in length.

3. Type the new password in the New Password and Confirm Password fields.
4. Click **OK** to save your changes.
5. Use the new user name and the new password from now on.

Creating an Administrator User

In addition to the Root Administrator, the NetScreen device supports the creation of up to 20 Administrator Users, which can be either Super Administrators (with all privileges) or Sub Administrators (with read-only privileges).

The NetScreen device identifies users by user name and password. Only the Root Administrator can change or add Administrator Users. Administrator Users can change their own passwords.

To create an Administrator User:

1. In the Name field, type the name of the new Administrator User.
2. Type the new password (between 1 and 31 characters) in the New Password field and Confirm Password fields.
3. For the privilege level, select either ALL (to create a Super Administrator, with the ability to configure and monitor the device) or READ_ONLY (to create a Sub Administrator, with the ability to monitor and perform basic troubleshooting, such as pinging).
4. Click **OK** to save your changes.

Note: Any configuration changes made by an administrator are logged with the name of the administrator making the change, the IP address from which the change was made, and the time the change was made.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

ADMIN >> NEW MANAGEMENT CLIENT IP

The screenshot shows the NetScreen-10 web interface. On the left is a sidebar menu with categories: System (Configure, Admin, Interface), Network (Policy, VPN, Virtual IP), Lists (Address, Service, Schedule, Users), and Monitor (Traffic, Counters, Alarm, Log). The main content area is titled 'MANAGEMENT CLIENT IP CONFIGURATION'. It contains a dialog box with two input fields: 'IP Address' (0.0.0.0) and 'Netmask' (255.255.255.255). At the bottom right of the dialog are 'OK' and 'Cancel' buttons. The top of the interface has links for help, support, about, and logout. Copyright information for NetScreen Technologies Inc. is visible in the bottom left of the sidebar.

Figure 1-17 Admin >> New Management Client IP

Management Client IP Configuration

Restricting Administration from One or Multiple Addresses of a Subnet

1. To allow administration from one or multiple addresses of a subnet:

To restrict administration to one address, type the specific IP address in the Management Client IP field and 255.255.255.255 in the Netmask field.

Or

To allow administration from multiple addresses in a subnet, type the specific IP network address in the Management Client IP field and its netmask in the Netmask field.

Or

To allow administration from any address, type 0.0.0.0.

Note: If you enter an invalid IP address and click **OK**, the setting reverts to the 0.0.0.0 default IP address.

2. Click **OK**.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

ADMIN >> SETTINGS

NETSCREEN-100 Administration

System IP Address: 0.0.0.0

Load New Configure Script Browse...

☒ Append to Configuration
☐ Replace Configuration

GMT Time Offset +8 hours

☐ Enable Network Time Protocol

Server 0.0.0.0 Update system clock every 10 minutes.

☒ Enable Daylight Saving Time

☐ Enable E-mail Notification for Alarms

SMTP Server Name ☐ Include Traffic Log

E-mail Address 1

E-mail Address 2

☒ Enable Secure Command Shell (for ssh compatible client management)

☒ Log Packets to Self that are dropped

Save Current Configuration Apply Cancel

Figure 1-18 Admin >> Settings

Downloading and Uploading System Configuration

You can download configuration settings from and upload settings to the NetScreen device. The configuration contains all the system parameters, Access Policies, VPN configurations, user-defined addresses and services, and user database settings. This data can be used to configure other devices or, in case of failure, as a backup.

Note: The configuration file is only valid for the same model. Do not attempt to upload a configuration to a different NetScreen model.

To download the existing configuration from the device to a file:

1. Click **Save Download Configuration**.
2. Browse to the location where you want to store the configuration file, and then click **Save**.

Note: Please record the administrator's name, password, and interface IP addresses to ensure easy access to the device at a later date.

To upload the configuration to a NetScreen device:

1. Type the configuration file path and filename in the Load New Configure Script field.
Or
2. Click **Browse**, navigate to the file location, select the file, and then click **Open**.
3. Select whether you wish to append or replace the existing configuration.
4. Click **Apply**.

The NetScreen device uploads the file and resets automatically. If the System Management IP address is different, you must reconnect to the new IP address.

GMT Time Offset

Select your time zone from the Greenwich Mean Time (GMT) Time Zone drop-down menu. The choices reflect GMT, plus or minus “n” hours.

Enabling Network Time Protocol

Network Time Protocol (NTP) is a feature that when enabled, synchronizes the NetScreen device system clock with that of an NTP server at specified intervals. NTP is a method by which computers synchronize system clocks on the Internet.

To enable Network Time Protocol (NTP):

1. Select the Enable Network Time Protocol check box.
2. Enter the IP address for the NTP server you want to use in the Server field.
3. In the Interval field, enter how often (in minutes), you want the NetScreen device to synchronize its system clock with the NTP server.

Enabling Daylight Saving Time

By default, the Enable Daylight Saving Time check box is selected. If you use the NetScreen device in an area that is unaffected by daylight saving time, clear the Enable Daylight Saving Time check box.

Note: At 2:00 A.M. on the first Sunday in April, the Daylight Savings Time feature automatically adjusts the clock one hour ahead. At 2:00 A.M. on the last Sunday in October, it adjusts the clock one hour back.

If you disable this feature, no time adjustments occur.

E-Mail Alert Notification

The NetScreen device can alert you via e-mail whenever an alarm is triggered.

1. Provide the following information:

E-Mail Notification Field	Description
Enable E-Mail Alert Notification	Select this check box to enable this feature.
SMTP Server Name	Enter the IP address of the SMTP mail server.
Include Traffic Log	Select this check box to include traffic logs with the event logs sent via the E-mail Alert Notification feature.
E-Mail Address 1	E-mail address of the first user to be notified.
E-Mail Address 2	E-mail address of the second user to be notified.

2. Click **Apply** to save your settings.

Administration Through Secure Command Shell (SCS)

You can administer the NetScreen device from an Ethernet connection or a dial-in modem using SCS (which is completely ssh compatible). To do this, you must have an ssh client that is compatible with version 1.5 of the ssh protocol. These clients are available for Windows 95, Windows 98, Windows NT, Linux, and UNIX.

The NetScreen device communicates with the ssh client through its built-in SCS server, which provides device configuration and management services.

To enable SCS, select the **Enable Secure Command Shell (for ssh compatible client management)** check box.

Log Packets

Select to enable a Self Log recording dropped packets.

Login Steps

For further information regarding login steps, consult the NetScreen Concepts & Examples ScreenOS Reference Guide.

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

ADMIN >> SYSLOG

Figure 1-19 Admin >> Syslog

Syslog Configuration

The NetScreen device generates syslog messages for system events, such as security alerts and other events. Messages are sent to the syslog host via UDP. Syslog messages may be used by the syslog host to create e-mail alerts and log files, or be displayed on the console of a designated host using UNIX syslog conventions and syslog servers.

To enable Syslog:

1. On the Syslog tab, provide the following information:

Syslog Field	Description
Enable SNMP VPN Encryption	Select this box to enable encryption for the data traffic between the NetScreen device and the system from which you are using the Central Management feature.
Enable Traffic Log	Select this box to enable the Traffic Log.

Syslog Field	Description
Syslog Host Name	The IP address of the syslog host.
Syslog Host Port	The port number for the syslog UDP packets. The default is 514.
Security Facility	Define the Security Facility level. The default is Local0.
Facility	Define the Facility level. The default is Local0. Set the level of messages (x) which should be sent:
Only log messages with a priority of "x" or higher	EMERGENCY -- System unusable message. Generates messages on SYN attacks, Tear Drop Attacks, and Ping of Death attacks.
	ALERT -- Take immediate action. Generates messages for multiple user authentication failures and other firewall attacks not included in the emergency category.
	CRITICAL -- Critical condition. Generates messages for URL blocks, high availability (HA) status changes, and global communications.
	ERROR -- Error message. Generates messages for administration name and password changes.
	WARNING -- Warning message. Generates messages for administration logins and logouts, failures to log in and log out, and user authentication failures, successes, and timeouts.
	NOTICE -- Normal but significant condition. Generates messages for link status changes, load balance server status changes, and traffic logs.
	INFO -- Informational message. Generates any kind of message not specified in other categories.
	DEBUG -- Debug message. Generates all messages.

**Enable
syslog
messages**

Select this box to enable this feature.

**Send traffic
log messages
via syslog**

Select this box if traffic messages should also be sent to syslog. Checking this option may generate large amounts of syslog messages.

2. Click **Apply** to save your settings.

To enable WebTrends Messages:

1. On the Syslog page.
2. Click **Enable WebTrends Messages** and provide the following information:

WebTrends Host Field	Details
WebTrends Host Name	The IP address of the WebTrends syslog host.
WebTrends Host Port	The port number for the WebTrends Syslog UDP packets. The default is 514.

Note: *WebTrends must be installed on a Windows NT system.*

3. Click **Apply** to save your changes.

Note: *When you enable syslog and WebTrends on a NetScreen device running in Transparent mode, you must set up a static route on the Route Table.*

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

ADMIN >> SNMP

NETSCREEN-100

• help • support • about • logout

Mon 12 Feb 2001 09:14:15

Administration

Admin Settings Syslog **SNMP** NS Global Web

System Name: NS100

System Contact: Joe

Location: jfraher@netscreen.com

☐ Enable SNMP VPN encryption

Communities:

Name	Write	Trap	Traffic	Hosts	Configure
Palouse	✓	✓	✓	172.16.10.154, 172.16.10.44	Edit Remove

[New Community](#) Apply Cancel

Copyright © 1998-2001
NetScreen Technologies
Inc.
All rights reserved.

Figure 1-20 Admin >> SNMP

Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) agent for the NetScreen device provides network administrators with a way to view statistical data about the network, the devices on it, and to receive notification of system events of interest

SNMP Field	Description
System Name	The hostname of the NetScreen device.
System Contact	The name of the network administrator for the NetScreen device.
Location	The NetScreen device administrator's contact information, such as an e-mail address, telephone number, or telephone extension number.
Enable SNMP VPN Encryption	Select this box to enable encryption for the data traffic between the NetScreen device and the system from which you are using the Central Management feature.

To modify an SNMP community, click **Edit**. To remove a community, click **Remove**.

Communities

To create a new SNMP community, click **New Community** and provide the following information:

SNMP Community Field	Details
Name	The name of the group, or "community," of administrators who can view data gathered by the SNMP agent and receive SNMP notification of system events.
Write	A check indicates that the community has read-write privileges for MIB II data. An X indicates read-only privileges.
Trap	<p>A check indicates that the community receives notifications, or "traps," when the following prespecified events or conditions occur:</p> <p>Cold start trap: The cold start trap is generated when the NetScreen device becomes operational after you power it on.</p> <p>Trap for SNMP authentication failure: The authentication failure trap is triggered if the SNMP manager sends the incorrect community string.</p> <p>Traps for system alarms: System alarms are triggered by firewall conditions and NetScreen device error conditions.</p> <p>An X indicates that the community does not receive system event traps.</p>
Traffic	A check indicates that the community receives traffic alarm traps, triggered when network traffic exceeds the alarm thresholds set in Access Policies. An X indicates that the community does not receive traffic alarm traps.
Hosts	The IP addresses of the workstations, or "hosts," of the members in the community.
Configure	To modify an SNMP community, click Edit . To remove a community, click Remove .

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

ADMIN >> SNMP >> NEW COMMUNITY

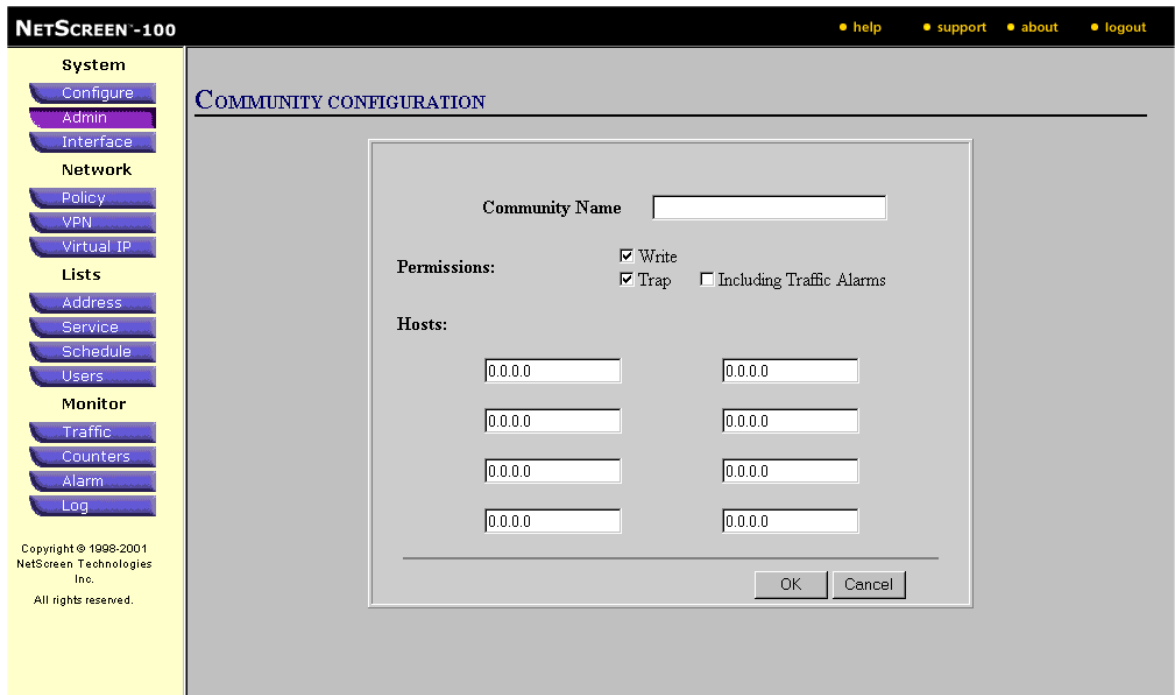


Figure 1-21 Admin >> SNMP >> New Community

Community Configuration Dialog Box

To configure a new community, complete the following fields:

Configuration Field	Description
Community Name	The name of the group, or "community," of administrators who can view data gathered by the SNMP agent and receive SNMP notification of system events.
Permission	
Write	A check indicates that the community has read-write privileges for MIB II data. An X indicates read-only privileges.
Trap	A check indicates that the community receives notifications, or "traps," when the following prespecified events or conditions occur:

Configuration Field	Description
	<p>Cold start trap: The cold start trap is generated when the NetScreen device becomes operational after you power it on.</p> <p>Trap for SNMP authentication failure: The authentication failure trap is triggered if the SNMP manager sends the incorrect community string.</p> <p>Traps for system alarms: System alarms are triggered by firewall conditions and NetScreen device error conditions.</p> <p>An X indicates that the community does not receive system event traps.</p> <p>A check indicates that the community receives traffic alarm traps, triggered when network traffic exceeds the alarm thresholds set in Access Policies. An X indicates that the community does not receive traffic alarm traps.</p> <p>The IP addresses of the workstations, or "hosts," of the members in the community.</p>
Traffic Alarms	
Hosts	

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

ADMIN >> NS GLOBAL

NETSCREEN-100 help support about logout

System Administration Mon 12 Mar 2001 10:40:40

Configure Admin Interface

Network Policy VPN Virtual IP

Lists Address Service Schedule Users

Monitor Traffic Counters Alarm Log

Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.

Admin Settings Syslog SNMP **NS Global** Web

☐ Enable Global Manager/PRO VPN encryption

☒ Enable Global Manager

Global Manager Server Settings

Server Name 10.100.2.130

Server Configuration (TCP) Port 15397

Server Reporting (UDP) Port 15397

Local NetScreen-100 Device Settings:

Local Listening Port 15397

☐ Enable Global PRO

Global PRO Server Settings

Primary IP Address 10.100.2.132

Secondary IP Address 0.0.0.0

Port 15400

☒ Protocol Distribution ☒ Policy Statistics

☒ Ethernet Statistics ☒ Flow Statistics

☒ Attack Statistics ☒ Attack Alarms

☒ Traffic Alarms ☒ Event Alarms

☒ Configuration Logs ☒ Information Logs

☒ Traffic Logs ☒ Self Logs

Apply Cancel

Figure 1-22 Admin >> NS Global

NS Global Manager

You can manage the NetScreen device from the NetScreen's central management software program, NetScreen-Global Manager. Running on Microsoft Windows NT/Workstation or Windows 2000, Global Manager provides a central place to configure and log information from multiple NetScreen devices.

To collect performance reporting data, you can run NetScreen Global PRO to collect data for display via NetScreen-Global Manager.

Enable Global Manager/PRO VPN Encryption

Select this box to enable encryption for the data traffic between the NetScreen device and the system from which you are using the Central Management feature.

Enabling NetScreen-Global Manager

Before you can use NetScreen-Global Manager, you must enable it on the NetScreen device.

1. To enable Central Management using NetScreen-Global Manager, provide the following information:

NetScreen Global Server Settings

Global Server Fields	Details
NetScreen Global Server Settings	
Enable Global Manager	Check this box to enable the Global Manager
Server Name	The IP address or the fully qualified domain name of the central management host (workstation). The default value is 0.0.0.0, which means that no host is defined.
Server Configuration (TCP) Port	This is the TCP port number that the central management station listens on for configuration update requests from the NetScreen device. The default port is 15397. A change in this value requires that the corresponding value be changed in the NetScreen-Global software.
Server Reporting (UDP) Port	This is the UDP port number that the central management station listens on for reporting messages from the NetScreen device. The default port is 15397. A change in this value requires that the corresponding value be changed in the NetScreen-Global software.
Local NetScreen Device Settings	
Local Listening Port	This is the TCP port number of the NetScreen device which listens for commands from the central management station. The default is 15397. A change in this value requires that the corresponding value be changed in the NetScreen-Global software.

2. To save, click **Apply**.

Enabling NetScreen Global PRO

1. To enable performance reporting on-demand, check the Enable Global PRO box, and provide the following information:

Global PRO Settings	Details
Primary IP address	The IP address or the fully qualified domain name of the primary data collector server. The default value is 0.0.0.0, which means that no host is defined.
Secondary IP address	The IP address or host name of the secondary data collector server. The default value is 0.0.0.0, which means that no host is defined.
Port Number	The fixed port is 15400.
Report Detail	To tailor the information displayed in your report, you can include or exclude the following statistics:
Protocol Distribution	Click to include a detail of protocol distributions.
Policy Statistics	Click to include a detail of policy traffic statistics.
Ethernet Statistics	Click to include a detail of ethernet statistics.
Flow Statistics	Click to include a detail of flow statistics.
Attack Statistics	Click to include the statistical details of attacks.
Attack Alarms	Click to include details of the Attack Alarm logs
Traffic Alarms	Click to include details of the Event Alarm logs.
Event Alarms	Click to include details of the Other Alarm logs.
Configuration Logs	Click to include details of Configuration Logs.
Information Logs	Click to include details from the Information Logs.
Traffic Logs	Check to include details from the Traffic Logs.
Self Logs	Click to include details of the Self Logs.

2. To save, click **Apply**.

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

ADMIN >> WEB

The screenshot shows the NetScreen-100 Administration interface. The left sidebar contains a menu with categories: System (Configure, Admin, Interface), Network (Policy, VPN, Virtual IP), Lists (Address, Service, Schedule, Users), and Monitor (Traffic, Counters, Alarm, Log). The main content area is titled 'Administration' and has tabs for Admin, Settings, Syslog, SNMP, NS Global, and Web. The 'Web' tab is selected, showing the 'Web Management Idle Timeout' configuration. The 'Enable Web Management Idle Timeout' checkbox is checked, with a value of 999 minutes. Below this, the 'HTTP Port' is set to 80, and the 'HTTPS (SSL) Port' is set to 1443. The 'Certificate' dropdown is set to 'None', and the 'Cipher' dropdown is set to 'RC4_40_MD5'. At the bottom right are 'Apply' and 'Cancel' buttons. The top right corner shows the date and time: 'Mon 12 Feb 2001 09:28:08'.

Figure 1-23 Admin >> Web

Web Management IP

The NetScreen device Web Management IP can be edited at the Configuration Menu through changing the below fields, and applying:

Web Management Field	Description
Enable Web Management Idle Timeout	<p>Check this box to enable.</p> <p>The amount of idle time in minutes that must elapse before the NetScreen disengages a session. The value can be from 0 to 255 minutes. A value of zero specifies that the NetScreen never terminates a session. The default of 10 minutes is highly recommended because shorter time intervals may be bothersome to normal usage and longer intervals might leave the network open to unwanted access.</p>

Web Management Field	Description
HTTP Port	The port number at which the NetScreen device listens for HTTP configuration requests. The default is 80, but you can change this to any secret number between the range of 1024 to 32,767 to discourage unauthorized access and modifications to the configuration of your NetScreen device.

Click **Apply** to save your changes or **Cancel** to return to the existing settings.

SSL Settings

Secure Sockets Layer (SSL), is a protocol designed by Netscape for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.

SSL Settings	Description
SSL Port	Enter the number of the port that you want to use for SSL. The default is 443.
Cert	All available certificates are listed in the drop-down menu. The default value is None.
Cipher	The following four ciphers are available: RC4_MD5, RC40_MD5, DES_SHA-1, and 3DES_SHA-1.

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

INTERFACE >> TRUSTED

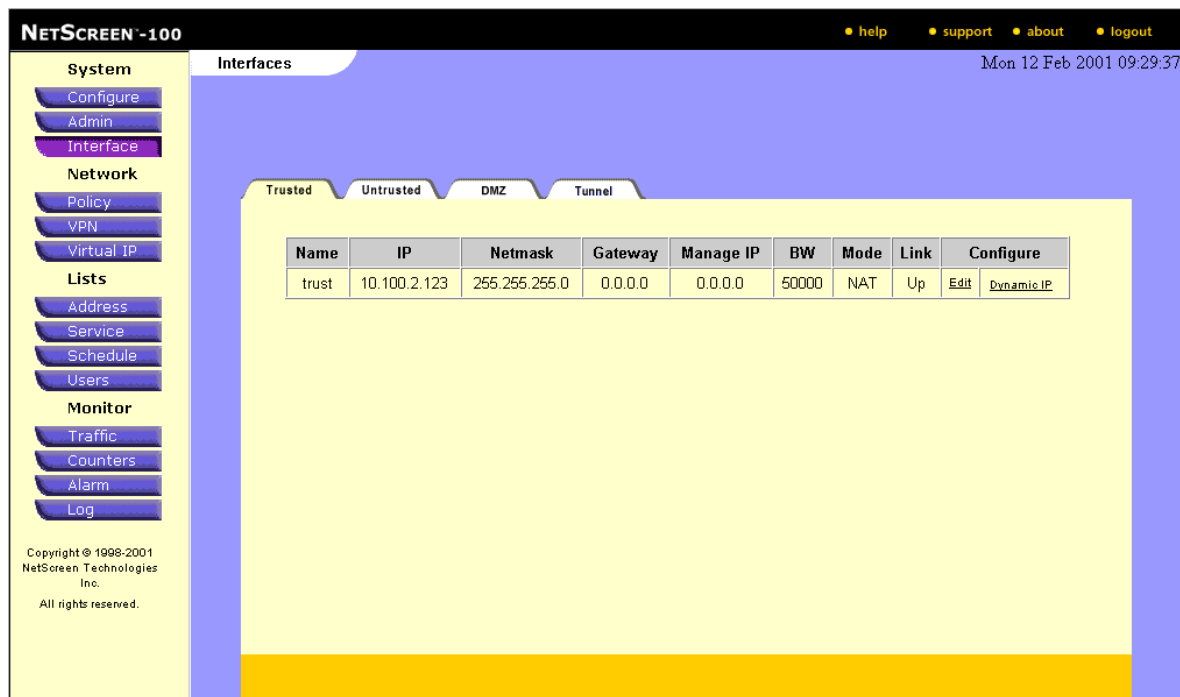


Figure 1-24 Interface >> Trusted

Trusted Interface

The trusted interface tab describes the physical and network characteristics of the trusted network connection.

Interface Field	Description
Name	The name of the physical Ethernet network interface: trust, untrust, DMZ or tunnel.
IP	The IP address of the interface.
Netmask	The subnet mask for the subnet on which the interface IP address is located.
Gateway	The IP address of the default gateway device leading to the interface. Generally, this is the address of a router, switch, or hub. If there is no such device, the gateway IP address is 0.0.0.0.
Manage IP	The logical IP address through which you can manage the NetScreen device.

Interface Field	Description
BW	The traffic bandwidth in kilobits per second (kbps) assigned to the interface.
Mode	"Route" indicates that the IP addresses of the devices on this interface have public, routable IP addresses. "NAT" indicates that the IP addresses of the devices on this interface have private, nonroutable IP addresses.
Link	"Up" indicates that the Trusted, Untrusted, or DMZ port is physically connected, or "linked," to a network device. "Down" indicates that the port is unconnected.
Configure	Click Edit to open an Interface Configuration dialog box with which you can modify the configuration.

INTERFACE >> TRUSTED >> EDIT

The screenshot shows the NetScreen-100 web interface. On the left is a navigation menu with categories: System (Configure, Admin, Interface), Network (Policy, VPN, Virtual IP), Lists (Address, Service, Schedule, Users), and Monitor (Traffic, Counters, Alarm, Log). The main area is titled 'INTERFACE CONFIGURATION'. A dialog box is open with the following fields and options:

- Interface Name:** trust (0010.dbff.0400, Up/100Mb)
- IP Address:** 10.100.2.123
- Netmask:** 255.255.255.0
- Default Gateway:** 0.0.0.0
- Manage IP:** 0.0.0.0 (with a secondary value 0010.db02.6000)
- Traffic Bandwidth:** 50000 Kbps
- Interface Mode:** ☒ NAT, ☐ Route
- Management Services:**
 - ☒ Web UI, ☒ Telnet
 - ☒ SSL, ☒ SCS
 - ☒ NS-Global, ☒ SNMP
 - ☒ NS-GlobalPRO
- Other Services:** ☒ Ping, ☐ Ident-reset

At the bottom of the dialog box are three buttons: Save, Cancel, and Save and Reset.

Figure 1-25 Interface >> Trusted >> Edit

Interface Configuration Dialog Box

1. Enter the values and select the services options that you want to use to define the interface:

Configuration Field	Description
Interface Name	<i>(Read-only)</i> The name of the physical Ethernet network interface--"trust," "untrust," or "DMZ"; the MAC address for the interface; and the link status--Up or Down--and Ethernet network speed (10 or 100 mbps).
IP Address	The IP address of the interface.
Netmask	The subnet mask for the subnet on which the interface IP address is located.

Configuration Field	Description
Default Gateway	The IP address of the default gateway device leading to the interface. Generally, this is the address of a router, switch, or hub. If there is no such device, the gateway IP address is 0.0.0.0.
Manage IP	The logical IP address through which you can manage the NetScreen-100. You can set a different Manage IP address on each available interface. The Manage IP address must be in the same subnet as the physical IP address. This Manage IP address will overwrite the system IP address and Interface IP address.
Traffic Bandwidth	The traffic bandwidth in kilobits per second (kbps) that you assign to the interface.
Interface Mode	(Trusted interface only) "NAT" indicates that the IP addresses of the devices on this interface are private and nonroutable. "Route" indicates that the IP addresses of the devices on this interface are public and routable ones.
Management Services	<p>WebUI Select to enable management through the Web user interface (WebUI).</p> <p>Telnet Select to allow management through a terminal emulation program for TCP/IP networks such as the Internet. Telnet is a common way to remotely control a network device.</p> <p>SCS Select to enable management using a secure command shell (SCS). You can administer the NetScreen device from an Ethernet connection or a dial-in modem using SCS (which is completely Secure Shell [SSH]-compatible). To do this, you must have an SCS client that is compatible with Version 1.5 of the SSH protocol. These clients are available for Windows 95, Windows 98, Windows NT, Linux, and UNIX. The NetScreen device communicates with the SCS client through its built-in SCS server, which provides device configuration and management services.</p>

Configuration Field	Description
	<p>SSL Select to enable Secure Sockets Layer (SSL), a protocol for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.</p> <p>SNMP Select to enable the use of Simple Network Management Protocol (SNMP). The NetScreen device supports the SNMPv1 protocol (described in RFC-1157) and all relevant MIB II (Management Information Base II) groups defined in RFC-1213.</p> <p>NS-Global Select to enable management by NetScreen-Global Manager, NetScreen's proprietary graphics-based, management application for multisite networks.</p> <p>NS-Global PRO Select to enable management by NetScreen-Global PRO, NetScreen's application for monitoring and management multisite systems.</p> <p>Ping Select to allow the NetScreen device to respond to an ICMP echo request, or "ping," which is a utility that enables you to determine whether a specific IP address is accessible.</p> <p>Ident-reset Services like Mail and FTP send identification requests. If they receive no acknowledgment, they send the request again. While the request is processing, there is no user access. An ident-reset restores access that has been blocked by an unacknowledged identification request.</p>

2. Click **Save** to put your changes into effect.

Save, Cancel and Save and Reset

Note: Clicking **Save** does not automatically reset the NetScreen device to use the new interface information you have entered. If you want to reset the NetScreen device at a later time, you can use the following command line interface (CLI) command: `set timer <mm/dd/yyyy> <hh:mm> action reset`.

Click **Save** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied. Click **Save and Reset** to reset the system with your changes.

INTERFACE >> TRUSTED >> DYNAMIC IP

NETSCREEN-100 [help](#) [support](#) [about](#) [logout](#)

System
[Configure](#)
[Admin](#)
[Interface](#)

Network
[Policy](#)
[VPN](#)
[Virtual IP](#)

Lists
[Address](#)
[Service](#)
[Schedule](#)
[Users](#)

Monitor
[Traffic](#)
[Counters](#)
[Alarm](#)
[Log](#)

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

DYNAMIC IPs -- Trust

[← New Entry](#) [Back](#)

ID	Start	End	Port translation	Configure
7	10.100.2.200	10.100.2.220	Enable	Edit , Remove

Figure 1-26 Interface >> Trusted >> Dynamic IP

Dynamic IP Menu

To revise the Dynamic IP fields, click on **Dynamic IP** in the Configuration heading and revise the following fields.

Dynamic IP Field	Description
DIP ID	Dynamic IP pool ID number.
DIP Low	Starting number of Dynamic IP address range.
DIP High	Ending number of Dynamic IP address range.
Port Translation	Whether Port Translation is enabled. When enabled, Port Translation allows multiple hosts to share the same IP address. Assigned port numbers distinguish which session belongs to which host.
Configure	Click Configure to configure Dynamic IP Table or Remove to remove the entry.

Click on **New Entry** to create a new Dynamic IP configuration.

Click **Back** to return to the System Interface menu.

INTERFACE >> TRUSTED >> NEW DYNAMIC IP CONFIGURATION

NETSCREEN-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

DYNAMIC IP CONFIGURATION

Interface IP/Netmask 10.100.2.123/255.255.255.0

ID 8 (4-255)

IP Address Range

Start 0.0.0.0

End 0.0.0.0

Port Translation ☒ Enable

OK Cancel

Figure 1-27 Interface >> Trusted >> New Dynamic IP Configuration

New Dynamic IP Configuration

To create a new Dynamic IP configuration, click on **New Entry** of the Dynamic IP menu and complete the following fields:

Dynamic IP Field	Description
Interface IP / Netmask	(<i>read only</i>) The Interface IP and Netmask addresses.
ID	ID number; can range up to 255.
IP Address Range	
Start	The starting value of the IP Address range.
End	The ending value of the IP Address range.
Port Translation	Whether Port Translation is enabled. When enabled, Port Translation allows multiple hosts to share the same IP address. Assigned port numbers distinguish which session belongs to which host.

INTERFACE >> UNTRUSTED



Figure 1-28 Interface >> Untrusted

Untrusted Interface Menu

The untrusted interface tab describes the physical and network characteristics of the untrusted network connection

System Interface Field	Description
Name	The name of the physical Ethernet network interface: trusted, untrusted, or DMZ.
IP	The IP address of the interface.
Netmask	The subnet mask for the subnet on which the interface IP address is located.
Gateway	The IP address of the default gateway device leading to the interface. Generally, this is the address of a router, switch, or hub. If there is no such device, the gateway IP address is 0.0.0.0.
Manage IP	The managed IP address of the interface.

System Interface Field	Description
BW	The traffic bandwidth in kilobits per second (kbps) assigned to the interface.
Mode	Not applicable to untrusted interface.
Link	“Up” indicates that the Trusted, Untrusted, or DMZ port is physically connected, or "linked," to a network device. "Down" indicates that the port is unconnected.
Configure	Click Edit to open an Interface Configuration dialog box with which you can modify the configuration.

INTERFACE >> UNTRUSTED >> EDIT

The screenshot shows the NetScreen-100 web interface. On the left is a navigation menu with categories: System (Configure, Admin, Interface), Network (Policy, VPN, Virtual IP), Lists (Address, Service, Schedule, Users), and Monitor (Traffic, Counters, Alarm, Log). The main area is titled 'INTERFACE CONFIGURATION'. A dialog box is open for editing the 'untrust' interface. The fields are: Interface Name (untrust (0010.dbff.0401, Down)), IP Address (2.2.2.2), Netmask (255.255.255.0), Default Gateway (0.0.0.0), Manage IP (0.0.0.0 with a link to 0010.db02.6001), and Traffic Bandwidth (50000 Kbps). Under 'Management Services', there are checkboxes for Web UI, SSL, NS-Global, NS-GlobalPRO, Telnet, SCS, and SNMP, all of which are checked. Under 'Other Services', there are checkboxes for Ping (checked) and Ident-reset (unchecked). At the bottom of the dialog are 'Save', 'Cancel', and 'Save and Reset' buttons. The footer of the interface shows 'Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.'

Figure 1-29 Interface >> Untrusted >> Edit

Interface Configuration Dialog Box

1. Enter the values and select the services options that you want to use to define the interface:

Dialog Field	Description
Interface Name	(READ-ONLY) The name of the physical Ethernet network interface--"trust," "untrust," or "DMZ"; the MAC address for the interface; and the link status--Up or Down--and Ethernet network speed (10 or 100 mbps).
Obtain IP using DHCP (NS-10 only)	Select this radio button to enable the NetScreen device to act as a DHCP client, receiving a dynamically assigned IP address for its Untrusted interface from an ISP.
Static IP	Select to use a Static IP number.
IP Address	The IP address of the interface.

Dialog Field	Description
Netmask	The subnet mask for the subnet on which the interface IP address is located.
Default Gateway	The IP address of the default gateway device leading to the interface. Generally, this is the address of a router, switch, or hub. If there is no such device, the gateway IP address is 0.0.0.0.
Manage IP	The managed IP address of the interface.
Traffic Bandwidth	The traffic bandwidth in kilobits per second (kbps) that you assign to the interface.
Management Services	<p>WebUI Select to enable management through the Web user interface (WebUI).</p> <p>Telnet Select to allow management through a terminal emulation program for TCP/IP networks such as the Internet. Telnet is a common way to remotely control a network device.</p> <p>SSL Select to enable Secure Sockets Layer (SSL), a protocol for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.</p> <p>SCS Select to enable management using a secure command shell (SCS). You can administer the NetScreen device from an Ethernet connection or a dial-in modem using SCS (which is completely Secure Shell [SSH]-compatible). To do this, you must have an SCS client that is compatible with Version 1.5 of the SSH protocol. These clients are available for Windows 95, Windows 98, Windows NT, Linux, and UNIX. The NetScreen device communicates with the SCS client through its built-in SCS server, which provides device configuration and management services.</p>

Dialog Field	Description
	<p>SNMP Select to enable the use of Simple Network Management Protocol (SNMP). The NetScreen device supports the SNMPv1 protocol (described in RFC-1157) and all relevant MIB II (Management Information Base II) groups defined in RFC-1213.</p> <p>NS-Global Select to enable management by NetScreen-Global Manager, NetScreen's proprietary graphics-based, management application for multisite networks.</p> <p>NS-Global PRO Select to enable management by NetScreen-Global PRO, NetScreen's application for monitoring and management multisite systems.</p> <p>Ping Select to allow the NetScreen device to respond to an ICMP echo request, or "ping," which is a utility that enables you to determine whether a specific IP address is accessible.</p> <p>Ident-reset Services like Mail and FTP send identification requests. If they receive no acknowledgment, they send the request again. While the request is processing, there is no user access. An ident-reset restores access that has been blocked by an unacknowledged identification request.</p>

- Click **Save** and **Reset** to save the settings and reset the NetScreen device.

Note: Clicking **Save** does not automatically reset the NetScreen device to use the new interface information you have entered. If you want to reset the NetScreen device at a later time, you can use the following command line interface (CLI) command: `set timer <mm/dd/yyyy> <hh:mm> action reset.`

The NS-100 and 1000 does not use DHCP to obtain an IP address for the Untrusted interface.

Save, Cancel and Save and Reset

Click **Save** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied. Click **Save and Reset** to reset the system with your changes.

INTERFACE >> UNTRUSTED >> MAPPED IP

NetScreen-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

MAPPED IPs -- Untrust

Mapped IP Table [New Entry](#) [Back](#)

Mapped IP	Netmask	Host IP	Configure
255.255.255.200	255.255.255.255	255.255.255.200	Remove

Figure 1-30 Interface >> Untrusted >> Mapped IP

Mapped IP Menu

Mapped IP (MIP) is a direct one-to-one mapping of traffic destined for one IP address to another IP address, based solely on IP addresses. By setting up MIP addresses, you can configure the NetScreen device to route traffic destined for many different IP addresses on the subnet of the Untrusted interface to specific addresses on the Trusted network.

To edit the Mapped IP fields, click on **Mapped IP** under the Configuration heading, and revise the following fields:

IP Fields	Description
Mapped IP	The Mapped IP address of the interface.
Netmask	The subnet mask for the subnet on which the interface IP address is located.
Host IP	The Host IP address of the interface.
Configure	Click Edit to open an Interface Configuration dialog box with which you can modify the configuration.

INTERFACE >> UNTRUSTED >> DYNAMIC IP

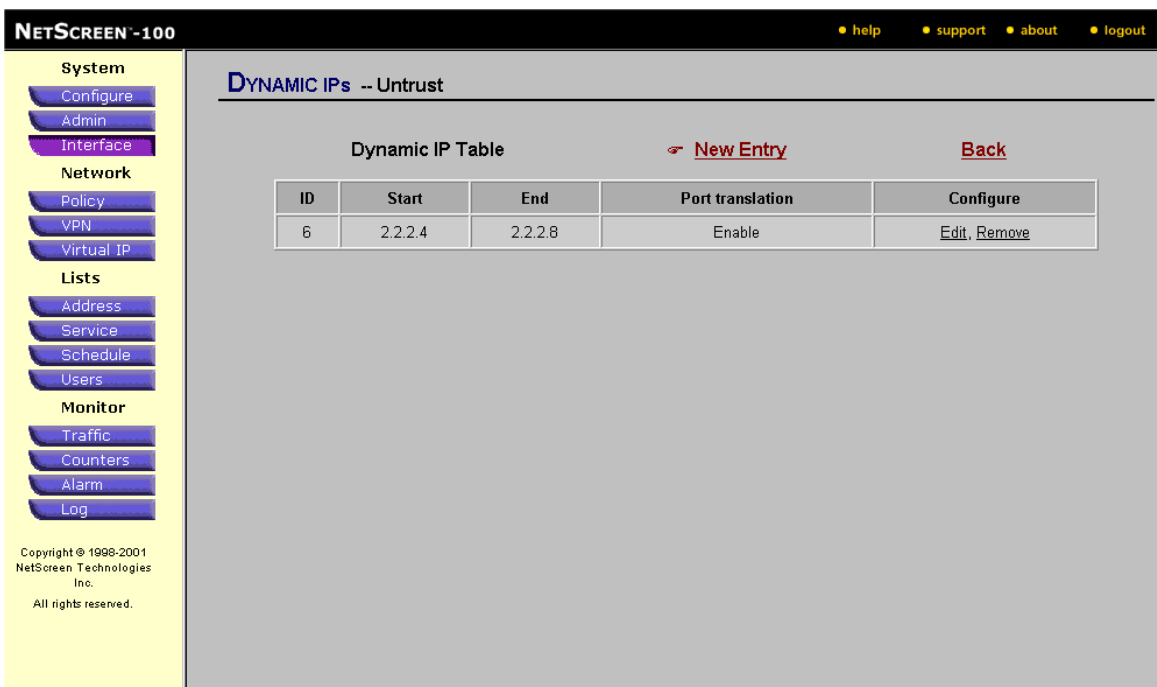


Figure 1-31 Interface >> Untrusted >> Dynamic IP

Dynamic IP Menu

To revise the Dynamic IP fields, click on **Dynamic IP** in the Configuration heading and revise the following fields.

Dynamic IP Field	Description
ID	Dynamic IP pool ID number.
Start	Starting number of Dynamic IP address range.
End	Ending number of Dynamic IP address range.
Port Translation	Whether Port Translation is enabled. When enabled, Port Translation allows multiple hosts to share the same IP address. Assigned port numbers distinguish which session belongs to which host.
Configure	Click Configure to configure Dynamic IP Table or Remove to remove the entry.

INTERFACE >> UNTRUSTED >> NEW DYNAMIC IP CONFIGURATION

NETSCREEN-100 help support about logout

System
 Configure
 Admin
 Interface
Network
 Policy
 VPN
 Virtual IP
Lists
 Address
 Service
 Schedule
 Users
Monitor
 Traffic
 Counters
 Alarm
 Log

DYNAMIC IP CONFIGURATION

Interface IP/Netmask 2.2.2.2/255.255.255.0

ID 7 (4-255)

IP Address Range

Start 0.0.0.0

End 0.0.0.0

Port Translation ☒ Enable

OK Cancel

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

Figure 1-32 Interface >> Untrusted >> New Dynamic IP

New Dynamic IP Configuration

To create a new Dynamic IP configuration, click on **New Entry** of the Dynamic IP menu and complete the following fields:

Dynamic IP Field	Description
Interface IP / Netmask	(<i>read only</i>) The Interface IP and Netmask addresses.
ID	ID number; can range up to 255.
IP Address Range	
Start	Starting IP address value.
End	Ending IP address value.
Port Translation	Whether Port Translation is enabled. When enabled, Port Translation allows multiple hosts to share the same IP address. Assigned port numbers distinguish which session belongs to which host.

INTERFACE >> DMZ

(NETSCREEN-10 AND -100 ONLY)



Figure 1-33 Interface >> DMZ

DMZ Interface

The DMZ interface tab describes the physical and network characteristics of the DMZ network connection.

System Interface Field	Description
Name	The name of the physical Ethernet network interface: trust, untrust, or DMZ.
IP	The IP address of the interface.
Netmask	The subnet mask for the subnet on which the interface IP address is located.
Gateway	The IP address of the default gateway device leading to the interface. Generally, this is the address of a router, switch, or hub. If there is no such device, the gateway IP address is 0.0.0.0.

System Interface Field	Description
Manage IP	The managed IP address of the interface.
BW	The traffic bandwidth in kilobits per second (kbps) assigned to the interface.
Mode	Not applicable to DMZ.
Link	"Up" indicates that the Trusted, Untrusted, or DMZ port is physically connected, or "linked," to a network device. "Down" indicates that the port is unconnected.
Configure	Click Edit to open an Interface Configuration dialog box with which you can modify the configuration.

INTERFACE >> DMZ >> EDIT

The screenshot shows the NetScreen-100 web interface. On the left is a navigation menu with categories: System (Configure, Admin, Interface), Network (Policy, VPN, Virtual IP), Lists (Address, Service, Schedule, Users), and Monitor (Traffic, Counters, Alarm, Log). The main area is titled 'INTERFACE CONFIGURATION'. A dialog box is open for editing the 'DMZ (0010.dbff.0402, Down)' interface. The fields are: IP Address (3.3.3.3), Netmask (255.255.255.0), Default Gateway (0.0.0.0), Manage IP (0.0.0.0) with a secondary address (0010.db02.6002), and Traffic Bandwidth (0 Kbps). There are checkboxes for Management Services (Web UI, SSL, NS-Global, NS-GlobalPRO, Telnet, SCS, SNMP) and Other Services (Ping, Ident-reset). At the bottom are 'Save', 'Cancel', and 'Save and Reset' buttons. Copyright information for NetScreen Technologies Inc. is at the bottom left.

Figure 1-34 Interface >> DMZ >> Edit

Interface Configuration Dialog Box

1. Enter the values and select the services options that you want to use to define the interface:

Configuration Field	Description
Interface Name	<i>(Read-Only)</i> The name of the physical Ethernet network interface--"trust," "untrust," or "DMZ"; the MAC address for the interface; and the link status--Up or Down--and Ethernet network speed (10 or 100 mbps).
IP Address	The IP address of the interface.
Netmask	The subnet mask for the subnet on which the interface IP address is located.

Configuration Field	Description
Default Gateway	The IP address of the default gateway device leading to the interface. Generally, this is the address of a router, switch, or hub. If there is no such device, the gateway IP address is 0.0.0.0.
Manage IP	The managed IP address of the interface.
Traffic Bandwidth	The traffic bandwidth in kilobits per second (kbps) that you assign to the interface.
Management Services	<p>WebUI Select to enable management through the Web user interface (WebUI).</p> <p>Telnet Select to allow management through a terminal emulation program for TCP/IP networks such as the Internet. Telnet is a common way to remotely control a network device.</p> <p>SSL Select to enable Secure Sockets Layer (SSL), a protocol for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.</p> <p>SCS Select to enable management using a secure command shell (SCS). You can administer the NetScreen device from an Ethernet connection or a dial-in modem using SCS (which is completely Secure Shell [SSH]-compatible). To do this, you must have an SCS client that is compatible with Version 1.5 of the SSH protocol. These clients are available for Windows 95, Windows 98, Windows NT, Linux, and UNIX. The NetScreen device communicates with the SCS client through its built-in SCS server, which provides device configuration and management services.</p> <p>SNMP Select to enable the use of Simple Network Management Protocol (SNMP). The NetScreen device supports the SNMPv1 protocol (described in RFC-1157) and all relevant MIB II (Management Information Base II) groups defined in RFC-1213.</p>

Configuration Field	Description
	NS-Global Select to enable management by NetScreen-Global Manager, NetScreen's proprietary graphics-based, management application for multisite networks.
	NS-Global PRO Select to enable management by NetScreen-Global PRO, NetScreen's application for monitoring and management multisite systems.
	Ping Select to allow the NetScreen device to respond to an ICMP echo request, or "ping," which is a utility that enables you to determine whether a specific IP address is accessible.
	Ident-reset Services like Mail and FTP send identification requests. If they receive no acknowledgment, they send the request again. While the request is processing, there is no user access. An ident-reset restores access that has been blocked by an unacknowledged identification request.

2. Click **Save** and **Reset** to save the settings and reset the NetScreen device.

Note: Clicking **Save** does not automatically reset the NetScreen device to use the new interface information you have entered. If you want to reset the NetScreen device at a later time, you can use the following command line interface (CLI) command: `set timer <mm/dd/yyyy> <hh:mm> action reset.`

Save, Cancel and Save and Reset

Click **Save** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied. Click **Save and Reset** to reset the system with your changes.

INTERFACE >> MANAGEMENT (NETSCREEN-1000)

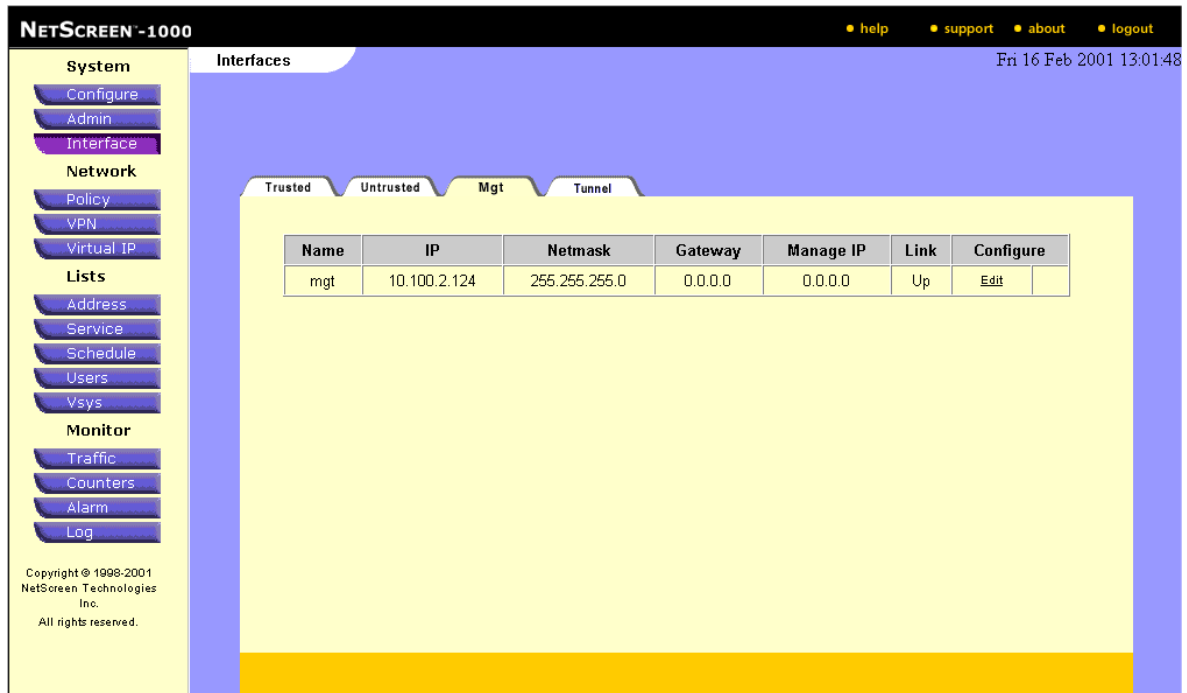


Figure 1-35 Interface >> Management

Management (MGT) Interface

The MGT interface tab describes the physical and network characteristics of the management network connection.

System Interface Field	Description
Name	The name of the physical Ethernet network interface: trust, untrust, MGT or Tunnel.
IP	The IP address of the interface.
Netmask	The subnet mask for the subnet on which the interface IP address is located.
Gateway	The IP address of the default gateway device leading to the interface. Generally, this is the address of a router, switch, or hub. If there is no such device, the gateway IP address is 0.0.0.0.
Manage IP	The managed IP address of the interface.

System Interface Field	Description
Link	“Up” indicates that the Trusted, Untrusted, or DMZ port is physically connected, or "linked," to a network device. "Down" indicates that the port is unconnected.
Configure	Click Edit to open an Interface Configuration dialog box with which you can modify the configuration.

INTERFACE >> MANAGEMENT >> EDIT

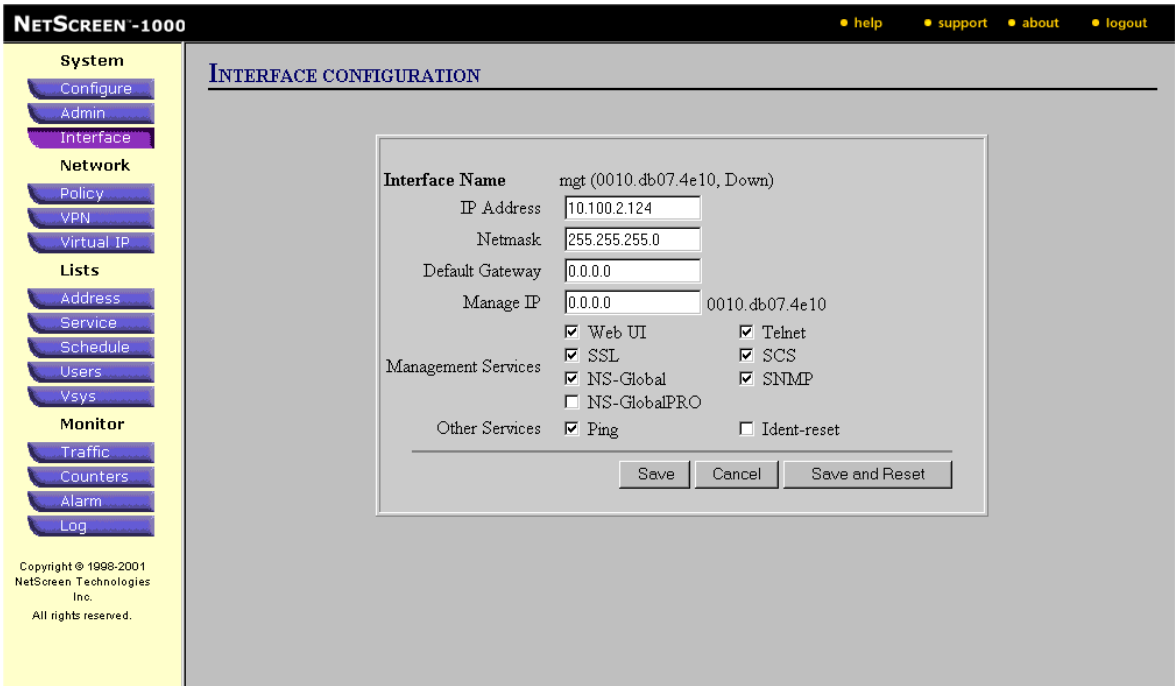


Figure 1-36 Interface >> DMZ >> Edit

Interface Configuration Dialog Box

1. Enter the values and select the services options that you want to use to define the interface:

Configuration Field	Description
Interface Name	<i>(Read-Only)</i> The name of the physical Ethernet network interface--"trust," "untrust," "Mgt" or "Tunnel"; the MAC address for the interface; and the link status--Up or Down--and Ethernet network speed (10 or 100 mbps).
IP Address	The IP address of the interface.
Netmask	The subnet mask for the subnet on which the interface IP address is located.

Configuration Field	Description
Default Gateway	The IP address of the default gateway device leading to the interface. Generally, this is the address of a router, switch, or hub. If there is no such device, the gateway IP address is 0.0.0.0.
Manage IP	The managed IP address of the interface.
Traffic Bandwidth	The traffic bandwidth in kilobits per second (kbps) that you assign to the interface.
Management Services	<p>WebUI Select to enable management through the Web user interface (WebUI).</p> <p>Telnet Select to allow management through a terminal emulation program for TCP/IP networks such as the Internet. Telnet is a common way to remotely control a network device.</p> <p>SSL Select to enable Secure Sockets Layer (SSL), a protocol for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.</p> <p>SCS Select to enable management using a secure command shell (SCS). You can administer the NetScreen device from an Ethernet connection or a dial-in modem using SCS (which is completely Secure Shell [SSH]-compatible). To do this, you must have an SCS client that is compatible with Version 1.5 of the SSH protocol. These clients are available for Windows 95, Windows 98, Windows NT, Linux, and UNIX. The NetScreen device communicates with the SCS client through its built-in SCS server, which provides device configuration and management services.</p> <p>SNMP Select to enable the use of Simple Network Management Protocol (SNMP). The NetScreen device supports the SNMPv1 protocol (described in RFC-1157) and all relevant MIB II (Management Information Base II) groups defined in RFC-1213.</p>

Configuration Field	Description
	<p>NS-Global Select to enable management by NetScreen-Global Manager, NetScreen's proprietary graphics-based, management application for multisite networks.</p> <p>NS-Global PRO Select to enable management by NetScreen-Global PRO, NetScreen's application for monitoring and management multisite systems.</p> <p>Ping Select to allow the NetScreen device to respond to an ICMP echo request, or "ping," which is a utility that enables you to determine whether a specific IP address is accessible.</p> <p>Ident-reset Services like Mail and FTP send identification requests. If they receive no acknowledgment, they send the request again. While the request is processing, there is no user access. An ident-reset restores access that has been blocked by an unacknowledged identification request.</p>

2. Click **Save** and **Reset** to save the settings and reset the NetScreen device.

Note: Clicking **Save** does not automatically reset the NetScreen device to use the new interface information you have entered. If you want to reset the NetScreen device at a later time, you can use the following command line interface (CLI) command: `set timer <mm/dd/yyyy> <hh:mm> action reset.`

Save, Cancel and Save and Reset

Click **Save** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied. Click **Save and Reset** to reset the system with your changes.

INTERFACE >> TUNNEL

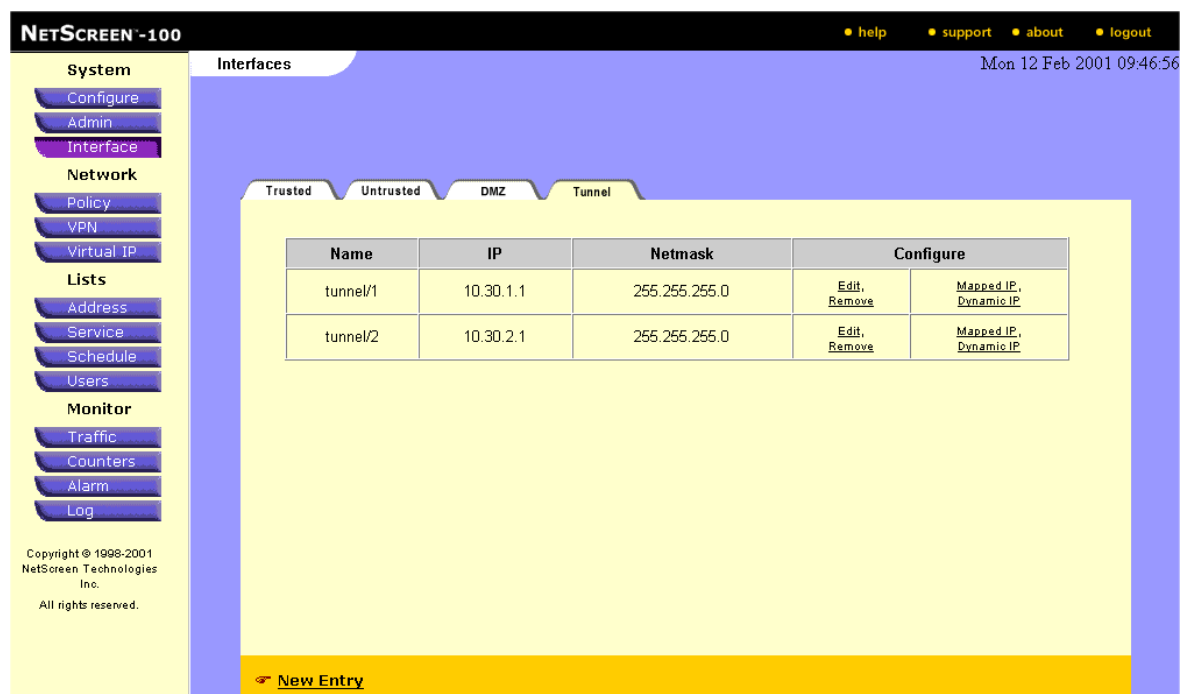


Figure 1-37 Interface >> Tunnel

Tunnel Interface

The below table shows the characteristics of the tunnel interfaces for a NetScreen device:

Tunnel Fields	Description
Name	The number of the interface tunnel.
IP	The IP address of the interface tunnel.
Netmask	The subnet mask for the interface tunnel.
Configure	Click Edit to revise the configuration of the tunnel; Click Remove to delete the tunnel; Click Mapped IP to configure as a Mapped IP; or Click Dynamic IP to configure as a Dynamic IP.

INTERFACE >> TUNNEL >> NEW ENTRY

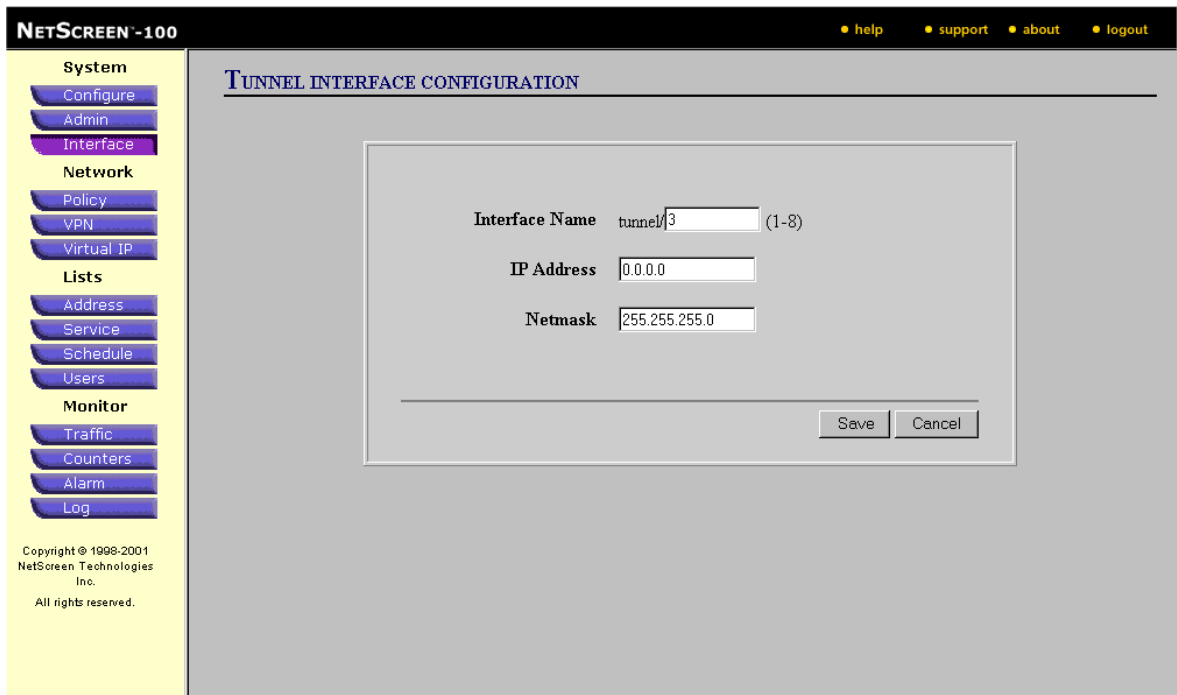


Figure 1-38 Interface >> Tunnel >> New Entry

New Tunnel Menu

To create a new tunnel, click **New Entry** on the Tunnel menu, and enter the following fields:

Tunnel Fields	Description
Name	The number of the interface tunnel.
IP	The IP address of the new interface tunnel.
Netmask	The subnet mask for the interface tunnel.

Save or Cancel

Click **Save** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

INTERFACE >> TUNNEL >> MAPPED IP

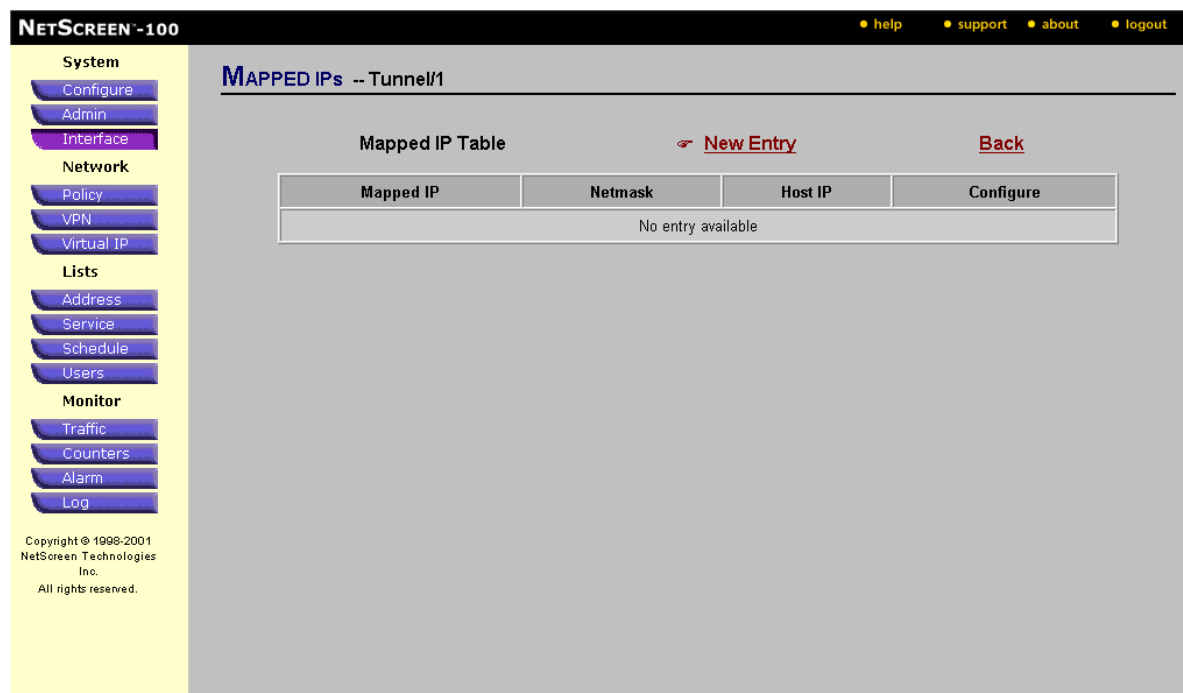


Figure 1-39 Interface >> Tunnel >> Mapped IP

Mapped IP Menu

Mapped IP (MIP) is a direct one-to-one mapping of traffic destined for one IP address to another IP address, based solely on IP addresses. By setting up MIP addresses, you can configure the NetScreen device to route traffic destined for many different IP addresses on the subnet of the Untrusted interface to specific addresses on the Trusted network.

To edit the Mapped IP fields, click on **Mapped IP** under the Configuration heading, and revise the following fields:

IP Fields	Description
Mapped IP	The Mapped IP address of the interface.
Netmask	The subnet mask for the subnet on which the interface IP address is located.
Host IP	The Host IP address of the interface.
Configure	Click Edit to open an Interface Configuration dialog box with which you can modify the configuration.

INTERFACE >> TUNNEL >> NEW MAPPED IP

NetScreen-100 help support about logout

System

- Configure
- Admin
- Interface

Network

- Policy
- VPN
- Virtual IP

Lists

- Address
- Service
- Schedule
- Users

Monitor

- Traffic
- Counters
- Alarm
- Log

Copyright © 1998-2001
NetScreen Technologies
Inc.
All rights reserved.

MAPPED IP CONFIGURATION

Interface IP/Netmask 10.30.1.1/255.255.255.0

Mapped IP Address

Netmask

Host IP Address

OK Cancel

Figure 1-40 Interface >> Tunnel >> New Mapped IP

New Mapped IP Configuration

To create a new Mapped IP configuration, click on **New Entry** of the Mapped IP menu and complete the following fields:

Dynamic IP Field	Description
Interface IP / Netmask	<i>(read only)</i> The Interface IP and Netmask addresses.
Mapped IP Address	The Mapped IP address of the interface.
Netmask	The subnet mask for the subnet on which the interface IP address is located.
Host IP Address	The Host IP address of the interface.

INTERFACE >> TUNNEL >> DYNAMIC IP

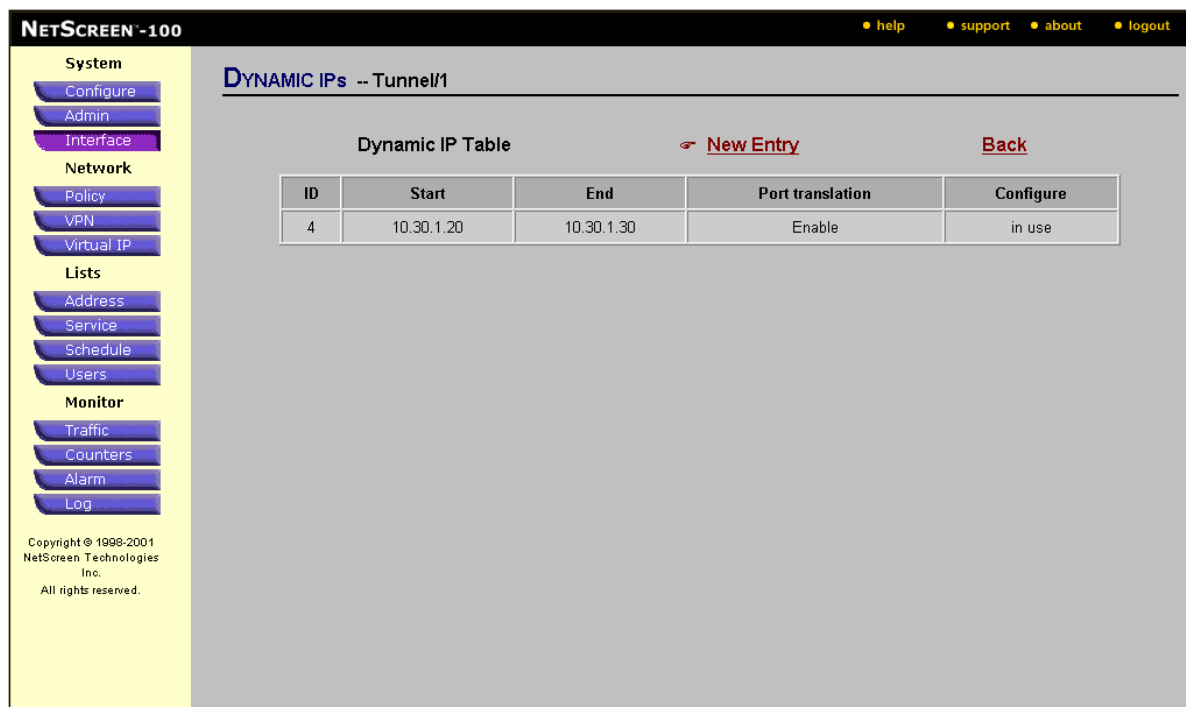


Figure 1-41 Interface >> Tunnel >> Dynamic IP

Dynamic IP Menu

To revise the Dynamic IP fields, click on **Dynamic IP** in the Configuration heading and revise the following fields.

Dynamic IP Field	Description
ID	Dynamic IP pool ID number.
Start	Starting number of Dynamic IP address range.
End	Ending number of Dynamic IP address range.
Port Translation	Whether Port Translation is enabled. When enabled, Port Translation allows multiple hosts to share the same IP address. Assigned port numbers distinguish which session belongs to which host.
Configure	Click Configure to configure Dynamic IP Table or Remove to remove the entry.

INTERFACE >> TUNNEL >> NEW DYNAMIC IP

SCREEN-100 help support about log

System
 Configure
 Admin
 Interface
Network
 Policy
 VPN
 Virtual IP
Lists
 Address
 Service
 Schedule
 Users
Monitor
 Traffic
 Counters
 Alarm
 Log

DYNAMIC IP CONFIGURATION

Interface IP/Netmask 10.30.1.1/255.255.255.0

ID (4-255)

IP Address Range

Start

End

Port Translation ☒ Enable

OK Cancel

Copyright © 1998-2001
 Screen Technologies
 Inc.
 All rights reserved.

Figure 1-42 Interface >> Tunnel >> New Dynamic IP

New Dynamic IP Configuration

To create a new Dynamic IP configuration, click on **New Entry** of the Dynamic IP menu and complete the following fields:

Dynamic IP Field	Description
Interface IP / Netmask	(<i>read only</i>) The Interface IP and Netmask addresses.
ID	ID number; can range up to 255.
IP Address Range	
Start	The starting value of the IP Address range.
End	The ending value of the IP Address range.
Port Translation	Whether Port Translation is enabled. When enabled, Port Translation allows multiple hosts to share the same IP address. Assigned port numbers distinguish which session belongs to which host.

Network

2

This chapter describes the WebUI pages grouped under Network in the menu column. The main sections and their subsections are as follows:

- Policy
 - Incoming
 - Outgoing
 - To DMZ (NetScreen-10 and NetScreen-100, when the DMZ port is enabled)
 - From DMZ (NetScreen-10 and -100, when the DMZ port is enabled)
- VPN
 - Manual Key
 - AutoKey IKE
 - Gateway
 - P1 Proposal
 - P2 Proposal
 - Certificates
- Virtual IP (when the NetScreen device is in NAT mode)
 - Virtual IP 1
 - Virtual IP 2 (NetScreen-10, -100, and -1000)
 - Virtual IP 3 (NetScreen device-100 and -1000)
 - Virtual IP 4 (NetScreen device-100 and -1000)

POLICY >> INCOMING



Figure 2-1 Policy >> Incoming

Incoming Access Policies

All security entries on the NetScreen device are Access Policies. Access Policies are comprised of addresses (source and destination), services, actions, and schedules.

The action of the Access Policy can be a simple firewall rule such as permit or deny, allowing you to determine what traffic passes across it based on IP session details. Access Policies protect the Trusted network from outsider attacks, such as the scanning of Trusted hosts. Access Policies create an environment in which you set up security to monitor and screen traffic attempting to cross your firewall in either direction.

Alternatively, your Access Policies can define connections that must be encrypted, thus forming a Virtual Private Network (VPN). You can define Access Policies that specify what services should be permitted, denied, encrypted, authenticated, logged, counted, or trigger an alarm. When the Access Policies feature is enabled, you can view counters, logs, and alarms in the NetScreen Administration Tools.

Note: Before you can create an Access Policy, the relevant source and destination addresses must already have entries in the address book.

Categorizing Access Policies







In NetScreen, you assign an Access Policy to one of four pages, based on the intended source and destination addresses. Determine which page (tab) you need from the following table:






Traffic	Outgoing Tab	Incoming Tab	To DMZ Tab	From DMZ Tab
Source	Trust	Untrust	Trust Untrust	DMZ
Destination	Untrust	Trust MIP	DMZ	Trust Untrust

Viewing Access Policies

Each Access Policy is assigned a sequential ID number when it's created. The preconfigured default policy is always given the ID number of 0 (zero).

Icons in the Access Policy listing graphically summarize policy configuration information:

Icon	Function	Description
	Permit (Untrust)	All traffic on the untrusted interface is passed.
	Permit (Trust)	All traffic meeting the criteria is passed.
	Deny	All traffic meeting the criteria is denied.
	Tunnel	All traffic is encrypted within a VPN tunnel.
	Encryption disabled	The VPN tunnel Access Policies conflict with each other.
	Authenticate	The user must authenticate himself.

Icon	Function	Description
	Log	All traffic is logged and made available for Syslog, and e-mail, if enabled. Double-clicking the icon takes you to the traffic log information available under the Monitor section.
	Count	The amount of traffic is counted. Double-clicking the icon takes you to the counter information available under the Monitor section.
	Alarm	Indicates that you have set alarm thresholds. Double-clicking the icon takes you to the alarm information available under the Monitor section.
	Traffic	Bandwidth shaping is active.
	Schedule	An Access Policy is only active during the time defined by the schedule.

Moving the cursor over any icon in the Action or Options columns provides specific details and/or a link to more detailed information.

Route Mode

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

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

Interface Settings

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

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

* Optional setting for traffic shaping

- † Selecting **Route** for the Trusted interface defines the mode as Route. Selecting **NAT** defines the mode as NAT.
- ‡ The default port number is 80. Changing this to any number between 1024 and 32,767 is advised for discouraging unauthorized access and modifications to the configuration.

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

POLICY >> INCOMING >> NEW POLICY

NETSCREEN-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1999-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

POLICY CONFIGURATION

Name (optional)

Source Address

Destination Address

Service

NAT ☒ Off
☐ DIP Off ☐ Fix-Port
☐ DIP On

Action

VPN Tunnel

L2TP

Authentication ☐

Logging ☐ Enable Counting ☐ Enable

Alarm Threshold Bytes/Sec Bytes/Min

Schedule

Traffic Shaping ☒ Off
☐ Guaranteed Bandwidth kbps
 Maximum Bandwidth kbps
 Traffic Priority
 DS Codepoint Marking ☐ Enable

OK Cancel

Figure 2-2 Network >> Incoming >> New Policy

Creating a New Access Policy

1. Click the **Incoming** tab.
2. Click **New Policy** at the bottom of the page.
 The Policy Configuration dialog box appears.
3. Specify the information for the Access Policy:

Access Policy Field	Description
Name (optional)	Assign a name that is meaningful to you.

Access Policy Field	Description
Source Address	Choose an address from the drop-down list for the host or network generating the connection. These are addresses that have already defined in the address book.
Destination Address	Choose an address from the drop-down list for the server receiving the connection request.
Service	Choose a service from the drop-down list for the type of connection to be established. Services define the type of traffic. NetScreen has predefined core Internet services or the administrator can define custom services. Services are defined in the List section
Action	Choose from Permit or Deny. The NetScreen device applies the action selected for this Access Policy against traffic that matches the first three criteria: source address, destination address, and service.
VPN Tunnel	If you select Tunnel for the action, then select the appropriate VPN tunnel that matches the source and destination. VPN Tunnels are defined in the Network section under VPN. If the action is not Tunnel, then leave None as the default.
L2TP	Select desired L2TP tunnel from the drop-down menu.
Authentication	Select Authentication to require that the users involved in the action authenticate themselves.
Logging	Select Enable to have the NetScreen device log all connections for this Access Policy.
Counting	Select Enable to have the NetScreen device count the total number of bytes for this Access Policy and record the information historical graphs.
Alarm Threshold	Type in the number of bytes per second, the number of bytes per minute, or both. A value of 0 indicates that the alarm has been disabled. Counting must be enabled to configure Alarm thresholds. Note: You can only enter integer values in the Alarm Threshold fields.

Access Policy Field	Description
Schedule	<p>Select a schedule that has been defined if this Access Policy should be enforced during certain times. Schedules are defined in the Lists section under Schedule. None means the Access Policy is always on.</p> <p>Note: Access Policies appear in green when they are not being enforced. That occurs when the current time is not within the defined schedule.</p>
Traffic Shaping	<p>If this function is enabled, all traffic corresponding to this Access Policy is controlled and shaped according to the specification. The traffic shaping parameters include:</p> <p>Guaranteed Bandwidth: Guaranteed throughput in kilobits per second (kbps). Traffic below this threshold will be passed with highest priority without being subject to any traffic management or shaping mechanism.</p> <p>Maximum Bandwidth: Secured bandwidth available to the type of connection being specified in kilobits per second (kbps). Traffic beyond this threshold will be throttled and dropped.</p>
Traffic Priority	<p>Traffic with higher priority will be passed first, and lower priority traffic is passed only if there is no other higher priority traffic for a certain period of time. There are eight priority levels.</p> <p>Note: It is advised that you do not use rates less than 10 kbps. Rates below this will lead to dropped packets and excessive retries that defeat the purpose of traffic management.</p>
DS Codepoint Marking	<p>DS Codepoint Marking: Differentiated Services (DiffServ) is a system for tagging (or "marking") traffic at a position within a hierarchy of priority. Selecting the Enable check box maps the 8 NetScreen priority levels to the DiffServ system. By default, the highest priority (priority 0) maps to 111 in the DS byte (see RFC 2474) or TOS byte (see RFC 1349) in the IP packet header and the lowest priority (priority 7) maps to 000.</p>

4. To add the Access Policy, click **OK**.

POLICY >> INCOMING >> EDIT

NETSCREEN-100 • help • support • about • logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1999-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

POLICY CONFIGURATION

Name (optional)

Source Address

Destination Address

Service

NAT ☒ Off
☐ ☐ DIP Off ☐ Fix-Port
☐ DIP On

Action

VPN Tunnel

L2TP

Authentication ☐

Logging ☐ Enable Counting ☐ Enable

Alarm Threshold Bytes/Sec Bytes/Min

Schedule

Traffic Shaping ☒ Off
☐ Guaranteed Bandwidth kbps
 Maximum Bandwidth kbps
 Traffic Priority
 DS Codepoint Marking ☐ Enable

OK Cancel

Figure 2-3 Policy >> Incoming >> Edit

Viewing and Changing Access Policies

1. Click the **Incoming** tab, as appropriate.

The DMZ tab appears only if the DMZ has been configured.

2. In the Configure column, click **Edit** for the Access Policy that you want to change.

The Policy Configuration page appears.

3. Specify the information for the access policy.
4. To save changes, click **OK**.

POLICY >> INCOMING >> REMOVE

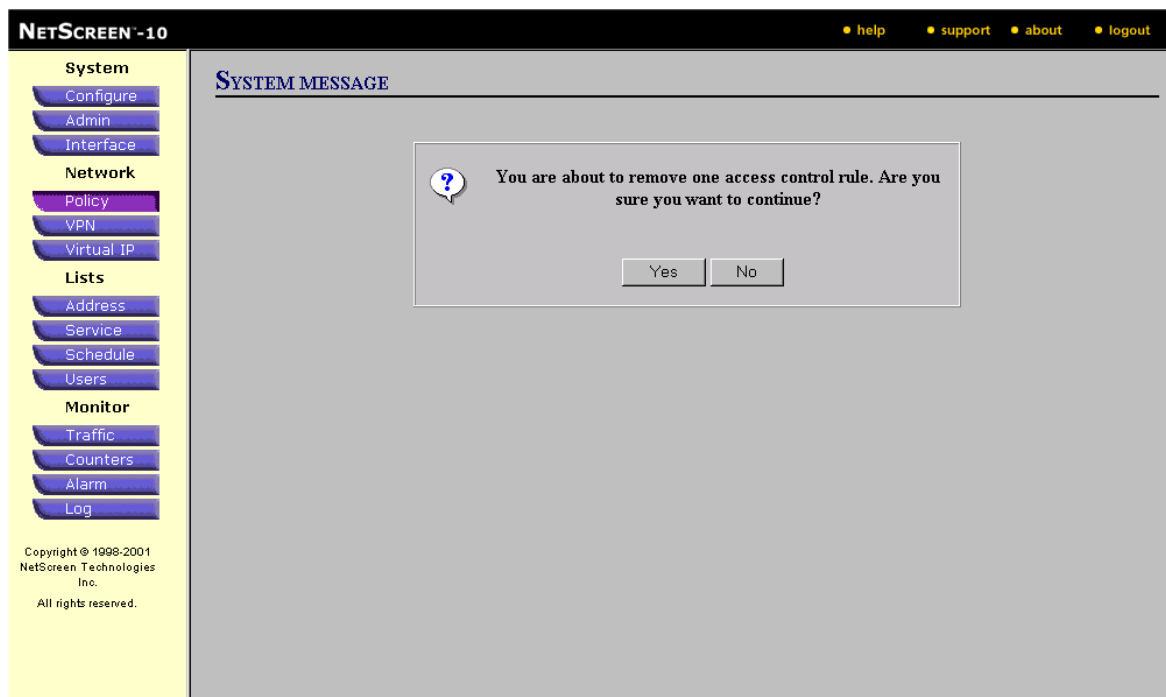


Figure 2-4 Policy >> Incoming >> Remove

Removing an Access Policy

1. Click the **Incoming** tab.
2. In the Configure column, click Remove for the Access Policy that you want to remove.
A system message window prompts for confirmation to proceed with the removal.
3. Click **Yes** to confirm the removal, or **No** to cancel it.

POLICY >> INCOMING >> MOVE

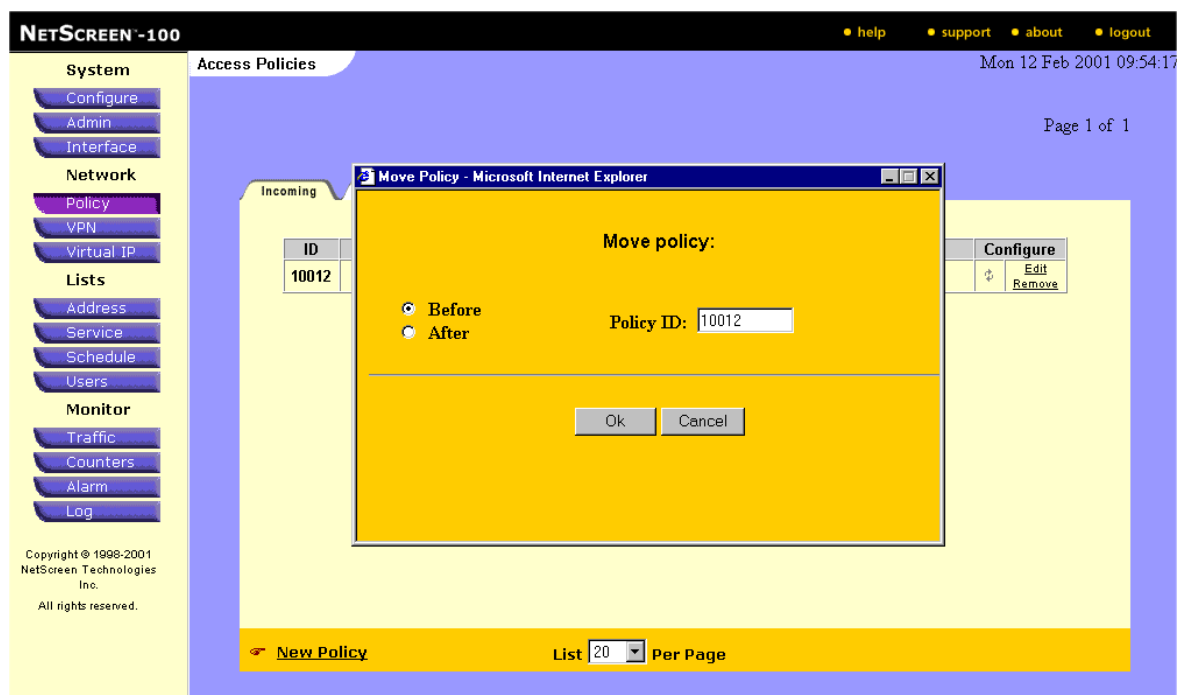


Figure 2-5 Policy >> Incoming >> Move

Reordering Access Policies

All attempted access is checked against Access Policies, beginning with the first Access Policy listed on the Access Policies page and moving through the list. Access Policies should be ordered from specific to general, as action applies to the first matching policy.

To order Access Policies:

1. Click the **Incoming** tab.
2. Click the circular arrows in the Configure column to display the Move Policy Micro dialog box.
3. Change the order of the Access Policy to fit your needs, and click **OK**.
4. Then the page redisplay with the Access Policies in the new order you have selected.

Note: Scheduled Access Policies are highlighted when they are not being enforced at that moment.

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

List <Number> Per Page

The user can list Access Policies per page in batches of 5, 10, 20, 50, 100 or maximum. The default display number per page is 20 per page.

New Policy

Click this to open the Policy Configuration dialog box to create a new Access Policy.

Note: When the NetScreen device is in NAT mode, the New Policy option only appears on the Incoming Access Policies page after you have set up a Virtual IP (VIP).

POLICY >> OUTGOING

NetScreen-100

Access Policies

Mon 12 Feb 2001 09:55:34

Page 1 of 1

Incoming Outgoing To DMZ From DMZ

ID	Source	Destination	Service	NAT	Action	Option	Configure
12	Trusted Interface	Joe Admin	ANY	N/A			Edit Remove
10	Tech Pubs	Outside Any	ANY				Edit Remove
5	Inside Any	All Virtual IPs	HTTP				Edit Remove
13	Inside Any	Dial-Up VPN	ANY				Edit Remove
8	Tech Pubs	LA_LAN	ANY				Edit Remove
11	Libby's	NS-Global	NS Global	N/A			Edit Remove

New Policy

List 20 Per Page

Copyright © 1999-2001
NetScreen Technologies
Inc.
All rights reserved.

Figure 2-6 Policy >> Outgoing

What Access Policies Are

All security entries on the NetScreen device are Access Policies. Access Policies are comprised of addresses (source and destination), services, actions, and schedules.

The action of the Access Policy can be a simple firewall rule such as permit or deny, allowing you to determine what traffic passes across it based on IP session details. Access Policies protect the Trusted network from outsider attacks, such as the scanning of Trusted hosts. Access Policies create an environment in which you set up security to monitor and screen traffic attempting to cross your firewall in either direction.

Alternatively, your Access Policies can define connections that must be encrypted, thus forming a Virtual Private Network (VPN). You can define Access Policies that specify what services should be permitted, denied, encrypted, authenticated, logged, counted, or trigger an alarm. When the Access Policies feature is enabled, you can view counters, logs, and alarms in the NetScreen Administration Tools.

Note: Before you can create an Access Policy, the relevant source and destination addresses must already have entries in the address book.

Categorizing Access Policies







In NetScreen, you assign an Access Policy to one of four pages, based on the intended source and destination addresses. Determine which page (tab) you need from the following table:






Traffic	Outgoing Tab	Incoming Tab	To DMZ Tab	From DMZ Tab
Source	Trust	Untrust	Trust Untrust	DMZ
Destination	Untrust	Trust MIP	DMZ	Trust Untrust

Viewing Access Policies

Each Access Policy is assigned a sequential ID number when it's created. The preconfigured default policy is always given the ID number of 0 (zero).

Icons in the Access Policy listing graphically summarize policy configuration information:

Icon	Function	Description
	Permit (Untrust)	All traffic on the untrusted interface is passed.
	Permit	All traffic meeting the criteria is passed.
	Deny	All traffic meeting the criteria is denied
	Tunnel	All traffic is encrypted within a VPN tunnel.
	Encryption disabled	The VPN tunnel Access Policies conflict with each other.
	Authenticate	The user must authenticate himself.

Icon	Function	Description
	Log	<p>All traffic is logged and made available for Syslog, and e-mail, if enabled.</p> <p>Double-clicking the icon takes you to the traffic log information available under the Monitor section.</p>
	Count	<p>The amount of traffic is counted.</p> <p>Double-clicking the icon takes you to the counter information available under the Monitor section.</p>
	Alarm	<p>Indicates that you have set alarm thresholds.</p> <p>Double-clicking the icon takes you to the alarm information available under the Monitor section.</p>
	Traffic	<p>Bandwidth shaping is active.</p>
	Schedule	<p>An Access Policy is only active during the time defined by the schedule.</p>

Moving the cursor over any icon in the Action or Options columns provides specific details and/or a link to more detailed information.

POLICY >> OUTGOING >> EDIT

The screenshot shows the 'POLICY CONFIGURATION' page for an outgoing policy. The left sidebar contains a navigation menu with categories: System (Configure, Admin, Interface), Network (Policy, VPN, Virtual IP), Lists (Address, Service, Schedule, Users), and Monitor (Traffic, Counters, Alarm, Log). The main area contains the following configuration fields:

- Name (optional):** Text input field.
- Source Address:** Dropdown menu set to 'Inside Any'.
- Destination Address:** Dropdown menu set to 'Outside Any'.
- Service:** Dropdown menu set to 'ANY'.
- NAT:** Radio button selected for 'Off'. A sub-section contains:
 - DIP Off:** Radio button selected, with a 'Fix-Port' checkbox.
 - DIP On:** Radio button unselected, with a dropdown menu set to 'None'.
- Action:** Dropdown menu set to 'Permit'.
- VPN Tunnel:** Dropdown menu set to 'None'.
- L2TP:** Dropdown menu set to 'None'.
- Authentication:** Checkbox unselected.
- Logging:** Checkbox unselected.
- Counting:** Checkbox unselected.
- Alarm Threshold:** Two input fields, both set to '0', with units 'Bytes/Sec' and 'Bytes/Min'.
- Schedule:** Dropdown menu set to 'None'.
- Traffic Shaping:** Radio button selected for 'Off'. A sub-section contains:
 - Guaranteed Bandwidth:** Input field set to '0', unit 'kbps'.
 - Maximum Bandwidth:** Input field set to '0', unit 'kbps'.
 - Traffic Priority:** Dropdown menu set to 'High priority'.
 - DS Codepoint Marking:** Checkbox unselected.

At the bottom right are 'OK' and 'Cancel' buttons. The footer of the sidebar contains copyright information: 'Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.'

Figure 2-7 Policy >> Outgoing >> Edit

Viewing and Changing Access Policies

1. Click the **Outgoing** tab.

The DMZ tab appears only if the DMZ has been configured.

2. In the Configure column, click **Edit** for the Access Policy that you want to change.

The Policy Configuration page appears.

3. Specify the information for the access policy.
4. To save changes, click **OK**.

POLICY >> OUTGOING >> REMOVE

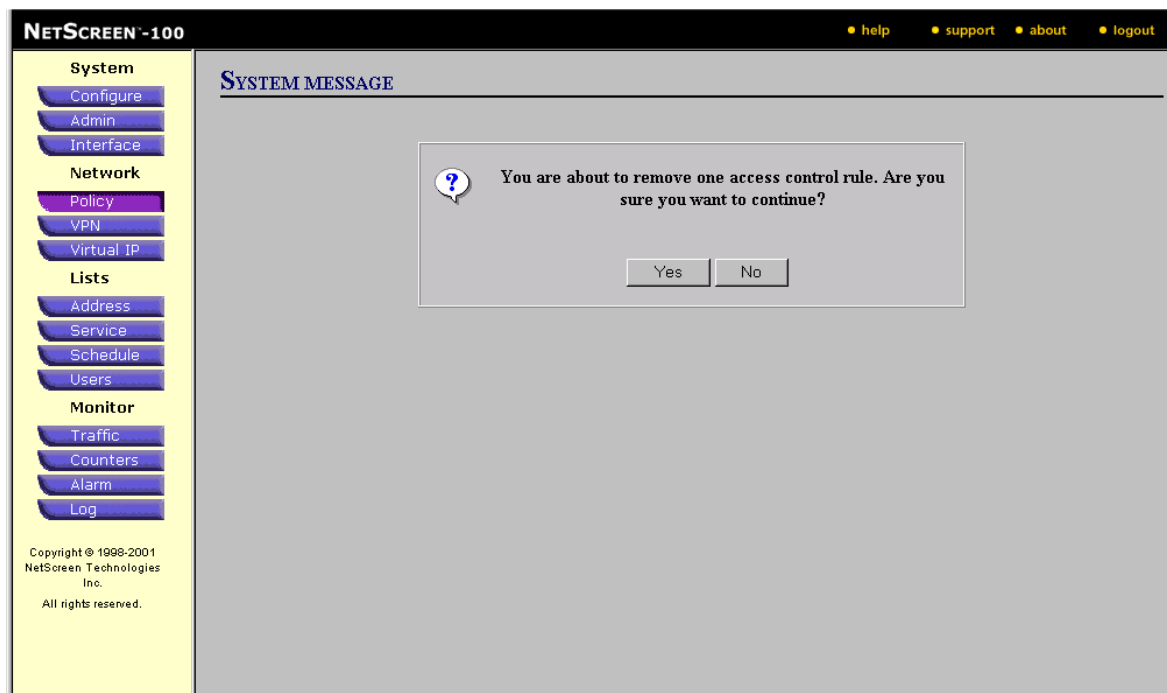


Figure 2-8 Policy >> Outgoing >> Remove

Removing an Access Policy

1. Click the **Outgoing** tab.
2. In the Configure column, click **Remove** for the Access Policy that you want to remove.
A system message window prompts for confirmation to proceed with the removal.
3. Click **Yes** to confirm the removal, or **No** to cancel it.

POLICY >> OUTGOING >> MOVE

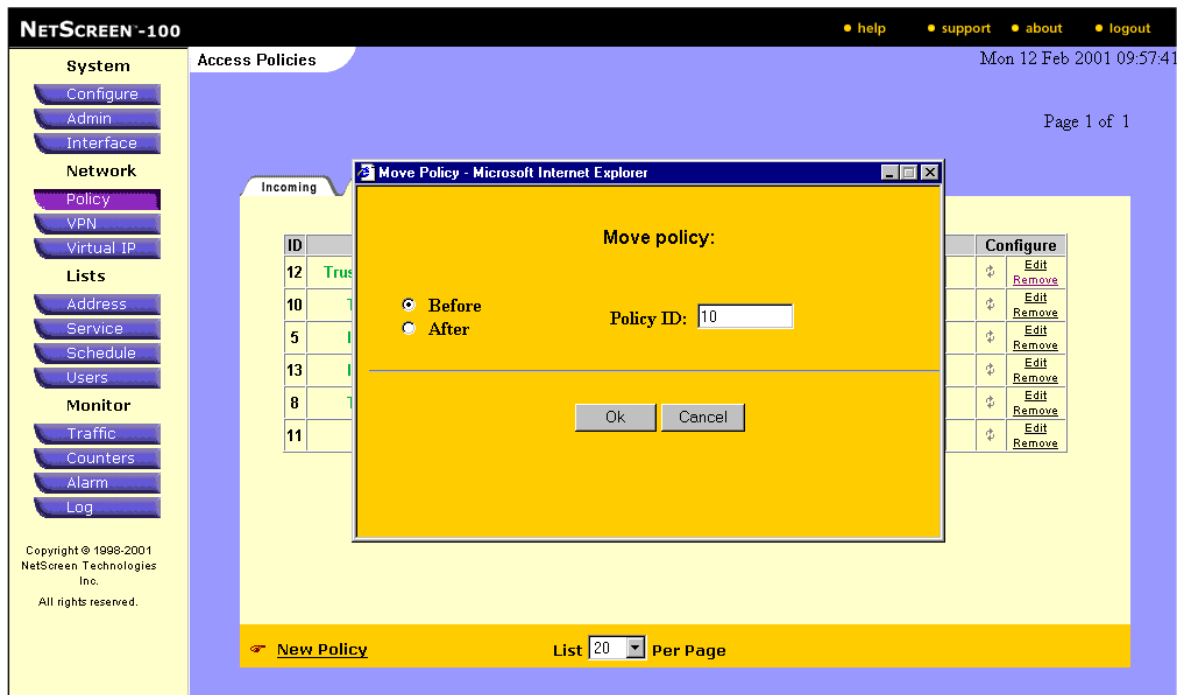


Figure 2-9 Policy >> Outgoing >> Move

Reordering Access Policies

All attempted access is checked against Access Policies, beginning with the first Access Policy listed on the Access Policies page and moving through the list. Access Policies should be ordered from specific to general, as action applies to the first matching policy.

To order Access Policies:

1. Click the **Outgoing** tab.
2. Click the circular arrows in the Configure column to display the Move Policy Micro dialog box.
3. Change the order of the Access Policy to fit your needs, and click **OK**.
4. Then the page redisplay with the Access Policies in the new order you have selected.

Note: Scheduled Access Policies are highlighted when they are not being enforced at that moment.

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

POLICY >> OUTGOING >> NEW POLICY

The screenshot shows the 'POLICY CONFIGURATION' dialog box in the NetScreen-100 web interface. The left sidebar contains a navigation menu with categories: System (Configure, Admin, Interface), Network (Policy, VPN, Virtual IP), Lists (Address, Service, Schedule, Users), and Monitor (Traffic, Counters, Alarm, Log). The main area is titled 'POLICY CONFIGURATION' and contains the following fields and options:

- Name (optional)**: Text input field.
- Source Address**: Dropdown menu with 'Inside Any' selected.
- Destination Address**: Dropdown menu with 'Outside Any' selected.
- Service**: Dropdown menu with 'ANY' selected.
- NAT**: Radio buttons for 'Off' (selected) and 'On'. The 'On' option is disabled.
- DIP**: Radio buttons for 'Off' (selected) and 'On'. The 'On' option is disabled.
- Fix-Port**: Check box, unchecked.
- None**: Dropdown menu, selected.
- Action**: Dropdown menu with 'Permit' selected.
- VPN Tunnel**: Dropdown menu with 'None' selected.
- L2TP**: Dropdown menu with 'None' selected.
- Authentication**: Check box, unchecked.
- Logging**: Check box, unchecked.
- Counting**: Check box, unchecked.
- Alarm Threshold**: Two input fields for 'Bytes/Sec' and 'Bytes/Min', both set to '0'.
- Schedule**: Dropdown menu with 'None' selected.
- Traffic Shaping**: Radio buttons for 'Off' (selected) and 'On'. The 'On' option is disabled.
- Guaranteed Bandwidth**: Input field set to '0' kbps.
- Maximum Bandwidth**: Input field set to '0' kbps.
- Traffic Priority**: Dropdown menu with 'High priority' selected.
- DS Codepoint Marking**: Check box, unchecked.

At the bottom right are 'OK' and 'Cancel' buttons. The footer of the dialog box contains the copyright notice: 'Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.'

Figure 2-10 Policy >> Outgoing >> New Policy

Creating a New Access Policy

1. Click the **Outgoing** tab.
2. Click **New Policy** at the bottom of the page.
The Policy Configuration dialog box appears.
3. Specify the information for the Access Policy:

Configuration Field	Description
Name (optional)	Assign a name that is meaningful to you.

Source Address

Choose an address from the drop-down list for the host or network generating the connection. These are addresses that have already defined in the address book.

Destination Address

Choose an address from the drop-down list for the server receiving the connection request.

Service

Choose a service from the drop-down list for the type of connection to be established. Services define the type of traffic. NetScreen has predefined core Internet services or the administrator can define custom services. Services are defined in the List section

NAT

Choose **NAT Off** to disable the Network Address Translation (NAT) option.

Choose **NAT** to activate the Network Address Translation (NAT) option.

DIP Off: Choose Fix Port to use a specified Port by the Access Policy.

DIP On: Choose DIP On to specify a Dynamic Interface Port pool to use, and click on the pull-down menu to select the specific pool the Access Policy will use.

Action

Choose from Permit, Deny, or Tunnel. The NetScreen device applies the action selected for this Access Policy against traffic that matches the first three criteria: source address, destination address, and service.

VPN Tunnel

If you select Tunnel for the action, then select the appropriate VPN tunnel that matches the source and destination. VPN Tunnels are defined in the Network section under VPN. If the action is not Tunnel then leave None as the default.

Authentication

Select Authentication to require that the users involved in the action authenticate themselves.

Logging

Select Enable to have the NetScreen device log all connections for this Access Policy.

Counting

Select Enable to have the NetScreen device count the total number of bytes for this Access Policy and record the information historical graphs.

Alarm Threshold

Type in the number of bytes per second, the number of bytes per minute, or both. A value of 0 indicates that the alarm has been disabled. Counting must be enabled to configure Alarm thresholds.

Note: You can only enter integer values in the Alarm Threshold fields.

Schedule

Select a schedule that has been defined if this Access Policy should be enforced during certain times. Schedules are defined in the Lists section under Schedule. None means the Access Policy is always on.

Note: Access Policies appear in green when they are not being enforced. That occurs when the current time is not within the defined schedule.

Traffic Shaping

If this function is enabled, all traffic corresponding to this Access Policy is controlled and shaped according to the specification. The traffic shaping parameters include:

Guaranteed Bandwidth: Guaranteed throughput in kilobits per second (kbps). Traffic below this threshold will be passed with highest priority without being subject to any traffic management or shaping mechanism.

Maximum Bandwidth: Secured bandwidth available to the type of connection being specified in kilobits per second (kbps). Traffic beyond this threshold will be throttled and dropped.

Traffic Priority

Traffic with higher priority will be passed first, and lower priority traffic is passed only if there is no other higher priority traffic for a certain period of time. There are eight priority levels.

Note: It is advised that you do not use rates less than 10 kbps. Rates below this will lead to dropped packets and excessive retries that defeat the purpose of traffic management.

4. To add the Access Policy, click **OK**.

POLICY >> To DMZ (NETSCREEN-5 AND 10 ONLY)

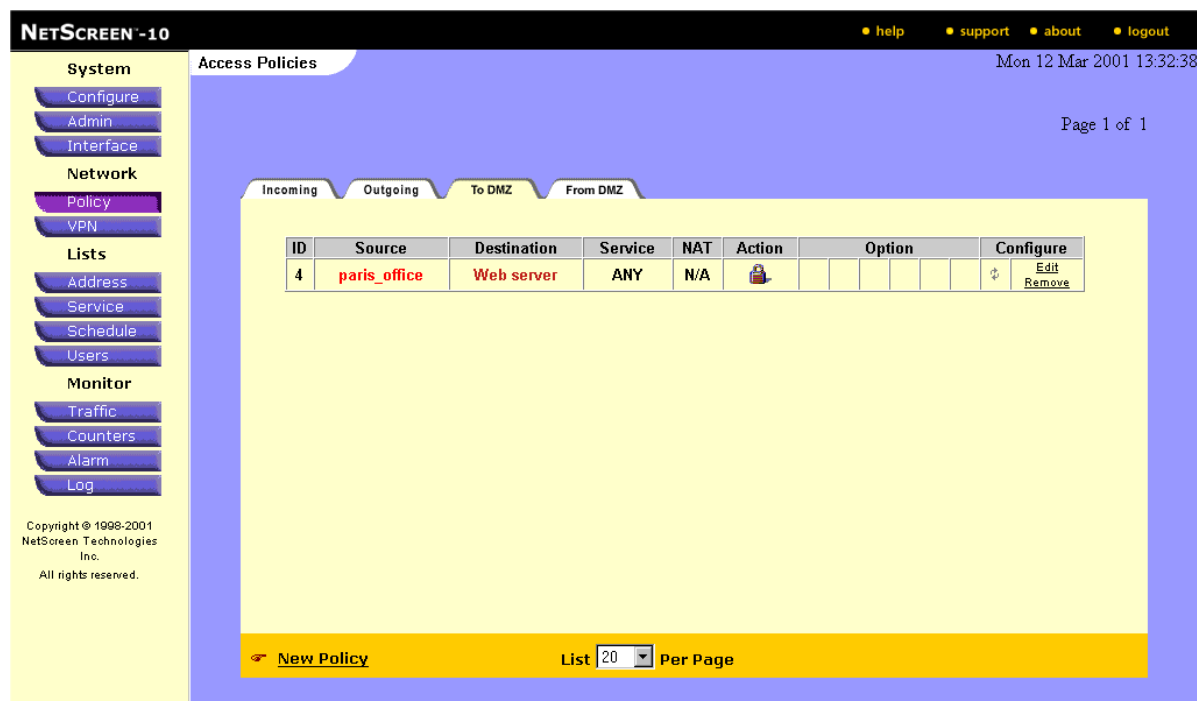


Figure 2-11 Policy >> To DMZ

What Access Policies Are

All security entries on the NetScreen device are Access Policies. Access Policies are comprised of addresses (source and destination), services, actions, and schedules.

The action of the Access Policy can be a simple firewall rule such as permit or deny, allowing you to determine what traffic passes across it based on IP session details. Access Policies protect the Trusted network from outsider attacks, such as the scanning of Trusted hosts. Access Policies create an environment in which you set up security to monitor and screen traffic attempting to cross your firewall in either direction.

Alternatively, your Access Policies can define connections that must be encrypted, thus forming a Virtual Private Network (VPN). You can define Access Policies that specify what services should be permitted, denied, encrypted, authenticated, logged, counted, or trigger an alarm. When the Access Policies feature is enabled, you can view counters, logs, and alarms in the NetScreen Administration Tools.

Note: Before you can create an Access Policy, the relevant source and destination addresses must already have entries in the address book.

Categorizing Access Policies







In NetScreen, you assign an Access Policy to one of four pages, based on the intended source and destination addresses. Determine which page (tab) you need from the following table:






Traffic	Outgoing Tab	Incoming Tab	To DMZ Tab	From DMZ Tab
Source	Trust	Untrust	Trust Untrust	DMZ
Destination	Untrust	Trust MIP	DMZ	Trust Untrust

Viewing Access Policies

Each Access Policy is assigned a sequential ID number when it's created. The preconfigured default policy is always given the ID number of 0 (zero).

Icons in the Access Policy listing graphically summarize policy configuration information:

Icon	Function	Description
	Permit (Untrust)	All traffic on the untrusted interface is passed.
	Permit	All traffic meeting the criteria is passed.
	Deny	All traffic meeting the criteria is denied
	Tunnel	All traffic is encrypted within a VPN tunnel.
	Encryption disabled	The VPN tunnel Access Policies conflict with each other.
	Authenticate	The user must authenticate himself.

Icon	Function	Description
	Log	<p>All traffic is logged and made available for Syslog, and e-mail, if enabled.</p> <p>Double-clicking the icon takes you to the traffic log information available under the Monitor section.</p>
	Count	<p>The amount of traffic is counted.</p> <p>Double-clicking the icon takes you to the counter information available under the Monitor section.</p>
	Alarm	<p>Indicates that you have set alarm thresholds.</p> <p>Double-clicking the icon takes you to the alarm information available under the Monitor section.</p>
	Traffic	<p>Bandwidth shaping is active.</p>
	Schedule	<p>An Access Policy is only active during the time defined by the schedule.</p>

Moving the cursor over any icon in the Action or Options columns provides specific details and/or a link to more detailed information.

POLICY >> To DMZ >> EDIT

The screenshot shows the NetScreen-10 web interface. On the left is a navigation menu with categories: System (Configure, Admin, Interface), Network (Policy, VPN), Lists (Address, Service, Schedule, Users), and Monitor (Traffic, Counters, Alarm, Log). The main area is titled 'POLICY CONFIGURATION'. It contains a form with the following fields: Name (optional) [text box], Source Address [Inside Any dropdown], Destination Address [DMZ Any dropdown], Service [ANY dropdown], Action [Permit dropdown], VPN Tunnel [None dropdown], Authentication [checkbox], Logging [checkbox Enable] and Counting [checkbox Enable], Alarm Threshold [0 Bytes/Sec] and [0 Bytes/Min], Schedule [None dropdown], and Traffic Shaping [radio Off] and [radio On]. The Traffic Shaping sub-form is expanded, showing Guaranteed Bandwidth [0 kbps], Maximum Bandwidth [0 kbps], Traffic Priority [High priority dropdown], and DS Codepoint Marking [checkbox Enable]. At the bottom are OK and Cancel buttons.

Figure 2-12 Policy >> To DMZ >> Edit**Viewing and Changing Access Policies**

1. Click the **To DMZ** tab.
The DMZ tab appears only if the DMZ has been configured.
2. In the Configure column, click **Edit** for the Access Policy that you want to change.
The Policy Configuration page appears.
3. Specify the information for the access policy.
4. To save changes, click **OK**.

POLICY >> To DMZ >> REMOVE

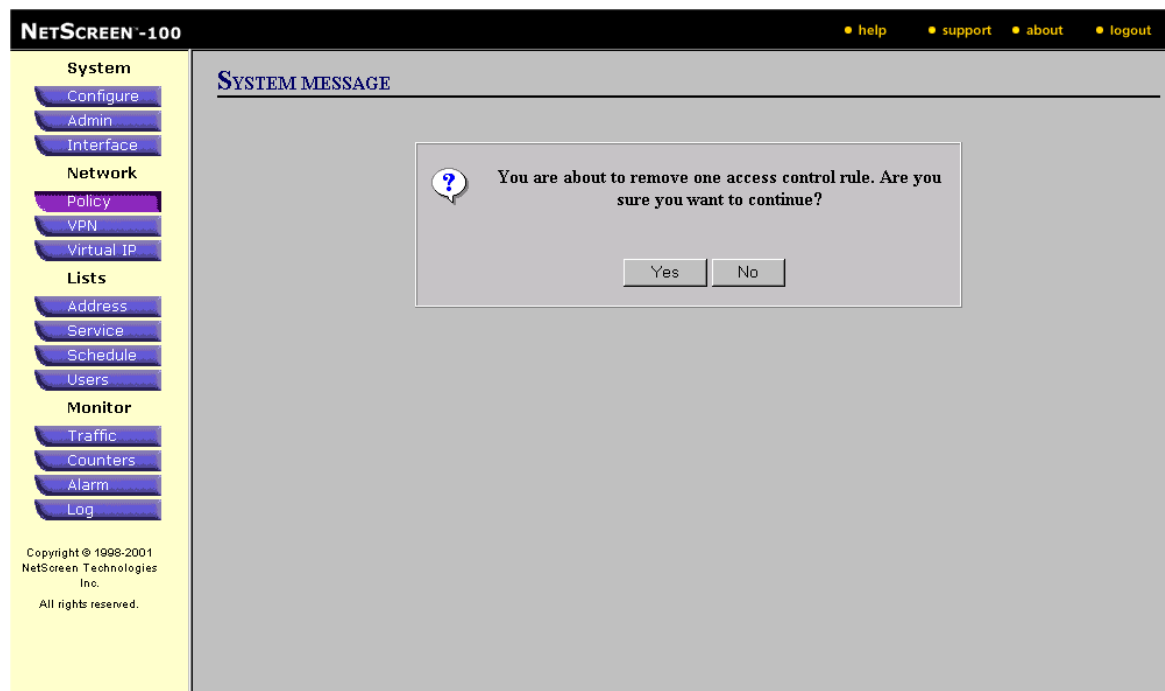


Figure 2-13 Policy >> To DMZ >> Remove

Removing an Access Policy

1. Click the **To DMZ** tab.
2. In the Configure column, click **Remove** for the Access Policy that you want to remove.
A system message window prompts for confirmation to proceed with the removal.
3. Click **Yes** to confirm the removal, or **No** to cancel it.

POLICY >> To DMZ >> MOVE

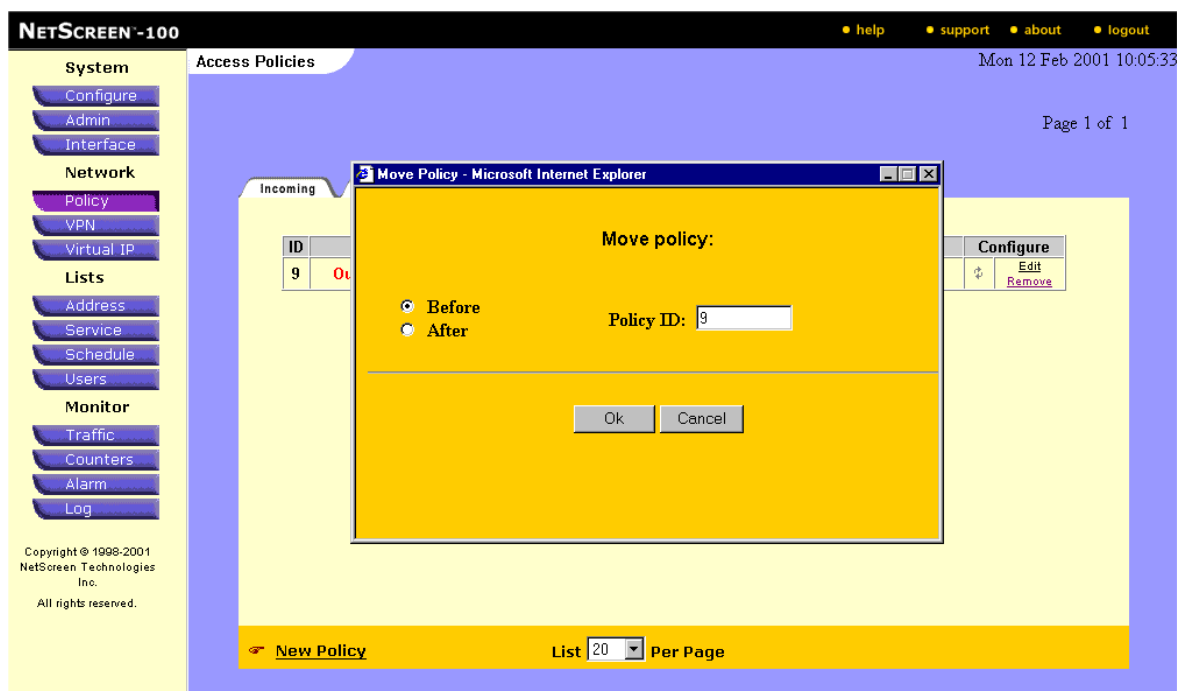


Figure 2-14 Policy >> To DMZ >> Move

Reordering Access Policies

All attempted access is checked against Access Policies, beginning with the first Access Policy listed on the Access Policies page and moving through the list. Access Policies should be ordered from specific to general, as action applies to the first matching policy.

1. Click the circular arrows in the Configure column to display the Move Policy Micro dialog box.
2. Change the order of the Access Policy to fit your needs, and click **OK**.
3. Then the page redisplay with the Access Policies in the new order you have selected.

Note: Scheduled Access Policies are highlighted when they are not being enforced at that moment.

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

POLICY >> To DMZ >> NEW POLICY

NETSCREEN-10 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

POLICY CONFIGURATION

Name (optional)

Source Address

Destination Address

Service

Action

VPN Tunnel

Authentication ☐

Logging ☐ Enable Counting ☐ Enable

Alarm Threshold Bytes/Sec Bytes/Min

Schedule

Traffic Shaping ☒ Off

Guaranteed Bandwidth kbps

Maximum Bandwidth kbps

Traffic Priority

DS Codepoint Marking ☐ Enable

OK Cancel

Figure 2-15 Policy >> To DMZ >> New Policy

Creating a New Access Policy

1. Click the **To DMZ** tab.
2. Click **New Policy** at the bottom of the page.
 The Policy Configuration dialog box appears.
3. Specify the information for the Access Policy:

Configuration Field	Description
Name (optional)	Assign a name that is meaningful to you.
Source Address	Choose an address from the drop-down list for the host or network generating the connection. These are addresses that have already defined in the address book.
Destination Address	Choose an address from the drop-down list for the server receiving the connection request.

Service	<p>Choose a service from the drop-down list for the type of connection to be established. Services define the type of traffic. NetScreen has predefined core Internet services or the administrator can define custom services. Services are defined in the List section</p>
NAT	<p>Choose NAT Off to disable the Network Address Translation (NAT) option.</p> <p>Choose NAT to activate the Network Address Translation (NAT) option.</p> <p>DIP Off: Choose Fix Port to use a specified Port by the Access Policy.</p> <p>DIP On: Choose DIP On to specify a Dynamic Interface Port pool to use, and click on the pull-down menu to select the specific pool the Access Policy will use.</p>
Action	<p>Choose from Permit, Deny, or Tunnel. The NetScreen device applies the action selected for this Access Policy against traffic that matches the first three criteria: source address, destination address, and service.</p>
VPN Tunnel	<p>If you select Tunnel for the action, then select the appropriate VPN tunnel that matches the source and destination. VPN Tunnels are defined in the Network section under VPN. If the action is not Tunnel then leave None as the default.</p>
Authentication	<p>Select Authentication to require that the users involved in the action authenticate themselves.</p>
Logging	<p>Select Enable to have the NetScreen device log all connections for this Access Policy.</p>
Counting	<p>Select Enable to have the NetScreen device count the total number of bytes for this Access Policy and record the information historical graphs.</p>
Alarm Threshold	<p>Type in the number of bytes per second, the number of bytes per minute, or both. A value of 0 indicates that the alarm has been disabled. Counting must be enabled to configure Alarm thresholds.</p> <p>Note: You can only enter integer values in the Alarm Threshold fields.</p>

Schedule

Select a schedule that has been defined if this Access Policy should be enforced during certain times. Schedules are defined in the Lists section under Schedule. None means the Access Policy is always on.

Note: Access Policies appear in green when they are not being enforced. That occurs when the current time is not within the defined schedule.

Traffic Shaping

If this function is enabled, all traffic corresponding to this Access Policy is controlled and shaped according to the specification. The traffic shaping parameters include:

Guaranteed Bandwidth: Guaranteed throughput in kilobits per second (kbps). Traffic below this threshold will be passed with highest priority without being subject to any traffic management or shaping mechanism.

Maximum Bandwidth: Secured bandwidth available to the type of connection being specified in kilobits per second (kbps). Traffic beyond this threshold will be throttled and dropped.

Traffic Priority

Traffic with higher priority will be passed first, and lower priority traffic is passed only if there is no other higher priority traffic for a certain period of time. There are eight priority levels.

Note: It is advised that you do not use rates less than 10 kbps. Rates below this will lead to dropped packets and excessive retries that defeat the purpose of traffic management.

4. To add the Access Policy, click **OK**.

POLICY >> FROM DMZ

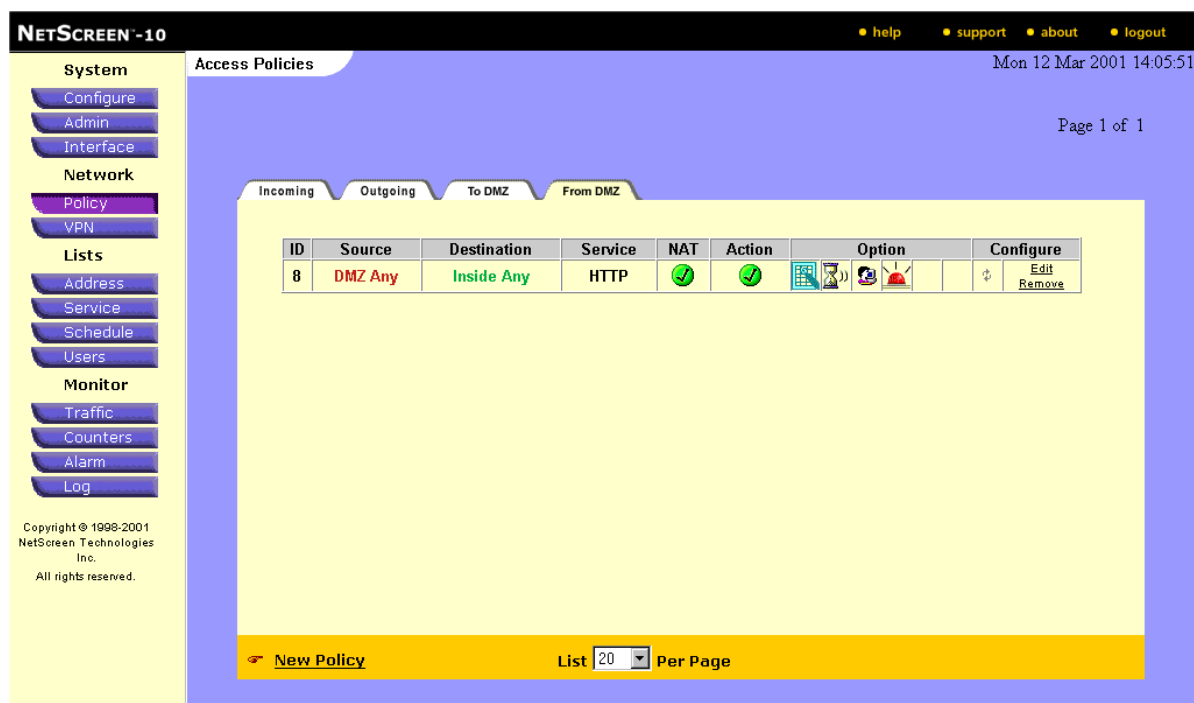


Figure 2-16 Policy >> From DMZ

What Access Policies Are

All security entries on the NetScreen device are Access Policies. Access Policies are comprised of addresses (source and destination), services, actions, and schedules.

The action of the Access Policy can be a simple firewall rule such as permit or deny, allowing you to determine what traffic passes across it based on IP session details. Access Policies protect the Trusted network from outsider attacks, such as the scanning of Trusted hosts. Access Policies create an environment in which you set up security to monitor and screen traffic attempting to cross your firewall in either direction.

Alternatively, your Access Policies can define connections that must be encrypted, thus forming a Virtual Private Network (VPN). You can define Access Policies that specify what services should be permitted, denied, encrypted, authenticated, logged, counted, or trigger an alarm. When the Access Policies feature is enabled, you can view counters, logs, and alarms in the NetScreen Administration Tools.

Note: Before you can create an Access Policy, the relevant source and destination addresses must already have entries in the address book.

Categorizing Access Policies







In NetScreen, you assign an Access Policy to one of four pages, based on the intended source and destination addresses. Determine which page (tab) you need from the following table:






Traffic	Outgoing Tab	Incoming Tab	To DMZ Tab	From DMZ Tab
Source	Trust	Untrust	Trust Untrust	DMZ
Destination	Untrust	Trust MIP	DMZ	Trust Untrust

Viewing Access Policies

Each Access Policy is assigned a sequential ID number when it's created. The preconfigured default policy is always given the ID number of 0 (zero).

Icons in the Access Policy listing graphically summarize policy configuration information:

Icon	Function	Description
	Permit (Untrust)	All traffic on the untrusted interface is passed.
	Permit	All traffic meeting the criteria is passed.
	Deny	All traffic meeting the criteria is denied
	Tunnel	All traffic is encrypted within a VPN tunnel.
	Encryption disabled	The VPN tunnel Access Policies conflict with each other.
	Authenticate	The user must authenticate himself.

Icon	Function	Description
	Log	<p>All traffic is logged and made available for Syslog, and e-mail, if enabled.</p> <p>Double-clicking the icon takes you to the traffic log information available under the Monitor section.</p>
	Count	<p>The amount of traffic is counted.</p> <p>Double-clicking the icon takes you to the counter information available under the Monitor section.</p>
	Alarm	<p>Indicates that you have set alarm thresholds.</p> <p>Double-clicking the icon takes you to the alarm information available under the Monitor section.</p>
	Traffic	<p>Bandwidth shaping is active.</p>
	Schedule	<p>An Access Policy is only active during the time defined by the schedule.</p>

Moving the cursor over any icon in the Action or Options columns provides specific details and/or a link to more detailed information.

POLICY >> FROM DMZ >> EDIT

NETSCREEN-10 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

POLICY CONFIGURATION

Name (optional) New Site Test

Source Address DMZ Any

Destination Address Inside Any

Service HTTP

Action Permit

VPN Tunnel None

Authentication ☒

Logging ☒ Enable Counting ☒ Enable

Alarm Threshold 236 Bytes/Sec 55 Bytes/Min

Schedule None

Traffic Shaping ☒ Off

☐ On

Guaranteed Bandwidth 0 kbps

Maximum Bandwidth 0 kbps

Traffic Priority Low priority

DS Codepoint Marking ☐ Enable

OK Cancel

Figure 2-17 Policy >> From DMZ >> Edit

Viewing and Changing Access Policies

1. Click the **From DMZ** tab.

The DMZ tab appears only if the DMZ has been configured.

2. In the Configure column, click **Edit** for the Access Policy that you want to change.

The Policy Configuration page appears.

3. Specify the information for the access policy.
4. To save changes, click **OK**.

POLICY >> FROM DMZ >> REMOVE POLICY



Figure 2-18 Policy >> From DMZ >> Remove Policy

Removing an Access Policy

1. Click the **From DMZ** tab.
2. In the Configure column, click **Remove** for the Access Policy that you want to remove.
A system message window prompts for confirmation to proceed with the removal.
3. Click **Yes** to confirm the removal, or **No** to cancel it.

POLICY >> FROM DMZ >> MOVE

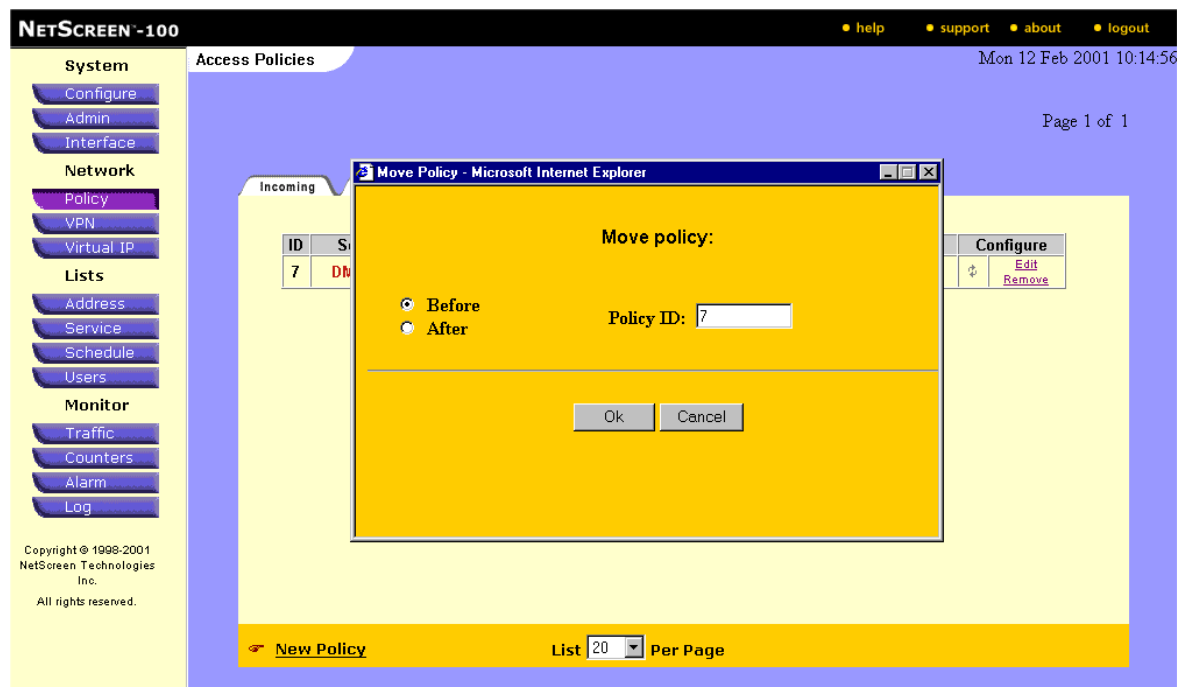


Figure 2-19 Policy >> From DMZ >> Move

Reordering Access Policies

All attempted access is checked against Access Policies, beginning with the first Access Policy listed on the Access Policies page and moving through the list. Access Policies should be ordered from specific to general, as action applies to the first matching policy.

1. Click the circular arrows in the Configure column to display the Move Policy Micro dialog box.
2. Change the order of the Access Policy to fit your needs, and click **OK**.
3. Then the page redisplay with the Access Policies in the new order you have selected.

Note: Scheduled Access Policies are highlighted when they are not being enforced at that moment.

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

POLICY >> FROM DMZ >> NEW POLICY

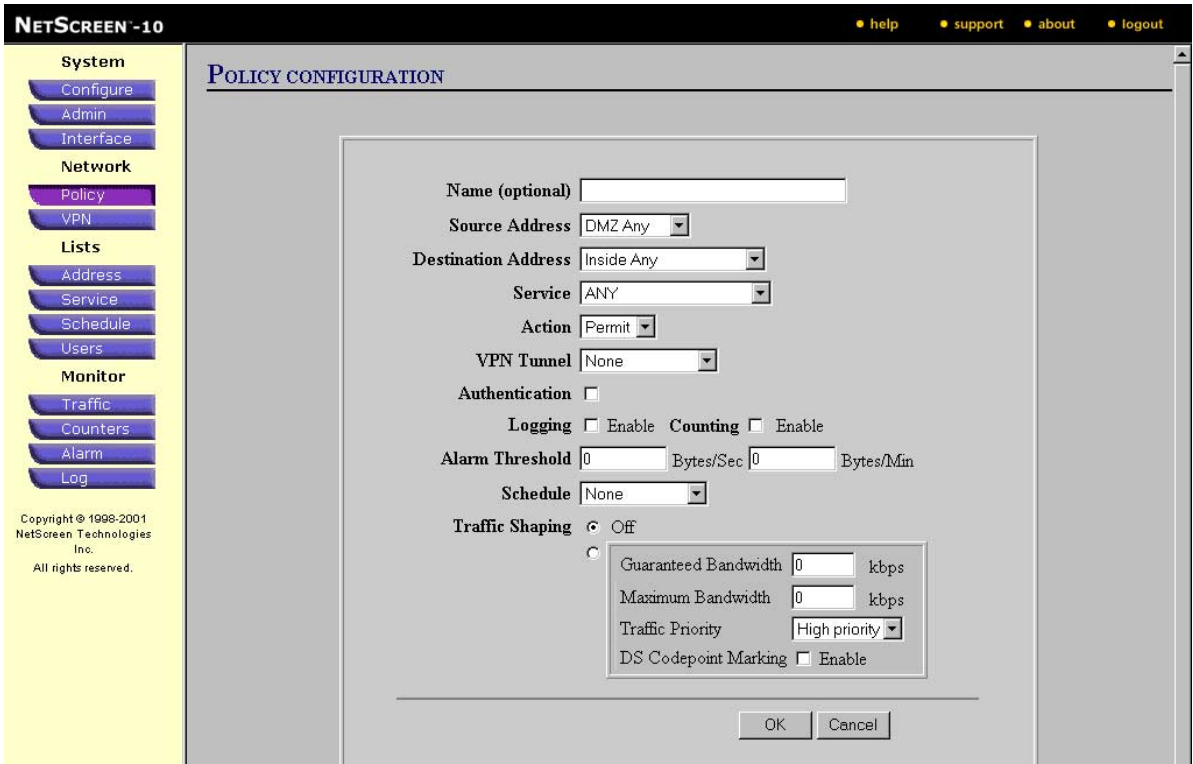


Figure 2-20 Policy >> From DMZ >> New Policy

Creating a New Access Policy

1. Click the **From DMZ** tab.
2. Click **New Policy** at the bottom of the page.
The Policy Configuration dialog box appears.
3. Specify the information for the Access Policy

Policy Field	Description
Name (optional)	Assign a name that is meaningful to you.
Source Address	Choose an address from the drop-down list for the host or network generating the connection. These are addresses that have already defined in the address book.
Destination Address	Choose an address from the drop-down list for the server receiving the connection request.

Policy Field	Description
Service	<p>Choose a service from the drop-down list for the type of connection to be established. Services define the type of traffic. NetScreen has predefined core Internet services or the administrator can define custom services. Services are defined in the List section</p>
NAT	<p>Choose NAT Off to disable the Network Address Translation (NAT) option</p> <p>Choose NAT to activate the Network Address Translation (NAT) option.</p> <p>DIP Off: Choose Fix Port to use a specified Port by the Access Policy.</p> <p>DIP On: Choose DIP On to specify a Dynamic Interface Port pool to use, and click on the pull-down menu to select the specific pool the Access Policy will use.</p>
Action	<p>Choose from Permit, Deny, or Tunnel. The NetScreen device applies the action selected for this Access Policy against traffic that matches the first three criteria: source address, destination address, and service.</p>
VPN Tunnel	<p>If you select Tunnel for the action, then select the appropriate VPN tunnel that matches the source and destination. VPN Tunnels are defined in the Network section under VPN. If the action is not Tunnel then leave None as the default.</p>
Authentication	<p>Select Authentication to require that the users involved in the action authenticate themselves.</p>
Logging	<p>Select Enable to have the NetScreen device log all connections for this Access Policy.</p>
Counting	<p>Select Enable to have the NetScreen device count the total number of bytes for this Access Policy and record the information historical graphs.</p>

Policy Field	Description
Alarm Threshold	<p>Type in the number of bytes per second, the number of bytes per minute, or both. A value of 0 indicates that the alarm has been disabled. Counting must be enabled to configure Alarm thresholds.</p> <p>Note: You can only enter integer values in the Alarm Threshold fields.</p>
Schedule	<p>Select a schedule that has been defined if this Access Policy should be enforced during certain times. Schedules are defined in the Lists section under Schedule. None means the Access Policy is always on.</p> <p>Note: Access Policies appear in green when they are not being enforced. That occurs when the current time is not within the defined schedule.</p>
Traffic Shaping	<p>If this function is enabled, all traffic corresponding to this Access Policy is controlled and shaped according to the specification. The traffic shaping parameters include:</p> <p>Guaranteed Bandwidth: Guaranteed throughput in kilobits per second (kbps). Traffic below this threshold will be passed with highest priority without being subject to any traffic management or shaping mechanism.</p> <p>Maximum Bandwidth: Secured bandwidth available to the type of connection being specified in kilobits per second (kbps). Traffic beyond this threshold will be throttled and dropped.</p>
Traffic Priority	<p>Traffic with higher priority will be passed first, and lower priority traffic is passed only if there is no other higher priority traffic for a certain period of time. There are eight priority levels.</p> <p>Note: It is advised that you do not use rates less than 10 kbps. Rates below this will lead to dropped packets and excessive retries that defeat the purpose of traffic management.</p>

4. To add the Access Policy, click **OK**.

VPN >> MANUAL KEY

NETSCREEN-100

• help • support • about • logout

Mon 12 Feb 2001 10:16:08

Page 1 of 1

Manual Key AutoKey IKE Gateway P1 Proposal P2 Proposal Certificates L2TP IPPool

Name	Gateway	Local SPI	Remote SPI	Monitor	Configure
PaulTest	2.2.2.1	2000	2001	Off	Edit Remove
Boston to Washington	3.3.3.0	3001	3002	On	Edit Remove
Tahoe to San Jose	3.3.3.1	22001	22002	Off	Edit Remove
Boston-to-Washington	2.2.2.1	20001	20002	Off	Edit Remove
Hula girl	223.34.45.56	3663	6336	Off	Edit Remove
LA_Chicago	172.1.1.1	3020	3030	Off	Edit
Admin Tunnel	172.16.10.154	4567	5555	On	Edit
NS- Global	172.16.10.61	5555	4444	On	Edit

Copyright © 1998-2001
NetScreen Technologies
Inc.
All rights reserved.

[New Manual Key Entry](#) List Per Page

Figure 2-21 Network >> VPN >> Manual Key

Manual Key VPN Tunnel

The table on this page lists the Manual Key VPN tunnels that have already been configured. Each entry displays the following information:

Manual Key Fields	Description
Name	This is the name that was assigned to the VPN tunnel when it was configured.
Gateway	The IP address of: the end of the VPN tunnel; or the remote gateway of the VPN tunnel; or the gateway of the remote end of the VPN tunnel.

Manual Key Fields	Description
Local SPI and Remote SPI	A security index number that uniquely distinguishes a particular encrypted tunnel from the others being used at the same time. The Local Security Index serves as the other end's Remote Security Index and vice versa. If you enter "Value_A Value_B", the other end of the tunnel must switch the order of the two components, as in "Value_B Value_A".
Monitor	The value On or Off indicates whether VPN monitoring has been enabled or not.
Configure	In this column, you can choose Edit and Remove . Remove is only available if the entry is not already in use in an access policy.

To create a manual key, click **New VPN Entry**, located at the bottom of the page, to display the Manual Key VPN Configuration page.

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VPN >> MANUAL KEY >> NEW MANUAL KEY ENTRY

NETSCREEN-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

MANUAL KEY CONFIGURATION

VPN Tunnel Name:

Gateway IP:

Security Index: (Local) (Remote)

☒ **ESP-CBC**

Encryption Algorithm:

☒ **HEX Key**

☐ **Generate Key by Password**

Authentication Algorithm:

☒ **HEX Key (16/24 Bytes)**

☐ **Generate Key by Password**

☐ **AH**

Hash Algorithm:

☒ **HEX Key (16/24 Bytes)**

☐ **Generate Key by Password**

VPN Monitor: ☐ Enable

Tunnel to Trusted Interface: ☐ Enable

OK Cancel

Figure 2-22 Network >> VPN >> Manual Key Configuration

Manual Key Configuration

In the NetScreen-100, the menu used for defining a manual key VPN tunnel is located on this interface page.

To create a manual key:

1. Click the **VPN** tab on the left side of the NetScreen Administration Tools page.
The VPN Configuration page appears.
2. Click the **Manual Key** tab at the top of the page.
3. Click **New VPN Entry**, located at the bottom of the page, to display the Manual Key VPN Configuration page.
4. Define the following fields:

VPN Entry Fields	Description
VPN Tunnel Name	The name identifying this VPN tunnel definition. Choose a descriptive name to help you identify the VPN tunnel. The name must be unique and is limited to 20 characters.

VPN Entry Fields	Description
Gateway IP	The IP address of the remote LAN NetScreen's Untrust interface.
Security Index (Local and Remote)	A security index number that uniquely distinguishes a particular encrypted tunnel from the others being used at the same time. Only a HEX value greater than 3000 is accepted. The Local Security Index serves as the other end's Remote Security Index and vice versa. If you enter "Value_A Value_B", the other end of the tunnel must switch the order of the two components, as in "Value_B Value_A".

5. Select either ESP-CBC or AH.

Encapsulating Security Payload (ESP) provides both encryption and authentication of an IP packet. Authentication Header (AH) provides authentication only.

ESP-CBC

ESP-CBC Entry Field	Description
Encryption Algorithm	An algorithm used for encryption. You can select either NULL, DES-CBC or 3DES-CBC.
Hex Key	An encryption key for the algorithm specified. Each field of the key is 8 bytes long represented in HEX. (The key is 16 characters long with two characters used to describe one byte in HEX.) For DES, only the left-most value needs to be defined. For 3DES, all three values must be defined.
Generate Key by Password	The NetScreen-100 provides assistance in creating the hex key by allowing a password to define the generation of the hex key. Note: The use of the password feature is a convenience and might lead to similar keys.
Authentication Algorithm	An algorithm used for authenticating the content of the encrypted IP packets. You can leave this field as NULL to omit authentication, or select either MD5 or SHA-1 from the drop-down list.

ESP-CBC Entry Field	Description
Hex Key	<p>A hexadecimal value used to perform the authentication hash algorithm. For MD5, the key must be 16 bytes long. For SHA-1, the key must be 20 bytes long. (Two hexadecimal characters equal one byte.) In the fields to the right of the HEX Key radio button, enter a key with the appropriate length.</p>
Generate Key by Password	<p>You can direct the NetScreen-100 to generate a key for your selected hash algorithm based on a password that you enter. If you wish to use this option, select the Generate Key by Password radio button and enter a password in the corresponding field.</p> <p>Note: The use of the password feature is a convenience and might lead to similar keys.</p>

AH

AH Entry Field	Description
AH	<p>The authentication header (AH) is used to verify a packet's authenticity. The header contains a cryptographic checksum calculated via a hash-based message authentication code (HMAC) coupled with MD5 or SHA-1. You can select either of these algorithms from the drop-down box.</p>
Hash Algorithm	<p>The hash algorithm is selectable. You can use either MD5 or SHA1. MD5 requires a 16-byte key; SHA1 requires a 20-byte key. In the fields to the right of the HEX Key radio button, enter a key with the appropriate length.</p>
Generate Key by Password	<p>You can direct the NetScreen-100 to generate a key for your selected hash algorithm based on a password that you enter. If you wish to use this option, select the Generate Key by Password radio button and enter a password in the corresponding field.</p> <p>Note: The use of the password feature is a convenience and might lead to similar keys.</p>

- To enable the VPN monitor, select the check box. This enables the NetScreen device to set SNMP traps to monitor the condition of the VPN tunnel.

7. To enable the Tunnel Interface, select the check box.
8. Click **OK** to save the new entry.

Note: *The number of VPN entries displayed on the page can be refined to 5, 10, 20 or 30 entries.*

Apply and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VPN >> MANUAL KEY >> CREATE VPN ENTRY

The screenshot shows the NetScreen-100 web interface for Manual Key Configuration. The left sidebar contains a navigation menu with categories: System (Configure, Admin, Interface), Network (Policy, VPN, Virtual IP), Lists (Address, Service, Schedule, Users), and Monitor (Traffic, Counters, Alarm, Log). The main content area is titled 'MANUAL KEY CONFIGURATION' and contains the following fields and options:

- VPN Tunnel Name:** Text input field.
- Gateway IP:** Text input field (0.0.0.0).
- Security Index:** Two text input fields for (Local) and (Remote), both set to 0.
- Encryption Algorithm:** Radio button selected for **ESP-CBC**.
 - Encryption Algorithm:** Dropdown menu set to DES-CBC.
 - Key Generation:** Radio button selected for **HEX Key** (with two text input fields) over **Generate Key by Password** (with one text input field).
- Authentication Algorithm:** Radio button selected for **HEX Key (16/24 Bytes)** (with two text input fields) over **Generate Key by Password** (with one text input field).
 - Authentication Algorithm:** Dropdown menu set to NULL.
- Hash Algorithm:** Radio button selected for **AH**.
 - Hash Algorithm:** Dropdown menu set to MD5.
 - Key Generation:** Radio button selected for **HEX Key (16/24 Bytes)** (with two text input fields) over **Generate Key by Password** (with one text input field).
- VPN Monitor:** Checkboxes for **Enable** (unchecked).
- Tunnel to Trusted Interface:** Checkboxes for **Enable** (unchecked).

At the bottom right are **OK** and **Cancel** buttons. The footer of the interface includes copyright information: Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.

Figure 2-23 Network >> VPN >> Manual Key Configuration

Create VPN Entry

In the NetScreen-100, both the Phase 1 and Phase 2 portions of defining a manual key VPN tunnel are located on this interface page.

To create a manual key:

To create a manual key:

1. Click the **VPN tab** on the left side of the NetScreen Administration Tools page.
The VPN Configuration page appears.
2. Click the Manual Key tab at the top of the page.
3. Click **New VPN Entry**, located at the bottom of the page, to display the Manual Key VPN Configuration page.

4. Define the following fields:

VPN Entry Fields	Description
VPN Tunnel Name	The name identifying this VPN tunnel definition. Choose a descriptive name to help you identify the VPN tunnel. The name must be unique and is limited to 20 characters.
Gateway IP	The IP address of the remote LAN NetScreen's Untrust interface.
Security Index (Local and Remote)	A security index number that uniquely distinguishes a particular encrypted tunnel from the others being used at the same time. Only a HEX value greater than 3000 is accepted. The Local Security Index serves as the other end's Remote Security Index and vice versa. If you enter "Value_A Value_B", the other end of the tunnel must switch the order of the two components, as in "Value_B Value_A".

5. Select either ESP-CBC or AH.

Encapsulating Security Payload (ESP) provides both encryption and authentication of an IP packet. Authentication Header (AH) provides authentication only.

ESP-CBC

ESP-CBC Entry Field	Description
Encryption Algorithm	An algorithm used for encryption. You can select either NULL, DES-CBC, 3DES-CBC or 40-bit DES-CBC.
Hex Key	An encryption key for the algorithm specified. Each field of the key is 8 bytes long represented in HEX. (The key is 16 characters long with two characters used to describe one byte in HEX.) For DES, only the left-most value needs to be defined. For 3DES, all three values must be defined.
Generate Key by Password	The NetScreen-100 provides assistance in creating the hex key by allowing a password to define the generation of the hex key. Note: The use of the password feature is a convenience and might lead to similar keys.

ESP-CBC Entry Field	Description
Authentication Algorithm	<p>An algorithm used for authenticating the content of the encrypted IP packets. You can leave this field as NULL to omit authentication, or select either MD5 or SHA-1 from the drop-down list.</p>
Hex Key	<p>A hexadecimal value used to perform the authentication hash algorithm. For MD5, the key must be 16 bytes long. For SHA-1, the key must be 20 bytes long. (Two hexadecimal characters equal one byte.) In the fields to the right of the HEX Key radio button, enter a key with the appropriate length.</p>
Generate Key by Password	<p>You can direct the NetScreen-100 to generate a key for your selected hash algorithm based on a password that you enter. If you wish to use this option, select the Generate Key by Password radio button and enter a password in the corresponding field.</p> <p>Note: The use of the password feature is a convenience and might lead to similar keys.</p>

AH

AH Entry Field	Description
AH	The authentication header (AH) is used to verify a packet's authenticity. The header contains a cryptographic checksum calculated via a hash-based message authentication code (HMAC) coupled with MD5 or SHA-1. You can select either of these algorithms from the drop-down box.
Hash Algorithm	The hash algorithm is selectable. You can use either MD5 or SHA1. MD5 requires a 16-byte key; SHA1 requires a 20-byte key. In the fields to the right of the HEX Key radio button, enter a key with the appropriate length.
Generate Key by Password	<p>You can direct the NetScreen-100 to generate a key for your selected hash algorithm based on a password that you enter. If you wish to use this option, select the Generate Key by Password radio button and enter a password in the corresponding field.</p> <p>Note: The use of the password feature is a convenience and might lead to similar keys.</p>

6. To enable the VPN monitor, select the check box. This enables the NetScreen device to set SNMP traps to monitor the condition of the VPN tunnel.
7. To enable the Tunnel to Trusted Interface, select the check box.
8. Click **OK** to save the new entry.

Note: The number of VPN entries displayed on the page can be refined to 5, 10, 20 or 30 entries.

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VPN >> AUTOKEY IKE

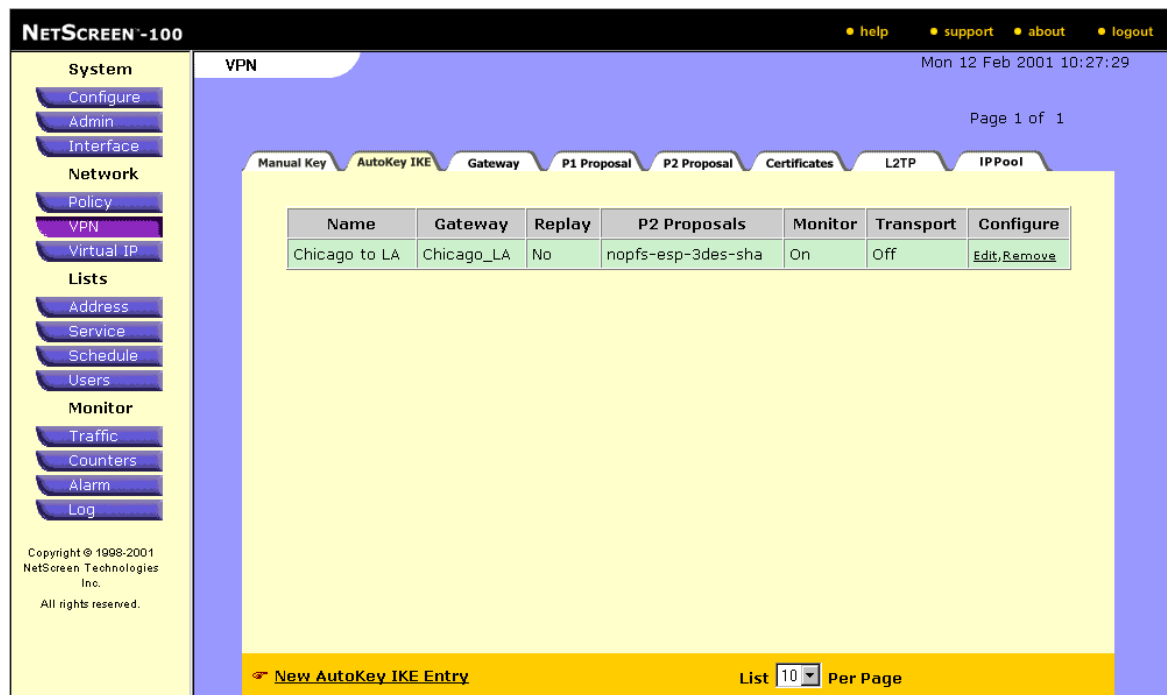


Figure 2-24 VPN >> Autokey IKE

Viewing an Autokey IKE

Phase 2 proposals describe how the data passing through the tunnel associated with a specific remote gateway is encrypted and authenticated. A Phase 2 proposal applies to both LAN-to-LAN and Dialup-to-LAN VPN communication.

AutoKey Field	Description
Name	The name that identifies this VPN tunnel definition
Gateway	The name of the remote gateway tunnel
Replay	Requires that each IKE negotiation have a sequence number.

AutoKey Field	Description
P2 Proposals	<p>Select a proposal for authentication (AH), or for encryption (and authentication) (ESP). For convenience, the NetScreen-100 comes with 8 predefined proposals for ESP. (You must create your own Phase 2 proposals for AH.) Each predefined SA features either "nopfs" or "g2" for key generation, DES or 3DES for encryption, and MD5 or SHA-1 for authentication.</p> <p>nopfs - No Perfect Forwarding Secrecy (PFS). The key used in Phase 2 is derived from that used in Phase 1. PFS generates each new key independently from its predecessor, which increases security but also increases processing overhead.</p> <p>g2 - Diffie-Hellman Group 2. In Phase 2, the participants renegotiate a new key using PFS.</p> <p>des - Data Encryption Standard, a cryptographic block algorithm with a 56-bit key</p> <p>3des - A more powerful version of DES in which the original DES algorithm is applied in three rounds, using a 168-bit key</p> <p>MD5 - Message Digest (version) 5, an algorithm that produces a 128-bit message digest (or hash) from a message of arbitrary length. The resulting hash is used, like a "fingerprint" of the input, to verify authenticity.</p> <p>sha-1 - Secure Hash Algorithm-1, an algorithm that produces a 160-bit hash from a message of arbitrary length. (It is generally regarded as more secure than MD5 because of the larger hashes it produces.)</p>
VPN Monitor	Enables the NetScreen device to set SNMP traps to monitor the condition of the VPN tunnel.

Click **OK** to save your settings.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VPN >> NEW AUTOKEY IKE ENTRY

NETSCREEN-100 help support about logout

System

- Configure
- Admin
- Interface

Network

- Policy
- VPN
- Virtual IP

Lists

- Address
- Service
- Schedule
- Users

Monitor

- Traffic
- Counters
- Alarm
- Log

Copyright © 1999-2001
NetScreen Technologies
Inc.
All rights reserved.

AUTOKEY IKE CONFIGURATION

Name

Enable Replay Protection ☐ Enable

Remote Gateway Tunnel Name [List Gateways](#)

Phase 2 Proposal

[List Phase 2 Proposals](#)

VPN Monitor ☐ Enable

Transport Mode ☐ Enable (For L2TP-over-IPSec only)

OK Cancel

Figure 2-25 VPN >> New AutoKey IKE Entry

Autokey IKE VPN Configuration

Here, you'll associate a remote gateway tunnel name with a Phase 2 Proposal describing how the data passing through the tunnel is to be encrypted. This applies whether you're setting up for LAN-to-LAN or Dialup-to-LAN communication.

To create an Autokey IKE VPN:

1. Define the following fields:

Autokey IKE VPN Fields	Description
Name	The name to identify this VPN tunnel definition. Choose a descriptive name to help you identify the VPN tunnel. The name must be unique and is limited to 20 characters.

Autokey IKE VPN Fields	Description
Enable Replay Protection	Requires that each IKE negotiation have a sequence number.
Remote Gateway Tunnel Name	From the drop-down menu, select the name of the remote gateway tunnel.
Phase 2 Proposal	<p>Select the encryption algorithm. It will either begin with a prefix of "nopfs" or "g2".</p> <p>nopfs - stands for "no perfect forwarding security". In this situation, the Phase 2 proposal will make use of the same key used in the Phase 1 proposal.</p> <p>g2 - stands for "Group 2". In this situation, the devices will renegotiate a new key for Phase 2.</p>

2. To enable the VPN Monitor, select the check box. This will require the user at the source address to authenticate his or her identity by supplying a user name and password before traffic is allowed to cross the firewall or enter the VPN tunnel.
3. To enable the Transport Mode (for L2TP-over-IPSec only), select the check box. This will cause the original IP packet not to be encapsulated within another IP packet.
4. Click **OK** to save your settings.

Apply and Cancel

Click **Apply** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VPN >> GATEWAY

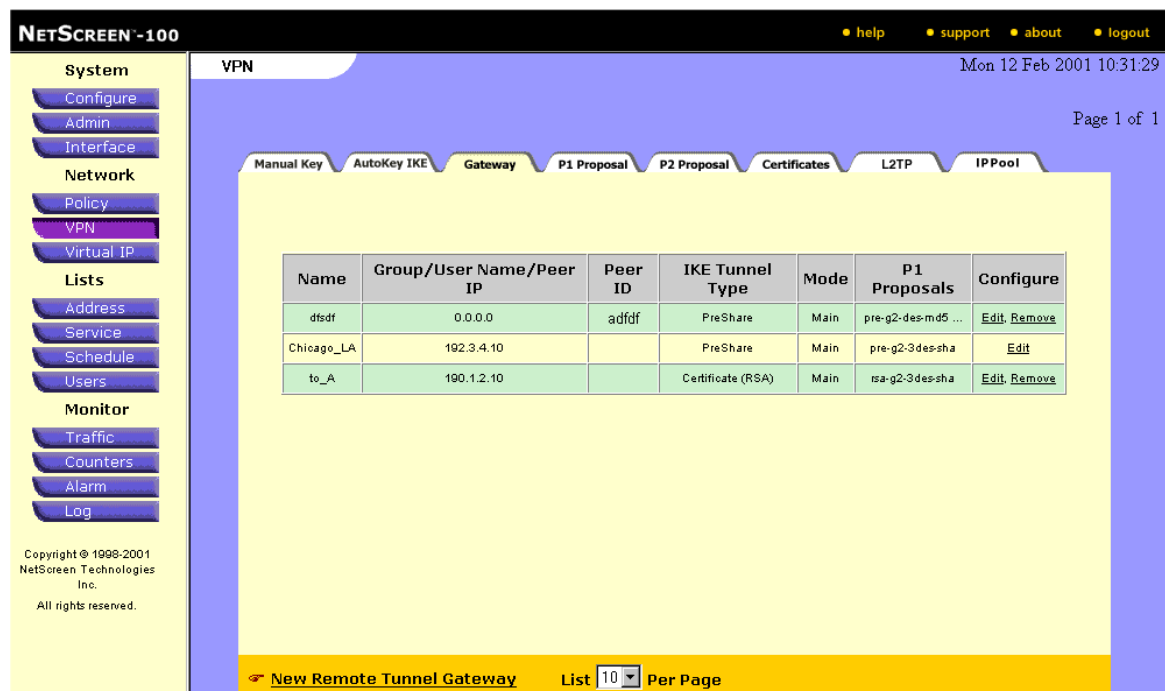


Figure 2-26 VPN >> Gateway

Gateway Definition

These first step in creating an IKE tunnel for LAN-to-LAN communication is to define the remote gateway, choosing the method of IKE and an appropriate Phase 1 proposal for negotiating the building of the tunnel. This page lists remote gateways that have been defined. You can reuse Phase 1 proposals in other gateways.

1. Provide definitions of the following fields:

Gateway Fields	Definition
Name	The name of the VPN tunnel.
Group/ User Name/ Peer IP	The fixed IP address of a remote gateway.
Peer ID	Same as the remote gateway ID. You can assign any optional descriptive name.

Gateway Fields	Definition
Mode	The NetScreen-100 supports two modes of Phase 1 ISAKMP exchange. In Main Mode, the handshake does not occur until a secure channel is established. In Aggressive Mode, there is no identity protection for the negotiating nodes, because both nodes must transmit their identities before establishing a negotiated secure channel.
P1 Proposals	For Preshare Key, Phase 1 Proposals begin with the prefix, "pre-". For PKI, Phase 1 Proposals begin with the prefix, "rsa-" or "dsa-".
Configure	In this column, you can choose Edit and Remove. Remove is only available if the entry is not already in use in an access policy.

- To create a new remote gateway tunnel, select **New Remote Gateway** at the bottom of the page.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VPN >> NEW REMOTE GATEWAY

NETSCREEN-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

REMOTE TUNNEL GATEWAY CONFIGURATION

Gateway Name

Remote Gateway
☒ Static IP Address IP Address
 Peer ID (optional)
☐ Dynamic IP Address Peer ID
☐ Dialup User User/Group
 Mode (Initiator) ☒ Main (ID Protection) ☐ Aggressive

Phase 1 Proposal

Preshared Key
 Local ID (optional)

Preferred Certificate (optional)
 Local Cert
 Peer CA
 Peer Type

OK Cancel

Figure 2-27 VPN >> New Remote Gateway

New Remote Gateway

The first step in creating an IKE tunnel for LAN-to-LAN communication is to define the remote gateway, choosing the method of IKE and an appropriate Phase 1 proposal for negotiating the building of the tunnel. You can reuse Phase 1 proposals in other gateways.

To create a gateway:

- Whether you are setting up LAN-to-LAN or Dialup-to-LAN communication, complete the following information:

Tunnel Field	Description
Name	Enter the name of the VPN tunnel you want to create. You can use up to a maximum of 32 characters.
Remote Gateway	Select the radio button for Static IP Address, Dynamic IP Address or Dialup User.
Static IP Address	This is the fixed IP address of the remote gateway.

Tunnel Field	Description
Dynamic IP Address	Enter the Peer ID of the Dynamic IP Address.
Dialup User	Use the pulldown menu at right to select dialup user.
Mode	The NetScreen device supports two modes of Phase 1 ISAKMP exchange. In Main Mode, the handshake does not occur until a secure channel is established. In Aggressive Mode, there is no identity protection for the negotiating nodes, because both nodes must transmit their identities before establishing a negotiated secure channel.
Phase 1 Proposal	Make selection from drop-down menu for either Preshared Key or PKI (see above). You can choose up to 4 Phase 1 proposals to accommodate a variety of VPN connections through the same tunnel.
Preshare Key	<p>You have the following options</p> <p>For Preshared Key: In the Preshared Key field, enter the same ASCII value that the user will be entering at the other end. Then select a Phase 1 proposal that begins with the prefix, "pre-".</p> <p>For PKI: Leave the Preshared Key field blank, and select a Phase 1 proposal that begins with either the prefix, "rsa-" or "dsa-". To use an RSA or DSA Phase 1 proposal, you must have generated a public/private key pair and have received and loaded a certificate from a Certificate Authority (CA).</p>
Local ID (Required only for certificates))	<p>Enter one of the following:</p> <p>E-mail address (RFC822)</p> <p>IP address (a.b.c.)</p> <p>Fully qualified domain name (FQDN)</p>
Preferred Cert Type	What RFC-defined certificate type you prefer to use: X509-SIGnature or PKCS7.
Preferred Peer CA	The Certificate Authority you prefer the remote gateway use.
Peer Type	Select peer type (the default is none).

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VPN >> EDIT REMOTE GATEWAY

NetScreen-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

REMOTE TUNNEL GATEWAY CONFIGURATION

Gateway Name: Chicago_LA

Remote Gateway

☒ Static IP Address IP Address: 192.3.4.10 Peer ID: (optional)

☐ Dynamic IP Address Peer ID:

☐ Dialup User User/Group: None Mode (Initiator): ☒ Main (ID Protection) ☐ Aggressive

Phase 1 Proposal

pre-g2-3des-sha none
 none none

Preshared Key
 Local ID: (optional)

Preferred Certificate (optional)
 Local Cert: None
 Peer CA: None
 Peer Type: NONE

OK Cancel

Figure 2-28 VPN >> Edit Remote Gateway

Remote Gateway Tunnel Configuration

The first step in creating an IKE tunnel for LAN-to-LAN communication is to define the remote gateway, choosing the method of IKE and an appropriate Phase 1 proposal for negotiating the building of the tunnel. You can reuse Phase 1 proposals in other gateways.

To edit a gateway:

- Whether you are setting up LAN-to-LAN or Dialup-to-LAN communication, complete the following information:

Tunnel Field	Description
Name	Enter the name of the VPN tunnel you want to create. You can use up to a maximum of 32 characters.
Remote Gateway	Select the radio button for Static IP Address, Dynamic IP Address or Dialup User.

Tunnel Field	Description
Static IP Address	This is the fixed IP address of the remote gateway.
Dynamic IP Address	Enter the Peer ID of the Dynamic IP Address.
Dialup User	Use the pulldown menu at right to select dialup user.
Mode	The NetScreen-100 supports two modes of Phase 1 ISAKMP exchange. In Main Mode, the handshake does not occur until a secure channel is established. In Aggressive Mode, there is no identity protection for the negotiating nodes, because both nodes must transmit their identities before establishing a negotiated secure channel.
Phase 1 Proposal	Make selection from drop-down menu for either Preshared Key or PKI (see above). You can choose up to 4 Phase 1 proposals to accommodate a variety of VPN connections through the same tunnel.
Preshare Key	<p>You have the following options</p> <p>For Preshared Key: In the Preshared Key field, enter the same ASCII value that the user will be entering at the other end. Then select a Phase 1 proposal that begins with the prefix, "pre-".</p> <p>For PKI: Leave the Preshared Key field blank, and select a Phase 1 proposal that begins with either the prefix, "rsa-" or "dsa-". To use an RSA or DSA Phase 1 proposal, you must have generated a public/private key pair and have received and loaded a certificate from a Certificate Authority (CA).</p>
Local ID (optional)	<p>Enter one of the following:</p> <p>E-mail address (RFC822)</p> <p>IP address (a.b.c.)</p> <p>Fully qualified domain name (FQDN)</p>
Preferred Cert Type	What RFC-defined certificate type you prefer to use: X509-SIGnature or PKCS7
Preferred Peer CA	The Certificate Authority you prefer the remote gateway use.

2. If the tunnel is for Dialup-to-LAN communication, click the **Remote Gateway/ User-Dynamic IP Address** radio button and complete the following information:

Remote Gateway Field	Description
IP Address	Enter the IP address of the remote gateway to which you want to establish the tunnel.
Remote Gateway ID	This optional field provides space for an identification that displays in the Gateway page.
Mode	The NetScreen-100 supports two modes of Phase 1 ISAKMP exchange. In Main Mode, the handshake does not occur until a secure channel is established. In Aggressive Mode, there is no identity protection for the negotiating nodes, because both nodes must transmit their identities before establishing a negotiated secure channel.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VPN >> P1 PROPOSAL

NETSCREEN-100

• help • support • about • logout

Mon 12 Feb 2001 10:37:09

Page 1 of 1

VPN

Manual Key AutoKey IKE Gateway **P1 Proposal** P2 Proposal Certificates L2TP IPPool

Name	Method	DH Group	Encrypt/Auth.	Lifetime	Configure
pre-g2-des-md5	Preshare	2	DES / MD5	28800	..
pre-g2-des-sha	Preshare	2	DES / SHA	28800	..
pre-g2-3des-md5	Preshare	2	3DES / MD5	28800	..
pre-g2-3des-sha	Preshare	2	3DES / SHA	28800	..
rsa-g2-des-md5	RSA-sig	2	DES / MD5	28800	..
rsa-g2-des-sha	RSA-sig	2	DES / SHA	28800	..
rsa-g2-3des-md5	RSA-sig	2	3DES / MD5	28800	..
rsa-g2-3des-sha	RSA-sig	2	3DES / SHA	28800	..
dsa-g2-des-md5	DSA-sig	2	DES / MD5	28800	..
dsa-g2-des-sha	DSA-sig	2	DES / SHA	28800	..
dsa-g2-3des-md5	DSA-sig	2	3DES / MD5	28800	..
dsa-g2-3des-sha	DSA-sig	2	3DES / SHA	28800	..
West-Coast	Preshare	2	3DES / SHA	1000	Edit Remove

Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.

[New Phase 1 Proposal](#) List Per Page < 1 2 > [Next](#)

Figure 2-29 VPN >> P1 Proposal

Creating a P1 Proposal

Setting up the VPN tunnel's encryption and authentication is actually a two-phase process.

Phase 1 essentially covers how the gateways will securely negotiate and handle the building of the tunnel. The P1 (Phase 1) Proposal sets the terms of the negotiation.

The predefined Phase 1 (P1) Proposals are listed with the following fields:

P1 Proposal Field	Description
Name	Assign any arbitrary text to name this proposal.
Method	This refers to the authentication method. The options are Preshare , when using a Preshared Secret, RSA-Sig when using a digital certificate from a Certificate Authority, or DSA , which also uses a Certificate Authority digital certificate.

P1 Proposal Field	Description
DH	The Diffie-Hellman Group used: Group 1 , Group 2 , or Group 5 .
Encrypt/Auth	Specified the encryption algorithm (3DES-CBC or DES-CBC) and the hash algorithm (MD5 or SHA-1).
Lifetime	The life of the key, as determined by the amount of time in Sec(onds), Min (utes), Hours , or Days .
Lifesize	The life of the key, as determined by the number of kilobytes of VPN traffic.
Configure	Allows you to Edit or Remove any custom P1 Proposals you create.

Although the NetScreen-100 comes with a selection of predefined Phase 1 Proposals, you may create your own.

To create a new Phase 1 (P1) Proposal, go to the bottom left-hand corner of the P1 Proposal page, and click on **New Phase 1 Proposal**.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VPN >> P1 PROPOSAL >> EDIT

NETSCREEN-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1999-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

PHASE 1 PROPOSAL CONFIGURATION

Name: West-Coast

Authentication Method: Preshare

DH Group: Group 2

Encryption & Data Integrity

Encryption Algorithm: 3DES-CBC

Hash Algorithm: SHA-1

Lifetime: 1000
☒ Sec ☐ Min ☐ Hours ☐ Days

OK Cancel

Figure 2-30 VPN >> P1 Proposal >> Edit

Phase 1 Proposal Edit

1. On the New Phase 1 Proposal Configuration page, complete the following information.

Configuration Field	Description
Name	Assign any arbitrary text to name this proposal.
Authentication Method	Select Preshare , when using a Preshared Secret, RSA-Sig when using a digital certificate from a Certificate Authority, or DSA , which also uses a Certificate Authority digital certificate.
DH Group	Select one of the following Diffie-Hellman Groups: Group 1 , Group 2 , or Group 5 .

Configuration Field	Description
Encryption & Data Integrity	
Encryption Algorithm	Choose either 3DES-CBC or DES-CBC .
Hash Algorithm	Choose either MD5 or SHA-1 .
Lifetime	For the quantity, type in an integer and select the units: Sec (onds), Min (utes), Hours , or Days .

2. To save the new Phase 1 Proposal Configuration, click **OK**.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VPN >> NEW PHASE 1 PROPOSAL

NETSCREEN-100 • help • support • about • logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

PHASE 1 PROPOSAL CONFIGURATION

Name:

Authentication Method:

DH Group:

Encryption & Data Integrity

Encryption Algorithm:

Hash Algorithm:

Lifetime: ☐ Sec ☐ Min ☒ Hours ☐ Days

OK Cancel

Figure 2-31 VPN >> New Phase 1 Proposal

Phase 1 Proposal Configuration

1. On the New Phase 1 Proposal Configuration page, complete the following information.

Configuration Field	Description
Name	Assign any arbitrary text to name this proposal.
Authentication Method	Select Preshare , when using a Preshared Secret, RSA-Sig when using a digital certificate from a Certificate Authority, or DSA , which also uses a Certificate Authority digital certificate.
DH Group	Select one of the following Diffie-Hellman Groups: Group 1 , Group 2 , or Group 5 .
Encryption & Data Integrity	

Configuration Field	Description
Encryption Algorithm	Choose either 3DES-CBC or DES-CBC .
Hash Algorithm	Choose either MD5 or SHA-1 .
Lifetime	For the quantity, type in an integer and select the units: Sec(onds) , Min(utes) , Hours , or Days .

2. To save the new Phase 1 Proposal Configuration, click **OK**.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VPN >> P2 PROPOSAL

NETSCREEN-100

help support about logout

Mon 12 Feb 2001 10:41:50

Page 1 of 1

VPN

Manual Key AutoKey IKE Gateway P1 Proposal P2 Proposal Certificates L2TP IPPool

Name	PFS	Encap.	Encrypt/Auth.	Lifetime	Lifesize	Configure
nopts-esp-des-md5	No PFS	ESP	DES / MD5	3600	0	--
nopts-esp-des-sha	No PFS	ESP	DES / SHA	3600	0	--
nopts-esp-3des-md5	No PFS	ESP	3DES / MD5	3600	0	--
nopts-esp-3des-sha	No PFS	ESP	3DES / SHA	3600	0	--
g2-esp-des-md5	DH Group 2	ESP	DES / MD5	3600	0	--
g2-esp-des-sha	DH Group 2	ESP	DES / SHA	3600	0	--
g2-esp-3des-md5	DH Group 2	ESP	3DES / MD5	3600	0	--
g2-esp-3des-sha	DH Group 2	ESP	3DES / SHA	3600	0	--
Auth_Only	DH Group 2	AH	NULL / MD5	1800	0	Edit Remove
nopts	DH Group 2	ESP	3DES / SHA	28800	0	Edit Remove

Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.

[New Phase 2 Proposal](#) List Per Page

Figure 2-32 VPN >> P2 Proposal

Phase 2 Proposal

Setting up the VPN tunnel's encryption and authentication is actually a two-phase process.

Phase 2 sets up how the data passing through the tunnel will be encrypted at one end and decrypted at the other. The encryption method you choose needs to account for both phases. This process is carried out on both sides of the tunnel. The P2 (Phase 2) Proposal sets the terms of the negotiation.

Although the NetScreen device comes with a selection of predefined Phase 2 Proposals, you may create your own.

Below is a listing of information available for each Phase 2 Proposal:

VPN Field	Description
Name	Any arbitrary text assigned to name this proposal.

VPN Field	Description
PFS	This stands for Perfect Forward Secrecy. Select from NO-PFS (No Perfect Forward Secrecy), DH (Dillie-Hellman) Group 1, DH Group 2, or DH Group 5.
Encap.	This refers to the type of encapsulation: either Encryption (ESP) or Authentication Only (AH).
Encrypt/Auth.	Specified the encryption algorithm (3DES-CBC or DES-CBC) and the hash algorithm (MD5 or SHA-1).
Lifetime	Defines the lifetime of the encryption key in Sec(onds), Min(utes), Hours, or Days.
Lifesize	Defines the lifetime of the encryption key in kilobytes.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VPN >> P2 PROPOSAL >> NEW PHASE 2 PROPOSAL

NETSCREEN-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

PHASE 2 PROPOSAL CONFIGURATION

Name

Perfect Forward Secrecy

Encapsulation
☒ Encryption (ESP)
 Encryption Algorithm
 Authentication Algorithm
☐ Authentication Only (AH)
 Authentication Algorithm

Lifetime
 In Time ☐ Sec ☐ Min ☒ Hours ☐ Days
 In Kbytes Kbytes

Figure 2-33 VPN >> P2 Proposal >> New Phase 2 Proposal

To create a new P2 Proposal:

1. On the New Phase 2 Proposal Configuration page, complete the following information:

Configuration Fields	Description
Name	Assign any arbitrary text to name this proposal.
Perfect Forward Secrecy	Select from NO-PFS (No Perfect Forward Secrecy), DH (Dillie-Hellman) Group 1, DH Group 2, or DH Group 5.
Encapsulation	Choose either Encryption (ESP) or Authentication Only (AH)
Encryption (ESP)	
Encryption Algorithm	Choose from Null , DES-CBC , or 3DES-CBC .

Configuration Fields	Description
Authentication Algorithm	Choose either Encryption (ESP) or Authentication Only (AH)
Authentication Algorithm	Choose either MD5 or SHA-1 .
Lifetime	Defines the lifetime of the encryption key in time or in kilobytes.
In Time	To determine the lifetime of the key in units of time, type in an integer and select the units: Sec (onds), Min (utes), Hours , or Days .
In Kbytes	To determine the lifetime of the key by the number of kilobytes of VPN traffic, enter the number of kilobytes.

2. To save the new Phase 2 Proposal Configuration, click **OK**.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VPN >> CERTIFICATES

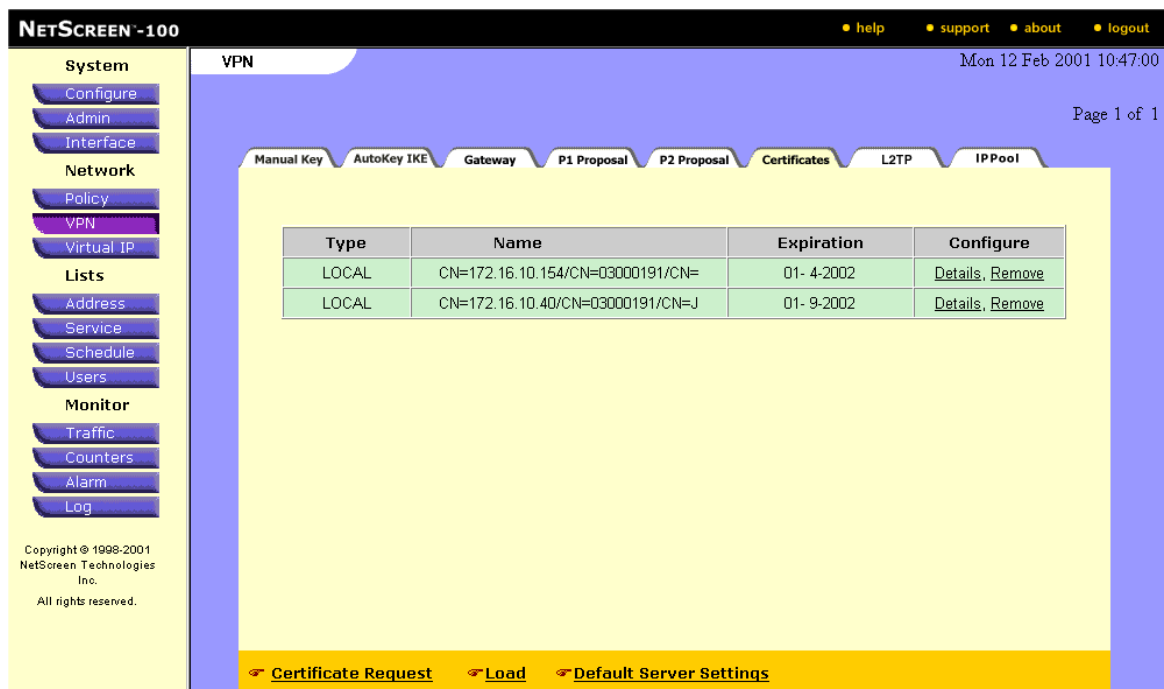


Figure 2-34 VPN >> Certificates

Viewing a VPN Certificate

In this section you set up where the NetScreen device checks for the Certificate Revocation List (CRL). The table displayed on this page summarizes the following information about each certificate you have loaded and is available:

Certificate Field	Description
Type	Whether the certificate is Local or from a Certificate Authority (CA).
Name	The name assigned from the Certificate Request.
Expiration	The date that the certificate expires.
Config	Click Details to view the details of the certificate or Remove to remove the certificate.

Note: *Be aware that if you remove a local certificate, you must regenerate the new key.*

1. To request a certificate, click **Cert Request**.
2. To generate key pairs, click **Cert Request** for a new certificate, or **Details** for an existing certificate.
3. To load a certificate that you have available, click **Load**.
4. To set up where the NetScreen device checks for the CRL, click **Default Server Settings**, complete fields in the Default Server Settings dialog box, and then click **OK**.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VPN >> CERTIFICATES >> CERTIFICATE REQUEST

NETSCREEN-100 • help • support • about • logout

CERTIFICATE REQUEST

Certificate Subject Information

Name: Yuki

Phone: (800) 555-1212

Unit/Department: Engineering

Organization: Hitachi

County/Locality: Funabashi

State: CH

Country: JP

E-mail:

IP Address: 172.16.10.40

Write Request File To:

☐ E-mail to: jfraher@netscreen.com

☒ Write to file

Key Pair Information:

☒ RSA ☐ DSA

Create new key pair of 1024 length.

Generate Get Cancel

Copyright © 1998-2001
NetScreen Technologies
Inc.

Figure 2-35 VPN >> Certificate >> Certificate Request

Generating Keys and Completing a Certificate Request

When you fill out the Certificate Request, the public key you generate becomes incorporated in the request itself and, eventually, into the digitally signed local certificate you receive back from the Certificate Authority. This certificate is essentially your ID card.

The NetScreen-100 uses the fields on the New Certificate Request dialog box to construct the Distinguished Name required for your PKI certificates.

1. To request a new certificate, under the heading **Certificate Subject Information**, enter the following information:

User Field	Description
Name	The key holder's name
Phone	The key holder's phone number
Unit/Department	The key holder's unit or department

User Field	Description
Organization	The key holder's organization
County/Locality	The key holder's county or locality
State	The key holder's state
Country	The key holder's country
E-mail	The key holder's e-mail address
IP Address	The key holder's IP address

2. Under the heading, Write Request File To:, you'll need to select one of two radio buttons.

The keys and the Request File are generated on the NetScreen device itself. In the selections that follow, you will choose whether the NetScreen device will save the appropriate information to a file on your workstation or into an e-mail sent to yourself (or, more likely, your System Administrator).

E-mail to: If you select this radio button and supply your System Administrator's e-mail address in this field, the certificate request will be mailed to that address.

Write to file: If you select this radio button, the certificate request is written to a file on your local hard drive, and you must either send it to your system administrator or convey it to the certificate authority in some other manner.

3. Under the heading, Key Pair Information: complete the following information.

Select which type of key pair you need: RSA or DSA.

Select the key length by clicking the drop-down box on the right hand side of the selection. You can choose 512, 786, 1024, or 2048 for the key length.

4. Click the **Generate** button.

Note: Before generating a public/private key pair, make sure that your Certificate Authority can support the key length you select. Key lengths greater than 1024 may require generation times greater than 10 minutes.

Note: Some Certificate Authorities may not accept all the downloaded entries. Please contact the Certificate Authority for more details.

VPN >> CERTIFICATES OR CRL >> LOAD

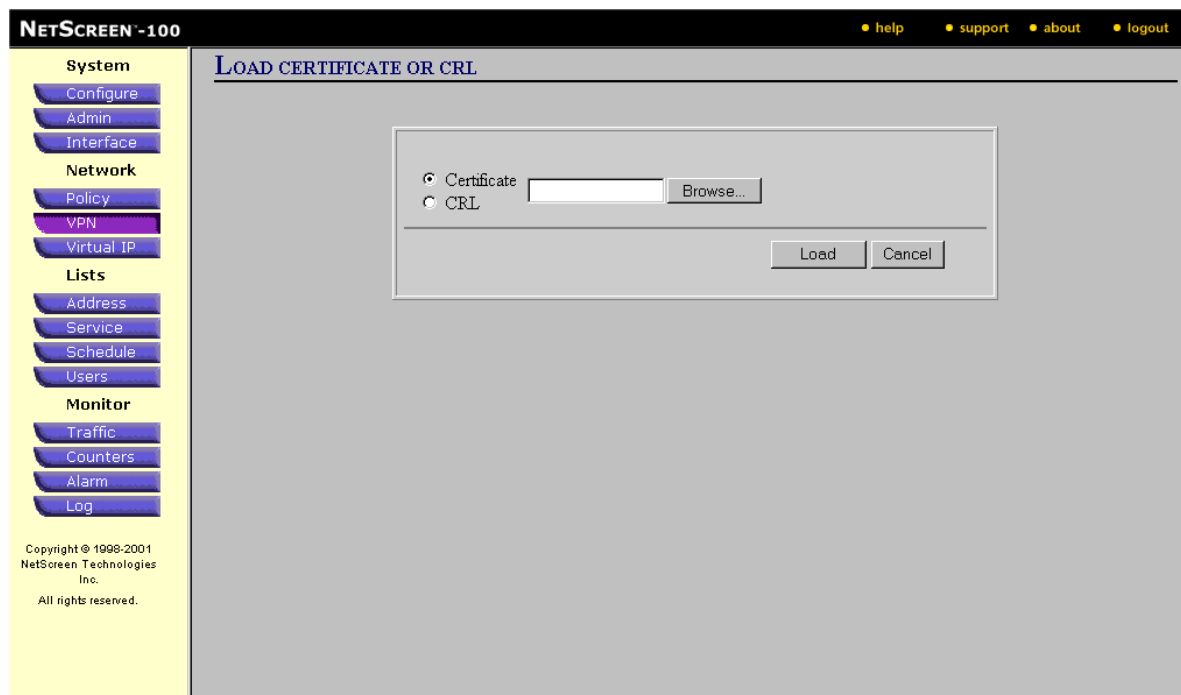


Figure 2-36 VPN >> Certificates or CRL >> Load

Loading Your Signed Certificates or CRL

Your system Administrator returns 2 files to you for loading into the NetScreen device:

- A CA Certificate, which is the CA's signed public key.
- A local certification (CRL) that verifies your local machine.

The file extension of these files is .cer. You must load both of these certificates into the NetScreen device.

1. Click **Load** to display the Load Certificate dialog box.
2. Select the CRL radio button, then click the Browse button to display the File Selection dialog box.
3. Select the directory where your .cer files are located.
4. Select a file with an extension of .cer, and click the **Open** button.

This places the file name in the CRL field on the Load Certificate dialog box.

5. Click the **Load** button to load the .cer file and redisplay the Certificates page.
6. Click Load at the bottom of the Certificate, and repeat the loading process for the second .cer file.

Loading the CRL

In addition, the Certificate Authority may provide a Certificate Revocation List (CRL). In Phase 1 negotiations, the CRL list is checked to see if certificates received during an IKE exchange are valid.

It is not mandatory to load the CRL. If none is loaded, the gateway will use the CRL location defined in the Server Settings field.

To load the CRL:

1. In Load Certificate dialog box, select the CRL radio button, then click the Browse button to display the File Selection dialog box.
2. Select the directory where your .crl files are located.
3. Select a file with an extension of .crl, and click the Open button.
4. This places the file name in the Cert field on the Load Certificate dialog box.
5. Click the Load button to load the .crl file and redisplay the Certificates page.

VPN >> CERTIFICATES >> DEFAULT LDAP SERVER SETTINGS

NETSCREEN-100 help support about logout

DEFAULT SERVER SETTINGS

LDAP Server: 2.2.2.121

CRL URL: www.darkalley.com/CRL_files

CRL Refresh Frequency: Daily

X509 Certificate Path Validation Level: ☐ Full ☒ Partial

OK Cancel

System: Configure, Admin, Interface

Network: Policy, VPN, Virtual IP

Lists: Address, Service, Schedule, Users

Monitor: Traffic, Counters, Alarm, Log

Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.

Figure 2-37 VPN >> Certificates >> Default Server Settings

Configuring LDAP Default Server Settings

1. In the Default Server Settings dialog box, complete the following information.

Settings Field	Description
Default LDAP Server	Enter the IP address or domain name of the LDAP Root CA server that manages the CRL.
Default CRL URL	The internal web-based URL of the LDAP server managing your CRL.
CRL Refresh Frequency	The interval at which the server checks the CRL. You can select Daily, Weekly, or Monthly.
X509 Cert_Path Validation Level	Within X.509 is a specification for a certificate which binds an entity's distinguished name to its public key through the use of a digital signature. Select Full or Partial validation.

2. Click **OK** to save your changes and return to the Certificates page.

VPN >> CERTIFICATE >> KEY PAIR

NETSCREEN-100 help support about logout

System

- Configure
- Admin
- Interface

Network

- Policy
- VPN
- Virtual IP

Lists

- Address
- Service
- Schedule
- Users

Monitor

- Traffic
- Counters
- Alarm
- Log

Copyright © 1998-2001
NetScreen Technologies
Inc.
All rights reserved.

Certificate Subject Information

Name: Yuki

Phone: (800) 555-1212

Unit/Department: Engineering

Organization: Hitachi

County/Locality: Funabashi

State: CH

Country: JP

E-mail:

IP Address: 172.16.10.40

Write Request File To:

☐ E-mail to: jfraher@netscreen.com

☒ Write to file

Key Pair Information:

☒ RSA ☐ DSA

Create new key pair of 1024 length.

Generate Get Cancel

Figure 2-38 VPN >> Certificate >> Key Pair Request

Generating a Key Pair Using Existing Information

If you are regenerating a certificate's key pair (for example, to change your key length), and you wish to use the information already filled into the property sheet, click the **Get** button.

If a local certificate is deleted after it is downloaded, a new key file and local certificate must be created.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VPN >> L2TP TUNNEL

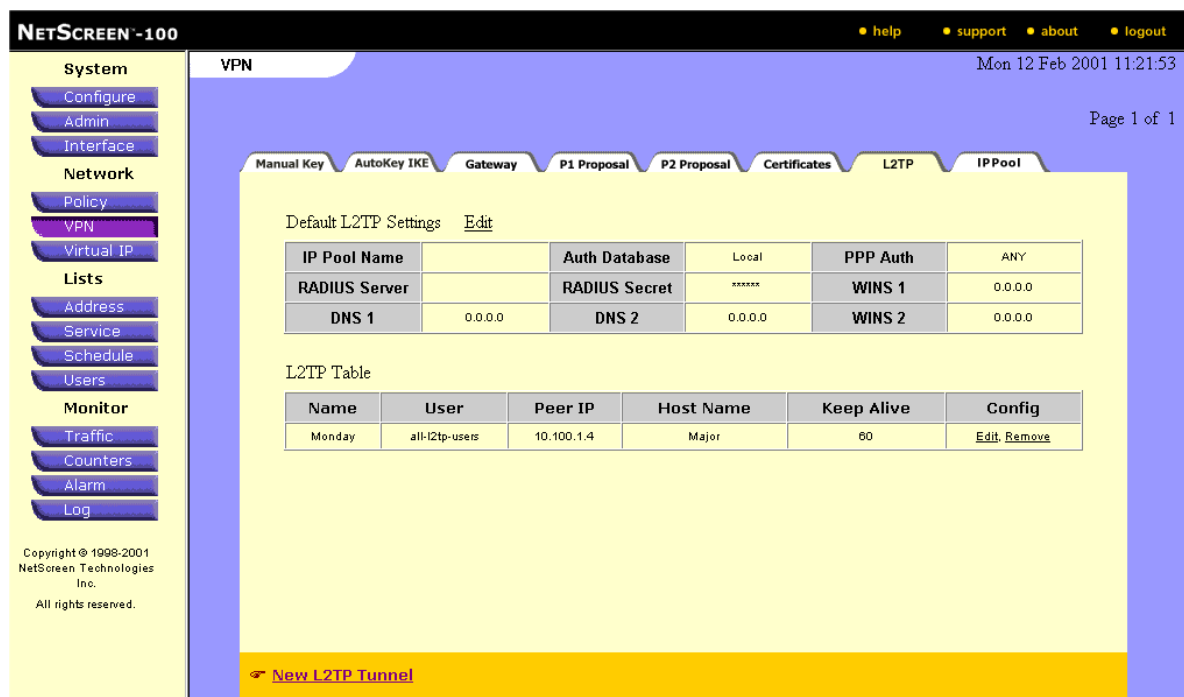


Figure 2-39 VPN >> L2TP Tunnel

Default L2TP Settings

This page displays the default L2TP settings and all existing L2TP tunnel configurations for the NetScreen device.

Default L2TP Fields	Description
IP Pool Name	Name for IP pool.
Auth Database	Name of authorized user database.
PPP Auth	PPP Authentication Method.
Radius Server	The name or IP address of the RADIUS server that stores authorized users.
Radius Secret	The shared secret of the RADIUS server and the NetScreen device.
DNS (#1, #2)	Name or IP addresses of DNS servers.
WINS (#1, #2)	Name or IP address of Windows Internet Naming Service (WINS) server of the Microsoft Network.

L2TP Table

L2TP Fields	Description
Name	Name of new L2TP tunnel.
User	Name of users or dialup user group.
Peer IP	Peer IP address of tunnel.
Host Name	Host name.
Keep Alive	Time interval, in seconds, for NetScreen device to send keep-alive messages.

VPN >> NEW L2TP TUNNEL

NETSCREEN-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

L2TP TUNNEL CONFIGURATION

Name

Dialup User/Group

Peer IP

Host Name

Secret

Keep Alive

OK Cancel

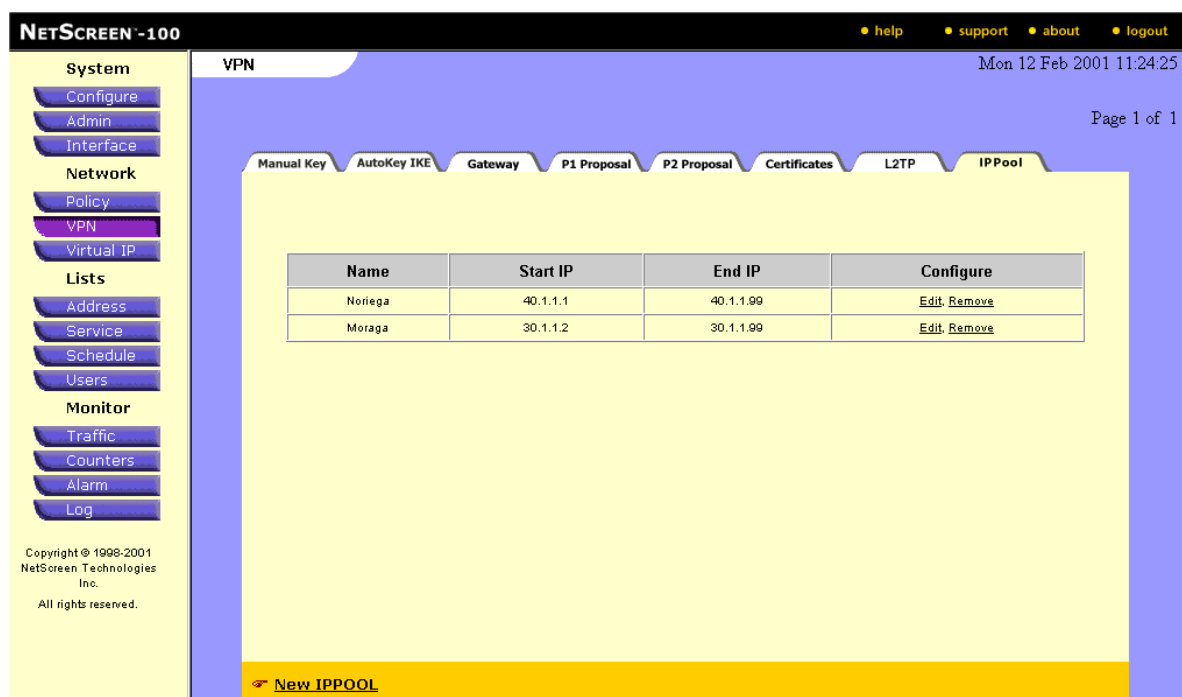
Figure 2-40 VPN >> New L2TP Tunnel

L2TP Tunnel Configuration

To create a new L2TP tunnel, click on **New L2TP Tunnel** on the L2TP Menu, and complete the following entries:

L2TP Fields	Description
Name	Name for new L2TP tunnel.
Dialup User/Group	Select user or dialup group from drop-down menu.
Peer IP	Peer IP address of L2TP tunnel.
Host Name	Host name for new L2TP tunnel.
Secret	Secret field for L2TP tunnel authentication.
Keep Alive	Time interval, in seconds, for NetScreen device to send keep-alive messages.

VPN >> IP POOL

**Figure 2-41** VPN >> IP Pool

IP Pool Addresses

The range of IP addresses in a VPN must be defined with a beginning and ending value.

IP Field	Description
Name	Name assigned to IP Pool.
Start IP	Starting IP address value.
End IP	Ending IP address value.
Configure	Click Edit to change IP Pool configuration, Remove to delete.

VPN >> NEW IP POOL

The screenshot shows the NetScreen-100 WebUI interface. On the left is a navigation menu with categories: System (Configure, Admin, Interface), Network (Policy, VPN, Virtual IP), Lists (Address, Service, Schedule, Users), and Monitor (Traffic, Counters, Alarm, Log). The main content area is titled 'IPPOOL CONFIGURATION'. It contains a form with three input fields: 'IPPool Name', 'Start IP' (set to 0.0.0.0), and 'End IP' (set to 0.0.0.0). At the bottom right of the form are 'Save' and 'Cancel' buttons. The footer of the interface includes copyright information: 'Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.'

Figure 2-42 VPN >> New IP Pool

New IP Pool Range

The range of IP addresses in an IP Pool must be defined with a beginning and ending value.

IP Field	Description
Name	Name assigned to IP Pool name.
Start IP	Starting IP address value.
End IP	Ending IP address value.

NETWORK >> VIRTUAL IP >> VIRTUAL IP 1 (NETSCREEN-100 AND -1000 ONLY)

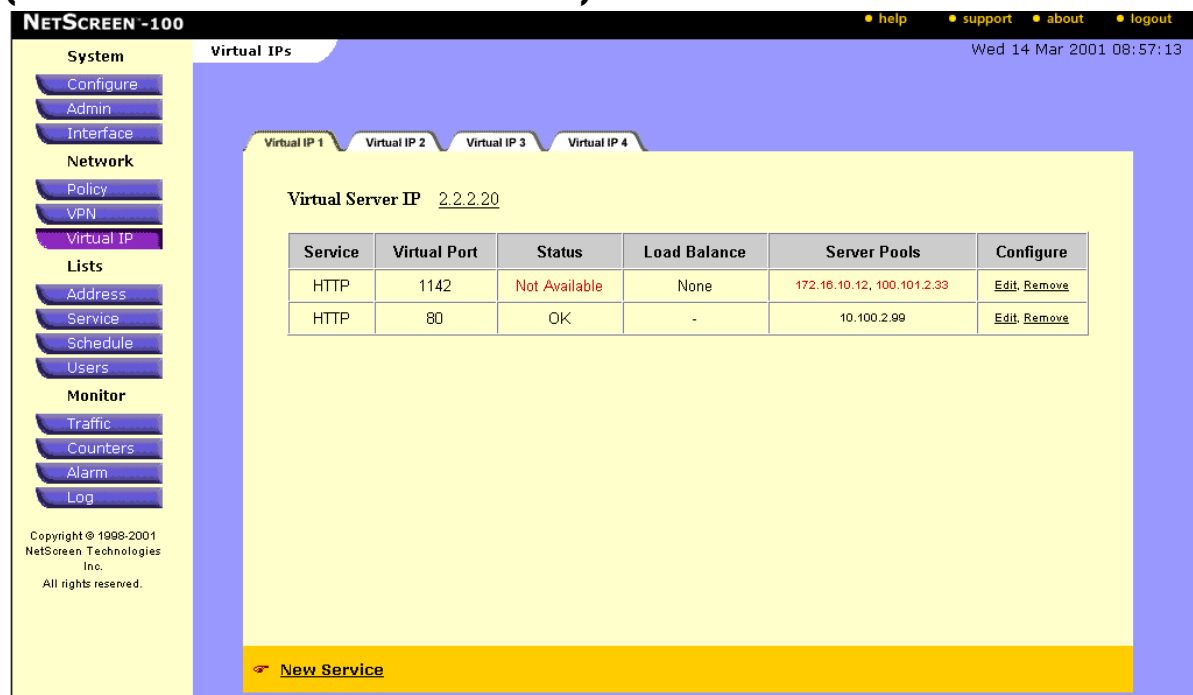


Figure 2-43 Network >> Virtual IP >> Virtual IP1

Virtual IP 1

Virtual IP is available on both the NetScreen-100 and the NetScreen-10. The Server Load-balancing functionality is available only on the NetScreen-100.

The NetScreen-100 supports up to four Virtual IP addresses and up to 8 services for each Virtual IP. The four NetScreen-100 addresses can forward traffic to eight different servers in the Trusted Network. NetScreen advises that extra caution be used in using this feature. If an attacker gains access to one of the internal servers, then your entire network could be vulnerable.

NetScreen Device	Number of Virtual IPs (Maximum)
NS-5	1
NS-10	3
NS-100	4
NS-1000	8

Setting up the Configurations

To configure Virtual IP 1 servers, with or without load balancing:

1. Click any **Virtual IP 1** tab.
2. Click the link, **click here to configure...**, to configure it. The Virtual IP Configuration dialog box appears.

Note: Setting the IP address to 0.0.0.0 or clicking the **clear** button on the Virtual IP Configuration dialog box clears the IP address.

3. Enter the public IP address to be mapped from the Untrusted interface to the Trusted or DMZ interface, and click **OK**. This Virtual IP address must be in the same subnet as the Untrusted port interface IP.
4. Define the service to be mapped by clicking the **New Service** link at the bottom of the Virtual IP page.
5. Enter the necessary information:

Virtual IP Field	Description
Virtual Port	The port that the service should be mapped to on the outside server. The user can use standard port numbers or use other port numbers. If non-standard port numbers are used, reconfiguration of the server may be required.
Service	Choose a service from the drop-down list for the server generating the connection. Available services include those with a fixed port and user-defined custom services.
Load Balance	If more than one server is defined, select the method of distributing the load balance between the inside servers: None, Round Robin, Weighted Round Robin, Least Connections, or Weighted Least Connections. Selecting None disables load balancing and only mapping will be applied to the first IP defined.
Server IP	Enter the IP address of the inside servers (on the Trusted or DMZ network) that will process the requests. An IP address of 0.0.0.0 indicates that no inside server is present. You can define up to eight servers. Note: If only one server is defined, then the IP address and service will map directly and no load balancing will be done.

Virtual IP Field	Description
Server Weight	<p>The weight factor represents the number of requests to be sent to a machine before they are re-routed to the next machine. In general, the server with the larger weight takes the heavier load of requests to process. Here is an example of the Weighted Round Robin method: if Server A has a weight of 10, Server B has a weight of 5, and Server C has a weight of 2, then the first 10 requests are sent to Server A, the next 5 requests are sent to Server B, and the next 2 requests to Server C, the next 10 requests once again to Server A, and so on.</p> <p>This field accepts a range of values from a minimum of 0 through a maximum of 1000. The higher the value, the greater the load-handling capacity of that specific inside server. A 0 indicates that load balancing on that server has been disabled.</p>

6. Click **OK** to save the settings.

You can configure up to eight services per Virtual IP for the NetScreen-100 and NetScreen-1000. However, you can only map one service at a time. In other words, you will need to complete the New Service page up to eight times per Virtual IP address for both the NetScreen-100 and the NetScreen-1000.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

Load Balancing (For NetScreen-100 Only)

For further information regarding load balancing, see the Concepts & Examples Manual.

VIRTUAL IP >> VIRTUAL IP1 >> NEW SERVICE

NETSCREEN-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

VIRTUAL IP SERVICE CONFIGURATION

Virtual IP: 2.2.2.20
 Virtual Port: 80
 Service: HTTP
 Load Balance: None

No	Server IP	Server Weight (1-1000)
1	0.0.0.0	0
2	0.0.0.0	0
3	0.0.0.0	0
4	0.0.0.0	0
5	0.0.0.0	0
6	0.0.0.0	0
7	0.0.0.0	0
8	0.0.0.0	0

OK Cancel

Figure 2-44 Virtual IP >> Virtual IP1 >> New Service

New Service Menu

To configure a Virtual IP 1 server, with or without load balancing:

1. Click the **Virtual IP 1** tab.
2. Click the link, **click here to configure...**, to configure it. The Virtual IP Configuration dialog box appears.

Note: Setting the IP address to 0.0.0.0 or clicking the **clear** button on the Virtual IP Configuration dialog box clears the IP address.

3. Enter the public IP address to be mapped from the Untrusted interface to the Trusted or DMZ interface, and click **OK**. This Virtual IP address must be in the same subnet as the Untrusted port interface IP.
4. Define the service to be mapped by clicking the **New Service** link at the bottom of the Virtual IP page.

5. Enter the necessary information:

Virtual IP Field	Description
Virtual Port	The port that the service should be mapped to on the outside server. The user can use standard port numbers or use other port numbers. If non-standard port numbers are used, reconfiguration of the server may be required.
Service	Choose a service from the drop-down list for the server generating the connection. Available services include those with a fixed port and user-defined custom services.
Load Balance	If more than one server is defined, select the method of distributing the load balance between the inside servers: None, Round Robin, Weighted Round Robin, Least Connections, or Weighted Least Connections. Selecting None disables load balancing and only mapping will be applied to the first IP defined.
Server IP	Enter the IP address of the inside servers (on the Trusted or DMZ network) that will process the requests. An IP address of 0.0.0.0 indicates that no inside server is present. You can define up to eight servers. Note: If only one server is defined, then the IP address and service will map directly and no load balancing will be done.
Server Weight	The weight factor represents the number of requests to be sent to a machine before they are re-routed to the next machine. In general, the server with the larger weight takes the heavier load of requests to process. Here is an example of the Weighted Round Robin method: if Server A has a weight of 10, Server B has a weight of 5, and Server C has a weight of 2, then the first 10 requests are sent to Server A, the next 5 requests are sent to Server B, and the next 2 requests to Server C, the next 10 requests once again to Server A, and so on. This field accepts a range of values from a minimum of 0 through a maximum of 1000. The higher the value, the greater the load-handling capacity of that specific inside server. A 0 indicates that load balancing on that server has been disabled.

6. Click **OK** to save the settings.

You can configure up to eight services per Virtual IP for a NetScreen-100, and one service per Virtual IP for a NetScreen-1000. However, you can only map one service at a time. In other words, you will need to complete the New Service page up to eight times per Virtual IP address for a NetScreen-100 and once per Virtual IP for a NetScreen-1000.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VIRTUAL IP >> VIRTUAL IP1 >> EDIT VIRTUAL SERVER IP

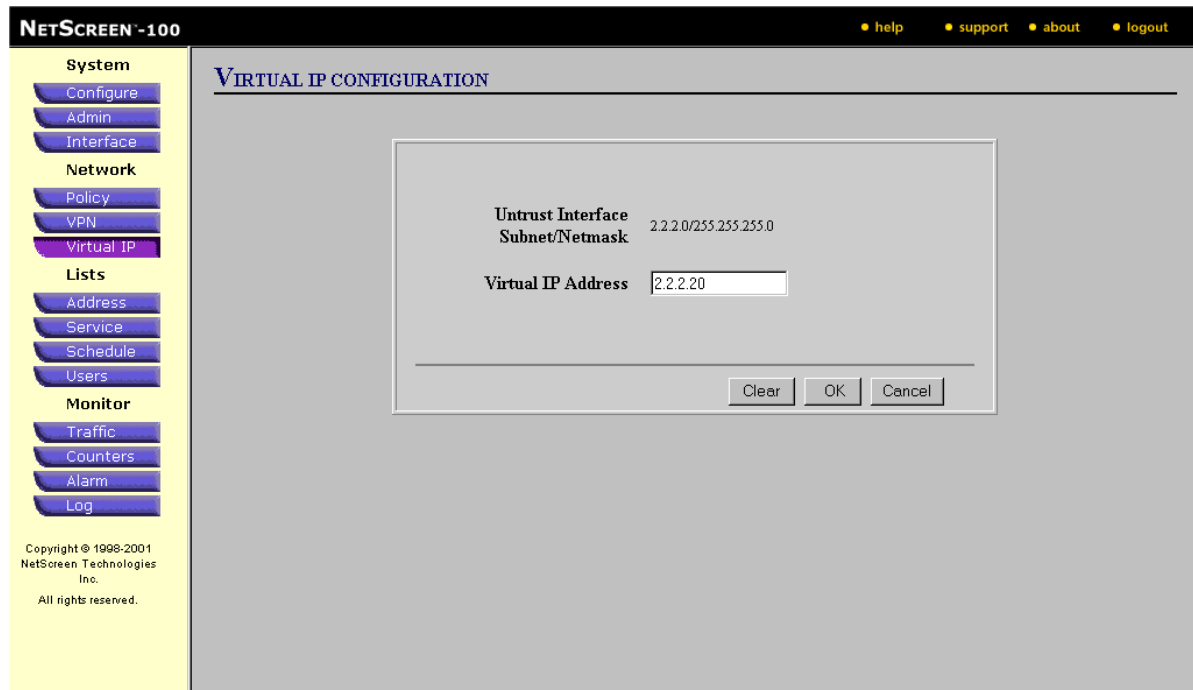


Figure 2-45 Virtual IP >> Virtual IP1 >> Edit Virtual Server IP

Edit Virtual Server Address

To modify a Virtual IP address:

1. Click on the Virtual Server IP link from the Virtual IP menu.
2. In the Virtual IP Configuration, enter the new address in the address field.

Virtual IP Address: Public IP address that is to be mapped to a host with a private IP address on the Trusted or DMZ network.

Note: Setting the IP address to 0.0.0.0 or clicking on the **clear** button on the configuration page clears the IP address.

3. Click **OK**.
The Virtual IP page reappears.
4. Click **New Service** to complete configuration.

VIRTUAL IP >> EDIT VIRTUAL IP1

NETSCREEN-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

VIRTUAL IP SERVICE CONFIGURATION

Virtual IP: 2.2.2.20
 Virtual Port: 80
 Service: HTTP
 Load Balance: None

No	Server IP	Server Weight (1-1000)
1	0.0.0.0	0
2	0.0.0.0	0
3	0.0.0.0	0
4	0.0.0.0	0
5	0.0.0.0	0
6	0.0.0.0	0
7	0.0.0.0	0
8	0.0.0.0	0

OK Cancel

Figure 2-46 Virtual IP >> Edit Virtual IP Settings

Virtual IP Service Menu

A new Virtual IP Service must have the following fields defined:

Virtual IP Server Field	Description
Virtual IP	IP address of virtual server (read-only).
Virtual Port	The port that the service should be mapped to on the outside server. The user can use standard port numbers or use other port numbers. If non-standard port numbers are used, reconfiguration of the server may be required.
Service	Choose a service from the drop-down list for the server generating the connection. Available services include those with a fixed port and user-defined custom services.

Virtual IP Server Field	Description
Load Balance	If more than one server is defined, select the method of distributing the load balance between the inside servers: None, Round Robin, Weighted Round Robin, Least Connections, or Weighted Least Connections. Selecting None disables load balancing and only mapping will be applied to the first IP defined.
Server IP	<p>Enter the IP address of the inside servers (on the Trusted or DMZ network) that will process the requests. An IP address of 0.0.0.0 indicates that no inside server is present. You can define up to eight servers.</p> <p>Note: If only one server is defined, then the IP address and service will map directly and no load balancing will be done.</p>
Server Weight	<p>The weight factor represents the number of requests to be sent to a machine before they are re-routed to the next machine. In general, the server with the larger weight takes the heavier load of requests to process. Here is an example of the Weighted Round Robin method: if Server A has a weight of 10, Server B has a weight of 5, and Server C has a weight of 2, then the first 10 requests are sent to Server A, the next 5 requests are sent to Server B, and the next 2 requests to Server C, the next 10 requests once again to Server A, and so on.</p> <p>This field accepts a range of values from a minimum of 0 through a maximum of 1000. The higher the value, the greater the load-handling capacity of that specific inside server. A 0 indicates that load balancing on that server has been disabled.</p>

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VIRTUAL IP >> VIRTUAL IP2 (NETSCREEN-100 AND NETSCREEN-1000)

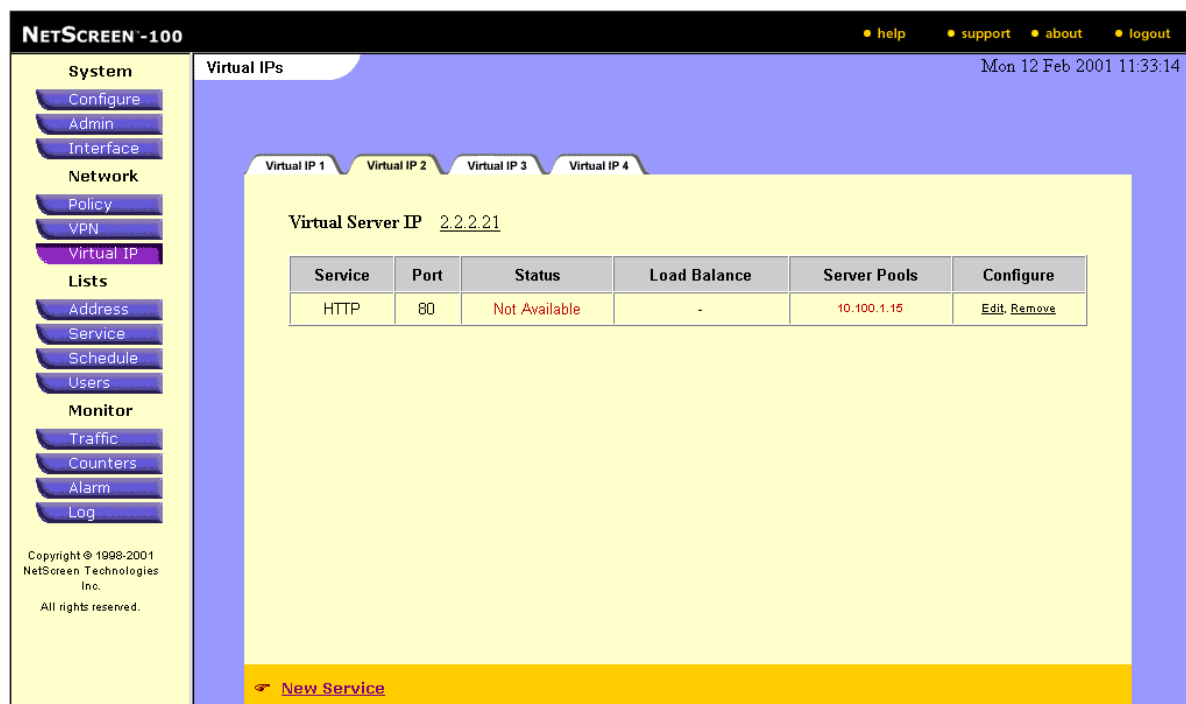


Figure 2-47 Virtual IP >> Virtual IP2

Virtual IP 2

You can configure up to eight services per Virtual IP for a NetScreen-100 and NetScreen-1000. However, you can only map one service at a time. In other words, you will need to complete the New Service page up to eight times per Virtual IP address for a NetScreen-100 and NetScreen-1000.

To configure a Virtual IP 2 server, with or without load balancing:

1. Click the **Virtual IP 2** tab.
2. Click the link, **click here to configure...**, to configure it. The Virtual IP Configuration dialog box appears.

Note: Setting the IP address to 0.0.0.0 or clicking the **clear** button on the Virtual IP Configuration dialog box clears the IP address.

3. Enter the public IP address to be mapped from the Untrusted interface to the Trusted or DMZ interface, and click **OK**. This Virtual IP address must be in the same subnet as the Untrusted port interface IP.
4. Define the service to be mapped by clicking the **New Service** link at the bottom of the Virtual IP page.
5. Enter the necessary information:

Virtual IP Field	Description
Virtual Port	The port that the service should be mapped to on the outside server. The user can use standard port numbers or use other port numbers. If non-standard port numbers are used, reconfiguration of the server may be required.
Service	Choose a service from the drop-down list for the server generating the connection. Available services include those with a fixed port and user-defined custom services.
Load Balance	If more than one server is defined, select the method of distributing the load balance between the inside servers: None, Round Robin, Weighted Round Robin, Least Connections, or Weighted Least Connections. Selecting None disables load balancing and only mapping will be applied to the first IP defined.
Server IP	Enter the IP address of the inside servers (on the Trusted or DMZ network) that will process the requests. An IP address of 0.0.0.0 indicates that no inside server is present. You can define up to eight servers. Note: If only one server is defined, then the IP address and service will map directly and no load balancing will be done.
Server Weight	The weight factor represents the number of requests to be sent to a machine before they are re-routed to the next machine. In general, the server with the larger weight takes the heavier load of requests to process. Here is an example of the Weighted Round Robin method: if Server A has a weight of 10, Server B has a weight of 5, and Server C has a weight of 2, then the first 10 requests are sent to Server A, the next 5 requests are sent to Server B, and the next 2 requests to Server C, the next 10 requests once again to Server A, and so on.

Virtual IP Field	Description
	This field accepts a range of values from a minimum of 0 through a maximum of 1000. The higher the value, the greater the load-handling capacity of that specific inside server. A 0 indicates that load balancing on that server has been disabled.

6. Click **OK** to save the settings.

You can configure up to eight services per Virtual IP for a NetScreen-100, and one service per Virtual IP for a NetScreen-1000. However, you can only map one service at a time. In other words, you will need to complete the New Service page up to eight times per Virtual IP address for a NetScreen-100 and once per Virtual IP for a NetScreen-1000.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VIRTUAL IP >> VIRTUAL IP3 (NETSCREEN-100 AND NETSCREEN-1000)

NETSCREEN-100

• help • support • about • logout

Mon 12 Feb 2001 11:35:35

Virtual IPs

Virtual IP 1 Virtual IP 2 Virtual IP 3 Virtual IP 4

Virtual Server IP 2.2.2.23

Service	Port	Status	Load Balance	Server Pools	Configure
HTTP	80	Not Available	-	10.100.1.20	Edit Remove

[New Service](#)

Copyright © 1999-2001
NetScreen Technologies
Inc.
All rights reserved.

Figure 2-48 Network >> Virtual IP >> Virtual IP3

Virtual IP 3

You can configure up to eight services per Virtual IP for a NetScreen-100 and for a NetScreen-1000. However, you can only map one service at a time. In other words, you will need to complete the New Service page up to eight times per Virtual IP address for a NetScreen-100 and for a NetScreen-1000.

To configure Virtual IP 3 server, with or without load balancing:

1. Click any **Virtual IP 3** tab.
2. Click the link, **click here to configure...**, to configure it. The Virtual IP Configuration dialog box appears.

Note: Setting the IP address to 0.0.0.0 or clicking the **clear** button on the Virtual IP Configuration dialog box clears the IP address.

3. Enter the public IP address to be mapped from the Untrusted interface to the Trusted or DMZ interface, and click **OK**. This Virtual IP address must be in the same subnet as the Untrusted port interface IP.
4. Define the service to be mapped by clicking the **New Service** link at the bottom of the Virtual IP page.
5. Enter the necessary information:

Virtual IP Field	Description
Virtual Port	The port that the service should be mapped to on the outside server. The user can use standard port numbers or use other port numbers. If non-standard port numbers are used, reconfiguration of the server may be required.
Service	Choose a service from the drop-down list for the server generating the connection. Available services include those with a fixed port and user-defined custom services.
Load Balance	If more than one server is defined, select the method of distributing the load balance between the inside servers: None, Round Robin, Weighted Round Robin, Least Connections, or Weighted Least Connections. Selecting None disables load balancing and only mapping will be applied to the first IP defined.
Server IP	Enter the IP address of the inside servers (on the Trusted or DMZ network) that will process the requests. An IP address of 0.0.0.0 indicates that no inside server is present. You can define up to eight servers. Note: If only one server is defined, then the IP address and service will map directly and no load balancing will be done.
Server Weight	The weight factor represents the number of requests to be sent to a machine before they are re-routed to the next machine. In general, the server with the larger weight takes the heavier load of requests to process. Here is an example of the Weighted Round Robin method: if Server A has a weight of 10, Server B has a weight of 5, and Server C has a weight of 2, then the first 10 requests are sent to Server A, the next 5 requests are sent to Server B, and the next 2 requests to Server C, the next 10 requests once again to Server A, and so on.

Virtual IP Field	Description
	This field accepts a range of values from a minimum of 0 through a maximum of 1000. The higher the value, the greater the load-handling capacity of that specific inside server. A 0 indicates that load balancing on that server has been disabled.

6. Click **OK** to save the settings.

You can configure up to eight services per Virtual IP for a NetScreen-100, and one service per Virtual IP for a NetScreen-1000. However, you can only map one service at a time. In other words, you will need to complete the New Service page up to eight times per Virtual IP address (for a NetScreen-100), or once (for a NetScreen-1000).

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

VIRTUAL IP >> VIRTUAL IP4 (NETSCREEN-100 AND NETSCREEN-1000)

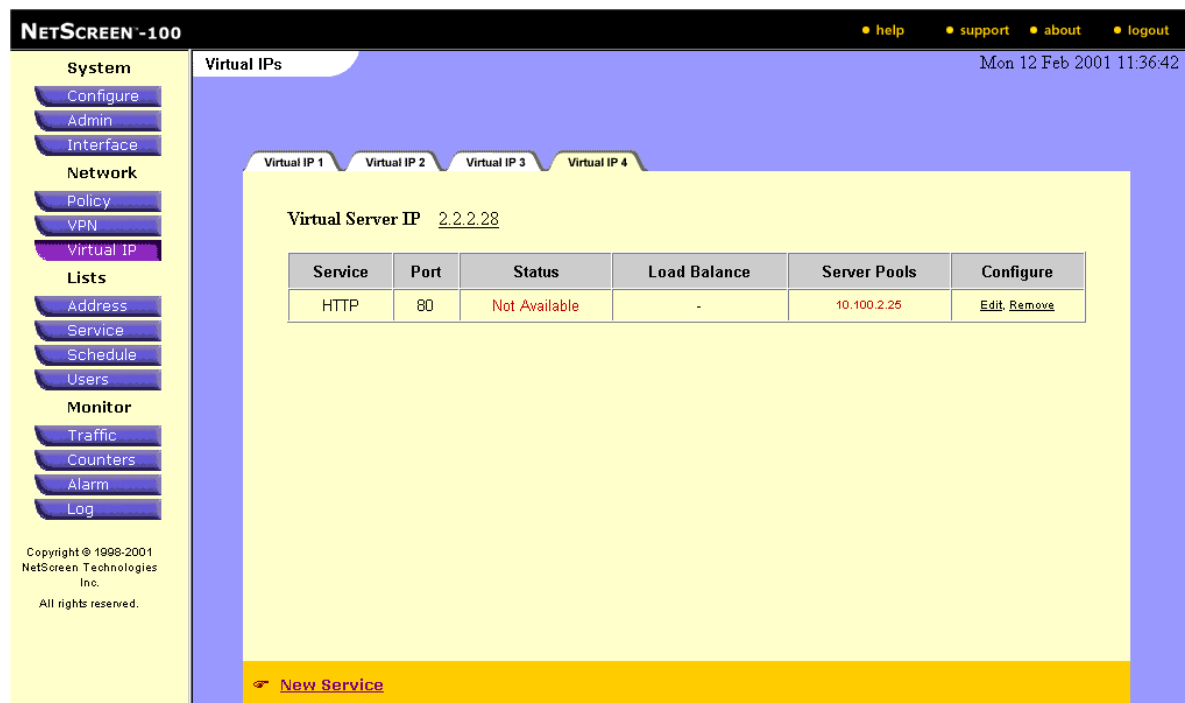


Figure 2-49 Virtual IP >> Virtual IP4

Virtual IP 4

You can configure up to eight services per Virtual IP for a NetScreen-100 or NetScreen-1000. However, you can only map one service at a time. In other words, you will need to complete the New Service page up to eight times per Virtual IP address for a NetScreen-100 or NetScreen-1000.

To configure Virtual IP 4, with or without load balancing:

1. Click the **Virtual IP 4** tab.
2. Click the link, **click here to configure...**, to configure it. The Virtual IP Configuration dialog box appears.

Note: Setting the IP address to 0.0.0.0 or clicking the **clear** button on the Virtual IP Configuration dialog box clears the IP address.

3. Enter the public IP address to be mapped from the Untrusted interface to the Trusted or DMZ interface, and click **OK**. This Virtual IP address must be in the same subnet as the Untrusted port interface IP.
4. Define the service to be mapped by clicking the **New Service** link at the bottom of the Virtual IP page.

5. Enter the necessary information:

Virtual IP Field	Description
Virtual Port	The port that the service should be mapped to on the outside server. The user can use standard port numbers or use other port numbers. If non-standard port numbers are used, reconfiguration of the server may be required.
Service	Choose a service from the drop-down list for the server generating the connection. Available services include those with a fixed port and user-defined custom services.
Load Balance	If more than one server is defined, select the method of distributing the load balance between the inside servers: None, Round Robin, Weighted Round Robin, Least Connections, or Weighted Least Connections. Selecting None disables load balancing and only mapping will be applied to the first IP defined.
Server IP	Enter the IP address of the inside servers (on the Trusted or DMZ network) that will process the requests. An IP address of 0.0.0.0 indicates that no inside server is present. You can define up to eight servers. Note: If only one server is defined, then the IP address and service will map directly and no load balancing will be done.
Server Weight	The weight factor represents the number of requests to be sent to a machine before they are re-routed to the next machine. In general, the server with the larger weight takes the heavier load of requests to process. Here is an example of the Weighted Round Robin method: if Server A has a weight of 10, Server B has a weight of 5, and Server C has a weight of 2, then the first 10 requests are sent to Server A, the next 5 requests are sent to Server B, and the next 2 requests to Server C, the next 10 requests once again to Server A, and so on. This field accepts a range of values from a minimum of 0 through a maximum of 1000. The higher the value, the greater the load-handling capacity of that specific inside server. A 0 indicates that load balancing on that server has been disabled.

6. Click **OK** to save the settings.

For the NetScreen-100, you can configure up to eight services per Virtual IP. For the NetScreen-100, you can configure one service per Virtual IP. However, you can only map one service at a time. In other words, you will need to complete the New Service page up to eight times (for a NetSpeed-100) or once (for a NetSpeed-1000) per Virtual IP address.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

Lists

3

This chapter describes the WebUI pages grouped under Lists in the menu column. The main sections and their subsections are as follows:

- Address
 - Trusted
 - Untrusted
 - DMZ (NetScreen-5 and -10 only)
- Service
 - Pre-defined
 - Custom
- Schedule
 - Configuration
 - New Schedule
- Users
 - Users
 - Dialup Group

ADDRESS >> TRUSTED | UNTRUSTED | DMZ (DMZ PORT FOR NETSCREEN-5 AND -10 ONLY)

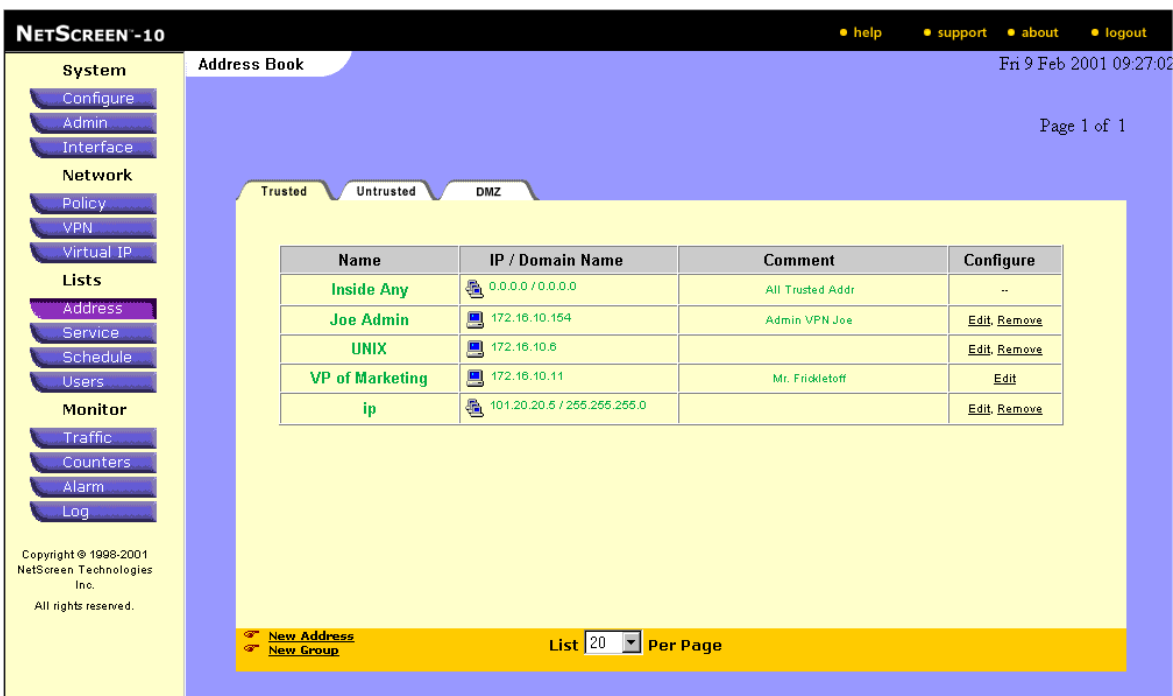


Figure 3-1 Lists >> Address >> Trusted

The NetScreen device classifies all other devices by types of addresses. Before you can set up any of the other NetScreen device firewall features, you need to define the address book. The address book contains the IP addresses of hosts that can have their traffic either be allowed, blocked, encrypted, or user-authenticated. The default IP address 0.0.0.0 is used for all inside and all outside traffic.

Addresses

For further information regarding addresses, consult the NetScreen Concepts & Examples ScreenOS Reference Guide.

Viewing the Address Book

Clicking on a tab will bring that tab to the front, enabling you to view the addresses defined for the Trusted port, Untrusted port, and DMZ port.

The address book always displays the Trusted and Untrusted tabs. The DMZ tab will only be visible if you have configured the DMZ interface.

Address Field	Description
Trusted addresses	Individual IP addresses or subnets which are located behind the port labeled Trusted on the NetScreen device. These entries appear in green on your screen.
Untrusted addresses	Individual IP addresses or subnets which are located behind the port labeled Untrusted. These entries appear in red on you screen.
The DMZ addresses	Individual IP addresses which are located behind the port labeled DMZ. These entries appear in a rust color on your screen.

Individual hosts have only a single IP address defined and are represented with a single computer icon. Networks are represented with multiple computer icons.

ADDRESS >> EDIT GROUP

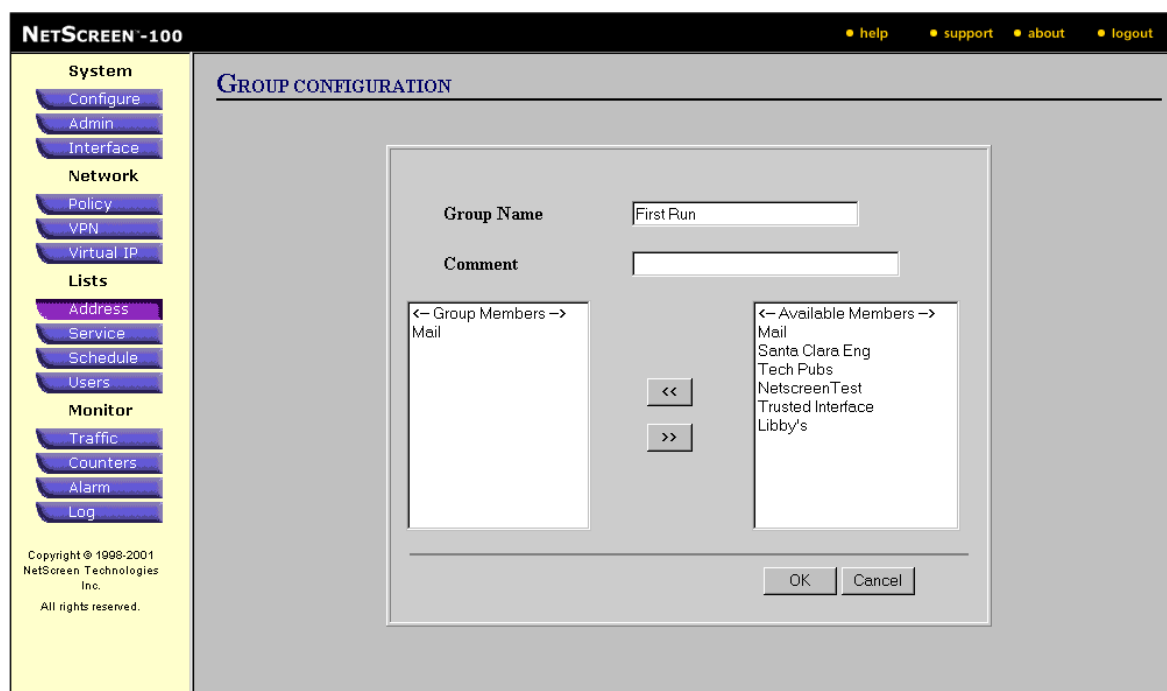


Figure 3-2 Addresses >> Edit Group

Modify Address Group

To modify an existing address group:

1. Click a tab to choose the **Trusted**, **Untrusted**, or **DMZ** port.
2. In the Configure column of the address group you want to modify, click **Edit**.

The Group Configuration dialog box appears.

3. Select the group members from the addresses you have created. Group members are located in the "Available" field on the right-hand side of the Group Configuration page.

To move each selection from the Available field to the Group Members field, click the << button between frames. You can remove group members by clicking the >> button.

Note: Remember that the address name must be unique. Once you have defined an address and it is referenced by an access Policy, you can change the address name but not its port type from Trusted to Untrusted or DMZ or vice versa. To change its port type, you must first remove the underlying access Policy.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

ADDRESS >> REMOVING ADDRESS ENTRIES

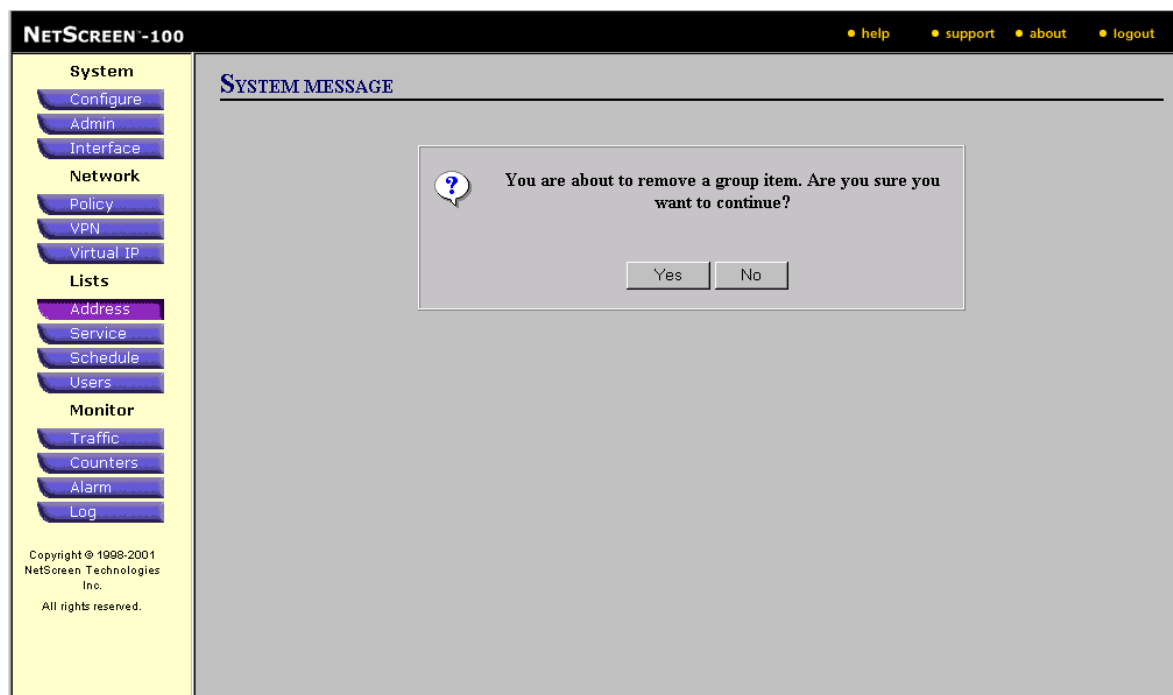


Figure 3-3 Address >> Remove Address

Remove Address Entry

To remove an existing address or group entry:

1. Click a tab to choose the **Trusted**, **Untrusted**, or **DMZ** port.
2. In the Configure column of the address or group you want to delete, click **Remove**.
3. Click **Yes** to confirm removal, or **No** to cancel.

Note: You cannot remove an address or group referenced by an Access Policy until you remove the underlying Access Policy first.

ADDRESS >> CREATING ADDRESS GROUPS

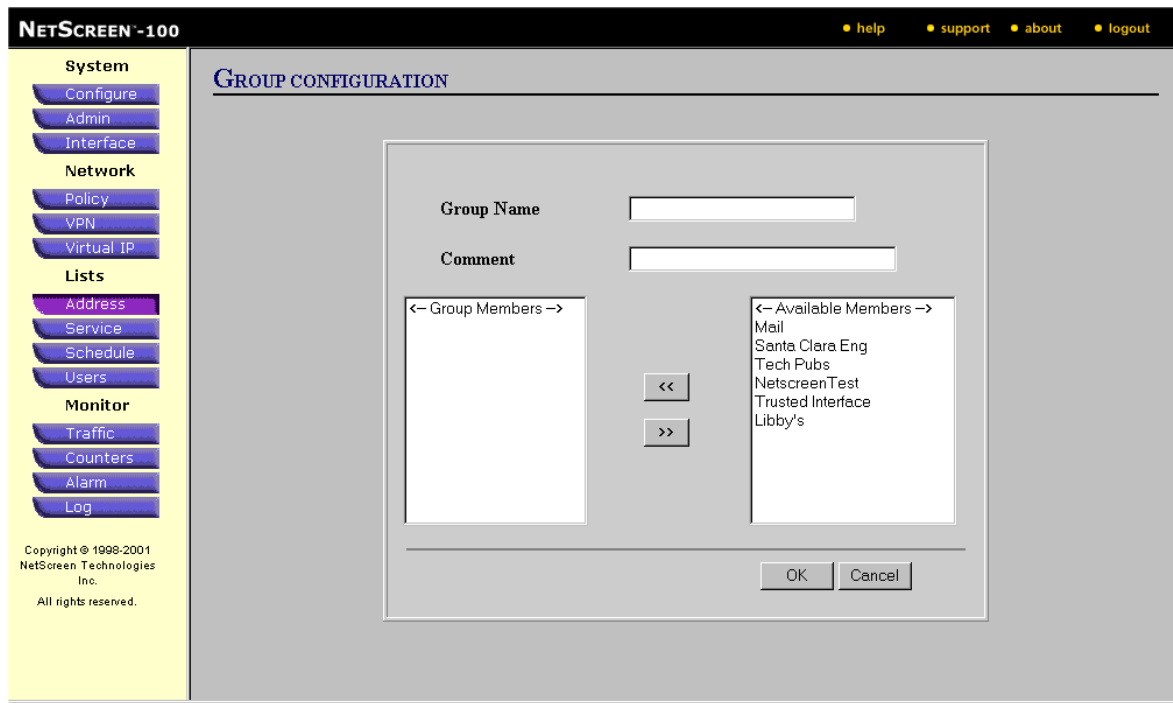


Figure 3-4 Address >> New Address Group

Create Address Group

Groupings allow you to group a number of addresses for use in policies. When grouped, changes to the group effect all the members of the group.

Address Groups

For further information regarding address groups, consult the NetScreen Concepts & Examples ScreenOS Reference Guide.

To create an address group, do the following:

1. Click the **New Group** choice shown in the lower left corner of the Address Book page.
The Group Configuration dialog box appears.
2. Name your new group by filling in the Group Name field.
3. Entries in the Comment field are optional.
4. Select the group members from the addresses you have created. Group members are located in the "Available" field on the right side of the Group Configuration dialog box.

5. To move each selection from the Available field to the Group Members field, click the << button between frames. You can remove group members by clicking the >> button.
6. Click **OK** to save your changes and return to the address book, which now contains your new address group.

When you click the drop-down list under Source Address or Destination Address in the Policy Configuration dialog box, the new address group appears at the bottom of the list.

Note: NetScreen can display entries 5, 10, 20, 50, 100 or all at one time.

The following table lists the group size limits for each platform:

Hardware Platform	Number of Groups	Members per Group
NetScreen-5	16	16
NetScreen-10	32	32
NetScreen-100	64	64
NetScreen-1000	256	256

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

ADDRESS >> TRUSTED | UNTRUSTED | DMZ >> NEW ADDRESS

The screenshot shows the NetScreen-100 web interface. On the left is a navigation menu with categories: System (Configure, Admin, Interface), Network (Policy, VPN, Virtual IP), Lists (Address, Service, Schedule, Users), and Monitor (Traffic, Counters, Alarm, Log). The main area is titled 'ADDRESS CONFIGURATION'. A dialog box is open with the following fields: 'Address Name' (empty), 'IP Address/Domain Name' (0.0.0.0), 'Netmask' (255.255.255.0), 'Comment' (empty), and 'Location' with radio buttons for Trust (selected), Untrust, and DMZ. 'OK' and 'Cancel' buttons are at the bottom right of the dialog. At the bottom left of the interface, there is copyright information: 'Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.'

Figure 3-5 Address >> Trusted | Untrusted | DMZ >> New Address

Adding to the Address Book

You must add each new address to one of three address tabs---Trusted, Untrusted, or DMZ---based on which of the NetScreen device's interfaces provides access to that address.

To add an individual address or range of addresses:

1. Click a tab to choose the **Trusted**, **Untrusted**, or **DMZ** port.
2. Click **New Address**. The Address configuration page appears.
3. Enter values for the following parameters:

Address Field	Description
Address Name	The descriptive name that will appear in the drop-down menu when you configure access policies, etc. Choose one that helps you easily identify the address. The name must be unique and is limited to 22 characters.

Address Field	Description
IP Address/Domain Name	<p>IP address of a network device.</p> <p>Here you have the option of using either a 4-octet numeric address (with a netmask) or a domain name expressed as a Web URL (Uniform Resource Locator). Web URLs are textual addresses that are translated into correlating IP addresses through DNSs (Domain Name Servers, that is, dedicated translation computers). To be able to use a domain name in this field, you must already have set up for DNS service on the Configure >> DNS tab.</p>
Netmask	<p>The netmask address, combined with the IP address, can specify a range of addresses. For example, for the IP address 201.2.3.4, a netmask address of 255.255.255.0 specifies a range of addresses from 201.2.3.0 to 201.2.3.255. Alternatively, for an IP address 201.2.3.4, a netmask address of 255.255.255.255 specifies just 201.2.3.4.</p>
Comment	<p>Enter any additional information here; limited to 31 characters.</p>
Location	<p>Location of the IP address relative to the NetScreen device port. By default, Trusted, Untrusted, or DMZ appears selected, depending upon which tab you initially choose on the main Address Book page.</p>

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

SERVICE >> PRE-DEFINED

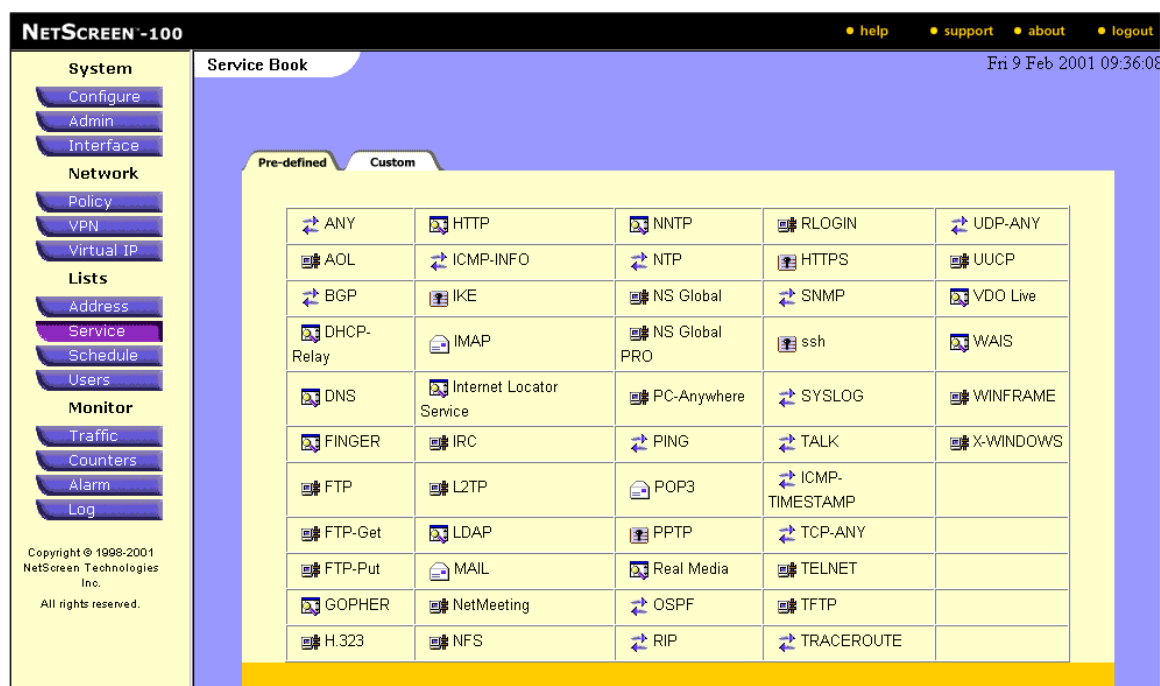


Figure 3-6 Service >> Pre-Defined

Viewing Pre-defined Services






The Service Book has two pages: one for pre-defined services and another for custom services.

Services are types of IP traffic for which protocol standards exist. Every Access Policy has a service associated with it, as well as an address. Each service has a port number associated with it, where the Access Policy accepts a request for that service.

When you create an Access Policy, you must define a service for it. You can select one of the preconfigured services from the Service Book, or select a custom service that you have created. Each Access Policy can reference either a single service, or a service group that you create from pre-defined and/or custom services.

Viewing Pre-defined Services

Each service displays as an icon that represents a classification of service: Remote, E-mail, Info Seeking, Security, or Other. Moving the mouse over any service listing will reveal its definition and standard TCP or UDP port assignment.

Icon	Name	Meaning
	Remote	Various remote connection utilities such as FTP, RLOGIN, and Telnet.
	E-mail	E-mail services such as POP3 and Mail.
	Info Seeking	Information search engines such as HTTP, GOPHER, and DNS.
	Security	Security services such as HTTPS.
	Other	Miscellaneous utilities such as ICMP, SNMP, TCP-ANY, and Syslog.

To view different types of services in the book, move the pointer over the icons that you want to see.

Viewing Custom Services and Service Groups

If any custom services have been configured, the Custom page will display a list of individual services, as well as a list of service groups.

SERVICE >> CUSTOM

NETSCREEN-100 help support about logout

Service Book

Fn 9 Feb 2001 09:55:00

Page 1 of 2

Pre-defined Custom

Custom Defined Services

Group Name	Members	Comment	Configure
Hikers	GOPHER, FTP-Get, FTP, ...	for those who want to leave hom	Edit , Remove
Com	FTP-Put, IMAP, POP3, MAIL	services for communication	Edit , Remove
group3	BGP, FTP, GOPHER		Edit , Remove
group4	FTP-Get, FINER, FTP		Edit , Remove
group5	H.323, ICMP-INFO		Edit , Remove
group6	BGP, DNS		Edit , Remove
group7	FTP-Put, FTP		Edit , Remove
group8	H.323, GOPHER		Edit , Remove
group9	NetMeeting, MAIL		Edit , Remove

Copyright © 1998-2001
NetScreen Technologies
Inc.
All rights reserved.

[New Service](#) [New Group](#) < 1 2 > [Next](#)

Figure 3-7 Service >> Custom

Custom Services

To add a configuration to the Service Book, click **New Service** at the bottom of the page. The Service Configuration page appears

Custom Parameter	Description
Group Name	The name of the custom group.
Members	The services in the custom group.
Comment	Notes regarding the group.
Configure	Click Edit to revise the service, or Remove to remove it.

To create a new service, click on **New Service**. To create a new group, click **New Group**.

SERVICE >> CUSTOM >> NEW

NETSCREEN-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

SERVICE CONFIGURATION

Service Name

No	Source Port		Destination Port		Transport
	Low	High	Low	High	
1	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other <input type="text" value="6"/>
2	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other <input type="text" value="6"/>
3	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other <input type="text" value="6"/>
4	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other <input type="text" value="6"/>
5	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other <input type="text" value="6"/>
6	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other <input type="text" value="6"/>
7	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other <input type="text" value="6"/>
8	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other <input type="text" value="6"/>

OK Cancel

Figure 3-8 Service >> Custom

Adding a Custom Service

To add a Custom Service:

1. To add a configuration to the Service Book, click **New Service** at the bottom of the page. The Service Configuration page appears.
2. Enter values for the following parameters:

Parameter	Description
Service Name	A name to identify the new service. This name is used in Policies that use this service.
Transport	The protocol used for transporting the traffic. This can be a TCP-based service or UDP-based service. You can also designate Other. (For this option, specify the protocol by inserting its protocol number.)

Parameter	Description
Source Port	The low and high ranges of internal port numbers valid for the service.
Destination Port	The low and high ranges of external port numbers that receive the service request.

3. To save the addition, click **OK**.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

SERVICE >> CUSTOM >> EDIT

NetScreen-100

• help • support • about • logout

System

- Configure
- Admin
- Interface

Network

- Policy
- VPN
- Virtual IP

Lists

- Address
- Service
- Schedule
- Users

Monitor

- Traffic
- Counters
- Alarm
- Log

Copyright © 1999-2001
NetScreen Technologies
Inc.
All rights reserved.

SERVICE CONFIGURATION

Service Name:

No	Source Port		Destination Port		Transport		
	Low	High	Low	High			
1	<input type="text" value="0"/>	<input type="text" value="65535"/>	<input type="text" value="0"/>	<input type="text" value="65535"/>	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP <input type="radio"/> Other	<input type="text" value="6"/>
2	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP <input type="radio"/> Other	<input type="text" value="6"/>
3	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP <input type="radio"/> Other	<input type="text" value="6"/>
4	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP <input type="radio"/> Other	<input type="text" value="6"/>
5	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP <input type="radio"/> Other	<input type="text" value="6"/>
6	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP <input type="radio"/> Other	<input type="text" value="6"/>
7	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP <input type="radio"/> Other	<input type="text" value="6"/>
8	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP <input type="radio"/> Other	<input type="text" value="6"/>

OK Cancel

Figure 3-9 Service >> Custom >> Edit

Modifying a Custom Service

You can edit or delete existing user-defined Custom service entries by using the Configure feature.

Note: You cannot modify or remove any of the pre-defined services.

Custom service groups

For further information regarding custom service groups, consult the NetScreen Concepts & Examples ScreenOS Reference Guide.

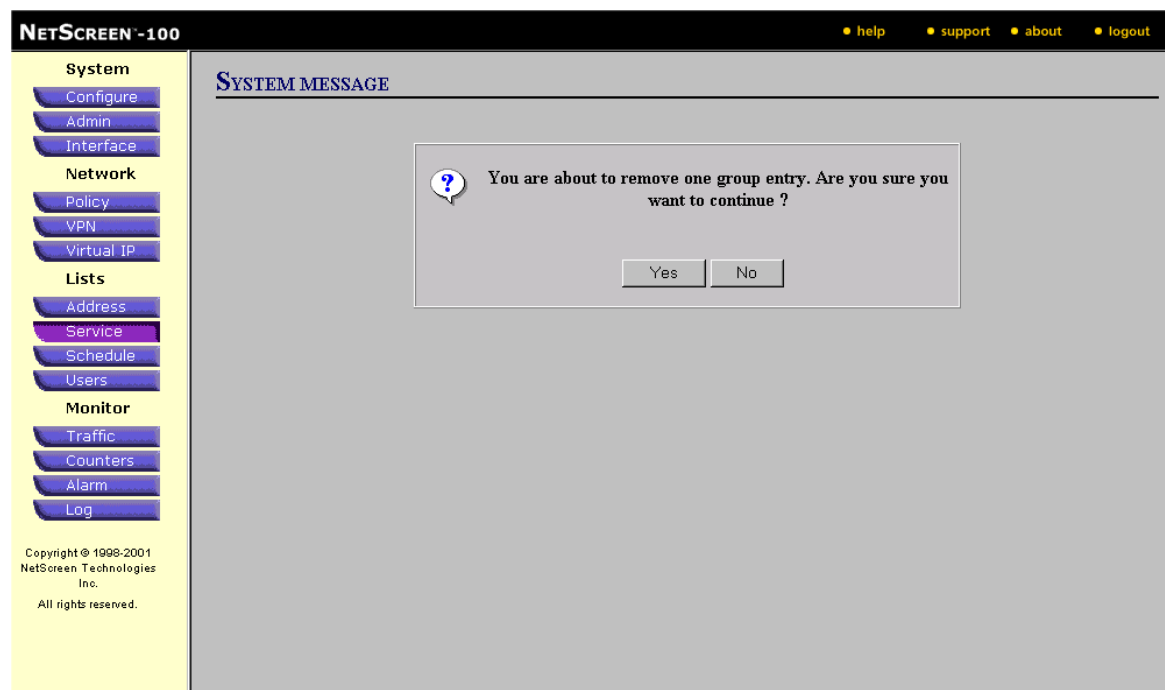
To modify an existing user-defined service entry:

1. In the Configure column, click **Edit** for the service that you want to modify.
The Service Configuration page appears.
2. Type in the new service information in the fields.
3. To save the new service information, click **OK**.

OK and Cancel

Click **OK** put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

SERVICE >> CUSTOM >> REMOVE

**Figure 3-10** Service >> Custom >> Remove

Removing a Custom Entry

To remove an existing service entry:

1. Click **Remove** for the service that you want to delete.
2. Click **Yes** to confirm removal, or **No** to cancel.

Yes and No

Click **Yes** to put your changes into effect and save your configuration to flash memory. Click **No** to undo any changes that you have made but have not yet applied.

SERVICE >> CUSTOM >> NEW GROUP

NETSCREEN-100 help support about logout

System

- Configure
- Admin
- Interface

Network

- Policy
- VPN
- Virtual IP

Lists

- Address
- Service
- Schedule
- Users

Monitor

- Traffic
- Counters
- Alarm
- Log

Copyright © 1998-2001
NetScreen Technologies
Inc.
All rights reserved.

GROUP CONFIGURATION

Group Name:

Comment:

<-- Group Members -->

<< >>

<-- Available Members -->

- AOL
- BGP
- DHCP-Relay
- DNS
- FINGER
- FTP
- FTP-Get
- FTP-Put
- GOPHER
- H.323
- HTTP

OK Cancel

Figure 3-11 Service >> Custom >> New Group**Adding a Service Group:**

1. Click **New Group** to add a configuration to the Custom Service Book. The Group Configuration page appears.
2. Fill out the Group Name field with a name of your choice.
3. Entries in the Comment field are optional.
4. From the list of available services (which includes all predefined services and any custom services you may define) select the service you want to include in the service group and click the << button. You can remove services from the group by clicking the >> button.

Click the **OK** button when you have completed your selections. Your new group displays at the top of the Custom Service Book tab.

The follow table lists the number of Service Groups supported by each platform.

Note: The number of Service Groups supported refers to the total number of address and service groups (including trust, untrust and DMZ).

Hardware Platform	Number of Service Groups
NetScreen-5	16
NetScreen-10	32
NetScreen-100	64
NetScreen-1000	256

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

SERVICE >> NEW SERVICE

NETSCREEN-100

helpsupportaboutlogout

System

ConfigureAdminInterface

Network

PolicyVPNVirtual IP

Lists

AddressServiceScheduleUsers

Monitor

TrafficCountersAlarmLog

Copyright © 1998-2001
NetScreen Technologies
Inc.
All rights reserved.

SERVICE CONFIGURATION

Service Name

No	Source Port		Destination Port		Transport	
	Low	High	Low	High		
1	0	0	0	0	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	6
2	0	0	0	0	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	6
3	0	0	0	0	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	6
4	0	0	0	0	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	6
5	0	0	0	0	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	6
6	0	0	0	0	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	6
7	0	0	0	0	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	6
8	0	0	0	0	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	6

OKCancel

Figure 3-12 Service >> New Service

Adding a Custom Service:

- 1. Enter the values for the following parameters:

Service Field	Description
Service Name	A name to identify the new service. This name will be available from a Service drop-down menu when you create an Access Policy.
Source Port	A range of internal port numbers valid for that service.
Destination Port	A range of external port numbers that will receive the service request.

Service Field	Description
Transport	A pre-defined number for the protocol used; TCP-based service or UDP-based service. You may also designate Other (For this option, specify protocol by inserting its standardized protocol number).

2. Click the **OK** button to save the addition.

SERVICE >> NEW GROUP

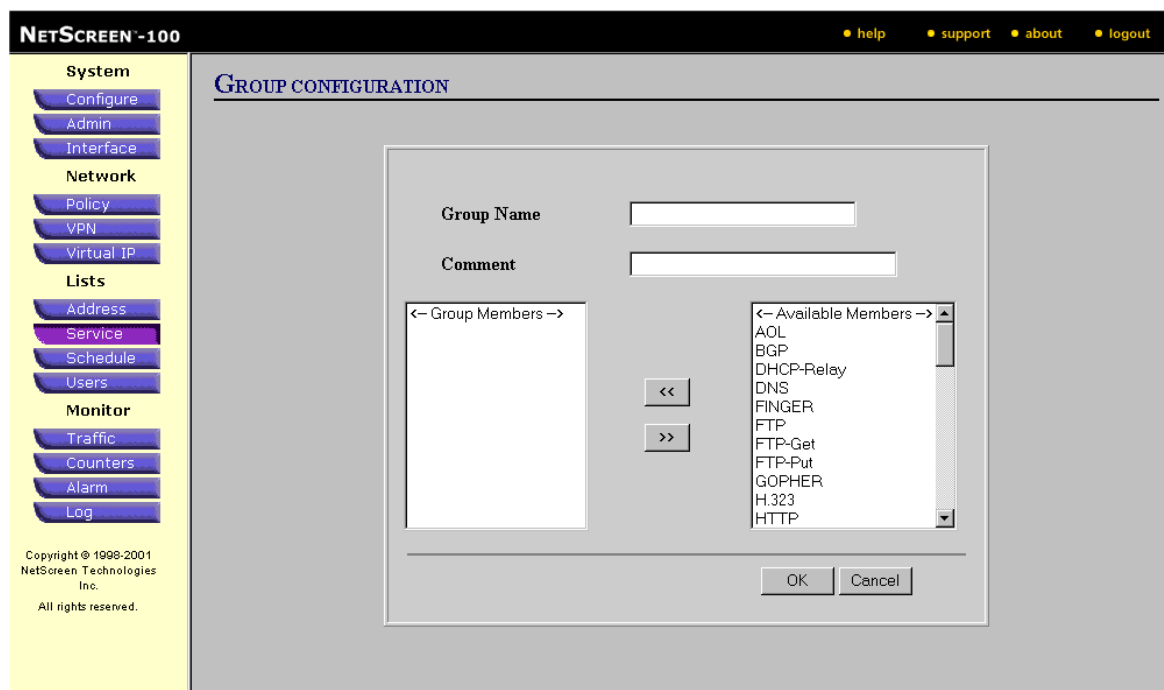


Figure 3-13 Service >> New Group

Configure a New Group

Groupings allow you to group a number of addresses or groups together for use in policies. When grouped, changes to the group affect all the members of the group.

New Group Configurations

For further information regarding new group configurations, consult the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

To create an address group, do the following:

1. Click the **New Group** choice shown at the lower left corner of the address book.
The Group Configuration dialog box appears
2. Name your new group by filling in the Group Name field.
3. Entries in the Comment field are optional.
4. Select the group members from the addresses you have created.

Group members are located in the "Available" field on the right-hand side of the Group Configuration page.

5. To move each selection from the Available field to the Group Members field, click the << button between frames. You can remove group members by clicking the >> button.

When you open the drop-down list under Source Address in the Policy Configuration dialog box, the new address group appears at the bottom of the list.

The following table lists the group size limits for each platform.

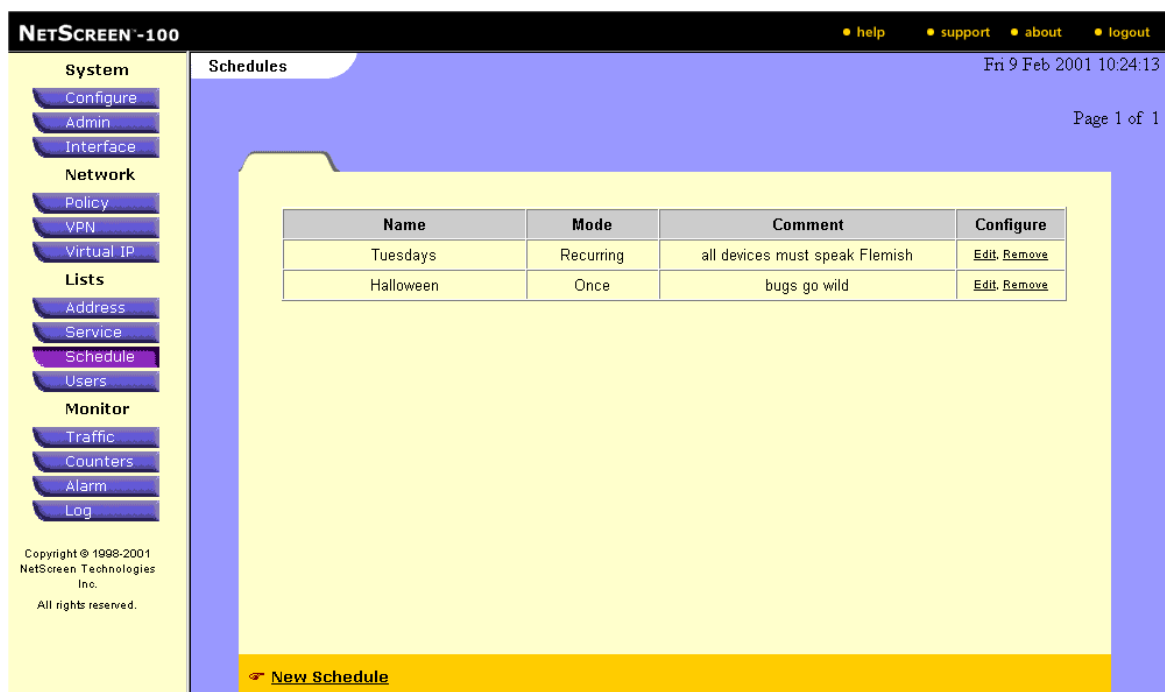
Note: The number of Service Groups supported refers to the total number of address and service groups (including trust, untrust and DMZ).

Hardware Platform	Number of Groups	Members per Group
NetScreen-5	16	16
NetScreen-10	32	32
NetScreen-100	64	64
NetScreen-1000	256	256

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

SCHEDULE



NETSCREEN-100 help support about logout

System Schedules Fri 9 Feb 2001 10:24:13

Page 1 of 1

Name	Mode	Comment	Configure
Tuesdays	Recurring	all devices must speak Flemish	Edit Remove
Halloween	Once	bugs go wild	Edit Remove

[New Schedule](#)

Copyright © 1998-2001
NetScreen Technologies
Inc.
All rights reserved.

Figure 3-14 Schedules

Viewing Schedule Detail

Schedules are used to limit when an Access Policy is in effect, and to set traffic control policies. Configurable as separate objects, schedules can be set on either a recurring or one-time basis and associated with any number of Access Policies.

Viewing the Schedule Book

All available schedule entries display on the Schedule page. Each entry lists the name assigned to a schedule and the mode (whether it is recurring or a one-time event). In addition, you can add comments.

SCHEDULE >> EDIT

NETSCREEN-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.

SCHEDULE CONFIGURATION

Schedule Name:

Comment:

☒ **Recurring** (hh:mm)

Week Day	Period 1		Period 2	
	Start Time	End Time	Start Time	End Time
Sunday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Monday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Tuesday	08:00	12:00	13:30	17:00
Wednesday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Thursday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Friday	12:01	14:31	<input type="text"/>	<input type="text"/>
Saturday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

☐ **Once**

Start Date and Time: (mm/dd/yyyy hh:mm)

Stop Date and Time: (mm/dd/yyyy hh:mm)

OK Cancel

Figure 3-15 Schedule >> Edit

Modifying a Schedule

To modify an existing schedule entry:

1. On the Schedule page, click **Edit** for the schedule that you want to modify.
 The Schedule Configuration dialog box appears.
2. Type in the new schedule information in the corresponding fields.
3. To save the new schedule information, click **OK**.

SCHEDULE >> REMOVE

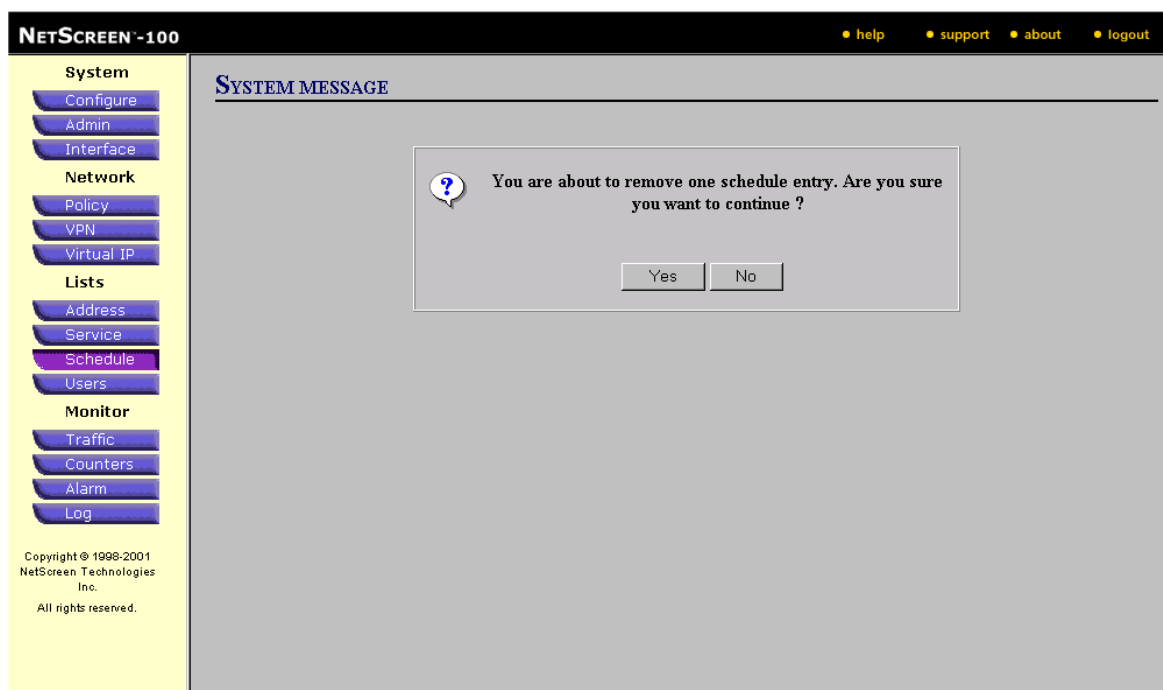


Figure 3-16 Schedule >> Remove

Removing a Schedule

To remove an existing schedule entry:

1. Click **Remove** for the schedule that you want to remove on the Schedule page.
2. Click **Yes** to confirm removal, or **No** to cancel.

Note: You cannot remove a schedule if it is referenced by an Access Policy. You must first remove it from the Access Policy.

SCHEDULE >> NEW SCHEDULE

NETSCREEN-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

SCHEDULE CONFIGURATION

Schedule Name

Comment

☒ **Recurring (hh:mm)**

Week Day	Period 1		Period 2	
	Start Time	End Time	Start Time	End Time
Sunday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Monday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Tuesday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Wednesday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Thursday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Friday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Saturday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

☐ **Once**

Start Date and Time (mm/dd/yyyy hh:mm)

Stop Date and Time (mm/dd/yyyy hh:mm)

OK Cancel

Figure 3-17 Schedule >> New Schedule

Adding a Schedule

1. Enter values for the following fields:

Schedule Field	Description
Schedule Name	The name that appears in the Configuration window. The name must be unique and is limited to 19 characters.
Comment	Any additional information you want to add, limited to 63 characters.
Recurring	Enable this when you want the schedule to repeat on a weekly period. You must configure both a start time and a stop time. You can specify up to two time periods within the same day.

Schedule Field	Description
Once	Enable this when you want the schedule to start and end one time only. You must enter both start and stop date and times. Make sure that you enter all four digits of the year.

2. To add the schedule, click **OK**.

USERS >> USER LIST

NETSCREEN-100 help support about logout Wed 14 Mar 2001 09:11:20

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

User List Page 1 of 1

Users **Dialup Group**

Name	Type	Group	Status	Identity/Cipher	Local SPI	Remote SPI	Configure
Laurel	auth	-	Enabled	-	-	-	Edit , Remove
Roger	auth	-	Disabled	-	-	-	Edit , Remove
Oscar	manual	-	-	ESP / DES	3880	4880	Edit , Remove
Mick	manual	A-1 Team	-	ESP / DES	3bb2	3cc2	Edit
Patricia	manual	belly-mo	-	ESP / DES	45dd	dd45	Edit
Yuki	l2tp,auth	field-sales	Enabled	-	-	-	Edit
Thomas	auth	-	Enabled	-	-	-	Edit , Remove
adam	l2tp,auth	field-sales	Enabled	-	-	-	Edit
betty	l2tp	field-sales	Disabled	-	-	-	Edit
carol	l2tp	field-sales	Disabled	-	-	-	Edit
Elly	ike,l2tp,auth	-	Disabled	-	-	-	Edit , Remove

[New Manual Key User](#)
[New AUTH/IKE/L2TP User](#)

List Per Page

Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.

Figure 3-18 Users >> User List

Viewing User Details

This page lists the VPN users and users who must authenticate themselves against the internal database. The VPN user is the person using a network host or workstation. Before a user can participate in the VPN, the NetScreen device needs to know some information about them, such as their name and their password.

User Detail

For more information regarding user detail, consult the *NetScreen Concepts & Examples ScreenOS Reference Guide*

Configuration Field	Description
User Name	This is the name assigned the remote user.
Type	This field specifies whether the member is an Authentication User, IKE User, L2TP User or Manual Key User.

Configuration Field	Description
Status	If the user is an Authentication user, the status will be either Enabled or Disabled, as specified in the profile. Otherwise, this column will be blank.
User Identity	If the user is an IKE Dynamic Peer, identity is established with an IP address, domain name, or e-mail address. If the user is a VPN Dialup User (Manual Key only), this column specifies the encryption and authentication algorithms.
Local SPI Local Security Index	This number uniquely distinguishes a particular encrypted tunnel from the others being used at the same time. The Local Security Index serves as the other end's Remote Security Index, and vice versa.
Remote SPI Remote Security Index	This number uniquely distinguishes a particular encrypted tunnel from the others being used at the same time.
Configure	Clicking on Edit allows you to change the user profile. Remove is only available if the user is not named in a policy (as either an individual or part of a dialup group).

Note: Users are listed in groups of 5, 10, 15, 20 or all at once.

USERS >> EDIT >> AUTH/IKE/L2TP USER CONFIGURATION

NETSCREEN-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
 Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001
 NetScreen Technologies
 Inc.
 All rights reserved.

USER CONFIGURATION

AUTH/IKE/L2TP User

User Name: User Group:

Status: ☐ Enable ☒ Disable

☐ IKE User
 IKE ID Type: IKE Identity:

☒ Authentication User User Password:

☐ L2TP User Confirm Password:

L2TP Remote Settings

☐ IP Pool: ☐ IP Address:

Primary DNS IP: Primary WINS IP:

Secondary DNS IP: Secondary WINS IP:

OK Cancel

Figure 3-19 Lists >> Users >> Auth/Ike/L2TP User

Modifying User Authentication

To modify an existing remote user configuration:

1. On the User Lists page, in the Configure section, click **Edit** for configuration you want to modify.
2. The User Configuration dialog box appears.
3. Type in the new information in the fields.

Configuration Fields	Description
User Name	User name
User Group	Select from drop-down menu the group the new user is a member of.
Status	Select appropriate button to enable or disable this user's membership in the group.
Authentication User	Select this check box to require the user at the specified source address to provide authentication when the action is set as Permit or Tunnel.

Configuration Fields	Description
L2TP User	Select this check box to configure the user as an L2TP member.
Authentication Password	Password to be provided.
Confirm Password	Confirmation of authentication password.
IKE User	Click to make the user an IKE User.
IKE ID Type	Select ID Type from drop-down menu.
IKE Identity	Enter one of the following: E-mail address (RFC822) IP address (a.b.c.) Fully qualified domain name (FQDN)
Remote Settings	
IP Pool	Click to make the user an IP Pool user. From the drop-down menu, specify which pool the new user will employ.
Primary DNS IP	Name or IP addresses of DNS servers.
Secondary DNS IP	Name or IP addresses of DNS servers.
Primary WINS IP	Name or IP address of Windows Internet Naming Service (WINS) server of the Microsoft Network.
Secondary WINS IP	Name or IP address of Windows Internet Naming Service (WINS) server of the Microsoft Network.

4. To save changes, click **OK**.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

USERS >> EDIT >> MANUAL KEY USER CONFIGURATION

NetScreen-100 help support about logout

System
 Configure
 Admin
 Interface

Network
 Policy
 VPN
 Virtual IP

Lists
 Address
 Service
 Schedule
Users

Monitor
 Traffic
 Counters
 Alarm
 Log

Copyright © 1998-2001 Screen Technologies Inc. All rights reserved.

USER CONFIGURATION

Manual Key User

User Name:

User Group:

Security Index: (Local) (Remote)

☒ **ESP**

Encryption Algorithm:

☒ HEX Key:

☐ Generate Key by Password:

Authentication Algorithm:

☒ HEX Key (16/20 Bytes):

☐ Generate Key by Password:

☐ **AH**

Hash Algorithm:

☒ HEX Key (16/20 Bytes):

☐ Generate Key by Password:

OK Cancel

Figure 3-20 Lists >> Users >> Edit Manual Key User

Modifying User Authentication

To modify an existing remote user configuration:

1. On the User Lists page, in the Configure section, click **Edit** for configuration you want to modify.
2. The User Configuration dialog box appears.
3. Type in the new information in the fields.

Configuration Fields	Description
User Name	New user name
User Group	Select appropriate user group (or select none) from drop down menu.

Configuration Fields	Description
Security Index	(Local/Remote) A security index number that uniquely distinguishes a particular encrypted tunnel from the others being used at the same time. Only a HEX value greater than 3000 is accepted. The Local Security Index serves as the other end's Remote Security Index and vice versa. If you enter "Value_A Value_B", the other end of the tunnel must switch the order of the two components, as in "Value_B Value_A".
ESP	Select either ESP-CBC or AH. Encapsulating Security Payload (ESP) provides both encryption and authentication of an IP packet. Authentication Header (AH) provides authentication only.
Encryption Algorithm	An algorithm used for encryption. You can select either NULL, DES-CBC, 3DES-CBC or 40-bit DES-CBC.
HEX Key	An encryption key for the algorithm specified. Each field of the key is 8 bytes long represented in HEX. (The key is 16 characters long with two characters used to describe one byte in HEX.) For DES, only the left-most value needs to be defined. For 3DES, all three values must be defined.
Generate Key by Password	The NetScreen-100 provides assistance in creating the hex key by allowing a password to define the generation of the hex key. Note: The use of the password feature is a convenience and might lead to similar keys.
Authentication Algorithm	An algorithm used for authenticating the content of the encrypted IP packets. You can leave this field as NULL to omit authentication, or select either MD5 or SHA-1 from the drop-down list.
HEX Key (16/20 Bytes)	A hexadecimal value used to perform the authentication hash algorithm. For MD5, the key must be 16 bytes long. For SHA-1, the key must be 20 bytes long. (Two hexadecimal characters equal one byte.) In the fields to the right of the HEX Key radio button, enter a key with the appropriate length.

Configuration Fields	Description
Generate Key by Password	<p>The NetScreen-100 provides assistance in creating the hex key by allowing a password to define the generation of the hex key.</p> <p>Note: The use of the password feature is a convenience and might lead to similar keys.</p>
AH	<p>Select either ESP-CBC or AH. Encapsulating Security Payload (ESP) provides both encryption and authentication of an IP packet. Authentication Header (AH) provides authentication only.</p>
Hash Algorithm	<p>The hash algorithm is selectable. You can use either MD5 or SHA1. MD5 requires a 16-byte key; SHA1 requires a 20-byte key. In the fields to the right of the HEX Key radio button, enter a key with the appropriate length.</p>
HEX Key (16/20 Bytes)	<p>A hexadecimal value used to perform the authentication hash algorithm. For MD5, the key must be 16 bytes long. For SHA-1, the key must be 20 bytes long. (Two hexadecimal characters equal one byte.) In the fields to the right of the HEX Key radio button, enter a key with the appropriate length.</p>
Generate Key by Password	<p>You can direct the NetScreen-100 to generate a key for your selected hash algorithm based on a password that you enter. If you wish to use this option, select the Generate Key by Password radio button and enter a password in the corresponding field.</p> <p>Note: The use of the password feature is a convenience and might lead to similar keys</p>

4. To save changes, click **OK**.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

USERS >> DIALUP GROUP

NETSCREEN-100

• help • support • about • logout

Wed 14 Mar 2001 14:34:57

Page 1 of 1

System

- Configure
- Admin
- Interface

Network

- Policy
- VPN
- Virtual IP

Lists

- Address
- Service
- Schedule
- Users

Monitor

- Traffic
- Counters
- Alarm
- Log

Copyright © 1998-2001
NetScreen Technologies
Inc.
All rights reserved.

User List

Users Dialup Group

Group Name	Group type	Members	Configure
belly-mo	Manual	Patricia	Edit Remove
field-sales	IKE/L2TP	betty, carol, adam, Yuki	Edit Remove
lily	-	None	Edit Remove
A-1 Team	Manual	Mick	Edit Remove

[New Group](#) List Per Page

Figure 3-21 Users >> Dialup Group

Creating, Viewing, and Removing Dialup Groups

NetScreen devices support the creation of users and groups. You must create a group before you can assign users to it as members. Each dial-up group can only contain one type of user. The policy assigned to a group applies to all group members.

To view information about a dial-up group:

Click **Details** in the row for the group you want to see. The details for the selected group appear.

Note: The Details page replaces the page on the Dialup Group tab. To return to the Dialup Group page, click the Users tab, then the Dialup Group tab.

Note: Dialup Groups are listed in groups of 5, 10, 15, 20 or all at once.

USERS >> DIALUP GROUP >> NEW GROUP

The screenshot shows the NetScreen-100 WebUI interface. On the left is a navigation menu with categories: System (Configure, Admin, Interface), Network (Policy, VPN, Virtual IP), Lists (Address, Service, Schedule, Users), and Monitor (Traffic, Counters, Alarm, Log). The 'Users' item under the 'Lists' category is highlighted. The main content area is titled 'GROUP CONFIGURATION'. It contains a form with a 'Group Name' text field, a 'Group Attribute' section with radio buttons for 'Manual' and 'Remote', and three buttons at the bottom: 'Add members', 'OK', and 'Cancel'. The top of the interface has a black header with 'NETSCREEN-100' and links for help, support, about, and logout. The bottom left of the interface contains copyright information: 'Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.'

Figure 3-22 Users >> Dialup Group >> New Group

To Create a New Dialup Group

1. On the Dialup Group tab, click **New Group**, located at the bottom of the page.
The Dialup Group Configuration box appears.
2. Type a group name in the Dialup Group Name text field.

OK and Cancel

Click **OK** to put your changes into effect and save your configuration to flash memory. Click **Cancel** to undo any changes that you have made but have not yet applied.

USERS >> DIALUP GROUP >> ADD MEMBERS

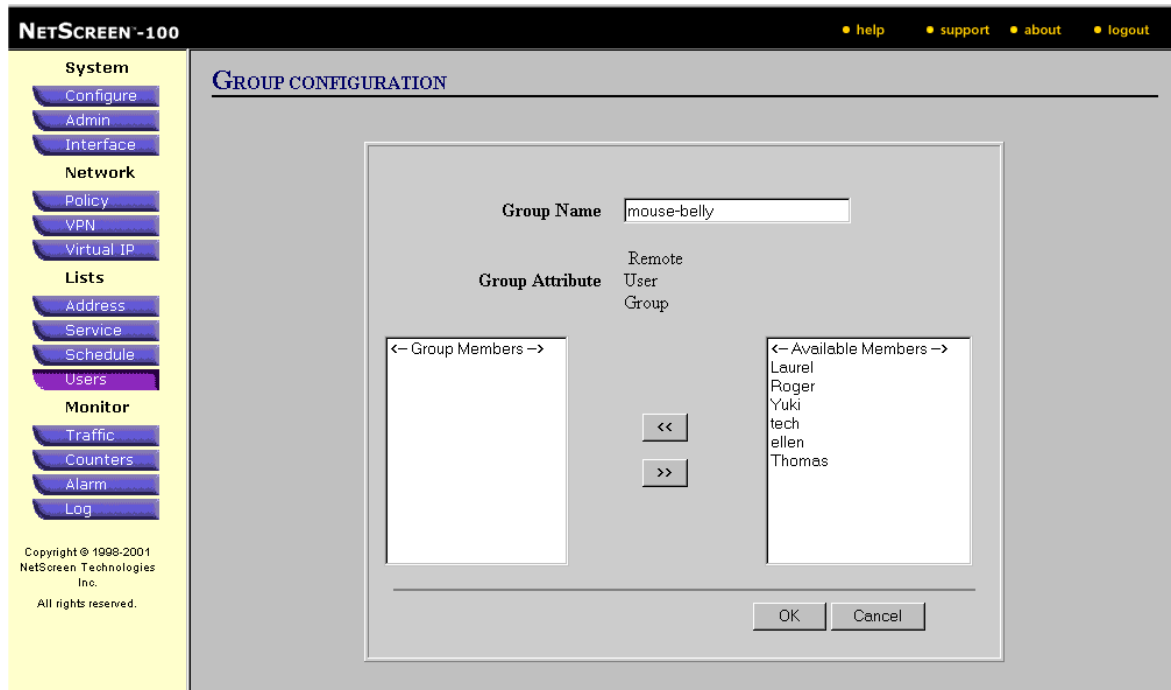


Figure 3-23 Users >> Dialup Group >> Add Members

Adding Members to a Group:

1. In the Group Configuration menu, click **Add Members** to add members to a group. The Group Configuration page appears.
2. From the list of available members, select the members you want to include in the group and click the << button. You can remove members from the group by clicking the >> button.

Click the **OK** button when you have completed your selections. Click **Cancel** to abandon any additions or removals. Your new group displays at the top of the Custom Service Book tab.

USERS >> REMOVE DIALUP GROUP



Figure 3-24 Users >> Remove Dialup Group

Remove a Dialup Group

To remove an existing group:

1. Click **Remove** in the row for the group to be removed.
The System Message appears, asking you to confirm the removal.
2. Click **Yes** to continue with the removal.

Note: *If a group is associated with a policy, it cannot be deleted.*

USERS >> REMOVE USER

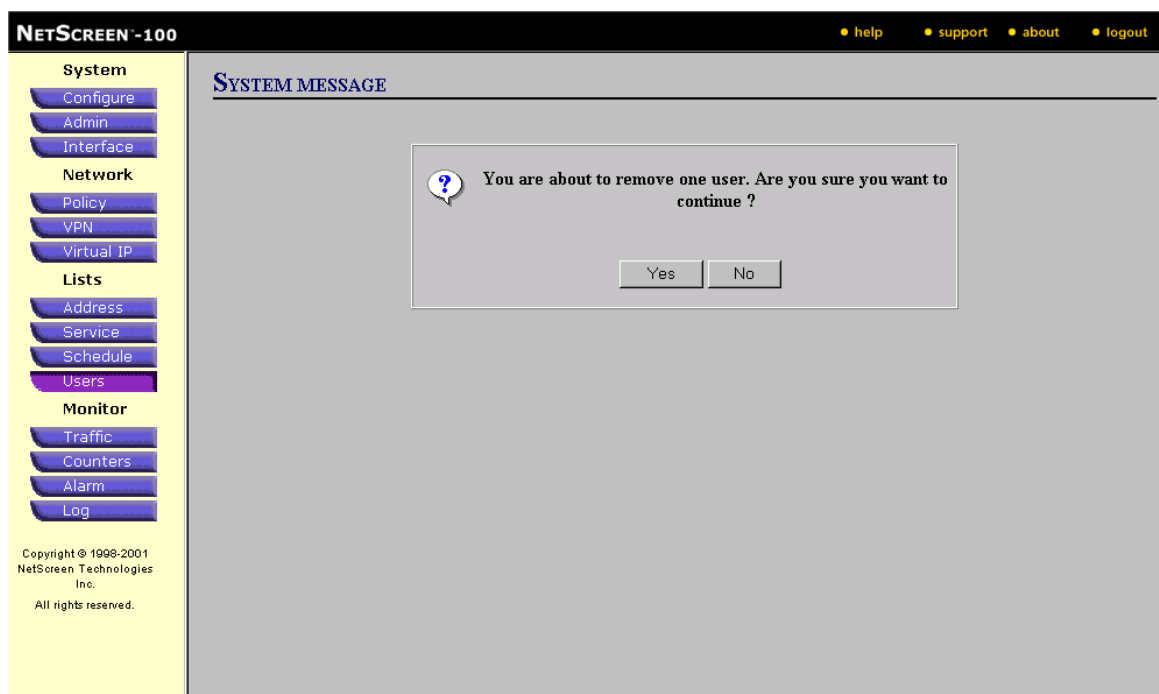


Figure 3-25 User >> Remove User

Remove a Dialup Group User

To remove a member from a dial-up group:

1. Click on the **Users** tab of the User List.
2. For the user that you want to remove from a group, click on **Edit** in the Configure column.
3. In the User Group field, select **None** from the pull-down menu.
4. To save the changes, click **Yes**.

Monitor

4

This chapter describes the WebUI pages grouped under Monitor in the menu column. The main sections and their subsections are as follows:

- Traffic
 - Policy
 - Interface
- Counters
- Alarm
 - Traffic Alarm
 - Event Alarm
- Log
 - Traffic Log
 - Event Log
 - Self Log

TRAFFIC >> POLICY

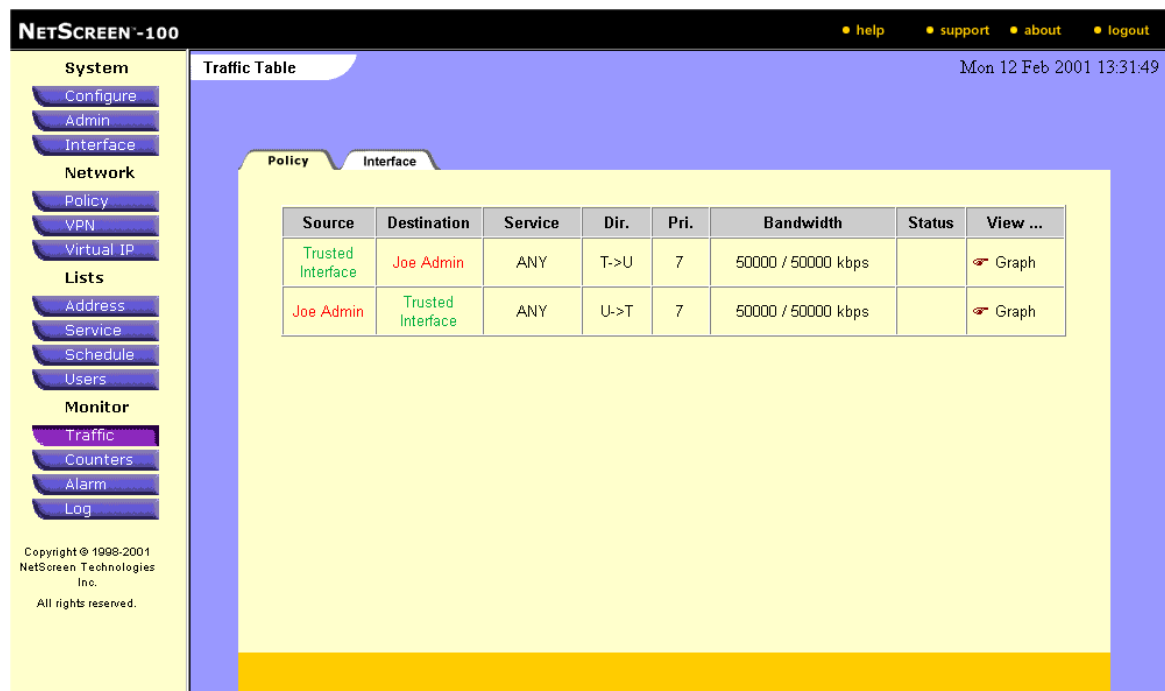


Figure 4-1 Traffic >> Policy

Viewing Traffic Allocation

The NetScreen device monitors your network traffic and connection activity to help you determine if there were any attempts to compromise the security of the network.

Policy Field	Description
Source	The source address of the policy.
Destination	The destination address of the policy.
Service	The type of policy service.
Direction	The direction field indicates whether it is a policy from Trust (T) to Untrust (U), Trust (T) to DMZ (D), Untrust (U) to Virtual IP (V) or other combinations.
Priority	The priority field indicated which level of priority was set in the policy. values are from 0 to 7, with 0 being the highest. If DS Codepoint Marking is enabled, there will be an asterisk to the right of the priority value.

Policy Field	Description
Bandwidth	The bandwidth field shows the guaranteed rate and the maximum rate.
Status	The status of the policy.
View	Click the Graph icon to link to the graph showing current traffic statistics.

TRAFFIC >> POLICY >> GRAPH

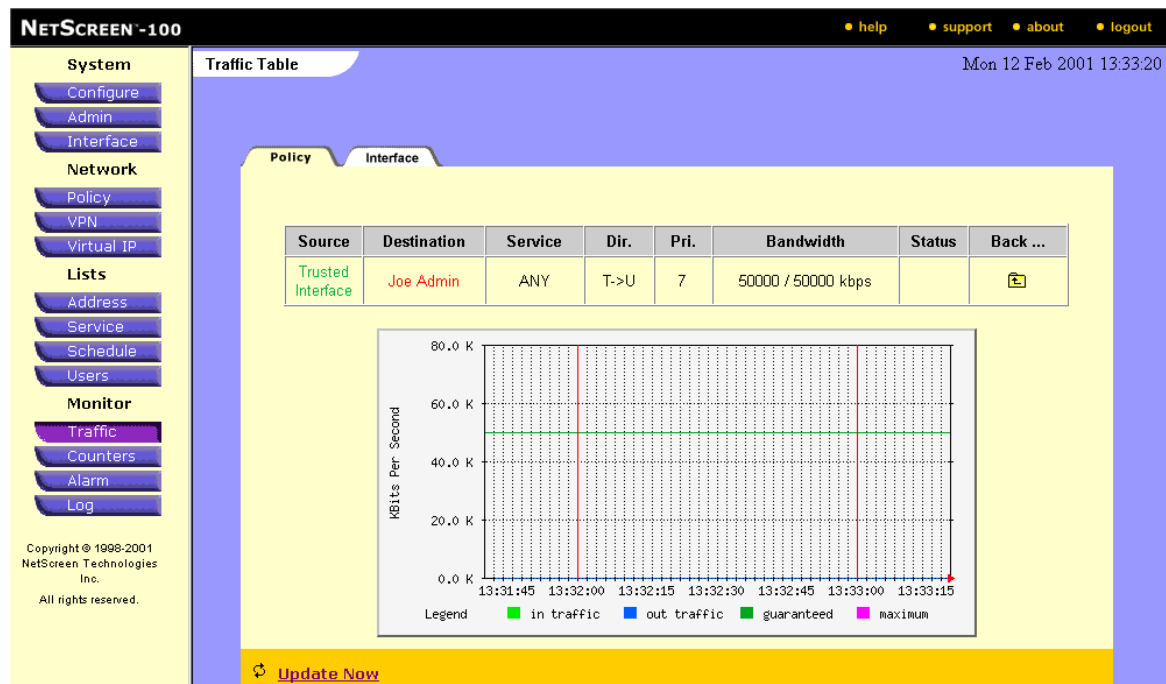


Figure 4-2 Traffic >> Policy >> Graph

Viewing Traffic Graph

To view the Policy traffic allocation:

1. On the NetScreen Administration Tools page, click the **View Graph** button, under Monitor on the left side of the screen.
The Policy Traffic Table page appears.
2. All Policies with traffic shaping enabled are shown on this table. Each Policy is identified by source address, destination address, service type, direction, priority, and traffic setting: The Direction field indicates whether it is a Policy from Trust (T) to Untrust (U), Trust (T) to DMZ (D), Untrust (U) to Virtual IP (V) or other combinations.

The Priority field indicated which level of priority was set in the Policy. Values are from 1 to 8, with 1 being the highest. If DS Codepoint Marking is enabled, there will be an asterisk to the right of the priority value.

The Bandwidth field shows the guaranteed rate and the maximum rate.

The View field has a link to a graph showing current traffic utilization.
3. Click the **Graph** icon to link to the graph of the traffic statistics.

The Traffic table appears.

4. Click **Update Now** to see the current information.

TRAFFIC >> INTERFACE

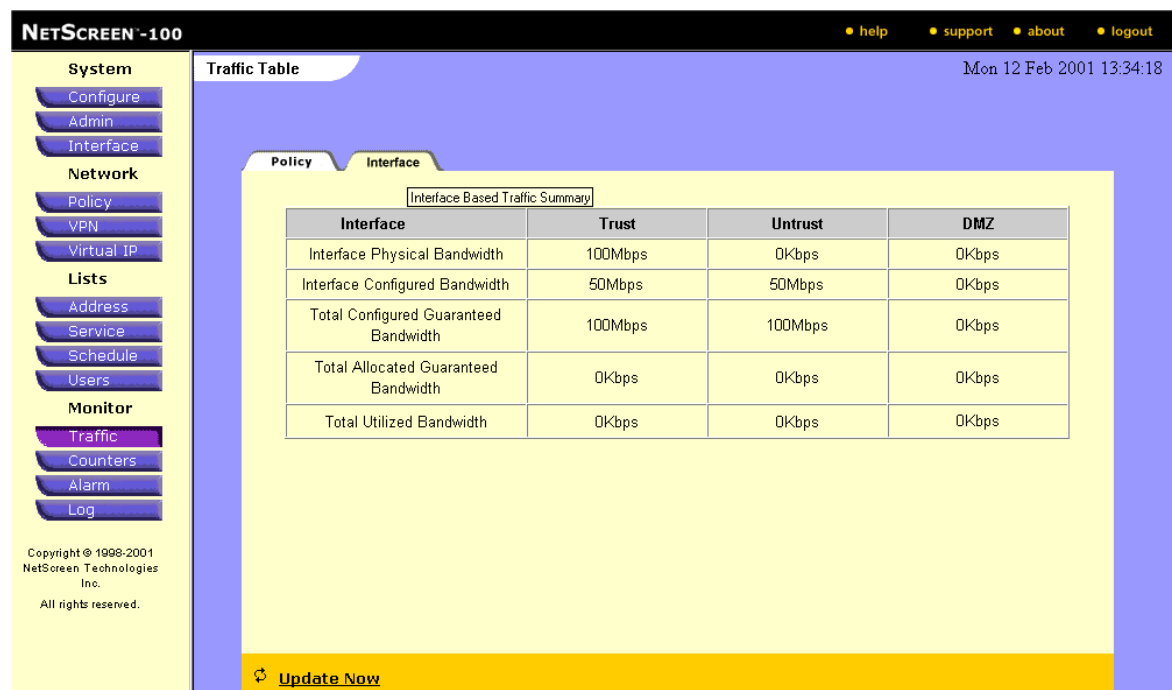


Figure 4-3 Traffic >> Interface

Viewing Interface Traffic Assignment

To view Interface traffic by interface type:

1. Click the **Interface** tab, at the top of the page.
The Interface Traffic Table appears.
2. The Interface Traffic Table shows the physical bandwidth, configured bandwidth, guaranteed bandwidth, and the total utilization bandwidth for NetScreen's Trust, Untrust, and DMZ interfaces.
3. Click **Update Now** to see the current information.

COUNTERS

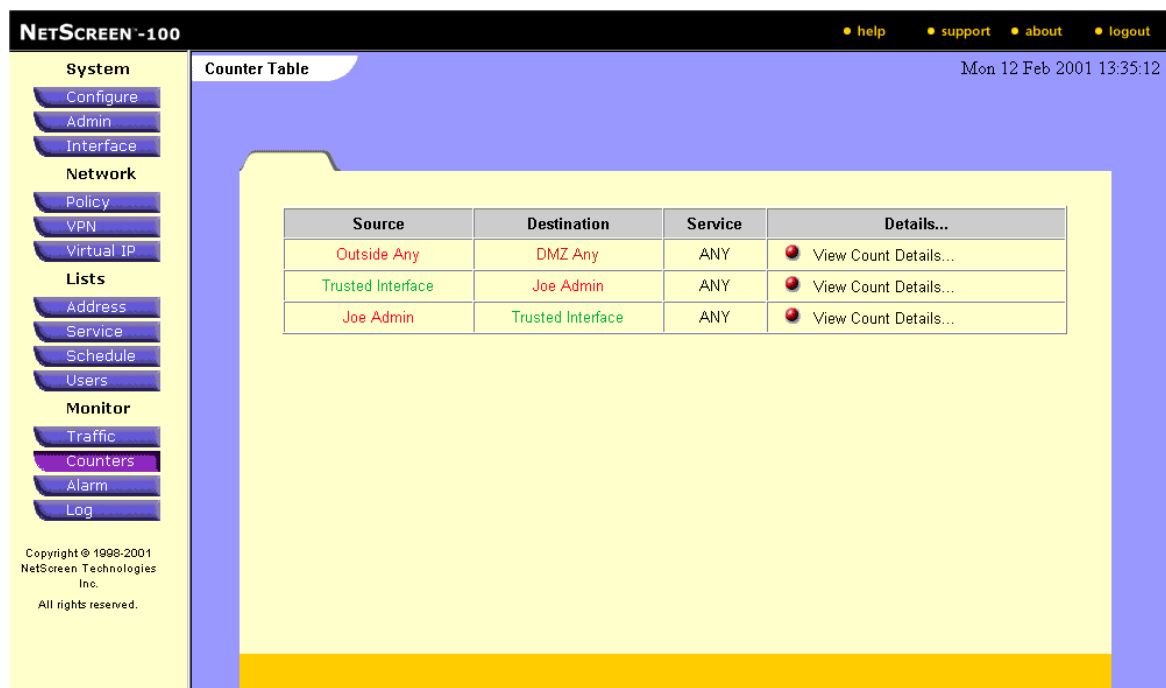


Figure 4-4 Counters

Viewing Counter Table

The Counter Table lists all policies for which counting has been enabled. These policies are listed based on the Source, Destination, and Service.

Counter Field	Description
Source	The source address of the policy.
Destination	The destination address of the policy.
Service	The service of the policy.
Details	Link to detail report.

To view a counter for traffic defined in the Access Policies section:

1. Click **View Counter Details** in the Details column for that counter.
The Counter Details page appears.
2. Click on a line in the graph to view information at that interval.

3. The X-axis represents time and the Y-axis represents the number of bytes. The X-axis displays seconds, minutes, hours, days, or months, depending on which tab you select. The color of the bar appears in blue, unless an alarm threshold was set and exceeded, in that case the bar is red.
4. Click **Download** to File to save the data to a desired location for review and analysis.
5. The data can be saved to your local C: drive in a *.txt text format. The file contents are tab-delimited.
6. Click **Update Now** to refresh the screen based on the most recent data available.

COUNTERS >> VIEW COUNT DETAILS

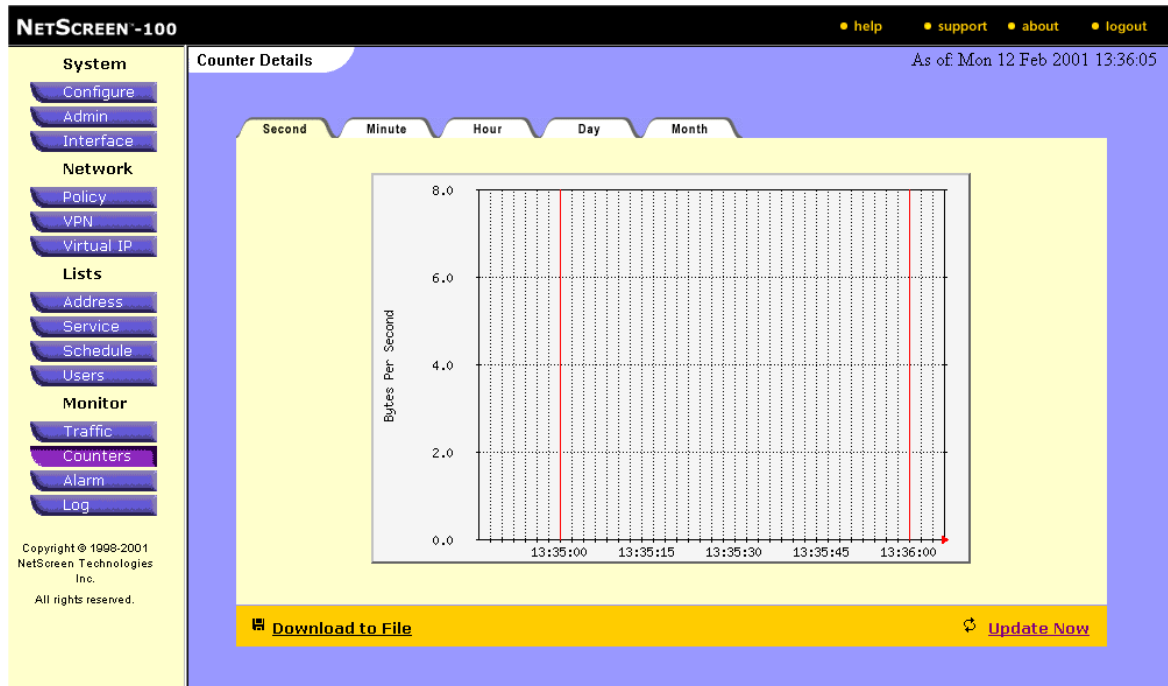


Figure 4-5 Counters >> View Count Details

Counter Details Reported

The Counter Table lists all policies for which counting has been enabled. These policies are listed based on the Source, Destination, and Service.

To view a counter for traffic defined in the Access Policies section:

1. Click **View Counter Details** in the Details column for that counter.

The Counter Details page appears.

2. Click on a second in the graph to view information at that interval.

The X-axis represents time and the Y-axis represents the number of bytes. The X-axis displays seconds, minutes, hours, days, or months, depending on which tab you select. The color of the bar appears in blue, unless an alarm threshold was set and exceeded, in that case the bar is red.

3. Click **Download to File** to save the data to a desired location for review and analysis.

The data can be saved to your local C: drive in a *.txt text format. The file contents are tab-delimited.

4. Click **Update Now** to refresh the screen based on the most recent data available.

ALARM >> TRAFFIC ALARM

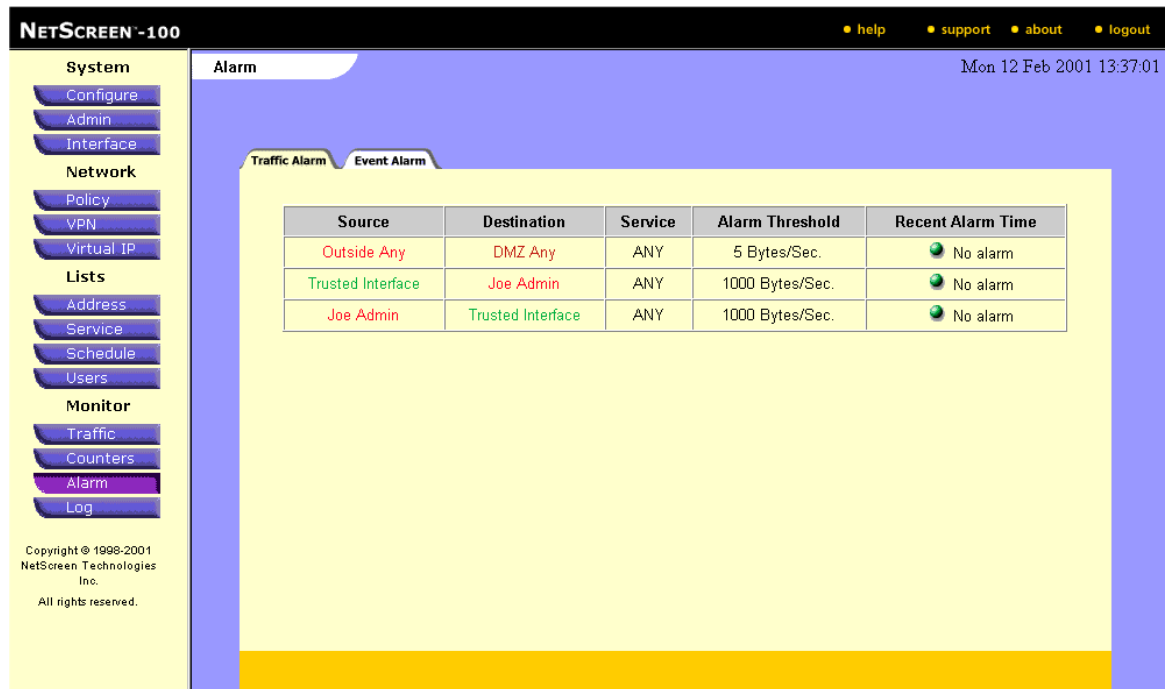


Figure 4-6 Alarm >> Traffic Alarm

Viewing Traffic Alarm

Traffic alarms are defined on the Access Policies page.

Traffic Field	Description
Source	The source of the traffic.
Destination	The destination of the traffic.
Service	The service of the traffic.
Alarm Threshold	The alarm threshold of the policy.

To view an alarm defined in the Access Policies section:

1. On the Traffic Alarm page, click **Recent Alarm Time** to view information about specific alarms.
2. The Alarm Details page appears.
3. Click **Download** to File to save the data to a desired location for review and analysis.

The data can be saved to your local C: drive in a *.txt text format. The file contents are tab-delimited.

4. Click **Clear Alarms** to erase all the data.
5. Click **Next/Previous** to move to the next/previous page.

ALARM >> EVENT ALARM

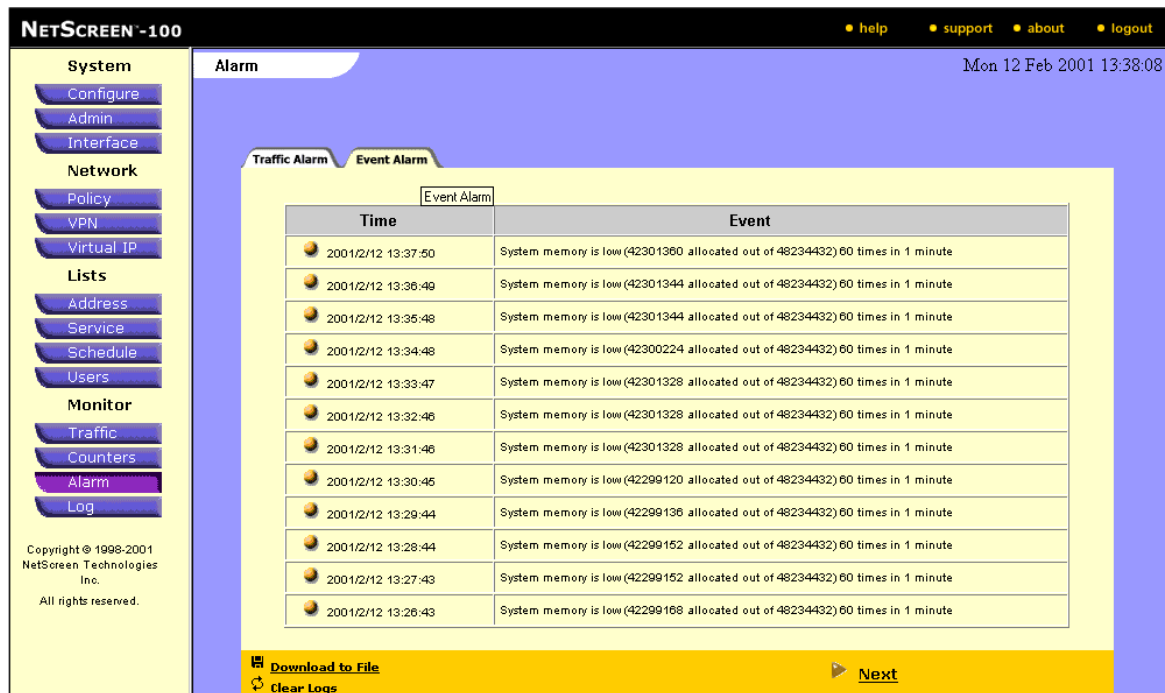


Figure 4-7 Alarm >> Event Alarm

Viewing Event Alarm

To view alarm events and download them to a file:

1. Click the **Alarms** tab under Monitor, on the left of the NetScreen Administration Tools page.
The Alarm page opens.
2. To view information about specific alarms, click on **Event Alarm** tab.
3. To save the data to a desired location for review and analysis, click on **Download to File**.
4. Click **Download to File** to save the data to a desired location for review and analysis.
5. Click **Next/Previous** to move to the next/previous page, to view other alarm information.

LOG >> TRAFFIC LOG



Figure 4-8 Log >> Traffic Log

Viewing Traffic Log

The traffic log details by source, destination, service and number of entries.

1. To view the details about a log entry, click **View Log Entries** in the Action column to display the Log Details page.

Traffic Field	Description
Source	The source of the traffic.
Destination	The destination of the traffic.
Service	The service of the traffic.
Entries	The number of traffic log entries.
Action	The details of a log entry.

2. Click **Download to File** to save the data to a desired location for review and analysis.

You can save the data to your local C: drive in a *.txt (text) format. The file contents are tab-delimited.

Note: *The Traffic Log can list entries in batches of 5, 10, 20, 50, 100 or maximum entries at once.*

LOG >> TRAFFIC LOG >> VIEW LOG ENTRIES

**Figure 4-9** Log >> Traffic Log >> View Log Entries

Viewing Log Entries

The log entries can be displayed by clicking on the “View Log Entries” field of the Traffic Log table.

Log Fields	Description
Time	Time of log entry.
Source Address	Source IP address of traffic.
Destination Address	Destination IP address of traffic.
Duration	Duration of entry.
Application	Application of traffic.

LOG >> EVENT LOG

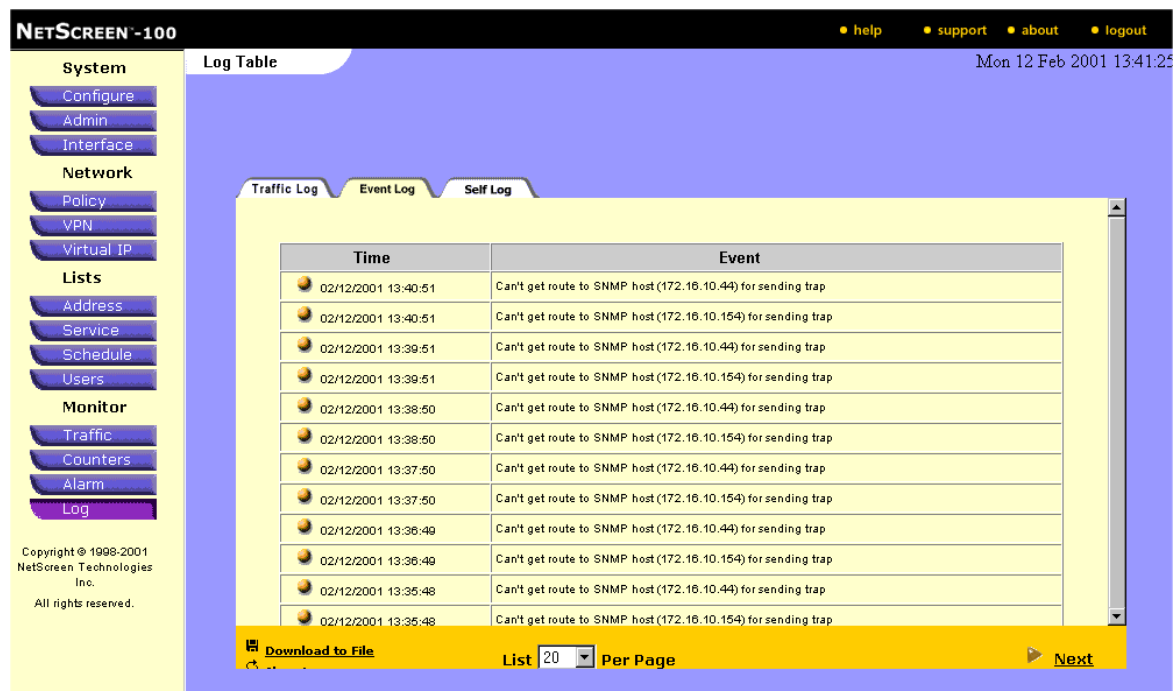


Figure 4-10 Log >> Event Log

Viewing Event Log

The Event Log lists system events of importance. The events are summarized and listed chronologically.

To view and save the Event Log:

1. Click the **Log** button, under Monitor on the left side of the screen.
The Log Table pages appear.
2. Click the **Event Log** tab to display the Event Log Table.
3. Click **Download to File** to save the data to a desired location for review and analysis.

You can save the data to your local C: drive in a *.txt (text) format. The file contents are tab-delimited.

Note: The Event Log can list entries in batches of 5, 10, 20, 50, 100 or maximum entries at once.

LOG >> SELF LOG

NETSCREEN-10

• help • support • about • logout

Mon 12 Feb 2001 13:47:23

Log Table

Traffic Log Event Log **Self Log**

Time	Source Addr	Destination Addr	Duration	Application
02/09/2001 16:12:16	10.100.2.132:15400	10.100.2.122:53348	0 sec.	TCP PORT 53348
02/09/2001 16:11:15	10.100.2.132:15400	10.100.2.122:53348	0 sec.	TCP PORT 53348
02/09/2001 16:10:15	10.100.2.132:15400	10.100.2.122:53348	0 sec.	TCP PORT 53348
02/09/2001 16:09:21	10.100.2.132:15400	10.100.2.122:53348	0 sec.	TCP PORT 53348
02/09/2001 16:08:55	10.100.2.132:15400	10.100.2.122:53348	0 sec.	TCP PORT 53348

Download to File Clear Logs

List 20 Per Page

Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.

Figure 4-11 Log >> Self Log

Viewing Self Log

The Self Log displays all the dropped packets detected by the NetScreen device.

To view the Self Log:

1. Click the **Log** button, located under Monitor in the menu column.
The Log Table page appears.
2. Click the **Self Log** tab to display the Self Log Table.
3. Click **Download to File** to save the data to a desired location for review and analysis.

You can save the data to your local C: drive in a *.txt (text) format. The file contents are tab-delimited.

Note: The Self Log can list entries in batches of 5, 10, 20, 50, 100 or maximum entries at once.

Index

A

- access policies 2-2, 2-14
 - changing 2-36
 - from DMZ 2-33
 - move 2-12, 2-19
 - to DMZ 2-24
- access policy
 - edit 2-27
 - move 2-12, 2-29, 2-38
 - new 2-21, 2-30, 2-39
 - remove 2-11, 2-18, 2-28, 2-37
- action 2-8, 2-22, 2-31, 2-40
- address
 - new 3-9
 - remove 3-6
- address group
 - create 3-7
 - edit 3-4
- address name 3-9
- administration 1-36
- Administration Tools 2-14
- administration user 1-40
- aggressive mode 2-62, 2-63
- AH 2-45, 2-46, 2-49, 2-51, 2-53, 3-36
- alarm 2-4, 2-16, 2-26, 2-35
- alarm threshold 2-8, 2-23, 2-31, 2-41
- application 4-15
- auth database 2-82
- authenticate 2-3, 2-15, 2-25, 2-34
- authentication 2-8, 2-22, 2-31, 2-40, 2-53
- authentication algorithm 2-45, 2-50, 3-35
- authentication header (AH) 2-45, 2-46, 2-51, 3-36
- authentication method 2-64, 2-66
- authentication port 1-8
- AutoKey IKE
 - new 2-54

B

- bandwidth 2-9, 4-3, 4-4
- blocked URL 1-15

C

- central management 1-54
- certificate authority 2-79
- certificate revocation list (CRL) 2-79
- client retries 1-9
- client timeout 1-9
- common name identifier 1-9
- communication timeout 1-15
- configuration 1-46
- count 2-4, 2-16, 2-26, 2-35
- counter details 4-9
- counter table 4-9
- counters 4-7
- counting 2-8, 2-22, 2-31, 2-40
- CRL 2-78, 2-79
- CRL refresh frequency 2-80
- CRL URL
 - default 2-80
- current server status 1-15
- custom entry
 - remove 3-18
- custom service
 - modify 3-16
 - new 3-14, 3-21
- custom services 3-11

D

- Data Encryption Standard 2-53
- default gateway 1-62, 1-79, 1-84
- default port number 1-8
- deny 2-3, 2-15, 2-25, 2-34
- des 2-53

destination 2-15, 2-25, 2-34
destination address 2-8, 2-22, 2-30, 2-39, 4-15
destination port 3-15, 3-21
DHCP 1-27, 1-31, 1-70
dialup group
 add 3-38, 3-39
 remove 3-40, 3-41
dialup groups 3-37
dialup user/group 2-84
Diffie-Hellman Group 2-65, 2-66, 2-68
Diffie-Hellman Group 2 2-53
Diffie-Hellman Groups 2-66, 2-68
DIP off 2-22, 2-31, 2-40
DIP on 2-22, 2-31, 2-40
direction 4-2
DMZ 1-61, 1-70, 1-78, 2-17, 2-24
DMZ addresses 3-3
DMZ interface 1-76
DNS 1-1, 2-82
DNS IP
 primary 3-33
 secondary 3-33
DNS lookup table 1-13
DNS refresh 1-12
Domain Name System (DNS) 1-3
download configuration 1-43
DS codepoint 2-9
duration 4-15
Dynamic Host Configuration Protocol (DHCP) 1-27
Dynamic IP 1-74, 1-90
 new configuration 1-75

E

Encapsulating Security Payload (ESP) 2-45, 3-36
encapsulation 2-71
encryption algorithm 2-45, 2-49, 2-65, 2-71, 3-35
encryption and authentication (ESP) 2-53
encryption disabled 2-3, 2-15, 2-25, 2-34
encryption type 1-9
ESP 2-45, 2-49, 2-53, 3-35, 3-36
event alarm 4-12

event log 4-16

F

fail count 1-25
FTP 1-71, 1-79, 1-80, 1-84

G

g2 2-53
gateway 2-42, 2-56
gateway IP 2-45, 2-49
gateway IP address 1-17
generate key 2-50, 2-51
Global Manager 1-53, 1-63, 1-72, 1-80, 1-85
 enable 1-54
Global PRO 1-53, 1-63, 1-72, 1-80, 1-85
GMT 1-44
graph 4-4
Greenwich Mean Time (GMT) 1-44
group
 remove 3-6
 size limits 3-8
group ID 1-21
guaranteed bandwidth 2-9, 2-23, 2-32, 2-41

H

HA port 1-21
hash algorithm 2-46, 2-51, 2-67, 2-69, 3-36
HEX key 3-35
hex key 2-45, 2-46, 2-49, 2-50, 3-35, 3-36
High Availability (HA) 1-20
host name 1-2, 2-83, 2-84
HTTP 1-71, 1-79, 1-84
HTTP port 1-58

I

ICMP flood 1-3
ident-reset 1-72, 1-80, 1-85
idle timeout 1-57
IKE ID type 3-33

IKE identity 3-33
interface mode 1-62
interface name 1-61
interface traffic 4-6
interval(s) 1-23
IP address 2-63, 3-10
IP addresses 2-85
 Manage 2-6
IP pool
 range 2-86
IP pool name 2-82

K

keep alive 2-83, 2-84
key generation 2-76
key pair 2-81

L

L2TP settings 2-82
L2TP tunnel
 configuration 2-84
L2TP user 3-33
LDAP 1-7
LDAP server 1-9
 default 2-80
LDAP server name 1-9
lifesize 2-65, 2-71
lifetime 2-65, 2-67, 2-69, 2-71, 2-73
link 1-60
load balance 2-88, 2-91, 2-95, 2-97, 2-100, 2-103
load balancing 2-89
local ID 2-59
local security index 3-31
local SPI 2-43, 3-31
log 2-4, 2-16, 2-26, 2-35
log entries 4-15
logging 2-8, 2-22, 2-31, 2-40

M

MAC address 1-32, 1-70, 1-78

Main Mode 2-63
main mode 2-63
main mode, 2-62
Manage IP 2-6
Management (MGT) Interface 1-81
Management Client IP 1-41
management services 1-84
manual key 2-42
 definition 2-48
Mapped IP (MIP) 1-73, 1-88
master server name 1-8
maximum bandwidth 2-9, 2-23, 2-32, 2-41
MD5 2-46, 2-53
metric 1-17
MGT 1-81
MIP 1-73, 1-88
mode 2-57, 2-59, 2-63
monitor 2-43

N

NAT 1-60, 1-62, 2-22, 2-31, 2-40
NAT off 2-22, 2-31, 2-40
netmask 1-17, 1-71, 1-73, 1-88, 1-89, 3-10
Network Time Protocol (NTP) 1-5, 1-44
No Perfect Forwarding Secrecy (PFS) 2-53
nopfs 2-53
NTP 1-44

O

operation mode 1-2

P

P1 proposal
 create 2-64
peer ID 2-56
peer IP 2-83, 2-84
Perfect Forward Secrecy 2-71
permit 2-15, 2-25, 2-34
permit (trust) 2-3
permit (untrust) 2-3, 2-15, 2-25, 2-34

ping 1-63, 1-72, 1-80, 1-85
PKI 2-62
Port
 default 2-6
 reassigning 2-6
port translation 1-74, 1-90
PPP auth 2-82
pre-defined services 3-11
preshare key 2-59, 2-62
priority 1-21, 4-2

R

RADIUS 1-7
radius secret 2-82
RADIUS Server 1-8
radius server 2-82
recurring 3-28
remote gateway 2-58
remote gateway ID 2-63
remote security index 3-31
remote SPI 2-43, 3-31
remote user
 modify 3-32
replay protection 2-55
Route 1-60, 1-62
Route mode 2-5
 interface settings 2-5
route table 1-16
route table entry
 modify 1-17
 new 1-17
 remove 1-17

S

schedule 2-4, 2-9, 2-16, 2-23, 2-26, 2-35, 2-41
 modify 3-26
 new 3-28
 remove 3-27
schedule book 3-25
schedule detail 3-25

SCS 1-45, 1-62, 1-71, 1-79, 1-84
secret 2-84
secure command shell (SCS) 1-45, 1-62
Secure Sockets Layer (SSL) 1-63
SecurID 1-7
SecurID server 1-8
Security Dynamics SecurID (ACE) 1-8
security index 2-45, 2-49, 3-35
self log 4-17
sequential ID 2-3
server IP 2-88, 2-91, 2-95, 2-97, 2-100, 2-103
server name 1-8
server settings
 default 2-80
server weight 2-89, 2-91, 2-95, 2-97, 2-100, 2-103
service 2-8, 2-22, 2-31, 2-40, 2-88, 2-91, 2-94,
 2-97, 2-100, 2-103, 3-11
 classification 3-12
 new 2-90, 3-13
service group
 new 3-19, 3-23
service name 3-14, 3-21
sha-1 2-53
shared secret 1-8
show DNS status 1-13
Simple Network Management Protocol (SNMP) 1-
 49, 1-63
slave server name 1-8
SNMP 1-49, 1-63, 1-72, 1-79, 1-84
SNMP community 1-50
 new 1-50
software key 1-34
software update 1-2
software version 1-2
source 2-15, 2-25, 2-34
source address 2-8, 2-22, 2-30, 2-39, 4-15
source port 3-21
SSL 1-63, 1-71, 1-79, 1-84
success rate 1-26
SYN attack 1-3
Syslog configuration 1-46

syslog configuration 1-46

T

TCP/IP 1-71, 1-79, 1-84

Telnet 1-62, 1-71, 1-79, 1-84

threshold 1-23, 1-25

time 4-15

Track IP Status table 1-25

traffic 2-4, 2-16, 2-25, 2-26, 2-35, 4-2

traffic alarm 4-10

traffic allocation 4-2

traffic bandwidth 1-60, 1-79, 1-84

traffic graph 4-4

traffic log 4-13

traffic priority 2-9, 2-23, 2-32, 2-41

traffic shaping 2-9, 2-23, 2-32, 2-41

Transparent mode 2-5

transport 3-14, 3-22

trust 1-61, 1-70, 1-78, 1-81

trusted 2-5

trusted addresses 3-3

tunnel 1-81, 2-3, 2-15, 2-25, 2-34

 new 1-87

tunnel interfaces 1-86

U

UDP flood 1-3

untrust 1-61, 1-70, 1-78, 1-81

untrusted 2-5

untrusted addresses 3-3

use duress 1-9

user 2-83

user details 3-30

user identity 3-31

V

value-added reseller (VAR) 1-34

virtual IP 2-87, 2-94

 edit 2-93

virtual IPs

 maximum 2-87

virtual port 2-88, 2-91, 2-94, 2-97, 2-100, 2-103

Virtual Private Network (VPN) 2-2

VPN 2-2, 2-14, 2-24, 2-33

VPN certificate

 viewing 2-74

VPN encryption 1-28

VPN entry

 new 2-43, 2-44

VPN license 1-34

VPN monitor 2-53, 2-55

VPN tunnel 1-34, 2-22, 2-31, 2-40

W

Websense 1-14, 1-15

Websense server 1-14

WebUI 1-79, 1-84

weight 1-23

Windows Internet Naming Service (WINS) 2-82, 3-33

WINS 2-82, 3-33

WINS IP

 primary 3-33

 secondary 3-33