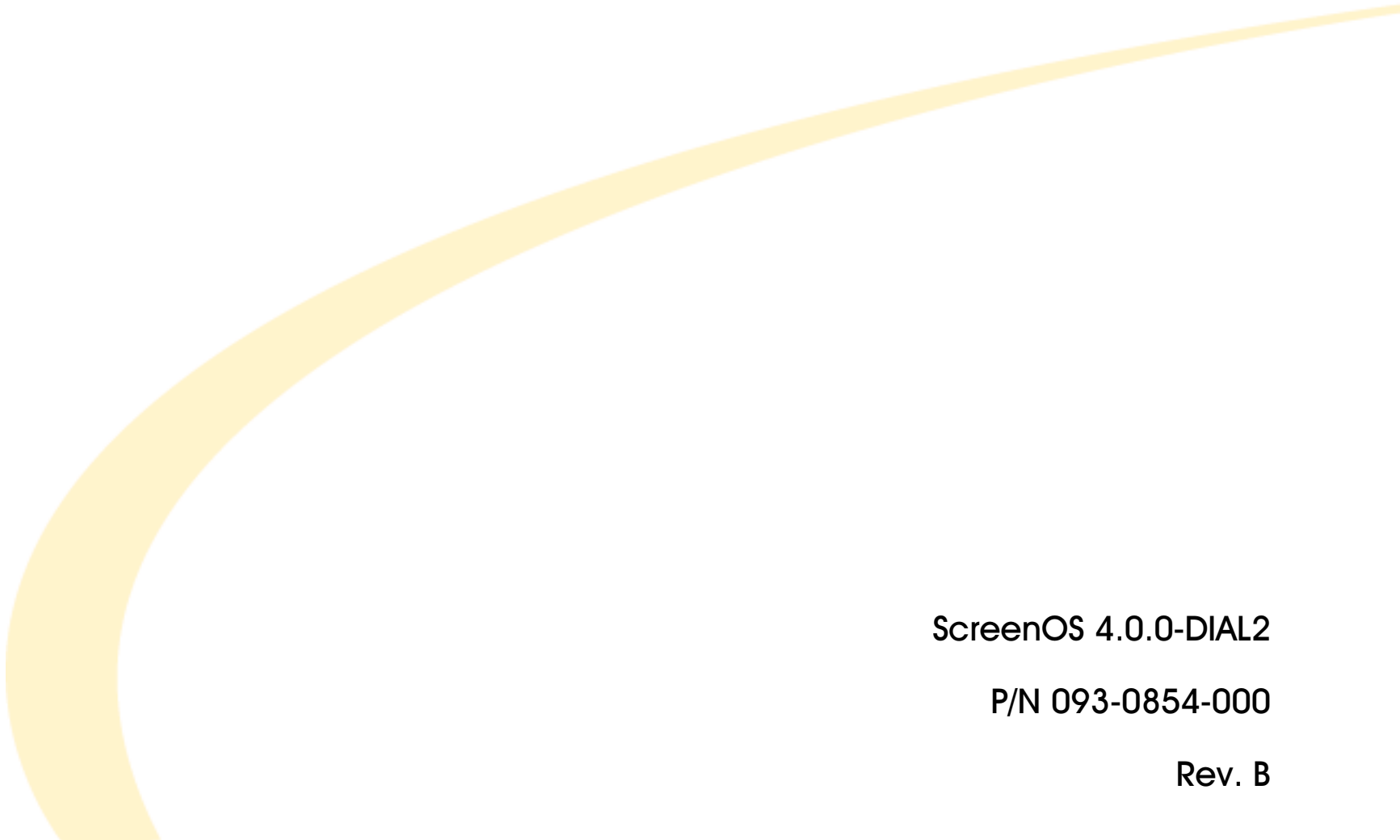


NetScreen New Features Guide



ScreenOS 4.0.0-DIAL2

P/N 093-0854-000

Rev. B

Copyright Notice

Copyright © 2003 NetScreen Technologies, Inc. All rights reserved.

NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-1000, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of NetScreen Technologies, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

NetScreen Technologies, Inc.
Building #3
805 11th Avenue
Sunnyvale, CA 94089
www.netscreen.com

FCC Statement

The following information is for FCC compliance of Class A devices: 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 when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. 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.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR NETSCREEN REPRESENTATIVE FOR A COPY.

Contents

Preface	V	ISP Configuration	33
Conventions	vi	Example: Configuring ISP Information	34
WebUI Navigation Conventions	vi	Serial Interface Failover	35
Example: Objects > Addresses > List > New	vi	Example: Configuring Dial Backup in the	
CLI Conventions	vii	Trust-Untrust Mode	36
NetScreen Documentation	viii	Example: Adding or Deleting a Default Route for	
Chapter 1 New Features and Enhancements.....	1	the Serial Interface	39
Port Modes	2	Example: Specifying a Policy as Inactive for	
Setting the Port Mode on the NetScreen-5XT and		Serial Interface Failover	40
NetScreen-5GT.....	10	Loopback Interfaces	41
Example: Setting Home-Work Port Mode	11	Using the Loopback Interface for MIPs	43
Home Zone/Work Zone	12	Interface Failover	44
Example: Configuring Home and Work Zones.....	14	Example: Configuring a Single MIP for	
Dual Untrust Interfaces.....	15	Different Tunnel Interfaces	44
Interface Failover.....	16	XAuth Client	48
Determining Interface Failover	17	Example: Configuring the NetScreen Device	
Interface Failover with IP Tracking	17	as an XAuth Client	49
Example: Configuring Automatic Failover with		Destination IP for VPN Monitor	50
IP Tracking	19	Example: Specifying a Destination IP for	
Interface Failover with VPN Tunnel Monitoring	22	VPN Monitoring.....	50
Example: Configuring Automatic Failover with		DHCP Server Enhancement	51
VPN Tunnel Monitoring	23	Example: Turning off DHCP Server Detection	51
PPPoE Configuration	28	Routing Information Protocol (RIP) Version 2	53
Example: Configuring PPPoE on Primary and		Basic RIP Configuration	54
Backup Untrust Interfaces	28	Creating a RIP Routing Instance in a	
Dial Backup	30	Virtual Router.....	54
Modem Settings.....	32	Example: Creating a RIP Routing Instance	55
Example: Configuring Modem Settings	33	Enabling the RIP Instance	55
		Example: Enabling a RIP Routing Instance	56

Example: Removing a RIP Routing Instance	57	interface	76
Redistributing Routes	58	Syntax	76
Example: Redistributing Routes into RIP	58	Keywords and Variables	78
Global Parameters.....	60	modem.....	84
Example: Advertising the Default Route to RIP Neighbors	61	Syntax	84
Interface Parameters	61	Keywords and Variables	85
Example: Setting RIP Interface Parameters.....	62	policy	91
Security Configuration	63	Syntax	91
Authenticating Neighbors.....	63	Keywords and Variables	91
Example: Configuring Neighbor Authentication...	63	port-mode	92
Filtering RIP Neighbors	64	Syntax	92
Example: Configuring Trusted Neighbors	64	Keywords and Variables	93
Rejecting Default Routes	65	pppoe	95
Example: Rejecting Default Routes	65	Syntax	95
Protecting Against Flooding	66	Keywords and Variables	95
Example: Configuring an Update Threshold.....	66	RIP Context Commands	97
Example: Configuring RIP for the Trust and Untrust Zones.....	67	advertise-def-route.....	100
Chapter 2 New and Modified CLI Commands	69	Syntax	100
bgp	70	Keywords and Variables	101
Syntax.....	70	config.....	102
Keywords and Variables.....	70	Syntax	102
failover	71	Keywords and Variables	102
Syntax.....	71	default-metric	103
Keywords and Variables.....	71	Syntax	103
ike.....	74	Keywords and Variables	103
Syntax.....	74	enable	104
Keywords and Variables.....	74	Syntax	104
		Keywords and Variables	104
		flush-timer	105
		Syntax	105
		Keywords and Variables	105

interface	106
Syntax	106
Keywords and Variables	106
invalid-timer	107
Syntax	107
Keywords and Variables	107
max-neighbor-count	108
Syntax	108
Keywords and Variables	108
neighbors	109
Syntax	109
Keywords and Variables	109
no-source-validation	110
Syntax	110
Keywords and Variables	110
redistribute	111
Syntax	111
Keywords and Variables	112
reject-default-route	113
Syntax	113
Keywords and Variables	113
route-map	114
Syntax	114
Keywords and Variables	114
routes-redistribute	116
Syntax	116
Keywords and Variables	116
rules-redistribute	117
Syntax	117
Keywords and Variables	117
threshold-update	118
Syntax	118
Keywords and Variables	118

timer	119
Syntax	119
Keywords and Variables	119
trusted-neighbors	120
Syntax	120
Keywords and Variables	120
update-timer	121
Syntax	121
Keywords and Variables	121
update-threshold	122
Syntax	122
Keywords and Variables	122
vpn	123
Syntax	123
Keywords and Variables	123
vrouter	125
Commands	125
Arguments	126
Chapter 3 New Messages	127
DHCP	128
Critical (00029)	128
Failover	130
Critical (00062)	130
Interface	132
Notification (00009)	132
PPP	133
Notification (00042)	133
PPPoE	134
Information (00537)	134

RIP..... 135
 Critical (00204) 135

VPN..... 137
 Notification (00017) 137

Preface

This document presents the new features in this release of NetScreen ScreenOS software. It is organized into the following chapters:

- [Chapter 1, “New Features and Enhancements” on page 1](#)
- [Chapter 2, “New and Modified CLI Commands” on page 69](#)
- [Chapter 3, “New Messages” on page 127](#)

This document is intended to be a supplement to the ScreenOS 4.0.0 documentation set. For more information about ScreenOS features, CLI commands, and messages, refer to the following documents:

- *NetScreen Concepts & Examples ScreenOS Reference Guide*
- *NetScreen CLI Reference Guide*
- *NetScreen Message Log Reference Guide*

CONVENTIONS

This book presents two management methods for configuring a NetScreen device: the Web user interface (WebUI) and the command line interface (CLI). The conventions used for both are introduced below.

WebUI Navigation Conventions

Throughout this book, a single chevron (>) is used to indicate navigation through the WebUI by clicking menu options and links.

Example: **Objects > Addresses > List > New**

To access the new address configuration dialog box, do the following:

1. Click **Objects** in the menu column.
The Objects menu option expands to reveal a subset of options for Objects.
2. (Applet menu) Hover the mouse over **Addresses**.
(DHTML menu) Click **Addresses**.
The Addresses option expands to reveal a subset of options for Addresses.
3. Click **List**.
The address book table appears.
4. Click the **New** link in the upper right corner.
The new address configuration dialog box appears.

CLI Conventions

Each CLI command description in this manual reveals some aspect of command syntax. This syntax may include options, switches, parameters, and other features. To illustrate syntax rules, some command descriptions use *dependency delimiters*. Such delimiters indicate which command features are mandatory, and in which contexts.

Dependency Delimiters

Each syntax description shows the dependencies between command features by using special characters.

- The { and } symbols denote a mandatory feature. Features enclosed by these symbols are essential for execution of the command.
- The [and] symbols denote an optional feature. Features enclosed by these symbols are not essential for execution of the command, although omitting such features might adversely affect the outcome.
- The | symbol denotes an “or” relationship between two features. When this symbol appears between two features on the same line, you can use either feature (but not both). When this symbol appears at the end of a line, you can use the feature on that line, or the one below it.

Nested Dependencies

Many CLI commands have *nested* dependencies, which make features optional in some contexts, and mandatory in others. The three hypothetical features shown below demonstrate this principle.

```
[ feature_1 { feature_2 | feature_3 } ]
```

The delimiters [and] surround the entire clause. Consequently, you can omit **feature_1**, **feature_2**, and **feature_3**, and still execute the command successfully. However, because the { and } delimiters surround **feature_2** and **feature_3**, you must include either **feature_2** or **feature_3** if you include **feature_1**. Otherwise, you cannot successfully execute the command.

The following example shows some of the feature dependencies of the **set interface** command.

```
set interface vlan1 broadcast { flood | arp [ trace-route ] }
```

The { and } brackets indicate that specifying either **flood** or **arp** is mandatory. By contrast, the [and] brackets indicate that the **trace-route** option for **arp** is not mandatory. Thus, the command might take any of the following forms:

```
ns-> set interface vlan1 broadcast flood
ns-> set interface vlan1 broadcast arp
ns-> set interface vlan1 broadcast arp trace-route
```

Availability of CLI Commands and Features

As you execute CLI commands using the syntax descriptions in this manual, you may find that certain commands and command features are unavailable for your NetScreen device model.

Because NetScreen devices treat unavailable command features as improper syntax, attempting to use such a feature usually generates the **unknown keyword** error message. When this message appears, confirm the feature's availability using the ? switch. For example, the following commands list available options for the **set vpn** command:

```
ns-> set vpn ?
ns-> set vpn vpn_name ?
ns-> set vpn gateway gate_name ?
```

NETSCREEN DOCUMENTATION

To obtain technical documentation for any NetScreen product, visit www.netscreen.com/support/manuals.html. To access the latest NetScreen documentation, see the **Current Manuals** section. To access archived documentation from previous releases, see the **Archived Manuals** section.

To obtain the latest technical information on a NetScreen product release, see the release notes document for that release. To obtain release notes, visit www.netscreen.com/support and select **Software Download**. Select the product and version, then click **Go**. (To perform this download, you must be a registered user.)

If you find any errors or omissions in the following content, please contact us at the e-mail address below:

techpubs@netscreen.com

New Features and Enhancements

This chapter describes the new features in ScreenOS 4.0.0-DIAL2. The specific topics covered are as follows:

- “Port Modes” on page 2
- “Home Zone/Work Zone” on page 12
- “Dual Untrust Interfaces” on page 15
 - “Interface Failover” on page 16
 - “Determining Interface Failover” on page 17
 - “PPPoE Configuration” on page 28
- “Dial Backup” on page 30
 - “Modem Settings” on page 32
 - “ISP Configuration” on page 33
 - “Serial Interface Failover” on page 35
- “Loopback Interfaces” on page 41
 - “Using the Loopback Interface for MIPs” on page 43
- “XAuth Client” on page 48
- “Destination IP for VPN Monitor” on page 50
- “DHCP Server Enhancement” on page 51
- “Routing Information Protocol (RIP) Version 2” on page 53
 - “Basic RIP Configuration” on page 54
 - “Global Parameters” on page 60
 - “Interface Parameters” on page 61
 - “Security Configuration” on page 63

PORT MODES

ScreenOS 4.0.0-DIAL2 provides four port modes that automatically set different port, interface, and zone bindings¹ on the NetScreen-5XT and NetScreen-5GT. You can configure one of the following port modes:

Warning: Changing the port mode removes any existing configurations on the NetScreen device, and requires a system reset.

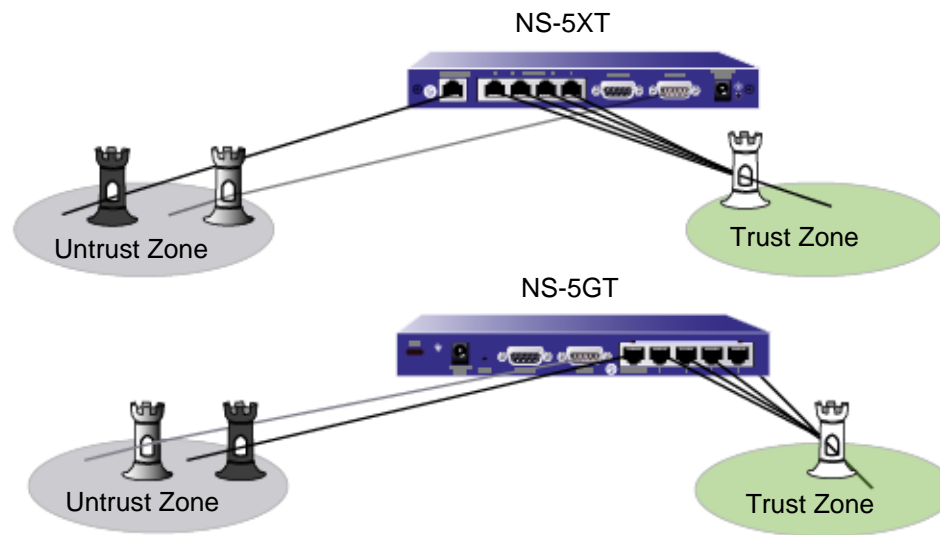
- Trust-Untrust mode is the default port mode. This mode provides the following port, interface, and zone bindings:
 - Binds the Untrusted Ethernet port to the Untrust interface, which is bound to the Untrust security zone
 - Binds the Modem port to the serial interface, which you can bind as a backup interface to the Untrust security zone
 - Binds the Trusted1 through Trusted4 Ethernet ports to the Trust interface, which is bound to the Trust security zone

1. In this document, *port* refers to a physical interface on the back of the NetScreen device. The ports are referenced by their labels: Untrusted, Trusted1-4, Console, or Modem. The term *interface* refers to a logical interface that can be configured through the WebUI or CLI. Each port can be bound to only one interface, but multiple ports can be bound to an interface.

The following illustration shows the port and zone bindings on the NetScreen-5XT and NetScreen-5GT for the Trust-Untrust port mode.

Trust-Untrust

The Untrust interface is the primary interface to the Untrust zone. You can bind the serial interface (shown in gray) as a backup interface to the Untrust zone.



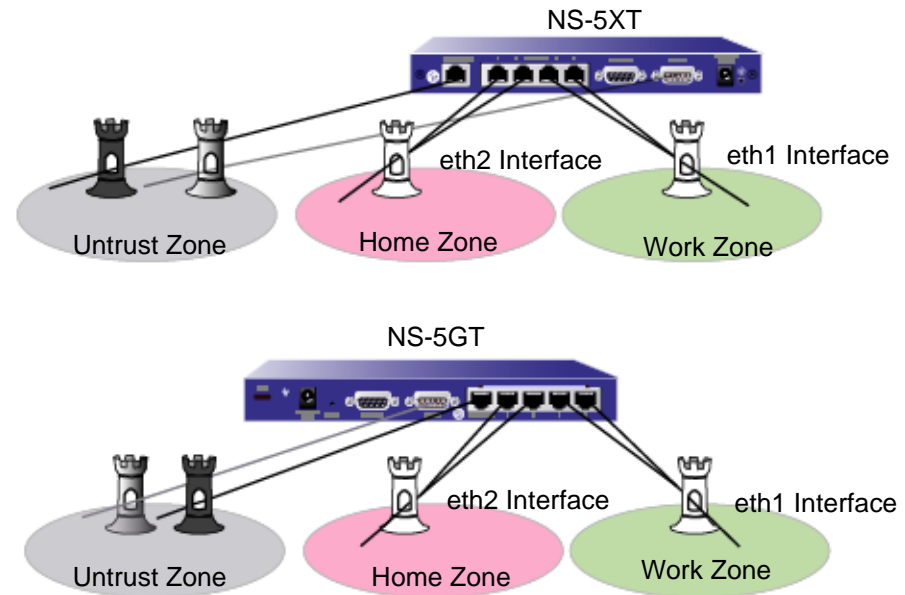
Note: The Initial Configuration Wizard only runs in Trust-Untrust port mode.

- Home-Work mode binds interfaces to the Untrust security zone and to new Home and Work security zones. The Work and Home zones allow you to segregate users and resources in each zone. In this mode, default policies allow traffic flow and connections from the Work zone to the Home zone, but do not allow traffic from the Home zone to the Work zone. By default, there are no restrictions for traffic from the Home zone to the Untrust zone. This mode provides the following port, interface, and zone bindings:
 - Binds the Trusted1 and Trusted2 Ethernet ports to the ethernet1 interface, which is bound to the Work security zone
 - Binds the Trusted3 and Trusted4 Ethernet ports to the ethernet2 interface, which is bound to the Home security zone
 - Binds the Untrusted Ethernet port to the ethernet3 interface, which is bound to the Untrust security zone
 - Binds the Modem port to the serial interface, which you can bind as a backup interface to the Untrust security zone

Following is an illustration of the port and zone bindings on the NetScreen-5XT and NetScreen-5GT for the Home-Work port mode:

Home-Work

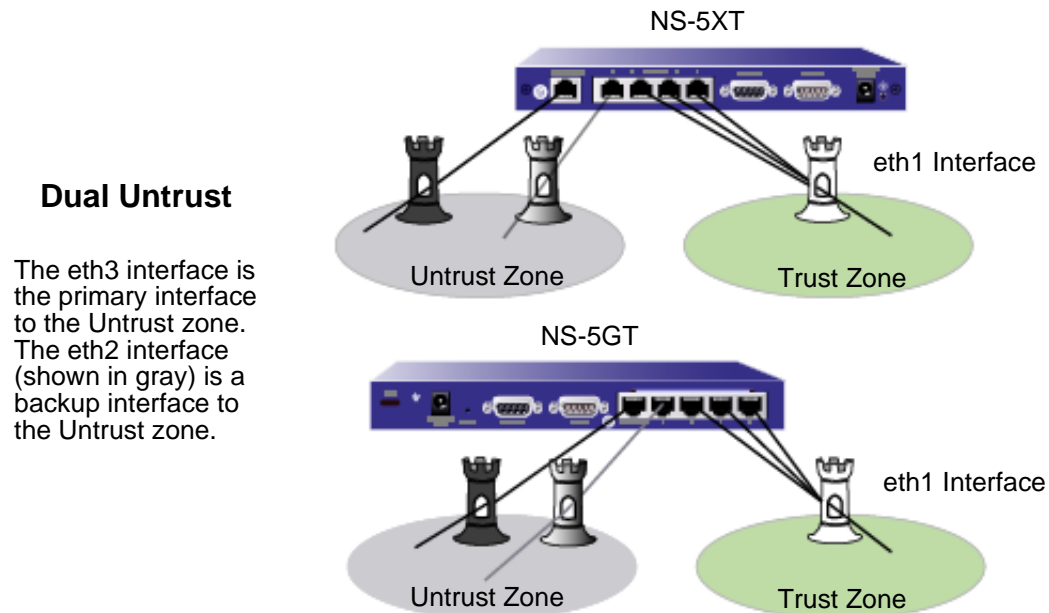
The eth3 interface is the primary interface to the Untrust zone. You can bind the serial interface (shown in gray) as a backup interface to the Untrust zone.



See [“Home Zone/Work Zone” on page 12](#) for more information about configuring and using Home-Work mode.

- Dual Untrust mode binds two interfaces, a primary and a backup, to the Untrust security zone. The primary interface is used to pass traffic to and from the Untrust zone, while the backup interface is used only when there is a failure on the primary interface. This mode provides the following port, interface, and zone bindings:
 - Binds the Untrusted Ethernet port to the ethernet3 interface, which is bound to the Untrust security zone
 - Binds the Trusted4 Ethernet port to the ethernet2 interface, which is bound as a backup interface to the Untrust security zone (the ethernet3 interface is the primary interface to the Untrust security zone)
 - Binds the Trusted1, Trusted2, and Trusted3 Ethernet ports to the ethernet1 interface, which is bound to the Trust security zone

Following is an illustration of the port and zone bindings on the NetScreen-5XT and NetScreen-5GT for the Dual Untrust port mode:



Note: The serial interface is not available in Dual Untrust port mode.

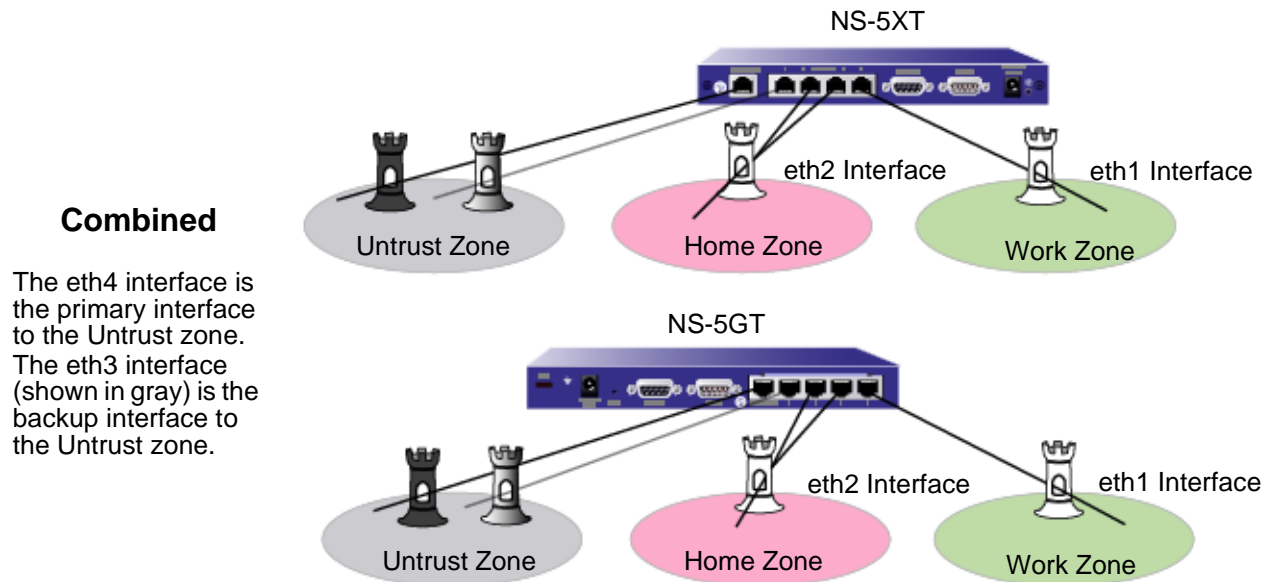
See [“Dual Untrust Interfaces” on page 15](#) for more information about configuring and using Dual Untrust mode.

- Combined mode allows both primary and backup interfaces to the Internet and the segregation of users and resources in Work and Home zones.

This mode provides the following port, interface, and zone bindings:

- Binds the Untrusted Ethernet port to the ethernet4 interface, which is bound to the Untrust zone
- Binds the Trusted4 Ethernet port to the ethernet3 interface, which is bound as a backup interface to the Untrust zone (the ethernet4 interface is the primary interface to the Untrust security zone)
- Binds the Trusted3 and Trusted2 ports to the ethernet2 interface, which is bound to the Home zone
- Binds the Trusted1 port to the ethernet1 interface, which is bound to the Work zone

Following is an illustration of the port and zone bindings on the NetScreen-5XT and NetScreen-5GT for the Combined port mode:



Note: The serial interface is not available in Combined port mode.

See [“Dual Untrust Interfaces” on page 15](#) and [“Home Zone/Work Zone” on page 12](#) for more information about configuring and using the Combined mode.

Setting the Port Mode on the NetScreen-5XT and NetScreen-5GT

The following table summarizes the port, interface, and zone bindings provided by the ScreenOS port modes:

Port	Trust-Untrust Mode*		Home-Work Mode		Dual Untrust Mode		Combined Mode	
	Interface	Zone	Interface	Zone	Interface	Zone	Interface	Zone
Untrusted	Untrust	Untrust	ethernet3	Untrust	ethernet3	Untrust	ethernet4	Untrust
1	Trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet1	Work
2	Trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet2	Home
3	Trust	Trust	ethernet2	Home	ethernet1	Trust	ethernet2	Home
4	Trust	Trust	ethernet2	Home	ethernet2	Untrust	ethernet3	Untrust
Modem	serial	Null	serial	Null	N/A	N/A	N/A	N/A

* Default port mode.

You change the port mode setting on the NetScreen device through either the WebUI or the CLI. Before setting the port mode, note the following:

- Changing the port mode *removes* any existing configurations on the NetScreen device and requires a system reset.
- Issuing the **unset all** CLI command does not affect the port mode setting on the NetScreen device. For example, if you want to change the port mode setting from the Combined mode back to the default Trust-Untrust mode, issuing the **unset all** command removes the existing configuration but does *not* set the device to the Trust-Untrust mode.

Example: Setting Home-Work Port Mode

In this example, you set the port mode to the Home-Work mode.

Warning: Changing the port mode removes any existing configurations on the NetScreen device and requires a system reset.

WebUI

1. Configuration > Operational Mode > Port Mode: Select Work-Home from the drop-down list, and then click **Apply**.
2. At the following prompt, click **OK**:
Operational mode change will erase current configuration and reset the device, continue?

CLI

1. `exec port-mode home-work`
2. At the following prompt, enter **y** (for yes):
Change port mode from <trust-untrust> to <home-work> will erase system configuration and reboot box
Are you sure y/[n] ?

To see the current port mode setting on the NetScreen device:

WebUI

Configuration > Operational Mode

CLI

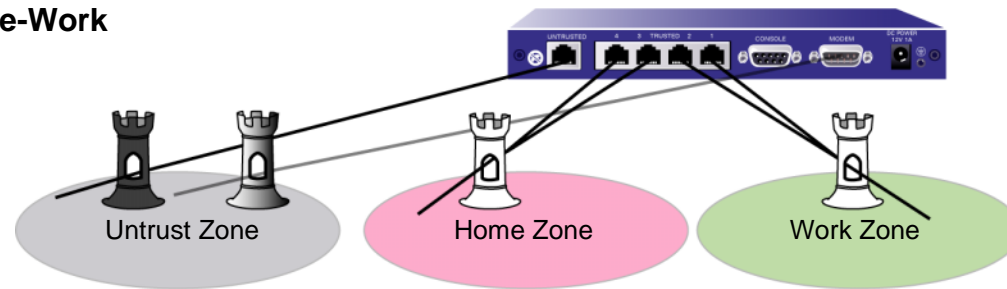
`get system`

HOME ZONE/WORK ZONE

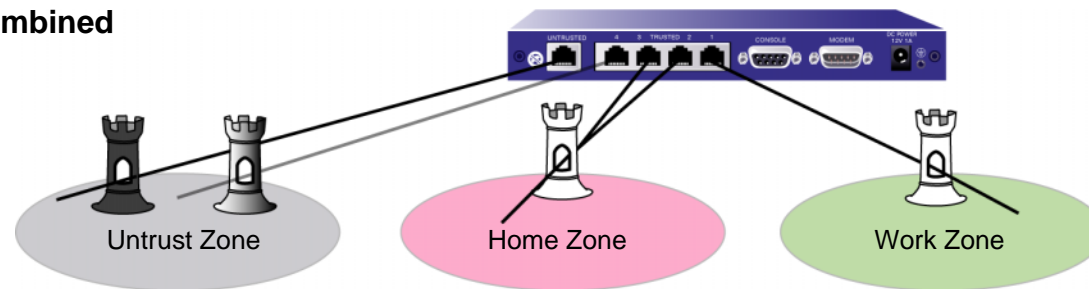
Security conflicts can arise as both employee telecommuting and home networks become commonplace. The home network used by both telecommuters and family members can become a dangerous back door to a corporate network, carrying threats such as worms and allowing access to corporate resources, such as servers and networks, by non-employees.

The Home-Work and Combined port modes bind the interfaces to special Work and Home zones. This allows segregation of business and home users and resources, while allowing users in both Home and Work zones access to the Untrust zone.

Home-Work



Combined



The Home-Work port mode also binds the Modem port to a serial interface, which you can bind as a backup interface to the Untrust security zone. For more information about using the serial interface as a backup interface to the Untrust security zone, see [“Dial Backup” on page 30](#).

The Combined port mode also binds the Trusted4 Ethernet port as a backup interface (ethernet3) to the Untrust security zone. The backup interface is used only when there is a failure on the primary interface to the Untrust zone. For more information about using the ethernet3 interface as a backup interface to the Untrust security zone, see [“Dual Untrust Interfaces” on page 15](#).

By default, some NetScreen devices act as a Dynamic Host Configuration Protocol (DHCP) server, allocating dynamic IP addresses to DHCP clients in the Work zone. (See [“DHCP Server Enhancement” on page 51](#) for more information about the DHCP server on the NetScreen device.)

You can configure the NetScreen device using a Telnet connection or the WebUI from the Work zone only. You cannot configure the NetScreen device from the Home zone. You cannot use any management services, including ping, on the Home zone interface. The default IP address of the Work zone interface, ethernet1, is 192.168.1.1/24.

The default policies in the Home-Work and Combined port modes provide the following traffic control between zones:

- Allow all traffic from the Work zone to the Untrust zone
- Allow all traffic from the Home zone to the Untrust zone
- Allow all traffic from the Work zone to the Home zone
- Block all traffic from the Home zone to the Work zone (you cannot remove this policy)

You can create new policies for traffic from the Work zone to the Untrust zone, from the Home zone to the Untrust zone, and from the Work zone to the Home zone. You can also remove the default policies that allow all traffic from the Work zone to the Untrust zone, from the Home zone to the Untrust zone, and from the Work zone to the Home zone. Note, however, that you cannot create a policy to allow traffic from the Home zone to the Work zone.

Example: Configuring Home and Work Zones

In this example, you configure a policy to allow only FTP traffic from the Home zone to the Untrust zone and remove the default policy that allows all traffic from the Home zone to the Untrust zone. In this example, the default policy, which allows traffic from any source address to any destination address for any service, has an ID of 2..

Warning: Changing the port mode removes any existing configurations on the NetScreen device and requires a system reset.

WebUI

1. Configuration > Operational Mode > Port Mode: Select Home-Work from the drop-down list, and then click **Apply**.
2. At the following prompt, click **OK**:
Operational mode change will erase current configuration and reset the device, continue?
3. Policies > (From: Home, To: Untrust) > New: Enter the following, and then click **OK**.
Source Address: Any
Destination Address: Any
Service: FTP
Action: Permit
4. Policies: In the “From Home to Untrust” policy list, click **Remove** in the Configure column for the policy with ID 2.

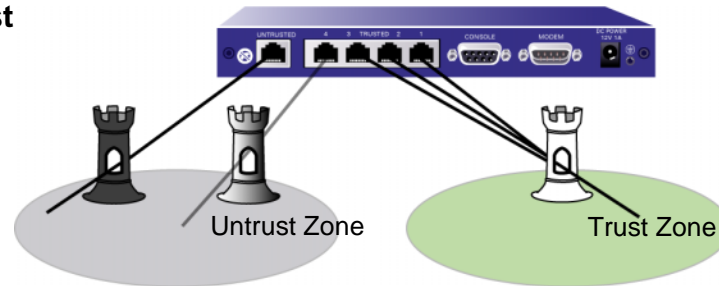
CLI

1. exec port-mode home-work
2. At the following prompt, enter **y** (for yes):
Change port mode from <trust-untrust> to <home-work> will erase system configuration and reboot box
Are you sure y/[n] ?
3. set policy from home to untrust any any ftp permit
4. unset policy 2

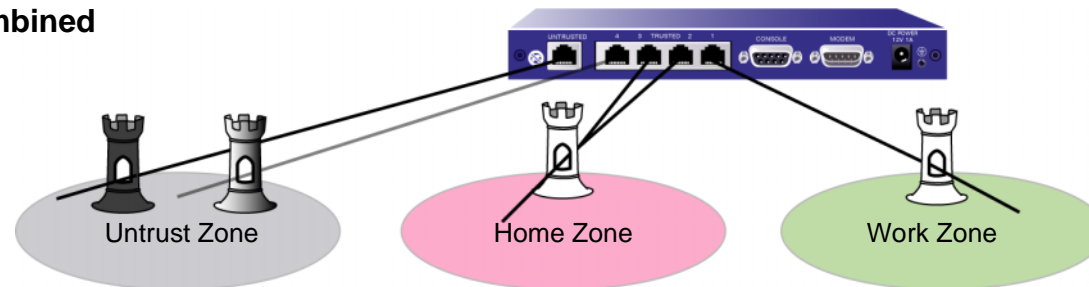
DUAL UNTRUST INTERFACES

In the default Trust-Untrust port mode, the NetScreen device allows only a single interface to be bound to the Untrust security zone. The Dual-Untrust and Combined port modes bind a second, backup interface to the Untrust zone. (See “[Port Modes](#)” on page 2.) In these modes, the backup interface is used only when there is a failure on the connection through the primary interface or when you manually switch traffic from the primary interface to the backup.

Dual Untrust



Combined



Warning: Changing the port mode removes any existing configurations on the NetScreen device and requires a system reset.

Interface Failover

When there are both primary and backup interfaces bound to the Untrust zone, you can manually switch traffic from the primary interface to the backup interface through the WebUI or the CLI.

To force traffic to switch from the primary interface to the backup interface:

WebUI

Network > Untrust Failover: Click **Force to Failover**.

CLI

```
exec failover force
```

When the primary interface is again available, you need to use the WebUI or the CLI to switch traffic from the backup to the primary interface.

To force traffic to switch from the backup interface to the primary interface:

WebUI

Network > Untrust Failover: Click **Force to Revert**.

CLI

```
exec failover revert
```

You can also configure the NetScreen device to automatically switch to the backup interface if ScreenOS detects a failure on the primary interface connection. By default, there is a 30-second interval before the switchover occurs. In automatic interface failover mode, when the connection through the primary interface is restored, ScreenOS automatically switches traffic from the backup interface to the primary.

To configure ScreenOS for automatic interface failover:

WebUI

Network > Untrust Failover > Automatic Failover (select) > Apply.

CLI

```
set failover auto
```

Determining Interface Failover

An interface failover can occur when ScreenOS detects a physical link problem on the primary interface connection, such as an unplugged cable. You can also define the following types of interface failover:

- when certain IP addresses become unreachable through a given interface using IP tracking
- when certain VPN tunnels on the primary untrust interface become unreachable using VPN tunnel monitoring

Interface Failover with IP Tracking

You can specify an interface failover when certain IP addresses become unreachable through a given interface, even if the physical link is still active. ScreenOS uses layer 3 path monitoring, or *IP tracking*, similar to that used for NSRP, to monitor the connection through the primary interface. For example, if an interface connects directly to a router, you can track the next-hop address on the interface to determine if the router is still reachable. Note that you can configure IP tracking without configuring automatic interface failover.

You can configure up to four IP addresses for ScreenOS to track. For each IP address to be tracked, you specify the following:

- Interval, in seconds, at which the pings are sent to the specified IP address.
- Number of consecutive unsuccessful ping attempts before the connection to the IP address is considered failed.
- Weight of the failed IP connection (once the sum of the weights of all failed IP connections crosses a specified threshold, ScreenOS initiates a switchover to the backup link).
- IP address of the next-hop (gateway) to be used to reach the tracked IP address. You must specify the gateway if the tracked IP address is on a different subnet. If you do not specify a gateway address, ScreenOS uses the default route for the interface to reach the tracked IP address.

Note that when you configure an IP address for ScreenOS to track, a host route for that IP address is not added to the routing table.

There are two types of configurable thresholds in tracking IP addresses:

- Track IP address failure threshold — The number of consecutive failures to elicit a ping response from a specific IP address that constitutes a failure. Not exceeding the threshold indicates an acceptable level of connectivity with the address; exceeding the threshold indicates an unacceptable level. You set this threshold for each IP address at any value between 1 and 200. The default value is 3.
- Interface failover threshold — The total weight of the cumulative failed attempts to reach IP addresses on the interface that constitutes an interface failure. You can set this threshold at any value between 1 and 255. The default value is 1.

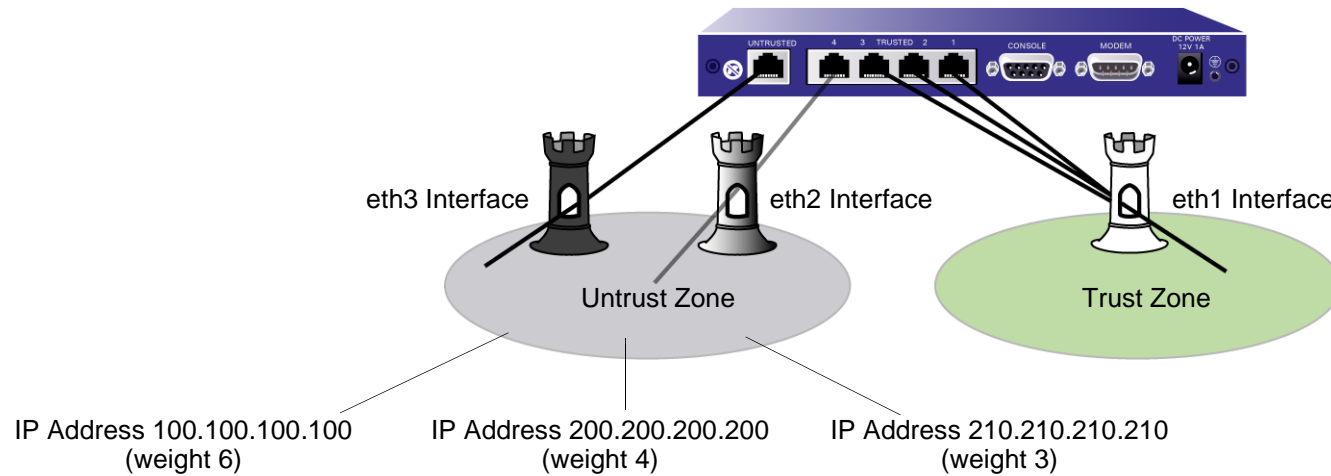
By applying a *weight*, or a value, to a tracked IP address, you can adjust the importance of connectivity to that address in relation to reaching other tracked addresses. You can assign comparatively greater weights to relatively more important addresses, and less weights to relatively less important addresses. Note that the assigned weights only come into play when a tracked IP address failure threshold is reached. For example, failure of a tracked IP address with a weight of 10 brings the interface closer to a failover than would the failure of a tracked IP address with a weight of 1. You can assign weights from 1 to 255. The default weight is 1.

Example: Configuring Automatic Failover with IP Tracking

In this example, you first configure the NetScreen device for Dual Untrust mode. You then configure it for automatic failover. If automatic failover from the primary interface to the backup interface occurs, the backup interface carries all traffic to and from the Untrust zone until the primary interface is restored. For the primary interface, ScreenOS monitors three IP addresses to determine when failover occurs; each tracked IP address has the following weight:

- 100.100.100.100 6
- 200.200.200.200 4
- 210.210.210.210 3

For each of the above tracked IP addresses, the failure threshold is the default value 3. This means that if ScreenOS is unable to obtain a ping response from 100.100.100.100 three or more consecutive times, it will consider the IP address unreachable through the primary interface. For the primary interface, failover occurs when the interface failover threshold reaches 10. This means that if both IP addresses 100.100.100.100 and 200.200.200.200 become unreachable through the primary interface, the cumulative weights of the failures would be 10, which would cause an automatic failover to the backup interface. Note that if IP addresses 200.200.200.200 and 210.210.210.210 both become unreachable through the primary interface, the cumulative weights of the failures would be 7, and no failover would occur.



WebUI

1. Configuration > Operational Mode > Port Mode: Select Dual-Untrust from the drop-down list, and then click **Apply**.
2. At the following prompt, click **OK**:
Operational mode change will erase current configuration and reset the device, continue?
3. Network > Untrust Failover > Automatic Failover (select) > Apply.
4. Network > Interface (ethernet3) > Edit > Track IP: Enter the following, and then click **Apply**:

Track IP: 100.100.100.100

Weight: 6

Enter the following, and then click **Apply**:

Track IP: 200.200.200.200

Weight: 4

Enter the following, and then click **Apply**:

Track IP: 210.210.210.210

Weight: 3

5. Network > Interface (ethernet3) > Edit > Track IP Options: Enter the following, and then click **OK**:

Enable Track IP: (select)

Failover Threshold: 10

CLI

1. exec port-mode dual-untrust
2. At the following prompt, enter **y** (for yes):
Change port mode from <trust-untrust> to <dual-untrust> will erase system configuration and reboot box
Are you sure y/[n] ?
3. set interface failover auto
4. set interface ethernet3 track-ip
5. set interface ethernet3 track-ip threshold 10
6. set interface ethernet3 track-ip ip 100.100.100.100 weight 6
7. set interface ethernet3 track-ip ip 200.200.200.200 weight 4
8. set interface ethernet3 track-ip ip 210.210.210.210 weight 3

Interface Failover with VPN Tunnel Monitoring

You can specify an interface failover when certain VPN tunnels on the primary interface are determined to be “down.” For each VPN tunnel, you specify a failover weight, in percent. The assigned weights only come into play when the status of one or more monitored tunnels is “down”. If the cumulative weight of the down VPN tunnels reaches or exceeds 100%, ScreenOS fails over to the backup interface.

By applying a *weight*, or a value, to a VPN tunnel, you can adjust the importance of the tunnel status in relation to other tunnels. You can assign comparatively greater weight to relatively more important tunnels, and less weight to relatively less important tunnels. Note that the accumulated weights of *all* monitored VPN tunnels determine when interface failover occurs. For example, failure of a VPN tunnel with a weight of 50 brings the primary interface closer to a failover than would the failure of a VPN tunnel with a weight of 10. Also note that tunnels that are in “inactive,” “ready,” or undetermined state are counted as 50% of the assigned weight. That is, if you assign a weight of 50 to a tunnel that is in inactive state, the tunnel’s weight that is counted toward interface failover is 25.

If failover to the backup interface occurs, ScreenOS can still try to establish new VPN tunnel(s) on the primary interface if the VPN monitor rekey feature is enabled. If one or more VPN tunnels on the primary interface returns to “up” status so that the accumulated failover weight is less than 100%, ScreenOS can revert traffic back to the primary interface. Enable the VPN monitor rekey feature to allow ScreenOS to switch traffic from the backup interface to the primary.

Example: Configuring Automatic Failover with VPN Tunnel Monitoring

In this example, you first configure the NetScreen device for Dual Untrust mode. You then configure three VPN tunnels with the primary Untrust zone interface (the untrust interface) as the outgoing interface. For the primary interface, ScreenOS monitors three VPN tunnels to determine when failover occurs; each tunnel has the following failover weight:

- to_remote1 60
- to_remote2 40
- to_remote3 40

You also configure the device for automatic failover. If automatic failover from the primary interface to the backup interface occurs, the backup interface carries all traffic to and from the Untrust zone until the primary interface is restored. Primary interface failover occurs when the cumulative failover weight reaches or exceeds 100%. This means that if both to_remote1 and to_remote2 are down, the cumulative weight of the failures would be 100%, which would cause an automatic failover to the backup interface. Note that if only to_remote2 and to_remote3 are down, the cumulative weight of the failures would be 80%, and no failover would occur.

In this example, you also enable the VPN monitor rekey feature. In the event of a failover, this feature allows ScreenOS to revert traffic from the backup interface to the primary if the accumulated weight of the VPN tunnels on the primary interface becomes less than 100%.

WebUI

1. Configuration > Operational Mode > Port Mode: Select Dual-Untrust from the drop-down list, and then click **Apply**.
2. At the following prompt, click **OK**:
Operational mode change will erase current configuration and reset the device, continue?

VPN Tunnels

3. Network > Interfaces > Tunnel IF > New: Enter the following, and then click **OK**:
Tunnel Interface Name: tunnel.1
Zone: Untrust

- Fixed IP: (select)
IP Address/Netmask: 1.1.1.1/24
4. Network > Interfaces > Tunnel IF > New: Enter the following, and then click **OK**:
Tunnel Interface Name: tunnel.2
Zone: Untrust
Fixed IP: (select)
IP Address/Netmask: 2.2.2.2/24
 5. Network > Interfaces > Tunnel IF > New: Enter the following, and then click **OK**:
Tunnel Interface Name: tunnel.3
Zone: Untrust
Fixed IP: (select)
IP Address/Netmask: 3.3.3.3/24
 6. VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:
Gateway Name: remote_a
Security Level: Basic
Remote Gateway Type:
Static IP Address: (select), IP Address: 4.4.4.4
Preshared Key: netscreen1
Outgoing Interface: ethernet3
 7. VPNs > Autokey IKE > New: Enter the following, and then click **OK**:
VPN Name: to_remote1
Security Level: Basic
Remote Gateway:
Predefined: (select), remote_a

> Advanced: Enter the following advanced settings, and then click Return to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface: (select), tunnel.1

VPN Monitor: (select)

Rekey: (select)

8. VPNs > Autokey IKE > New: Enter the following, and then click **OK**:

VPN Name: to_remote2

Security Level: Basic

Remote Gateway:

Predefined: (select), remote_a

> Advanced: Enter the following advanced settings, and then click Return to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface: (select), tunnel.2

VPN Monitor: (select)

Rekey: (select)

9. VPNs > Autokey IKE > New: Enter the following, and then click **OK**:

VPN Name: to_remote3

Security Level: Basic

Remote Gateway:

Predefined: (select), remote_a

> Advanced: Enter the following advanced settings, and then click Return to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface: (select), tunnel.3

VPN Monitor: (select)

Rekey: (select)

Tunnel Failover

10. Network > Untrust Failover > Select the following, and then click **Apply**:

Failover Type: Tunnel Interface (select)

Automatic Failover (select)

Select **Edit Weight**. Enter the following, and then click **Apply**:

weight for VPN “to_remote1”: 60

weight for VPN “to_remote2”: 40

weight for VPN “to_remote3”: 40

CLI

1. exec port-mode dual-untrust
2. At the following prompt, enter **y** (for yes):
Change port mode from <trust-untrust> to <dual-untrust> will erase system configuration and reboot box
Are you sure y/[n] ?
3. set interface failover auto

VPN Tunnels

4. set interface tunnel.1 zone untrust
5. set interface tunnel.2 zone untrust
6. set interface tunnel.3 zone untrust
7. set interface tunnel.1 ip 1.1.1.1/24
8. set interface tunnel.2 ip 2.2.2.2/24
9. set interface tunnel.3 ip 3.3.3.3/24
10. set ike gateway remote_a ip 4.4.4.4 outgoing-interface untrust preshare netscreen1 sec-level basic
11. set vpn to_remote1 gateway remote_a sec-level basic
12. set vpn to_remote1 bind interface tunnel.1

13. set vpn to_remote1 monitor rekey
14. set vpn to_remote2 gateway remote_a sec-level basic
15. set vpn to_remote2 bind interface tunnel.2
16. set vpn to_remote2 monitor rekey
17. set vpn to_remote3 gateway remote_a sec-level basic
18. set vpn to_remote3 bind interface tunnel.3
19. set vpn to_remote3 monitor rekey

Tunnel Failover

20. set failover type tunnel-if
21. set vpn to_remote1 failover-weight 60
22. set vpn to_remote2 failover-weight 40
23. set vpn to_remote3 failover-weight 40

PPPoE Configuration

PPP-over-Ethernet (PPPoE) merges the Point-to-Point Protocol (PPP), which is usually used for dialup connections, with the Ethernet protocol, which can connect multiple users at a site to the same customer premises equipment. While many users can share the same physical connection, access control, billing, and type of service are handled on a per-user basis.

When there are two Ethernet interfaces (a primary and a backup) in the Untrust zone, you can configure one or both interfaces for PPPoE. For example, in Dual Untrust port mode, you can configure the primary interface (ethernet3) for DHCP and the backup interface (ethernet2) for PPPoE. Or, you can configure PPPoE for both the primary and backup interfaces. In ScreenOS, you configure a specific instance of PPPoE with a user name and password and other parameters, and bind the instance to an interface.

Example: Configuring PPPoE on Primary and Backup Untrust Interfaces

For this example, the NetScreen device is in Dual Untrust mode, and configured for automatic failover and IP tracking for the primary (ethernet3) interface, as shown in [“Example: Configuring Automatic Failover with IP Tracking” on page 19](#). In the following example, you configure PPPoE for both the primary (ethernet3) and backup (ethernet2) interfaces to the Untrust zone.

WebUI

PPPoE Configuration for ethernet3 Interface

1. Network > PPPoE > New: Enter the following, and then click **OK**:
 - PPPoE instance: eth3-pppoe
 - Bound to interface: ethernet3 (select)
 - Username: user1
 - Password: 123456
 - Authentication: Any (select)
 - Access Concentrator: ac-11

PPPoE Configuration for ethernet2 Interface

2. Network > PPPoE > New: Enter the following, and then click **OK**:
 - PPPoE instance: eth2-pppoe
 - Bound to interface: ethernet2 (select)
 - Username: user2
 - Password: 654321
 - Authentication: Any (select)
 - Access Concentrator: ac-22

CLI

PPPoE Configuration for ethernet3 Interface

1. set pppoe name eth3-pppoe username user1 password 123456
2. set pppoe name eth3-pppoe ac ac-11
3. set pppoe name eth3-pppoe authentication any
4. set pppoe name eth3-pppoe interface ethernet3

PPPoE Configuration for ethernet2 Interface

5. set pppoe name eth2-pppoe username user2 password 654321
6. set pppoe name eth2-pppoe ac ac-22
7. set pppoe name eth2-pppoe authentication any
8. set pppoe name eth2-pppoe interface ethernet2

DIAL BACKUP

You can connect an external modem to the RS-232 serial port on the NetScreen device to allow it to establish a PPP connection to an ISP. This provides a dial-up backup interface for traffic to the Untrust zone if there is a failure on the connection through the primary interface. The dial backup feature is enabled by default in ScreenOS 4.0.0-DIAL2 for the Trust-Untrust and Home-Work port modes (see [“Port Modes” on page 2](#)).

The dial backup feature allows two interfaces to the Untrust zone:

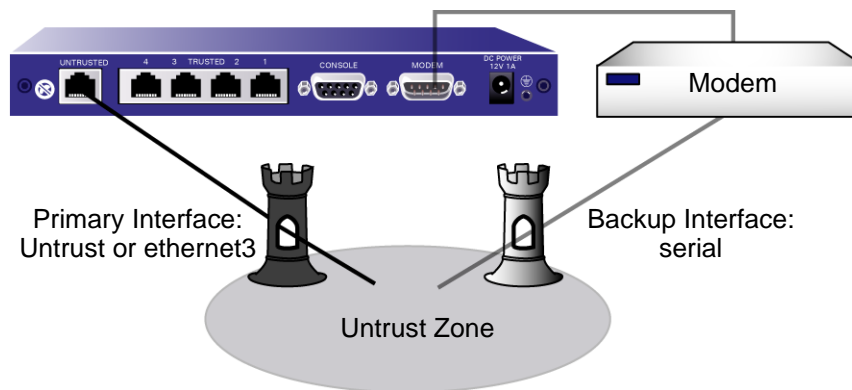
- The primary physical interface is the Untrusted Ethernet port. In ScreenOS, the primary logical interface is the Untrust interface in Trust-Untrust port mode and the ethernet3 interface in the Home-Work port mode.
- The backup physical interface is the modem port. In ScreenOS, the backup interface is the serial interface in either Trust-Untrust or Home-Work port modes. By default, the serial interface is bound to the Null zone and you need to bind it to the Untrust zone to use it as the backup interface.

You configure ScreenOS to dial through the modem to an existing ISP account when traffic is switched to the serial interface. When a switch to the serial interface occurs, the modem does not dial unless there is traffic² to be sent. ScreenOS can queue up to 64 packets while the dial-up link is brought up, so there is minimal data loss when traffic is switched to the serial interface.

By default, interface failover on the NetScreen device is manual. With manual failover, you need to force ScreenOS to switch traffic from one interface to the other using the CLI or WebUI. When the primary interface is again available, you need to use the CLI or WebUI to direct ScreenOS to switch traffic from the backup to the primary interface.

2. Only policy-enabled through (user-generated) traffic causes the modem to dial. Management or routing protocol related messages such as OSPF hellos do not cause modem dialup.

The NetScreen device can automatically fail over to the serial interface, including dialing and authenticating to a pre-existing ISP account. When the connection through the primary interface is restored, ScreenOS can automatically switch traffic from the serial interface back to the primary interface.



Modem Settings

The modem you use for the dial-up connection must support the following features:

- Hardware flow control
- Provide clear to send (CTS) signals
- Able to respond to request to send (RTS) signals
- Asynchronous only
- Support AT command set

You can configure the following serial link parameters in ScreenOS:

- The maximum amount of time that the serial link can be idle before ScreenOS automatically disconnects the modem (the default is 10 minutes)
- The number of times ScreenOS retries the dial-up connection if the line is busy or there is no response (the default is 3 times)
- The interval, in seconds, between dial-up retries (the default is 10 seconds)
- The maximum baud rate for the serial link (the default rate is 115200 bps)

ScreenOS uses a default modem initialization string. You can configure up to four modem initialization strings, but you can activate only one of the configured initialization strings at a time. The modem initialization string must meet the following requirements:

- Hardware flow control is recommended, but not required (you can specify no flow control)
- Software flow control is not used
- Result code must be displayed in verbal mode

Example: Configuring Modem Settings

In this example, you configure the modem idle time to be 20 minutes. You also define a modem initialization string for a new modem setting, *mod1*, and activate it.

WebUI

Network > Interfaces (serial) > Edit > Modem: Enter the following, and then click **OK**:

Modem Name: mod1

Init String: AT&FS7=255S32=6

Status: Enable (select)

Inactivity Timeout: 20

CLI

1. set modem idle-time 20
2. set modem settings mod1 init-strings AT&FS7=255S32=6
3. set modem settings mod1 active

ISP Configuration

You configure the NetScreen device to dial to an ISP account if a failover to the serial interface occurs and there is traffic to be sent. You can configure up to four ISP connections, assigning each a different priority number (1 is the highest priority). The priority number determines the order that ScreenOS uses in attempting the dial-up connection; ScreenOS dials up the ISP with the highest priority first. If ScreenOS is unable to log in to the ISP account with the highest priority, it will dial the ISP with the next highest priority number, and so on, until there are no more ISP configurations.

Note: By default, ScreenOS attempts to dial to a configured ISP account up to three times (see [“Modem Settings” on page 32](#) for information on modem parameters). If ScreenOS is not able to connect to any configured ISP account, it sends a connect fail message and waits until the primary interface is available again.

For each ISP configuration, you specify the following:

- Account login and password.³
- Primary phone number and, optionally, an alternate phone number. If the modem uses pulse dial by default but you want to use tone dial, precede the phone number with a **T**.
- Priority for this connection, relative to other configured ISP connections.

Example: Configuring ISP Information

In this example, you configure information for two different ISP accounts: the *isp1* account has a priority value of 1, while the *isp2* account has a priority value of 2. This means that ScreenOS will always dial up the *isp1* account first if failover to the serial interface occurs.

WebUI

1. Network > Interfaces (serial) > Edit > ISP: Enter the following, and then click **OK**:

ISP Name: isp1
Primary Number: 4085551111
Alternative Number: 4085552222
Login Name: kgreen
Login Password: 98765432
Priority: 1

2. Network > Dialup Backup > ISP: Enter the following, and then click **OK**:

ISP Name: isp2
Primary Number: 4085551212
Alternative Number:
Login Name: kgreen

3. The ISP account must be a standard Point-to-Point Protocol (PPP) account that only requires a username and password for login.

Login Password: 12345678

Priority: 2

In the WebUI, configured ISPs appear in a table at the bottom of the Interface (ISP) page. The root administrator and root-level admin users, including read-only admin users, can test an ISP configuration by clicking the Test button in the Configure column. Make sure that there is a modem connected to the serial interface on the NetScreen device that is properly configured (see [“Modem Settings” on page 32](#)), as ScreenOS will attempt to dial up the ISP account.

CLI

1. set modem isp isp1 account login kgreen password 98765432
2. set modem isp isp1 primary-number 4085551111 alternative-number 4085552222
3. set modem isp isp1 priority 1
4. set modem isp isp2 account login kgreen password 12345678
5. set modem isp isp2 primary-number 4085551212
6. set modem isp isp2 priority 2

Serial Interface Failover

By default, you must use the WebUI or CLI to force ScreenOS to switch over to the serial interface when the primary interface (Untrust or ethernet3 interface) connection fails and to switch back to the primary interface when the primary is again available. You can configure the interface failover to be automatic. You can also configure IP tracking to monitor failure on the Untrust or ethernet3 interfaces. See [“Interface Failover” on page 16](#) for more information.

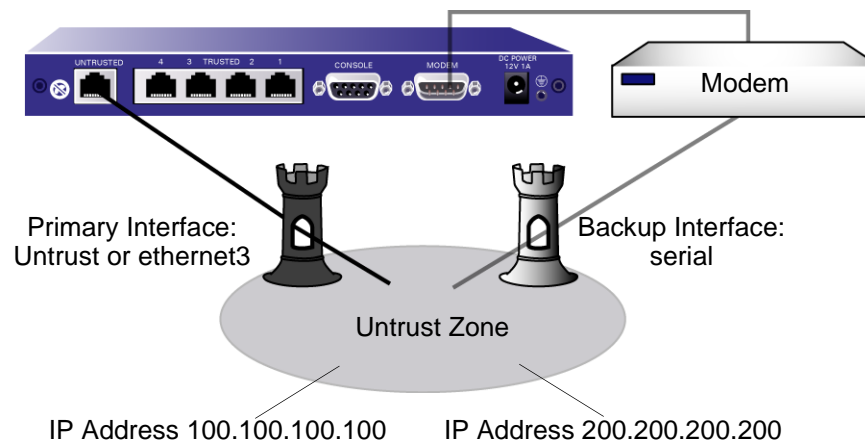
By default, policies that are enabled for traffic from the Trust zone to the Untrust zone or from the Untrust zone to the Trust zone are still active after a failover to the serial interface. Normal traffic through the primary interface can include large files that cannot be handled by the dialup link. When you define a policy, you can specify whether or not the policy should be active if ScreenOS switches to the serial interface. See [“Example: Specifying a Policy as Inactive for Serial Interface Failover” on page 40](#) for information on how to configure this in the WebUI and the CLI.

The serial interface is bound by default to the Null zone and you need to explicitly bind it to the Untrust zone to use it as a backup interface. If you bind the serial interface to the Untrust zone using the WebUI, ScreenOS automatically adds a default route for the serial interface. If you bind the serial interface to the Untrust zone using the CLI, ScreenOS does *not* add a default route to the serial interface and you must explicitly add a default route for the serial interface if traffic is to be routed through the serial interface. See [“Example: Adding or Deleting a Default Route for the Serial Interface” on page 39](#) for information on how to configure this in the WebUI and the CLI.

Example: Configuring Dial Backup in the Trust-Untrust Mode

In this example, you first bind the serial interface to the Untrust zone. The serial interface becomes the backup interface to the primary (the Untrust interface). You then configure ScreenOS to automatically fail over to the serial interface when the primary interface connection fails.

You configure IP tracking to determine failure of the primary interface—if IP addresses 100.100.100.100 and 200.200.200.200 become unreachable through the primary interface, ScreenOS automatically switches over to the backup interface.



WebUI

1. Network > Interfaces (serial) > Edit: Enter the following, and then click **OK**:
Zone Name: (select) Untrust
2. Network > Interfaces (serial) > Edit > Modem: Enter the following, and then click **OK**:
Modem Name: mod1
Init String: AT&FS7=255S32=6
Inactivity Timeout: 20
3. Network > Interfaces (serial) > Edit > ISP: Enter the following, and then click **OK**:
ISP Name: isp1
Primary Number: 4085551111
Alternative Number: 4085552222
Login Name: kgreen
Login Password: 98765432
Priority: 1
4. Network > Dialup Backup > ISP: Enter the following, and then click **OK**:
ISP Name: isp2
Primary Number: 4085551212
Alternative Number:
Login Name: kgreen
Login Password: 12345678
Priority: 2
5. Network > Untrust Failover > Automatic Failover: (select), and then click **Apply**.
6. Network > Interface (ethernet3) > Edit > Track IP: Enter the following, and then click **Apply**:

Track IP: 100.100.100.100

Weight: 6

Enter the following, and then click **Apply**:

Track IP: 200.200.200.200

Weight: 4

Enter the following, and then click **Apply**:

Track IP: 210.210.210.210

Weight: 3

7. Network > Interface (ethernet3) > Edit > Track IP Options: Enter the following, and then click **OK**:

Enable Track IP: (select)

Failover Threshold: 10

CLI

1. set interface serial zone untrust
2. set failover auto
3. set modem idle-time 20
4. set modem settings mod1 init-strings AT&FS7=255S32=6
5. set modem settings mod1 active
6. set modem isp isp1 account login kgreen password 98765432
7. set modem isp isp1 primary-number 4085551111 alternative-number 4085552222
8. set modem isp isp1 priority 1
9. set modem isp isp2 account login kgreen password 12345678
10. set modem isp isp2 primary-number 4085551212

11. set modem isp isp2 priority 2
12. set interface ethernet3 track-ip
13. set interface ethernet3 track-ip threshold 10
14. set interface ethernet3 track-ip ip 100.100.100.100 weight 6
15. set interface ethernet3 track-ip ip 200.200.200.200 weight 4
16. set interface ethernet3 track-ip ip 210.210.210.210 weight 3

Example: Adding or Deleting a Default Route for the Serial Interface

If you bind the serial interface to the Untrust zone using the WebUI, ScreenOS automatically adds a default route for the serial interface. In this example, you use the WebUI to bind the serial interface to the Untrust zone. You then delete the default route that has been automatically created for the serial interface.

WebUI

1. Network > Interfaces (serial) > Edit: Enter the following, and then click **OK**:
Zone Name: (select) Untrust
2. Network > Routing > Routing Table: In the Configure column, click **Remove** for the default route to 0.0.0.0/0 through the serial interface.

If you bind the serial interface to the Untrust zone using the CLI, ScreenOS does *not* add a default route to the serial interface and you must explicitly add a default route for the serial interface if traffic is to be routed through the serial interface. In this example, you use the CLI to bind the serial interface to the Untrust zone. You then add a default route for the serial interface, which is bound to the Untrust zone.

CLI

1. set interface serial zone untrust
2. set route 0.0.0.0/0 interface serial

Example: Specifying a Policy as Inactive for Serial Interface Failover

In this example, normal traffic through the primary interface (ethernet3) to the Untrust zone includes large files transferred via FTP from host22 in the Trust zone to ftp_srv in the Untrust zone. If a failover to the serial interface occurs, this particular FTP traffic should be dropped by the dialup link. The policy permitting this traffic on the primary interface becomes a deny policy when there is a failover to the backup interface.

WebUI

Policies > (From: Trust, To: Untrust) > New: Enter the following, and then click **OK**:

Source Address:

Address Book: (select), host22

Destination Address:

Address Book: (select), ftp_srv

Service: FTP

Action: Permit

> Advanced: Clear **Valid for Serial**, and then click **Return** to set the advanced options and return to the basic configuration page.

CLI

```
set policy from trust to untrust host22 ftp_srv ftp permit no-session-backup
```

LOOPBACK INTERFACES

A loopback interface is a logical interface that emulates a physical interface on the NetScreen device. However, unlike a physical interface, a loopback interface is always in the up state as long as the device on which it resides is up. Loopback interfaces are named `loopback.id_num`, where `id_num` is a number from 1 to 10^4 and denotes a unique loopback interface on the device. Like a physical interface, you must assign an IP address to a loopback interface and bind it to a security zone.

For example, to create the loopback interface `loopback.1`, bind it to the Untrust zone, and assign the IP address `1.1.1.2/24` to it, do the following.

WebUI

Network > Interfaces > Loopback IF (select) > New: Enter the following, and then click **OK**:

Interface Name: `loopback.1`

Zone: Untrust (select)

IP Address/Netmask: `1.1.1.2/24`

CLI

1. `set interface loopback.1 zone untrust`
2. `set interface loopback.1 ip 1.1.1.27`

Note that the loopback interface is not directly accessible from networks or hosts that reside in other zones. You must define a policy to permit traffic to and from the interface.

You can manage the NetScreen device using either the loopback interface's IP address or a managed IP address that you assign to the loopback interface. For example, to manage a device using the previously-defined `loopback.1` IP address `1.1.1.2/24`, do the following.

4. The maximum `id_num` value you can specify is platform-specific.

WebUI

Network > Interfaces > loopback.1 > Edit: Make sure that all management services are selected (checked), and then click **OK**.

CLI

```
set interface loopback.1 manage
```

Like a physical interface, the loopback interface can support BGP applications running on the NetScreen device. To enable the BGP routing protocol on the loopback.1 interface, do the following.

Note: To enable BGP on the loopback interface, you must first create a BGP instance for the virtual router in which the interface will be bound.

WebUI

Network > Interfaces > loopback.1 > Edit: Select Protocol BGP, and then click **OK**.

CLI

```
set interface loopback.1 protocol bgp
```

You can configure Virtual Security Interfaces (VSIs) for NSRP on a loopback interface. The physical state of the VSI on the loopback interface is always up. The interface can be active or not, depending upon the state of the VSD group to which the interface belongs.

WebUI

Network > Interfaces > New VSI IF: Enter the following, and then click **OK**:

Interface Name: VSI Base: loopback.1

VSD Group: 1

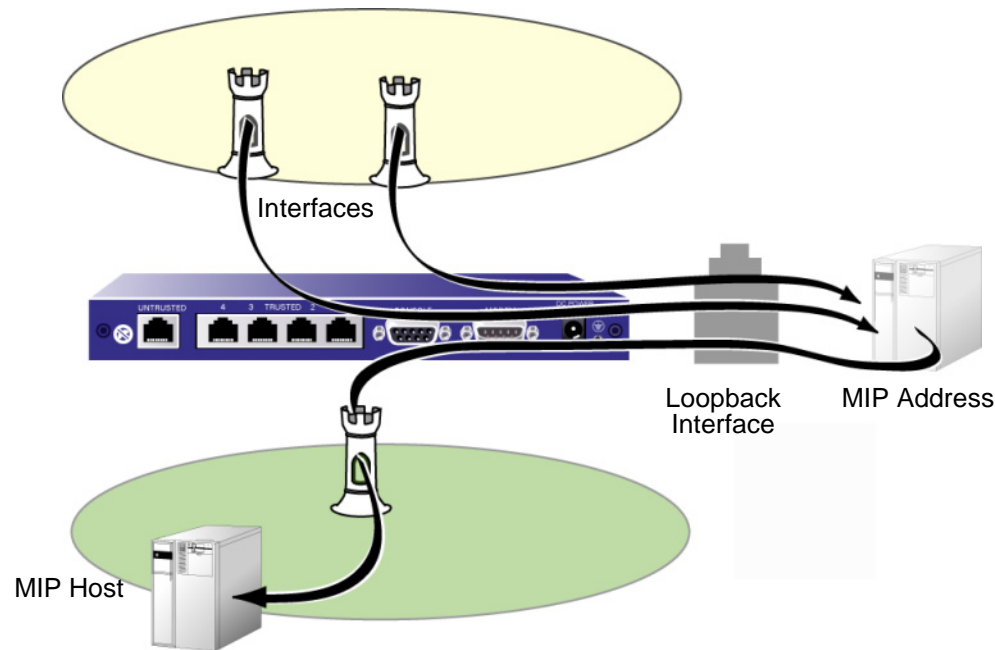
IP Address/netmask: 1.1.1.1/24

CLI

```
set interface loopback.1:1 ip 1.1.1.1/24
```

Using the Loopback Interface for MIPs

Mapped IP (MIP) is a one-to-one mapping of an IP address in an IP packet header to another static IP address. Defining a MIP on the loopback interface allows a MIP to be accessed by a group of interfaces. The primary application for this is to allow a node to reach a MIP host through one of several VPN tunnels using a single MIP address. The MIP host can also reach a node through the appropriate tunnel.



You can think of the loopback interface as a resource holder that contains the MIP address mapping. You configure a loopback interface with the name `loopback.id_num` (where `id_num` is an index number that uniquely identifies the interface in the device), and assign an IP address to the interface (see [“Loopback Interfaces” on page 41](#)). To allow other interfaces to use the MIP on the loopback interface, you then add the interfaces as members of the loopback group.

The maximum number of members in a loopback group is 10. The loopback interface and its member interfaces must be in different IP subnets in the same zone. Any type of interface can be a member of a loopback group as long as the interface has an IP address. If you configure a MIP on both a loopback interface and one of its member interfaces, the loopback interface configuration takes precedence.

A loopback interface cannot be a member of another loopback group.

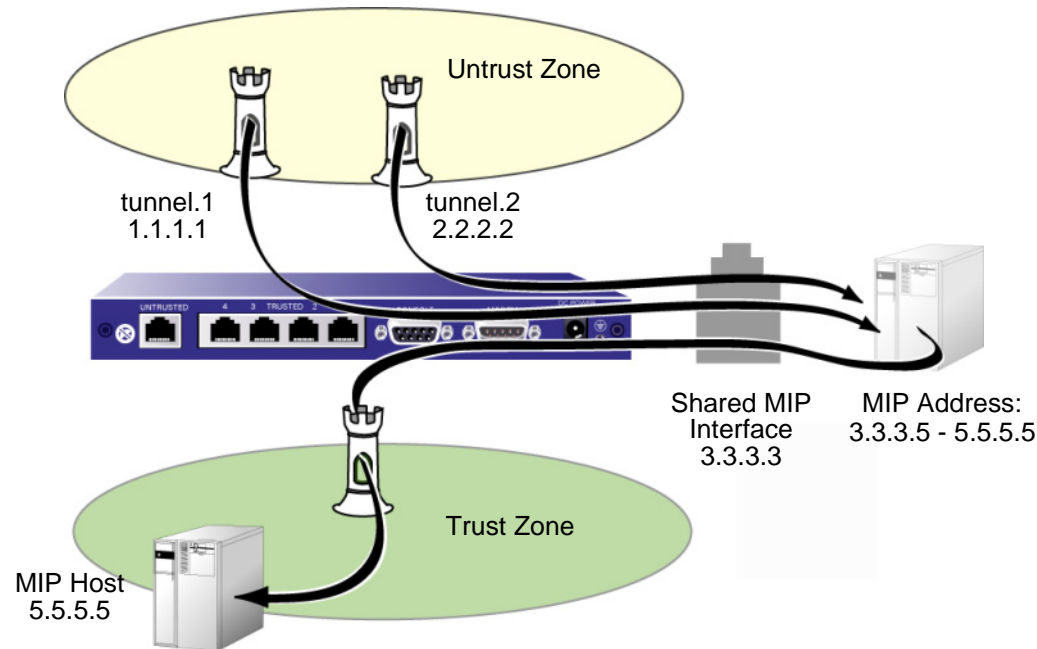
Interface Failover

Multiple tunnels to the same VPN destination must run in active-backup mode only; the tunnels cannot be active at the same time. By default, you must use the WebUI or the CLI to switch over the backup tunnel interface when the active interface connection fails. You can configure automatic interface failover. You can also configure IP tracking to monitor the status of the tunnel interfaces and determine when an interface has failed (see [“Interface Failover” on page 16](#)).

Example: Configuring a Single MIP for Different Tunnel Interfaces

In this example, you configure a loopback interface, `loopback.3`, in the Trust zone, with the IP address 3.3.3.3. Members of the loopback interface group are `tunnel.1` and `tunnel.2`. The loopback interface holds the MIP 3.3.3.5, which maps to the host 5.5.5.5. When a packet destined for 3.3.3.5 arrives at `tunnel.1`, ScreenOS first searches for the MIP at `tunnel.1`, then at the loopback interface `loopback.3`. When it finds a match at `loopback.3`, it translates the

original destination IP (3.3.3.5) to the host IP address 5.5.5.5 and the packet is routed to the MIP host. Note that traffic destined for 3.3.3.5 can also arrive at tunnel.2. ScreenOS searches for the MIP at tunnel.2, then at the loopback interface loopback.3. Again, ScreenOS finds a match at loopback.3 and translates the original destination IP 3.3.3.5 to the host IP address 5.5.5.5 and the packet is routed to the MIP host.



For replies that are returned from the MIP host back to the original sender, ScreenOS performs a routing table lookup to determine on which interface to route the reply. The route that has the lowest metric is chosen. Note that the reply from the MIP host can be routed on a different interface than the original message to the MIP host. For example, packets for the MIP host from a sender in the Untrust zone can arrive at the tunnel.1 interface, but replies from the MIP host to the sender can be routed back through the tunnel.2 interface.

WebUI

Loopback Interface and MIP

1. Network > Interfaces > Loopback IF (select) > New: Enter the following, and then click **Apply**:

Interface Name: loopback.3

Zone: Trust (select)

IP Address/Netmask: 3.3.3.3./24

> MIP: Enter the following, and then click **OK**:

Mapped IP: 3.3.3.5

Netmask: 255.255.255.255

Host IP Address: 5.5.5.5

Host Virtual Router Name: trust-vr

Loopback Group Members

2. Network > Interfaces > Tunnel IF (select) > New: Enter the following for tunnel.1, and then click **OK**:

Member of Loopback Group: loopback.3

Zone: Trust (select)

Fixed IP:

IP Address/Netmask: 1.1.1.1/24

3. Network > Interfaces > Tunnel IF (select) > New: Enter the following for tunnel.2, and then click **OK**:

Member of Loopback Group: loopback.3

Zone: Trust (select)

Fixed IP:

IP Address/Netmask: 2.2.2.2/24

CLI

Loopback Interface

1. set interface loopback.3 zone trust
2. set interface loopback.3 ip 3.3.3.3/24

Loopback Group Members

3. set interface tunnel.1 zone trust
4. set interface tunnel.2 zone trust
5. set interface tunnel.1 ip 1.1.1.1/24
6. set interface tunnel.2 ip 2.2.2.2/24
7. set interface tunnel.1 loopback-group loopback.3
8. set interface tunnel.2 loopback-group loopback.3

MIP

9. set interface loopback.3 mip 3.3.3.5 host 5.5.5.5

XAUTH CLIENT

An XAuth client is a remote user or device that connects to an XAuth server via an AutoKey IKE VPN tunnel. Whereas the authentication of IKE users is actually the authentication of individual devices, the authentication of XAuth users is the authentication of the users themselves. ScreenOS can act as an XAuth client, responding to authentication requests from a remote XAuth server.

NetScreen supports XAuth version 6 (v6). To confirm that both parties in Phase 1 IKE negotiations support XAuth v6, they each send the vendor ID 0x09002689DFD6B712 to each other in the first two Phase 1 messages. This vendor ID number is specified in the XAuth Internet draft, draft-beaulieu-ike-xauth-02.

After the completion of Phase 1 negotiations, the remote XAuth server sends a login prompt to the NetScreen device. If ScreenOS successfully logs in with the correct user name and password, ScreenOS and the XAuth server continue with Phase 2 negotiations. ScreenOS initiates Phase 2 negotiations only after XAuth authentication is completed and blocks any Phase 2 negotiation requests from the XAuth server before the authentication is completed.

To configure an XAuth client on the NetScreen device, you specify the following:

- IKE gateway name
- Xauth user name and password

You can configure the following types of XAuth authentication for the ScreenOS client:

- any — allows any authentication type
- chap — allows Challenge Handshake Authentication Protocol (CHAP) only

Example: Configuring the NetScreen Device as an XAuth Client

In this example, you first configure a remote IKE gateway *gw1* with IP address 220.2.2.21. You specify standard security level and use the preshared key *netscreen1*. You then configure an XAuth client for the IKE gateway with the username *beluga9* and the password *1234567*. You also specify CHAP authentication for the client.

WebUI

VPN > AutoKey Advanced > Gateway > New: Enter the following, and then click **Advanced**:

Gateway Name: gw1

Security Level: Standard (select)

Static IP address: (select)

IP Address: 220.2.2.21

Preshared Key: netscreen1

Enter the following, and then click **Return**:

XAuth Client: (select)

User Name: beluga9

Password: 1234567

Allowed Authentication Type (select) CHAP Only

Click **OK**

CLI

1. set ike gateway "gw1" ip 220.2.2.21 Main outgoing-interface "untrust" preshare "netscreen1" sec-level standard
2. set ike gateway "gw1" xauth client chap username beluga1 password 1234567

DESTINATION IP FOR VPN MONITOR

NetScreen devices can monitor network connectivity between VPN gateways by sending pings at specified intervals through the tunnel to the remote gateway. On some devices, however, the remote gateway may not be capable of responding to ping requests. In this case, you can specify a different remote IP address to which the NetScreen device sends the ping requests. The remote IP address does not have to be on the same subnet as the gateway address.

For more information about VPN monitoring, see Chapter 2, “Monitoring NetScreen Devices,” in Volume 3, “Administration,” in the *NetScreen Concepts and Examples ScreenOS Reference Guide*.

Example: Specifying a Destination IP for VPN Monitoring

In this example, you configure the VPN monitor on the NetScreen device to send pings to the IP address 100.10.10.10.

WebUI

1. VPNs > AutoKey IKE > New: Configure the VPN, and then click **Advanced**.
Enter the following, and then click **Return** to go back to the basic VPN configuration screen:
VPN Monitor: (select)
Source Interface: (select)
Destination IP: 100.10.10.10
2. Click **OK**.

CLI

1. set vpn *name_str* gateway *name_str*
2. set vpn *name_str* monitor source-interface *interface* destination-ip 100.10.10.10

DHCP SERVER ENHANCEMENT

By default, some NetScreen devices act as Dynamic Host Configuration Protocol (DHCP) servers, allocating dynamic IP addresses to DHCP clients. When the NetScreen device boots ScreenOS 4.0.0-DIAL2, the system automatically stops the local DHCP server process from starting if another DHCP server is detected on the network. To detect another DHCP server, ScreenOS sends out DHCP boot requests at two-second intervals. If the NetScreen device does not receive any response to its boot requests, it then starts its local DHCP server process.

If the NetScreen device receives a response from another DHCP server, the system generates a message indicating that the DHCP service is enabled on the NetScreen device but not started because another DHCP server is present on the network. The log message includes the IP address of the existing DHCP server.

The default Auto mode causes the Netscreen device to always check for an existing DHCP server at bootup. You can configure ScreenOS to not attempt to detect another DHCP server on an interface by setting the NetScreen DHCP server to Enable or Disable mode. In Enable mode, the DHCP server is always on and ScreenOS does not check if there is an existing DHCP server on the network. In Disable mode, the DHCP server is always off.

Example: Turning off DHCP Server Detection

In this example, you set the DHCP server on the ethernet1 interface to start up without checking to see if there is an existing DHCP server on the network.

WebUI

Network > Interfaces > Edit (for ethernet1) > DHCP: Enter the following, and then click **OK**:

DHCP Server: (select)

Enable: (select)

CLI

```
set interface ethernet1 dhcp server enable
```

Note: Issuing the CLI command **set interface** interface **dhcp server service** command activates the DHCP server. The default mode of the server is to automatically check first to see if there is an existing DHCP server on the network. The DHCP server on the NetScreen device starts only if it does not find an existing server on the network. Issuing the **unset interface** interface **dhcp server service** command disables the DHCP server on the NetScreen device and also deletes any existing DHCP configuration.

ROUTING INFORMATION PROTOCOL (RIP) VERSION 2

Routing information protocol (RIP) is a distance vector protocol used as an Interior Gateway Protocol (IGP) in moderate-sized autonomous systems (ASs). ScreenOS supports RIP version 2 (RIPv2), as defined by RFC 2453. While RIPv2 supports only simple password (plain text) authentication, NetScreen's RIP implementation also supports MD5 authentication extensions, as defined by RFC 2082.

As mentioned previously, RIP is intended for moderate-sized networks. It can also be used to manage route information within a small, homogeneous, network such as a corporate LAN. The longest path allowed in a RIP network is 15 hops. A metric value of 16 indicates an invalid or unreachable destination (this value is also referred to as "infinity" since it is larger than the 15-hop maximum allowed in RIP networks).

RIP is not intended for large networks or networks where routes are chosen based on real-time parameters such as measured delay, reliability, or load. RIP supports both point-to-point networks (used with VPNs) and broadcast/multicast Ethernet networks. RIP does not support point-to-multipoint interfaces.

RIP sends out messages that contain the complete routing table to every neighboring router every 30 seconds. These messages are normally sent as multicasts to address 224.0.0.9 from the RIP port.

The RIP routing database contains one entry for every destination that is reachable through the RIP routing instance. The RIP routing database includes the following information:

- IPv4 address of a destination. Note that RIP does not distinguish between networks and hosts.
- IP address of the first router along the route to the destination (the next hop).
- Network interface used to reach the first router.
- Metric that indicates the distance, or cost, of getting to the destination. Most RIP implementations use a metric of 1 for each network.
- A timer that indicates the time that has elapsed since the database entry was last updated.

Basic RIP Configuration

Like OSPF and BGP, you create RIP on a per-Virtual Router basis on a NetScreen device. If you have multiple virtual routers (VRs) in a system, you can enable multiple instances of RIP, one instance for each VR.

This section describes the following basic steps to configure RIP on a NetScreen device:

1. Create the RIP routing instance in a Virtual Router.
2. Enable the RIP instance.
3. Redistribute routes learned from different routing protocols (such as OSPF, BGP, or statically configured routes) into the RIP instance.

This section describes how to perform each of these tasks using either the CLI or the WebUI.

You can also optionally configure other RIP parameters such as the following:

- Global parameters, such as timers and trusted RIP neighbors, that are set at the VR level for the RIP protocol (see [“Global Parameters” on page 60](#))
- Interface parameters, such as neighbor authentication, that are set on a per-interface basis for the RIP protocol (see [“Interface Parameters” on page 61](#))
- Security-related RIP parameters, that are set at either the VR level or on a per-interface basis (see [“Security Configuration” on page 63](#))

Creating a RIP Routing Instance in a Virtual Router

As described previously, you create a RIP routing instance on a specific virtual router on a NetScreen device. Deleting a RIP routing instance in a VR removes the corresponding RIP configurations for all interfaces that are in the VR. For more information about virtual routers and configuring a virtual router on NetScreen devices, see Chapter 3, “Routing and Virtual Routers,” in Volume 2, “Fundamentals,” in the *NetScreen Concepts and Examples ScreenOS Reference Guide*.

Example: Creating a RIP Routing Instance

In this example, you create a RIP routing instance on the virtual router trust-vr.

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit: Select **Create RIP Instance**, and then click **OK**.

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol rip

Enabling the RIP Instance

You enable (and disable) RIP functions at two different levels:

- Enabling and disabling RIP at the VR level affects the RIP instance in the VR. When you enable RIP at the VR level, RIP can transmit and process RIP packets received on all RIP-enabled interfaces in the VR. When you disable RIP at the VR level, RIP stops transmitting and processing RIP packets on *all* RIP-enabled interfaces in the VR.
- Enabling and disabling RIP on an interface affects RIP on only a *specific* interface. By default, RIP is disabled on all interfaces in the VR and you must explicitly enable it on an interface. When you disable RIP at the interface level, RIP does not transmit or receive packets on the specified interface. Interface configuration parameters are preserved when you disable RIP on an interface.

Example: Enabling a RIP Routing Instance

In this example, you enable the RIP routing instance on the virtual router trust-vr and enable RIP on the trust interface.

WebUI

RIP Routing Instance

1. Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIP Instance: Select **Enable**, and then click **OK**.

RIP Interface

2. Network > Interface > Edit (for Trust interface) > RIP: Select **Enable**, and then click **Apply**.

CLI

RIP Routing Instance

1. ns-> set vrouter trust-vr protocol rip enable

RIP Interface

2. ns-> set interface trust protocol rip enable

Example: Removing a RIP Routing Instance

As mentioned previously, you can delete RIP for the VR or for a specific interface. In this example, you delete the RIP routing instance on the virtual router trust-vr and disable RIP on the trust interface.

WebUI

RIP Routing Instance

1. Network > Routing > Virtual Router (trust-vr) > Edit: Select **Delete RIP Instance**, and then click **OK** at the confirmation prompt.

RIP Interface

2. Network > Interface (for Trust interface) > RIP: Clear **Enable**, and then click **Apply**.

CLI

RIP Routing Instance

1. ns-> unset vrouter trust-vr protocol rip

RIP Interface

2. ns-> unset interface trust protocol rip

Redistributing Routes

Route redistribution is the exchange of route information between routing protocols. For example, you can redistribute the following types of routes into the RIP routing instance in the same virtual router:

- Routes learned from BGP
- Routes learned from OSPF
- Directly connected routes
- Imported routes
- Statically configured routes

You need to configure a route map to filter the routes that are redistributed. For more information about creating route maps for route redistribution, see Chapter 3, “Routing and Virtual Routers” in Volume 2, “Fundamentals,” of the *NetScreen Concepts and Examples ScreenOS Reference Guide*.

Routes imported into RIP from other protocols have a default metric of 1. You can change the default metric (see [“Global Parameters” on page 60](#)).

Example: Redistributing Routes into RIP

In this example, you redistribute static routes that are in the subnetwork 20.1.0.0/16 to RIP neighbors in the trust-vr virtual router. To do this, you first create an access list to permit addresses in the 20.1.0.0/16 subnetwork. Then, configure a route map that permits addresses that match the access list you configured. Use the route map to specify the redistribution of static routes into the RIP routing instance.

WebUI

1. Network > Routing > Virtual Router (trust-vr) > Access List > New: Enter the following, and then click **OK**:
 - Access List ID: 20
 - Sequence No.: 1
 - IP/Netmask: 20.1.0.0/16
 - Action: Permit (select)

2. Network > Routing > Virtual Router (trust-vr) > Route Map > New: Enter the following, and then click **OK**:
 - Map Name: rtmap1
 - Action: Permit (select)
 - Sequence No.: 1
 - Match Properties:
 - Access List: 20 (select)
3. Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIP Instance > Redistributable Rules: Enter the following, and then click **Add**:
 - Route Map: rtmap1 (select)
 - Protocol: Static (select)

CLI

1. set vrouter trust-vr acc-list 20 permit ip 20.1.0.0/16 1
2. set vrouter trust-vr route-map name rtmap1 permit 1
3. set vrouter trust-vr route-map rtmap1 1 match ip 20
4. set vrouter trust-vr protocol rip redistribute route-map rtmap1 protocol static

Global Parameters

This section describes RIP global parameters that you can configure at the VR level. When you configure a RIP parameter at the VR level, the parameter setting affects operations on all RIP-enabled interfaces. You can modify global parameter settings through the RIP routing protocol context in the CLI or by using the WebUI.

The following table describes the RIP global parameters and their default values.

RIP Global Parameter	Description	Default Value
Default metric	Default metric value for routes imported into RIP from other protocols, such as OSPF and BGP.	10
Update timer	Specifies, in seconds, when to issue updates of RIP routes to neighbors.	30 seconds
Maximum packets per update	Specifies the maximum number of packets received per update.	No maximum
Invalid timer	Specifies, in seconds, when a route becomes invalid from the time a neighbor stops advertising the route.	180 seconds
Flush timer	Specifies, in seconds, when a route is removed from the time the route is invalidated.	120 seconds
Maximum neighbors	The maximum number of RIP neighbors allowed.	16
Trusted neighbors	Specifies an access list that defines RIP neighbors. If no neighbors are specified, RIP uses multicasting or broadcasting to detect neighbors on an interface.	No neighbors are configured
Allow neighbors on different subnet	Specifies that RIP neighbors on different subnets are allowed.	Disabled
Advertise default route	Specifies whether the default route (0.0.0.0/0) is advertised.	Disabled
Reject default route	Specifies whether RIP rejects a default route learned from another protocol.	Disabled
Incoming route map	Specifies the filter for routes to be learned by RIP.	None
Outgoing route map	Specifies the filter for routes to be advertised by RIP.	None

Example: Advertising the Default Route to RIP Neighbors

By default, the default route (0.0.0.0/0) is not advertised to RIP neighbors. The following command advertises the default route to RIP neighbors in the trust-vr virtual router with a metric of 5 (you must enter a metric value). The default route must exist in the routing table.

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIP Instance: Enter the following, and then click **OK**.

Advertising Default Route: (select)

Metric: 5

CLI

```
set vrouter trust-vr protocol rip adv-default-route always metric number 5
```

See [Chapter 2 “New and Modified CLI Commands” on page 69](#) for more information about global parameters that you can configure in the RIP routing protocol context.

Interface Parameters

This section describes RIP parameters that you configure at the interface level. When you configure a RIP parameter at the interface level, the parameter setting affects the RIP operation only on the specific interface. You can modify interface parameter settings with **interface** commands in the CLI or by using the WebUI.

The following table describes the RIP interface parameters and their default values.

RIP Interface Parameter	Description	Default Value
Split-horizon	Specifies whether to enable split-horizon (do not advertise routes learned from a neighbor back to the same neighbor). If this is disabled, routes that are learned from a neighbor are advertised back to the same neighbor with a metric of 16.	Disabled

RIP Interface Parameter	Description	Default Value
RIP metric	Specifies the RIP metric for the interface.	1
Authentication	Specifies either clear text password or MD5 authentication.	No authentication used.
Passive mode	Specifies that the interface is to receive but not transmit RIP packets.	No
Incoming route map	Specifies the filter for routes to be learned by RIP.	None
Outgoing route map	Specifies the filter for routes to be advertised by RIP.	None

You can define incoming and outgoing route map filters at the VR level or at the interface level. A route map filter you define at the interface level takes precedence over a route map filter defined at the VR level. For example, if you define an incoming route map at the VR level and a different incoming route map at the interface level, the incoming route map defined at the interface level takes precedence.

Example: Setting RIP Interface Parameters

In this example, you configure the following RIP parameters for the trust interface:

- Set MD5 authentication, with the key 1234567898765432 and the key ID 215.
- Enable split horizon for the interface.

WebUI

Network > Interfaces(Edit) > RIP: Enter the following, and then click **OK**:

Authentication: MD5 (select)

Key: 1234567898765432

Key ID: 215

Split Horizon: (select)

CLI

1. set interface trust protocol rip authentication md5 1234567898765432 key -id 215
2. set interface trust protocol rip split-horizon

Security Configuration

This section describes possible security problems in the RIP routing domain and methods of preventing attacks.

Note: *To make RIP more secure, you should configure all routers in the RIP domain to be at the same security level. Otherwise, a compromised RIP router can bring down the entire RIP routing domain.*

Authenticating Neighbors

A RIP router can be easily spoofed, since RIP packets are not encrypted and most protocol analyzers provide decapsulation of RIP packets. Authenticating RIP neighbors is the best way to fend off these types of attacks.

RIP provides both simple password and MD5 authentication to validate RIP packets received from neighbors. All RIP packets received on the interface that are not authenticated are discarded. By default, there is no authentication enabled on any RIP interface.

Example: Configuring Neighbor Authentication

In this example, you configure MD5 authentication, with the key 1234567898765432 and the key ID 215, for the trust interface.

WebUI

Network > Interfaces (Edit) > RIP: Enter the following, and then click **OK**:

Authentication: MD5 (select)

Key: 1234567898765432

Key ID: 215

CLI

```
set interface trust protocol rip authentication md5 1234567898765432 key -id 215
```

Filtering RIP Neighbors

Multi-access environments can allow devices, including routers, to be connected into a network relatively easily. This can cause stability or performance issues if the connected device is not reliable. To prevent this problem, you can use an access list to filter the devices that are allowed to become RIP neighbors. By default, RIP neighbors are limited to devices that are on the same subnet as the NetScreen virtual router.

Example: Configuring Trusted Neighbors

In this example, you configure the following global parameters for the RIP routing instance running in the trust-vr virtual router:

- Maximum number of RIP neighbors is 1.
- The IP address of the trusted neighbor, 10.1.1.1, is specified in an access-list.

WebUI

1. Network > Routing > Virtual Router (trust-vr) > Access List > New: Enter the following, and then click **OK**:
 - Access List ID: 10
 - Sequence No.: 1
 - IP/Netmask: 10.1.1.1/32
2. Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIP Instance: Enter the following, and then click **OK**:
 - Maximum Neighbors: 1
 - Trusted Neighbors: 10

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set access-list 10 permit ip 10.1.1.1/32 1
3. ns(trust-vr)-> set protocol rip
4. ns(trust-vr/rip)-> set max-neighbor-count 1
5. ns(trust-vr/rip)-> set trusted-neighbors 10

Rejecting Default Routes

In a Route Detour Attack, a router injects a default route (0.0.0.0/0) into the routing domain in order to detour packets to itself. The router can then either drop the packets, causing service disruption, or it can obtain sensitive information in the packets before forwarding them. On NetScreen devices, RIP by default accepts any default routes that are learned in RIP and adds the default route to the routing table.

Example: Rejecting Default Routes

In this example, you configure the RIP routing instance running in the trust-vr virtual router to reject any default routes that are learned in RIP.

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIP Instance: Enter the following, and then click **OK**:

Reject Default Route Learnt by RIP: (select)

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr) -> set protocol rip
3. ns(trust-vr)-> set reject-default-route

Protecting Against Flooding

A malfunctioning or compromised router can flood its neighbors with RIP routing update packets. On NetScreen virtual routers, you can configure the maximum number of update packets that can be received on a RIP interface within a certain interval to avoid flooding of update packets. All update packets that exceed the configured update threshold are dropped. If you do not set an update threshold, all update packets are accepted.

You need to exercise care when configuring an update threshold when neighbors have large routing tables, as the number of routing updates can be quite high within a given duration because of flash updates. Update packets that exceed the threshold are dropped and valid routes may not be learned.

Example: Configuring an Update Threshold

In this example, you set the maximum number of routing update packets that RIP can receive on an interface to 4.

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIP Instance: Enter the following, and then click **OK**:

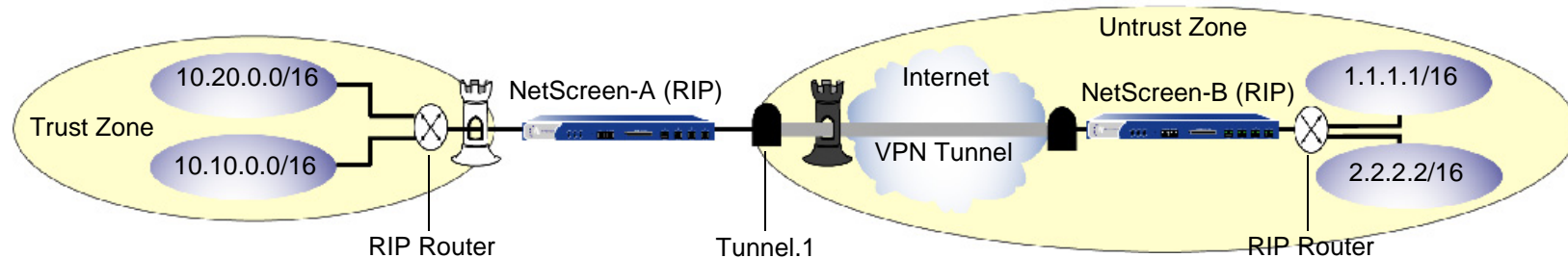
Maximum Number Packets per Update Time: 4

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol rip
3. ns(trust-vr/rip)-> set threshold-update 4

Example: Configuring RIP for the Trust and Untrust Zones

The following example creates and enables a RIP routing instance in the Trust-VR virtual router on the device NetScreen-A. You enable RIP on both the VPN tunnel interface and the Trust zone interface. Only routes that are in the subnet 10.10.0.0/16 are advertised to the RIP neighbor on NetScreen-B. This is done by first configuring an access list that permits only addresses in the subnet 10.10.0.0/16, then specifying a route map *abcd* that permits routes that match the access list. You then specify the route map to filter the routes that are advertised to RIP neighbors.



WebUI

1. Network > Routing > Virtual Router > Edit (for trust-vr) > Create RIP Instance: Select **Enable RIP**, and then click **OK**.
2. Network > Routing > Virtual Router > Access List (for trust-vr) > New: Enter the following, and then click **OK**:

Access List ID: 10

Sequence No.: 10

IP/Netmask: 10.10.0.0/16

Action: Permit

3. Network > Routing > Virtual Router > Route Map (for trust-vr) > New: Enter the following, and then click **OK**:
 - Map Name: abcd
 - Sequence No.: 10
 - Action: Permit
 - Match Properties:
 - Access List: (select), 10
4. Network > Routing > Virtual Router > Edit (for trust-vr) > Edit RIP Instance: Select the following, and then click **OK**:
 - Outgoing Route Map Filter: abcd
5. Network > Interfaces > Edit (for tunnel.1) > RIP: Enter the following, and then click **Apply**:
 - Enable RIP: (select)
6. Network > Interfaces > Edit (for trust) > RIP: Enter the following, and then click **Apply**:
 - Enable RIP: (select)

CLI

1. set vrouter trust-vr protocol rip
2. set vrouter trust-vr protocol rip enable
3. set interface tunnel.1 protocol rip enable
4. set interface trust protocol rip enable
5. set vrouter trust-vr access-list 10 permit ip 10.10.0.0/16 10
6. set vrouter trust-vr route-map name abcd permit 10
7. set vrouter trust-vr route-map abcd 10 match ip 10
8. set vrouter trust-vr protocol rip route-map abcd out

New and Modified CLI Commands

This chapter introduces the following new commands:

- **failover** on page 71
- **modem** on page 84
- **port-mode** on page 92
- **RIP Context Commands** on page 97

In addition, it presents changes to the following commands:

- **bgp** on page 70
- **ike** on page 74
- **interface** on page 76
- **policy** on page 91
- **pppoe** on page 95
- **vpn** on page 123
- **vrouter** on page 125

New command elements in the Syntax sections appear in **red**. For example, in the following command, **retry-time number** is new in this release:

```
set vrouter vrouter protocol bgp retry-time number
```

The following command descriptions focus only on the new elements added in this release. For more information about other command elements, refer to the *NetScreen CLI Reference Guide*.

Description: Use the **bgp** context commands to configure the Border Gateway Protocol (BGP) on a virtual router in a NetScreen device.

Note: This section only describes the new **retry-time** keyword for the **bgp** commands. For more information on other keywords and variables for the **bgp** commands, refer to the NetScreen CLI Reference Guide.

Syntax

set

```
set vrouter vrouter protocol bgp retry-time number
```

Keywords and Variables

retry-time

```
set vrouter vrouter protocol bgp retry-time number
```

retry-time Specifies the interval, in seconds, at which ScreenOS tries to re-establish a TCP connection to a BGP peer. The default is 10 seconds.

Example: The following command sets a retry interval of 20 seconds for BGP in the Trust-VR:

```
set vrouter trust-vr protocol bgp retry-time 20
```

Description: Use the **failover** commands to configure failover settings on the NetScreen device.

Syntax

set

```
set failover { auto | holddown number | { type track-ip | tunnel-if } }
```

unset

```
unset failover { auto | holddown }
```

exec

```
exec failover { force | revert }
```

Keywords and Variables

auto

```
set failover auto
```

```
unset failover auto
```

auto

Instructs the NetScreen device to automatically fail over from the primary interface to the backup and from the backup interface to the primary. By default, failover is manual (the administrator must use the CLI or WebUI to switch from the primary interface to the backup and from the backup interface to the primary).

force

```
exec failover force
```

force Forces traffic to be switched to the backup interface.

holddown

```
set failover holddown number
```

```
unset failover holddown
```

holddown Specifies the time interval (*number*), in seconds, for the following conditions:

- The NetScreen device switches traffic to the backup interface.
- The NetScreen device switches traffic from the backup interface to the primary interface.

The default is 30 seconds.

Example: The following command sets a failover delay of 45 seconds:

```
set failover holddown 45
```

revert

```
exec failover revert
```

revert Forces traffic to be switched from the backup interface to the primary.

type

```
set failover type track-ip | tunnel-if
```

type

Specifies the type of event that determines interface failover. You can specify the following types:

- **track-ip** instructs ScreenOS to use IP tracking to determine failover.
- **tunnel-if** instructs ScreenOS to use VPN tunnel status to determine failover.

Description: Use the **ike** commands to configure an XAuth client on the NetScreen device.

Note: This section only describes the new keywords and variables for the **ike** commands. For more information on other keyword and variables for the **ike** commands, refer to the NetScreen CLI Reference Guide.

Syntax

set

Gateway

```
set ike gateway name_str xauth client { any | chap | securid }  
      username name_str password name_str
```

Keywords and Variables

xauth client	Specifies that the NetScreen device is an XAuth client. You can specify the following authentication types: <ul style="list-style-type: none">• any Instructs the device to allow any authentication type.• chap Instructs the device to allow Challenge Handshake Authentication Protocol (CHAP) only.• securid Instructs the device to allow SecurID only.
password	Specifies the password for the XAuth client to use on the XAuth server.
username	Specifies the username for the XAuth client to use on the XAuth server.

Example: The following example:

- Configures an XAuth client for the gateway kg1
- Allows any authentication type
- Configures the username kgreen and the password pubs123

```
set ike gateway kg1 xauth client any username kgreen password pubs123
```

interface

Description: Use the **interface** commands to configure:

- IP tracking
- Loopback interface and members of the loopback interface group
- DHCP server enhancement
- RIP interface parameters

Note: This section only describes new keywords and variables for the **interface** commands. For more information on other keywords and variables for the **interface** commands, refer to the NetScreen CLI Reference Guide.

Syntax

get

```
get interface interface { track-ip | dhcp server | protocol rip }
```

set (IP Tracking)

```
set interface interface track-ip  
  [  
    dynamic |  
    threshold number |  
    ip ip_addr  
      [  
        gateway ip_addr |  
        interval number |  
        threshold number |  
        weight number  
      ]  
  ]
```

set (Loopback Interface)

```
set interface interface loopback-group interface
```

set (DHCP Server)

```
set interface interface dhcp server { enable | auto | disable }
```

set (RIP)

```
set interface interface protocol rip  
  [  
    authentication { password pswd_str | md5 key_str key-id id_num }  
    enable |  
    metric number |  
    passive-mode |  
    route-map name_str |  
    split-horizon  
  ]
```

unset (IP Tracking)

```
unset interface interface track-ip  
  [  
    dynamic |  
    threshold |  
    ip ip_addr [ gateway | interval | threshold | weight ]  
  ]
```

unset (Loopback Interface)

```
unset interface interface loopback-group interface
```

unset (RIP)

```
unset interface interface protocol rip
[
  authentication |
  enable |
  metric |
  passive-mode |
  route-map name_str |
  split-horizon
]
```

Keywords and Variables

Variable Parameter

```
get interface interface [ ... ]
set interface interface { ... } [ ... ]
unset interface interface { ... } [ ... ]
```

interface The interface on which IP tracking or RIP is enabled. By default, IP tracking and RIP are disabled. This release supports a new interface type, loopback interfaces. **loopback.n** specifies a loopback interface. Use this interface to allow a MIP to be accessed by other interfaces.

Examples: The following command enables IP tracking on the ethernet3 interface:

```
set interface ethernet3 track-ip
```

dhcp server

```
get interface interface dhcp server
set interface interface dhcp server { enable | auto | disable }
```

- dhcp server** Specifies the operating mode for the DHCP server on the NetScreen device. The default DHCP server mode is Auto. You can specify the following operating modes:
- **enable** causes the DHCP server to always be on. The DHCP server on the NetScreen device always starts when the device is powered on.
 - **auto** instructs the NetScreen device to check to see if there is a DHCP server already running on the network. If there is such a server, the DHCP server on the NetScreen device is disabled. If there is no DHCP server running on the network, the DHCP server on the NetScreen device is enabled. This is the default mode.
 - **disable** causes the DCHP server to always be off.

Example: The following command causes the DHCP server on the interface ethernet1 to always be off:

```
set interface ethernet1 dhcp server disable
```

loopback-group

```
set interface interface loopback-group interface
unset interface interface loopback-group interface
```

loopback-group Specifies the loopback interface group into which the member interface is added.

Example: The following command adds the interface ethernet3 to the loopback.3 interface group.

```
set interface ethernet3 loopback-group loopback.3
```

protocol

```
get interface interface protocol rip
set interface interface protocol rip
  [
    authentication { password pswd_str | md5 key_str key-id id_num }
    enable |
    metric number number |
    passive-mode |
    route-map name_str { in | out } |
    split-horizon
  ]
unset interface interface protocol rip
  [
    authentication |
    enable |
    metric |
    passive-mode |
    route-map name_str { in | out } |
    split-horizon
  ]
```

- protocol rip** Sets, unsets, or displays the current routing protocol settings for the interface.
- **route-map** *name_str* Specifies the route-map on which to filter incoming routes (routes learned by RIP) or outgoing routes (routes advertised by RIP).
 - **in** Specifies the route map is to be used for incoming routes.
 - **out** Specifies the route map is to be used for outgoing routes.

- **authentication** { **password** *pswd_str* | **md5** *key_str* **key-id** *id_num* } Specifies the authentication method used to verify RIP neighbors.
 - **password** specifies a clear-text password used for verification. If you specify password authentication, you must also specify an 8-byte password.
 - **md5** directs the Netscreen device to use the Message Digest version 5 (MD5) authentication algorithm for verification. If you specify MD5 authentication, you must also specify a 16-byte key and key identifier.
- **enable** Enables RIP on the specified interface.
- **metric** *number* Configures the RIP metric for the specified interface. The default metric is 1.
- **passive-mode** Specifies that the interface is to receive but not transmit RIP packets.
- **split-horizon** Enables the split-horizon function on the specified interface. If split-horizon is enabled, RIP does not advertise routes learned from a neighbor back to the same neighbor. If split-horizon is disabled, RIP advertises routes learned from a neighbor back to the same neighbor with a metric of 16. By default, split-horizon is disabled.

track-ip

```
get interface interface track-ip
set interface interface track-ip
[
  dynamic |
  threshold number |
  ip ip_addr
  [
    gateway ip_addr |
    interval number |
    threshold number |
    weight number
  ]
]
```

```
unset interface interface track-ip  
[  
  dynamic |  
  threshold |  
  ip ip_addr [ gateway | interval | threshold | weight ]  
]
```

track-ip

Sets, unsets, or displays the tracking of IP addresses for the specified interface.

- **dynamic** Configures tracking of the IP address of the default gateway for the interface.
- **threshold *number*** Specifies the failure threshold for the interface. If the weighted sum of all tracked IP failures on the interface is equal to or greater than the threshold, the interface is considered down and failover to the backup occurs. Unsetting the tracked IP threshold on the interface sets the threshold to the default value of 1.
- **ip *ip_addr*** Configures tracking for the specified IP address. You can specify the following options:
 - **gateway *ip_addr*** Specifies the static routing gateway for the tracked IP address. If you are unsetting the gateway for the tracked IP address, the device changes the gateway to the default 0.0.0.0 (uses the interface's default gateway).
 - **interval *number*** Specifies the interval, in seconds, that ping requests are sent to the tracked IP address. If you are unsetting the interval for the tracked IP address, the interval is changed to the default value of 1.
 - **threshold *number*** Specifies the failure threshold for the tracked IP address. If the number of consecutive ping failures to the tracked IP address is equal to or greater than the threshold, the tracked IP address is considered failed. If you are unsetting the threshold for the tracked IP address, the device changes the threshold to the default value (3).
 - **weight *number*** Specifies the weight associated with the failure of the tracked IP address. If a tracked IP address fails, its weight is used to calculate the weighted sum of all tracked IP failures on the interface. If you are unsetting the weight for the tracked IP address, the weight is changed to the default value of 1.

Examples: The following command:

- Defines IP tracking for the IP address 1.1.1.1 on the ethernet3 interface
- Assigns a ping interval of 10 seconds
- Assigns a tracked IP address failure threshold of 5

```
set interface ethernet3 track-ip ip 1.1.1.1 interval 10 threshold 5
```

The following command sets the tracking threshold for the ethernet3 interface to 3:

```
set interface ethernet3 track-ip threshold 3
```

modem

Description: Use the **modem** commands to configure modem and dial-up settings for the serial link.

Syntax

get

```
get modem
[
  config |
  settings |
  state |
  stats
]
```

set

```
set modem
{
  idle-time number |
  interval number |
  isp name_str
  {
    account login string password pswd_str |
    primary-number string [ alternative-number string ] |
    priority number
  }
  retry number |
  settings name_str { active | init-strings string } |
  speed num
}
```

unset

```
unset modem
{
  idle-time number |
  interval number |
  isp name_str [ alternative-number ] |
  retry number |
  settings name_str |
  speed
}
```

exec

```
exec modem command string
```

Keywords and Variables

account

```
set modem isp name_str account login string password pswd_str
```

account Specifies the user login and password for the ISP account.

Example: The following command configures the login kgreen and the password bodie45 for the ISP account isp1:

```
set modem isp isp1 account login kgreen password bodie45
```

active

```
set modem settings name_str active
unset modem settings name_str
```

active Activates the specified modem settings and deactivates any other configured settings.

Example: The following command activates settings for the modem `usr14400`:

```
set modem settings usr14400 active
```

alternative-number

```
set modem isp name_str primary-number string alternative-number string
```

alternative-number Specifies an alternate phone number to access the ISP.

Example: The following command configures primary and alternate phone numbers to access the ISP 'isp1':

```
set modem isp isp1 primary-number 4085551212 alternative-number 4085551313
```

command

```
exec modem command string
```

command Sends Hayes AT commands to the modem.

config

```
get modem config
```

config Displays HDLC/PPP configuration.

idle-time

```
set modem idle-time number  
unset modem idle-time number
```

idle-time Specifies the number of minutes that elapse with no traffic on the dial-up connection before the Netscreen device disconnects the modem. The default is 10 minutes. A value of 0 means the modem never disconnects, even if there is no traffic on the dial-up connection.

Example: The following command sets an idle time of 12 minutes:

```
set modem idle-time 12
```

init-strings

```
set modem settings name_str init-strings string  
unset modem settings name_str
```

init-strings Specifies the initialization string for the specified modem.

Example: The following command sets an initialization string for the modem usr14400:

```
set modem settings usr14400 init-strings AT&FX4&A3&B1&D2&H1&I0&K1&M4&R2S7=60
```

interval

```
set modem interval number  
unset modem interval number
```

interval Specifies the number of seconds between dial-up retries. The default is 60 seconds.

Example: The following command sets a dial-up interval of 45 seconds:

```
set modem interval 45
```

isp

```
set modem isp name_str { ... }  
unset modem isp name_str
```

isp Specifies the ISP .

Example: The following command configures the login kgreen and the password bodie45 for the ISP isp1:

```
set modem isp isp1 account login kgreen password bodie45
```

primary-number

```
set modem isp name_str primary-number string
```

primary-number Specifies the primary phone number to access the ISP. If your modem uses tone dial by default, but you want to use pulse dial, precede the phone number with a **P**. If your modem uses pulse dial by default, but you want to use tone dial, precede the phone number with a **T**.

Example: The following command configures the primary phone number to access the ISP isp1 and specifies tone dial:

```
set modem isp isp1 primary-number T4085551212
```

priority

```
set modem isp name_str priority number
```

priority Specifies the priority of this ISP for dial-up backup, relative to other ISPs that may be configured. A value of 1 is the highest priority.

Example: The following command configures the ISP isp1 as the highest priority for dial-up backup:

```
set modem isp isp1 priority 1
```

retry

```
set modem retry number
unset modem retry number
```

retry Specifies the number of times ScreenOS dials the primary number, and then the alternative-number, if the line is busy or there is no answer from the ISP. The default is 3 times.

Example: The following command sets the number of dial-up retries to 4:

```
set modem retry 4
```

settings

```
set modem settings name_str active | init-strings string
unset modem settings name_str
get modem settings
```

settings Configures settings for the specified modem.

Example: The following command activates settings for the modem usr14400:

```
set modem settings usr14400 active
```

speed

set modem speed *number*

unset modem speed

speed Specifies the maximum baud rate for the serial link. The baud rate can be 9600, 19200, 38400, 57600, or 115200 bps. The default is 115200 bps.

Example: The following command sets a maximum baud rate of 56Kbps for the serial link:

```
set modem speed 57600
```

state

get modem state

state Shows modem state information.

stats

get modem stats

stats Shows modem status.

Description: Use the **policy** commands to define access policies that control network and VPN traffic.

Note: This section only describes the new keyword **no-session-backup** for the **policy** command. For more information on other keywords and variables for the **policy** commands, refer to the NetScreen CLI Reference Guide.

Syntax

set

```
set policy name name_str { ... } no-session-backup
```

Keywords and Variables

no-session-backup

no-session-backup Specifies that the access policy effectively becomes a deny policy if either the administrator or ScreenOS switches traffic from the primary Untrust zone interface to the backup interface.

port-mode

Description: Use the **port-mode** commands to set the port, interface, and zone bindings for the NetScreen device. (Use the **get system** command to see the current port mode setting.)

Warning: *Setting the port mode removes any existing configurations on the device and requires a system reset.*

Syntax

`exec`

```
exec port-mode { trust-untrust | home-work | dual-untrust | combined }
```

Keywords and Variables

trust-untrust

Defines the following port, interface, and zone bindings:

- Binds the Untrusted Ethernet port to the untrust interface, which is bound to the Untrust zone
- Binds the Trusted1 through Trusted4 Ethernet ports to the trust interface, which is bound to the Trust zone
- Binds the Modem port to the serial interface, which you can bind as a backup interface to the Untrust zone.

This is the default port mode.

home-work

Defines the following port, interface, and zone bindings:

- Binds the Untrusted Ethernet port to the ethernet3 interface, which is bound to the Unturst zone
- Binds the Trusted4 and Trusted3 Ethernet ports to the ethernet2 interface, which is bound to the Home security zone
- Binds the Trusted2 and Trusted1 Ethernet ports to the ethernet1 interface, which is bound to the Work security zone
- Binds the Modem port to the serial interface, which you can bind as a backup interface to the Untrust zone

dual-untrust

Defines the following port, interface, and zone bindings:

- Binds the Untrusted port to the ethernet3 interface, which is bound to the Untrust zone
- Binds the Trusted4 Ethernet port to the ethernet2 interface, which is bound as a backup interface to the Untrust zone
- Binds the Trusted1 through Trusted3 Ethernet ports to the ethernet1 interface, which is bound to the Trust zone

combined

Defines the following port, interface, and zone bindings:

- Binds the Untrusted Ethernet port to the ethernet4 interface, which is bound to the Untrust zone
- Binds the Trusted4 Ethernet port to the ethernet3 interface, which is bound as a backup interface to the Untrust zone
- Binds the Trusted3 and Trusted2 Ethernet ports to the ethernet2 interface, which is bound to the Home zone
- Binds the Trusted1 Ethernet port to the ethernet1 interface, which is bound to the Work zone

Warning: *Setting the port mode removes any existing configurations on the device and requires a system reset.*

Description: Use the **pppoe** commands to configure a specific instance of PPPoE.

Note: This section only describes the new **name** keyword for the **pppoe** commands. For more information on other keywords and variables for the **pppoe** commands, refer to the NetScreen CLI Reference Guide.

Syntax

get

```
get pppoe [ name name_str | all ]
```

set

```
set pppoe [ name name_str ] ...
```

unset

```
unset pppoe [ name name_str ]
```

Keywords and Variables

name

```
get pppoe [ name name_str | all ]
```

```
set pppoe [ name name_str ] ...
```

```
unset pppoe [ name name_str ]
```

name Defines the name for a specific PPPoE instance. You can assign a username and password, interface, and other PPP/PPPoE parameters to the instance.
If you do not specify **name**, ScreenOS automatically configures the parameters for the default interface bound to the Untrust zone.

Example: The following commands:

- Configure the user name and password for the PPPoE instance pppoe-user-1
- Bind the PPPoE instance pppoe-user-1 to the ethernet2 interface

```
set pppoe name pppoe-user-1 username user1 password 123456
```

```
set pppoe name pppoe-user-1 interface ethernet2
```

RIP CONTEXT COMMANDS

The commands described in the following pages are **rip** context commands. Use the **rip** context commands to configure the Routing Information Protocol (RIP) on a virtual router in a NetScreen device. You issue these commands within the context of a specific virtual router and the RIP protocol.

Initiating the **rip** context requires two steps:

1. Enter the virtual router context by executing the **set vrouter** command.

```
ns-> set vrouter trust-vr
```

2. Enter the RIP context by executing the **set protocol rip** command.

```
ns(trust-vr)-> set protocol rip
```

The following commands are executable in the **rip** context.

advertise-def-route

Use the **advertise-def-route** commands to advertise the default route (0.0.0.0/0) of the current virtual router in all areas.

Every virtual router has a default route entry, which matches every destination. (Any entry with a more specific prefix overrides the default route entry.)

Command options: **get, set, unset**

config

Use the **config** command to display all commands executed to configure the RIP routing instance.

Command options: **get**

default-metric

Use the **default-metric** commands to set the RIP metric for redistributed routes. The default value is 10.

Command options: **set, unset**

enable

Use the **enable** commands to enable or disable RIP in the virtual router.

Command options: **set, unset**

flush-timer

Use the **flush-timer** commands to configure the number of seconds that elapse before ScreenOS automatically removes an invalidated route. The default is 120 seconds.

Command options: **set, unset**

interface	Use the interface command to display all RIP interfaces in the virtual router. Command options: get
invalid-timer	Use the invalid-timer commands to configure the number of seconds that elapse after a neighbor stops advertising a route before the route becomes invalid. The default is 180 seconds. Command options: set, unset
max-neighbor-count	Use the max-neighbor-count commands to set the maximum number of RIP neighbors allowed. The default is 16. Command options: set, unset
neighbors	Use the neighbors command to display the status of RIP neighbors. Command options: get
no-source-validation	Use the no-source-validation commands to accept responses from RIP neighbors in other subnets or to reject such responses. Command options: set, unset
redistribute	Use the redistribute commands to import known routes from a router running a different protocol into the current routing instance. You can import the following types of routes: <ul style="list-style-type: none">• Manually created routes• BGP routes• OSPF routes• Routes sent by an external router that has at least one interface with an assigned IP address• Routes that have already been imported Command options: set, unset
reject-default-route	Use the reject-default-route commands to cause RIP to reject a default route learned from another protocol. Command options: get, set, unset
route-map	Use the route-map commands to filter and offset metric routes. Command options: get, set, unset

routes-redistribute	Use the routes-redistribute command to display redistributed routes. Command options: get
rules-redistribute	Use the rules-redistribute command to display redistribution rules. Command options: get
threshold-update	Use the threshold-update commands to set the maximum number of routing packets allowed per update interval. Command options: set, unset
timer	Use the timer command to display RIP timers. Command options: get
trusted-neighbors	Use the trusted-neighbors commands to set an access list that defines RIP neighbors. Command options: get, set, unset
update-timer	Use the update-timer commands to set the interval, in seconds, when route updates are issued to RIP neighbors. Command options: set, unset
update-threshold	Use the update-threshold command to display the number of routing packets per update interval. Command options: get

advertise-def-route

Description: Use the **advertise-def-route** commands to advertise the default route (0.0.0.0/0) of the current virtual router.

Every router has a default route entry, which matches every destination. (Any entry with a more specific prefix overrides the default route entry.)

Before you can execute the **advertise-def-route** commands, you must initiate the **rip** context. (See [“RIP Context Commands” on page 97.](#))

Syntax

get

```
get advertise-def-route
```

set

```
set advertise-def-route [ always ] [ metric number ]
```

unset

```
unset advertise-def-route
```

Keywords and Variables

always

```
set advertise-def-route always [ ... ]
```

always Directs the routing instance to advertise the default route under all conditions, even if there is no default route in the routing table.

metric

```
set advertise-def-route [always ] [ metric number ]
```

metric Specifies the metric (cost), which indicates the overhead associated with the default route.

config

Description: Use the **config** command to display all commands executed to configure the RIP local virtual router. Before you can execute the **config** command, you must initiate the **rip** context. (See [“RIP Context Commands” on page 97.](#))

Syntax

get

get config

Keywords and Variables

None.

default-metric

Description: Use the **default-metric** commands to set the RIP metric for redistributed routes.

Before you can execute the **default-metric** commands, you must initiate the **rip** context. (See [“RIP Context Commands” on page 97.](#))

Syntax

set

set default-metric *number*

unset

unset default-metric

Keywords and Variables

Variable Parameter

set default-metric *number*

number The metric for the routes redistributed into RIP. Enter a value between 1-16.

enable

Description: Use the **enable** commands to enable or disable RIP from the current virtual router.

Before you can execute the **enable** commands, you must initiate the **rip** context. (See [“RIP Context Commands” on page 97.](#))

Syntax

set

set enable

unset

unset enable

Keywords and Variables

None.

flush-timer

Description: Use the **flush-timer** commands to configure the time that elapses before an invalid route is removed.

Before you can execute the **flush-timer** commands, you must initiate the **rip** context. (See [“RIP Context Commands”](#) on page 97.)

Syntax

set

set flush-timer *number*

unset

unset flush-timer

Keywords and Variables

Variable Parameter

set flush-timer *number*

number The number of seconds that elapses before an invalid route is removed. The default value is 120.

interface

Description: Use the **interface** command to display all RIP interfaces on the current virtual router.

Before you can execute the **interface** command, you must initiate the **rip** context. (See [“RIP Context Commands” on page 97.](#))

Syntax

get

get interface

Keywords and Variables

None.

invalid-timer

Description: Use the **invalid-timer** commands to configure the time that elapses after a neighbor stops advertising a route before the route becomes invalid.

Before you can execute the **invalid-timer** commands, you must initiate the **rip** context. (See [“RIP Context Commands”](#) on page 97.)

Syntax

set

```
set invalid-timer number
```

unset

```
unset invalid-timer
```

Keywords and Variables

Variable Parameter

```
set invalid-timer number
```

number The number of seconds after a neighbor stops advertising a route that the route becomes invalid. The default value is 180.

max-neighbor-count

Description: Use the **max-neighbor-count** commands to set the maximum number of RIP neighbors allowed.

Before you can execute the **max-neighbor-count** commands, you must initiate the **rip** context. (See “[RIP Context Commands](#)” on page 97.)

Syntax

set

set max-neighbor-count *number*

unset

unset max-neighbor-count

Keywords and Variables

Variable Parameter

set max-neighbor-count *number*

number The maximum number of RIP neighbors allowed. The default is 16.

neighbors

Description: Use the **neighbors** command to display the status of all RIP neighbors.

Before you can execute the **neighbors** command, you must initiate the **rip** context. (See [“RIP Context Commands” on page 97.](#))

Syntax

get

get neighbors

Keywords and Variables

None.

no-source-validation

Description: Use the **no-source-validation** commands to accept or reject responses from RIP neighbors in different subnets.

Before you can execute the **no-source-validation** commands, you must initiate the **rip** context. (See [“RIP Context Commands”](#) on page 97.)

Syntax

set

```
set no-source-validation
```

unset

```
unset no-source-validation
```

Keywords and Variables

None.

redistribute

Description: Use the **redistribute** commands to import known routes from a router running a different protocol into the current RIP routing instance.

You can import the following types of routes:

- Manually-created routes (**static**)
- BGP routes (**bgp**)
- OSPF routes (**ospf**)
- Directly-connected interface with an IP address assigned to it (**connected**)
- Routes that have already been imported (**imported**)

Before you can execute the **redistribute** commands, you must initiate the **rip** context. (See “[RIP Context Commands](#)” on page 97.)

Syntax

get

```
get routes-redistribute  
get rules-redistribute
```

set

```
set redistribute route-map name_str protocol  
{ bgp | connected | imported | ospf | static }
```

unset

```
unset redistribute route-map name_str protocol  
{ bgp | connected | imported | ospf | static }
```

Keywords and Variables

protocol

```
set redistribute route-map name_str protocol { ... }
```

- protocol** Specifies the routing protocol. The route map can use the protocol type to determine whether to forward or deny an incoming packet.
- **bgp** specifies that the route map performs an action only on BGP routes in the subnetwork.
 - **connected** specifies that the route map performs an action only on routes sent from an external router that has at least one interface with an IP address assigned to it.
 - **imported** specifies that the route map performs an action only on imported routes in the subnetwork.
 - **ospf** specifies that the route map performs an action only on OSPF routes in the subnetwork.
 - **static** specifies that the route map performs an action only on static routes in the subnetwork.

route-map

```
set redistribute route-map name_str protocol { ... }
```

route-map Identifies the route map that specifies the routes to be imported.

Example: The following command redistributes a route that originated from a BGP routing domain into the current RIP routing instance:

```
ns(trust-vr/rip)-> set redistribute route-map map1 protocol bgp
```

reject-default-route

Description: Use the **reject-default-route** commands to cause RIP to reject default routes learned from another protocol.

Before you can execute the **reject-default-route** commands, you must initiate the **rip** context. (See [“RIP Context Commands” on page 97.](#))

Syntax

get

`get reject-default-route`

set

`set reject-default-route`

unset

`unset reject-default-route`

Keywords and Variables

None.

route-map

Description: Use the **route-map** commands to filter incoming or outgoing routes.

Before you can execute the **route-map** commands, you must initiate the **rip** context. (See [“RIP Context Commands” on page 97.](#))

Syntax

get

```
get route-map
```

set

```
set route-map name_str { in | out }
```

unset

```
set route-map name_str { in | out }
```

Keywords and Variables

Variable Parameter

```
set route-map name_str
```

name_str The name of the route map to filter routes.

in

set route-map *name_str* **in**

in Specifies the route map is applied to routes to be learned by RIP.

out

set route-map *name_str* **out**

out Specifies the route map is applied to routes to be advertised by RIP.

Example: The following command applies the route map map1 to routes to be advertised by RIP:

```
ns(trust-vr/rip)-> set route-map map1 out
```

routes-redistribute

Description: Use the **routes-redistribute** command to display details about routes imported from a protocol other than RIP.

Before you can execute the **routes-redistribute** command, you must initiate the **rip** context. (See [“RIP Context Commands” on page 97.](#))

Syntax

get

get routes-redistribute

Keywords and Variables

None.

rules-redistribute

Description: Use the **rules-redistribute** command to display conditions set for routes imported from a protocol other than RIP.

Before you can execute the **rules-redistribute** command, you must initiate the **rip** context. (See [“RIP Context Commands” on page 97.](#))

Syntax

get

get rules-redistribute

Keywords and Variables

None.

threshold-update

Description: Use the **threshold-update** commands to set the maximum number of routing packets allowed per update interval.

Before you can execute the **threshold-update** commands, you must initiate the **rip** context. (See [“RIP Context Commands”](#) on page 97.)

Syntax

set

```
set threshold-update number
```

unset

```
unset threshold-update
```

Keywords and Variables

Variable Parameter

```
set threshold-update number
```

number The maximum number of routing packets allowed per update interval.

timer

Description: Use the **timer** command to display information about various RIP timers.

Before you can execute the **timer** command, you must initiate the **rip** context. (See [“RIP Context Commands” on page 97.](#))

Syntax

get

get timer

Keywords and Variables

None.

trusted-neighbors

Description: Use the **trusted-neighbors** commands to specify an access list that defines allowed RIP neighbors.

Before you can execute the **trusted-neighbors** commands, you must initiate the **rip** context. (See “[RIP Context Commands](#)” on page 97.)

Syntax

get

```
get trusted-neighbors
```

set

```
set trusted-neighbors id_num
```

unset

```
set trusted-neighbors id_num
```

Keywords and Variables

Variable Parameter

```
set trusted-neighbors id_num
```

id_num The number of the access list that defines the allowed RIP neighbors.

update-timer

Description: Use the **update-timer** commands to set the interval that RIP sends route updates to neighbors.

Before you can execute the **update-timer** commands, you must initiate the **rip** context. (See [“RIP Context Commands”](#) on page 97.)

Syntax

set

```
set update-timer number
```

unset

```
unset update-timer
```

Keywords and Variables

Variable Parameter

```
set update-timer number
```

number The interval, in seconds, that RIP sends route updates to neighbors. The default is 30.

update-threshold

Description: Use the **update-threshold** command to display the number of routing packets per update interval.

Before you can execute the **update-threshold** command, you must initiate the **rip** context. (See [“RIP Context Commands” on page 97.](#))

Syntax

get

get update-threshold

Keywords and Variables

None.

Description: Use the **vpn** commands to specify the remote IP address to which the NetScreen device sends VPN monitor pings and to set failover weights for VPN tunnels.

Note: This section only describes the new **destination-ip** keyword for the **set vpn** command. For more information on other keywords and variables for the **vpn** commands, refer to the NetScreen CLI Reference Guide.

Syntax

set (VPN Monitor)

```
set vpn name_str monitor source-interface interface destination-ip ip_addr
```

set (VPN Tunnel Failover Weight)

```
set vpn name_str failover-weight number
```

Keywords and Variables

destination-ip

```
set vpn name_str { ... } destination-ip ip_addr
```

destination-ip Specifies the remote IP address to which the NetScreen device sends VPN monitor pings.

failover-weight

```
set vpn name_str failover-weight number }
```

failover-weight Assigns a weight to a VPN tunnel. When the accumulated weight of failed or “down” VPN tunnels bound to the primary Untrust zone interface reaches or exceeds 100%, ScreenOS fails over to the backup Untrust zone interface.

Example: The following command assigns a failover weight of 50% to the VPN to_remote1:

```
set vpn to_remote1 failover-weight 50
```

vrouter

Description: Use the **vrouter** commands to configure the virtual router on the NetScreen device.

Executing the **set vrouter *name_str*** command without specifying further options places the CLI in the virtual router context. For example, the following command places the CLI in the trust-vr virtual router context:

```
ns-> set vrouter trust-vr
```

Once you initiate the routing context, all subsequent command executions apply to the specified local virtual router (**trust-vr** in this example). You can then initiate the **rip** protocol context.

To enter the rip context, execute the set protocol rip command.

```
ns(trust-vr)-> set protocol rip
```

In the **rip** protocol context, all command executions apply to the protocol.

Commands

get

```
get vrouter name_str protocol rip1
```

set

```
set vrouter name_str protocol rip1
```

unset

```
unset vrouter name_str protocol rip1
```

1. For more information on the **protocol rip** options, refer to the **rip** command descriptions.

Arguments

protocol rip

Places the NetScreen device in the RIP context. (For information on this context, refer to [“RIP Context Commands” on page 97.](#))

New Messages

This chapter introduces the new NetScreen messages for this release. This chapter presents each message and explains its meaning, and—where appropriate—provides the recommended administrative action. The messages are grouped by message type, and then within that type by severity level, from the most severe to the least.

- “DHCP” on page 128
- “Failover” on page 130
- “Interface” on page 132
- “PPP” on page 133
- “PPPoE” on page 134
- “RIP” on page 135
- “VPN” on page 137

For a complete list of NetScreen messages, refer to the *NetScreen Message Log Reference Guide*.

DHCP

The following messages relate to the Dynamic Host Configuration Protocol (DHCP) server on the NetScreen device.

Critical (00029)

- Message** DHCP server set to OFF on <interface> (another server found on <ip_addr>)
- Meaning** Although the DHCP server is enabled on the NetScreen device, the DHCP service has not been started on the specified interface because ScreenOS detected another DHCP server already running on the network. The IP address of the DHCP server found by ScreenOS is displayed.
- Action** No recommended action.

Notification (00009)

- Message** DHCP client has been disabled on interface <interface>
- Meaning** An admin has disabled the DHCP client on the specified interface.
- Action** No recommended action.

Notification (00024)

Message DHCP server has been enabled | disabled

Meaning An admin has enabled or disabled the DHCP server.

Action No recommended action.

Message DHCP server option have been changed | removed

Meaning An admin has changed or removed the DHCP server option settings.

Action No recommended action.

Message DHCP relay agent settings have been changed

Meaning An admin has changed the configuration of the DHCP relay agent.

Action No recommended action.

FAILOVER

The following messages relate to failovers.

Critical (00062)

Message Failover to Secondary untrust interface

Meaning Traffic to the Untrust zone is switched from the primary interface to the backup interface. Either the administrator has manually forced the switch to the backup interface or ScreenOS is configured to automatically switch to the backup if there is a failure on the primary interface.

Action No recommended action.

Message Recover to Primary untrust interface.

Meaning Traffic to the Untrust zone is switched from the backup interface back to the primary interface. Either the administrator has manually forced the switch to the primary interface or ScreenOS is configured to automatically revert to the primary when the primary interface is restored.

Action No recommended action.

Information (00545)

Message Modem <name_str> has been disconnected.

Meaning The specified modem has been disconnected as a result of an interface failover from the serial interface to the primary Untrust zone interface.

Action No recommended action.

Message Modem <name_str> is connected. Phone number: <string1>, Account name: <string2>, Status <string3>.

Meaning The specified modem is connected to the indicated phone number, with the specified login and status.

Action No recommended action.

INTERFACE

The following messages relate to interface configurations.

Notification (00009)

Message Delete interface <interface1> from <interface2>.

Meaning An administrator has removed the interface <interface1> from the loopback interface <interface2>.

Action No recommended action.

Message Interface <interface1> was added into <interface2>.

Meaning An administrator has added the interface <interface1> to the loopback interface <interface2>.

Action No recommended action.

Message Interface <interface1> was removed from <interface2>.

Meaning An administrator has removed the interface <interface1> from the loopback interface <interface2>.

Action No recommended action.

PPP

These messages relate to the Point-to-Point protocol (PPP) on the NetScreen device.

Notification (00042)

Message PPP Settings changed.

Meaning An administrator has changed the PPP configuration.

Action No recommended action.

Information (00539)

Message Dialup HDLC PPP session has successfully established.

Meaning The NetScreen device has successfully connected over the dialup link.

Action No recommended action.

PPPoE

The following messages related to the Point-to-Point Protocol over Ethernet (PPPoE) connections.

Information (00537)

Message	PPPoE session shuts down for instance <name_str>: System reset
Meaning	The NetScreen device closed the specified PPPoE session because the system was reset. When the session is closed, the PPPoE peer is notified of the termination.
Action	No recommended action.

RIP

The following messages relate to the Routing Information Protocol (RIP) used for dynamic routing.

Critical (00204)

- Message** <vrouter> update packet flood on by neighbor <id_num> interface <interface> has dropped a packet
- Meaning** The NetScreen device detected a flood of update packets coming from the specified RIP neighbor arriving at the specified interface. The NetScreen device is dropping update packets it receives from that neighbor.
- Action** Remove the connection between the virtual router and the RIP neighbor.

Notification (00045)

- Message** RIP instance in vrouter <vrouter> created
- Meaning** An admin has configured a RIP instance in the specified virtual router.
- Action** No recommended action.
-
- Message** rip instance in vrouter <vrouter> deleted
- Meaning** An admin has removed a RIP instance in the specified virtual router.
- Action** No recommended action.

Information (00544)

- Message** RIP neighbor <id_num> in vrouter <vrouter> is added
- Meaning** The specified device was added as a RIP neighbor to the virtual router.
- Action** No recommended action.
-
- Message** RIP neighbor <id_num> in vrouter <vrouter> is removed
- Meaning** The specified device was removed as a RIP neighbor to the virtual router.
- Action** No recommended action.

VPN

The following messages related to IPSec virtual private network (VPN) tunnels, and VPN-related technologies.

Notification (00017)

- Message** VPN <name_str> monitor enabled source I/F <interface> dst IP <ip_addr>
- Meaning** An admin has configured VPN monitoring so that ScreenOS sends pings to the specified remote destination IP address from the source interface. The remote destination IP address can be a different IP address than the remote VPN gateway being monitored, if the remote VPN gateway cannot respond to ping requests.
- Action** No recommended action.

