

NetScreen ADSL Reference Guide

ScreenOS 5.0.0

P/N 093-1198-000

Rev. B

Copyright Notice

Copyright © 2004 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, 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:

Juniper Networks, Inc.

ATTN: General Counsel

1194 N. Mathilda Ave.

Sunnyvale, CA 94089-1206

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	iii		
Conventions	iv		
WebUI Navigation Conventions	iv		
Example: Objects > Addresses > List > New	iv		
CLI Conventions	v		
NetScreen Documentation	vi		
Chapter 1 ADSL	1		
ADSL Overview	2		
The ADSL Interface on the NetScreen Device	3		
PPPoA	5		
Configuration Examples	7		
Example: (Small Business/Home) PPPoA on ADSL Interface	8		
Example: (Small Business/Home) 1483 Bridging on ADSL Interface	12		
Example: (Small Business/Home) Dialup Backup ..	16		
Example: (Small Business/Home) Ethernet Backup	22		
Example: (Small Business) Allow Access to Local Servers	26		
		Example: (Branch Office) VPN Tunnel through ADSL31	
		Example: (Branch Office) Secondary VPN Tunnel	38
		Example: 1483 Routing on ADSL Interface	48
Chapter 2 New and Modified CLI Commands	53		
pppoa	54		
Syntax	54		
Keywords and Variables	56		
interface	60		
Syntax	60		
Variable Parameter	60		
Keywords	61		
Chapter 3 New Messages	65		
ADSL	66		
Notification (00555)	66		
PPPoA	69		
Notification (00055)	69		
Notification (00556)	69		
Index	I-1		

Preface

This document describes the ADSL interface available on the Juniper Networks NetScreen-5GT ADSL device. It is organized into the following chapters:

- [Chapter 1, “ADSL”](#) describes the ADSL feature on the NetScreen device and presents example configurations.
- [Chapter 2, “New and Modified CLI Commands”](#) describes ScreenOS CLI commands that are new or changed for ADSL support.
- [Chapter 3, “New Messages”](#) describes messages that are new for ADSL support.

See the *NetScreen-5GT ADSL User’s Guide* for information about installing the device and performing basic configuration.

This document is intended to be a supplement to the ScreenOS 5.0.0 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

The following conventions are used when presenting the syntax of a command line interface (CLI) command:

- Anything inside square brackets [] is optional.
- Anything inside braces { } is required.
- If there is more than one choice, each choice is separated by a pipe (|). For example,
 `set interface { ethernet1 | ethernet2 | ethernet3 } manage`
means “set the management options for the ethernet1, ethernet2, or ethernet3 interface”.
- Variables appear in *italic*. For example:

```
set admin user name password
```

When a CLI command appears within the context of a sentence, it is in **bold** (except for variables, which are always in *italic*). For example: “Use the **get system** command to display the serial number of a NetScreen device.”

Note: When typing a keyword, you only have to type enough letters to identify the word uniquely. For example, typing **set adm u joe j12fmt54** is enough to enter the command **set admin user joe j12fmt54**. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.

NETSCREEN DOCUMENTATION

To obtain technical documentation for any Juniper Networks NetScreen product, visit www.juniper.net/techpubs/.

For technical support, open a support case using the Case Manager link at <http://www.juniper.net/support/> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).

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

techpubs-comments@juniper.net

ADSL

The NetScreen-5GT ADSL device provides ADSL connection with integrated IPsec VPN and firewall services for a broadband telecommuter, a branch office, or a retail outlet. This section describes the ADSL interface on the NetScreen device and provides example configurations.

Note: For information about configuring IPsec VPN and firewall features on the NetScreen device, see the NetScreen Concepts & Examples ScreenOS Reference Guide.

The specific topics covered are as follows:

- [“ADSL Overview” on page 2](#)
- [“The ADSL Interface on the NetScreen Device” on page 3](#)
 - [“PPPoA” on page 5](#)
- [“Configuration Examples” on page 7](#)
 - [“Example: \(Small Business/Home\) PPPoA on ADSL Interface” on page 8](#)
 - [“Example: \(Small Business/Home\) 1483 Bridging on ADSL Interface” on page 12](#)
 - [“Example: \(Small Business/Home\) Dialup Backup” on page 16](#)
 - [“Example: \(Small Business/Home\) Ethernet Backup” on page 22](#)
 - [“Example: \(Small Business\) Allow Access to Local Servers” on page 26](#)
 - [“Example: \(Branch Office\) VPN Tunnel through ADSL” on page 31](#)
 - [“Example: \(Branch Office\) Secondary VPN Tunnel” on page 38](#)
 - [“Example: 1483 Routing on ADSL Interface” on page 48](#)

ADSL OVERVIEW

Asymmetric Digital Subscriber Line (ADSL) is a Digital Subscriber Line (DSL) technology that allows existing telephone lines¹ to carry both voice telephone service and high-speed digital transmission. A growing number of service providers offer ADSL service to home and business customers.

The transmission is *asymmetric* because the rate at which you can send data (the *upstream* rate) is considerably less than the rate at which you can receive data (the *downstream* rate). This is ideal for Internet access because most messages that you send to the Internet are small and do not require much upstream bandwidth, while most data that you receive from the Internet — such as graphic, video, or audio content — require greater downstream bandwidth. The data transmission rates available to you depend upon the type of DSL service you obtain from your service provider. Most service providers offer several rate levels, with higher speed transmissions being more costly than lower rate transmissions.

Traditional telephone lines use analog signals to carry voice service through twisted-pair copper wires. However, analog transmission uses only a small portion of the available bandwidth. Digital transmission allows the service provider to use a wider bandwidth on the same media. The service provider can separate the analog and digital transmissions, using only a small portion of the available bandwidth to transmit voice. This allows you to use your telephone and computer at the same time on the same line. At the service provider's central office, the Digital Subscriber Line Access Multiplexer (DSLAM) connects many DSL lines to a high-speed network such as an Asynchronous Transfer Mode (ATM) network.²

1. In some areas, the telephone lines between the service provider's central office and the customer's premises (known as the *local loop*) need to be upgraded to carry ADSL transmissions.

2. Voice calls are not sent through the DSLAM but are instead sent through a voice telephone network.

THE ADSL INTERFACE ON THE NETSCREEN DEVICE

You use the ADSL cable provided with the NetScreen device to connect the ADSL port on the device to your telephone outlet. No ADSL modem is needed. You can also install signal splitters and microfilters obtained from your service provider. See the *NetScreen-5GT ADSL User's Guide* for more information about connecting the NetScreen device to your network.

The ADSL interface uses ATM as its transport layer. There are two types of ATM virtual circuits: switched virtual circuits (SVCs) are temporary logical network connections that are created and maintained for individual data transfer sessions, while permanent virtual circuits (PVCs) are continuously-available logical connections to the network. The ADSL interface supports multiple PVCs on a single physical line.

The ADSL interface on the NetScreen device is referred to as “adsl1” in configuration³. The information that you configure for the adsl1 interface must match the DSLAM configuration for your ADSL connection, so you must obtain the following information from your service provider:⁴

- Virtual Path Identifier and Virtual Channel Identifier (VPI/VCI), which identifies the virtual circuit on the DSLAM.
- ATM encapsulation method. The ADSL interface supports the following ATM Adaptation Layer 5 (AAL5)⁵ encapsulations:
 - Virtual Circuit (VC)-based multiplexing, in which each protocol is carried over a separate ATM virtual circuit.
 - Logical Link Control (LLC), which allows several protocols to be carried on the same ATM virtual circuit. This is the default encapsulation method.

Check with your service provider for the type of multiplexing used on the ADSL line.

3. You can configure additional virtual circuits on the NetScreen device by creating subinterfaces; ADSL subinterfaces are named “adsl1.1”, “adsl1.2”, and so on. See the *NetScreen-5GT ADSL User's Guide* for information on how to create subinterfaces.

4. For information about ADSL line compatibility information, see <http://www.juniper.net/products/integrated/5GT-ADSL/>.

5. AAL5 is an ATM Adaptation Layer recommended by the Telecommunication Standardization Sector of the International Telecommunications Union (ITU-T), based in Geneva, Switzerland.

- Point-to-Point Protocol (PPP) is a standard protocol for transmitting IP packets over serial point-to-point links, such as an ATM PVC. The NetScreen device supports the following methods of transporting PPP packets:
 - PPP over Ethernet (PPPoE). RFC 2516 describes the encapsulation of PPP packets over Ethernet. For more information about PPPoE, see the “System Parameters” chapter of the “Fundamentals” volume.
 - PPP over AAL5 (PPPoA). RFC 1483 describes the encapsulation of network traffic over AAL5. For more information about PPPoA, see [“PPPoA” on page 5](#).

If the service provider’s network uses PPPoE or PPPoA, the service provider needs to give you the user name and password for the connection, the authentication method used, and any other protocol-specific parameters.

- The service provider may give your network a static IP address or a range of IP addresses. The service provider should also give you the address of the DNS server to use for DNS name and address resolution.
- Discrete multitone (DMT) is a method for encoding digital data in an analog signal. By default, the ADSL interface automatically negotiates the DMT operating mode with the service provider’s DSLAM. You can change the mode on the `adsl1` interface to cause the interface to use only one of the following DMT standards:
 - American National Standards Institute (ANSI) T1.413 Issue 2, which supports rates up to 8 Mbps downstream and 1 Mbps upstream.
 - International Telecommunications Union (ITU) G.992.1 (also known as G.dmt), which supports minimum data rates of 6.144 Mbps downstream and 640 kbps upstream.
 - ITU 992.2 (also known as G.lite), which supports up to data rates of 1.536 Mbps downstream and 512 kbps upstream. This standard is also called “splitterless DSL” because you do not have to install a signal splitter on your ADSL line; the service provider’s equipment splits the signal remotely.

PPPoA

PPPoA is usually used for PPP sessions that are to be terminated on a NetScreen device with an ADSL interface. PPPoA is primarily used for business class services as it does not require a desktop client.

You configure a PPPoA client instance on the ADSL interface or its subinterfaces. You configure a specific instance of PPPoA with a user name and password and other parameters, and bind the instance to the interface. The following are parameters you can configure for a PPPoA instance:

- User name and password for the PPPoA connection.
- Interface to which the PPPoA instance is bound (the ADSL interface or subinterface) and the netmask for the interface (the default is 255.255.255.255).
- Authentication method: Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or any authentication protocol (any is the default).
- Auto connect: the number of seconds before a previously-closed connection is automatically reinitiated. The default (0) disables this function.
- Clear on disconnect: specifies that IP information is cleared when a connection is closed. This is disabled by default.
- Idle interval: Specifies the number of minutes that the connection is idle before the NetScreen device terminates the connection. The default is 30 minutes.
- PPP Link Control Protocol (LCP) parameters for sending LCP-Echo requests.

When the NetScreen device initiates a PPPoA connection, the PPPoA server automatically provides the IP addresses for the Untrust zone interface and for the Domain Name Service (DNS) servers. When the NetScreen device receives DNS server addresses via PPPoA, it updates the DHCP server on the device with these DNS server addresses. If you do not want the DNS server addresses updated on the DHCP server, you can disable the automatic updating of DNS parameters received through the PPPoA connection.

You can display the state of the PPPoA instance through the WebUI (Network > PPPoA) or the CLI (using the **get pppoa all** command). The **get pppoa all** command also shows the state of the physical interface.

The default timeout value for a PPP session on a NetScreen device is 1800 seconds (30 minutes). This is based on the default number of times that an LCP-Echo request is retried (10) multiplied by the interval between each request (180 seconds). You can configure the number of times an LCP-Echo request is retried and the interval between requests.

In the following example, you set the number of times an LCP-Echo request is retried to 12 and the interval between requests to 190.

WebUI

Network > PPPoA > Edit (for PPPoA instance): Enter the following, and then click OK:

PPP Lcp Echo Retries: 12

PPP Lcp Echo Timeout: 190

CLI

```
set pppoa ppp lcp-echo-retries 12
set pppoa ppp lcp-echo-timeout 190
save
```

CONFIGURATION EXAMPLES

This section contains configurations for the following examples:

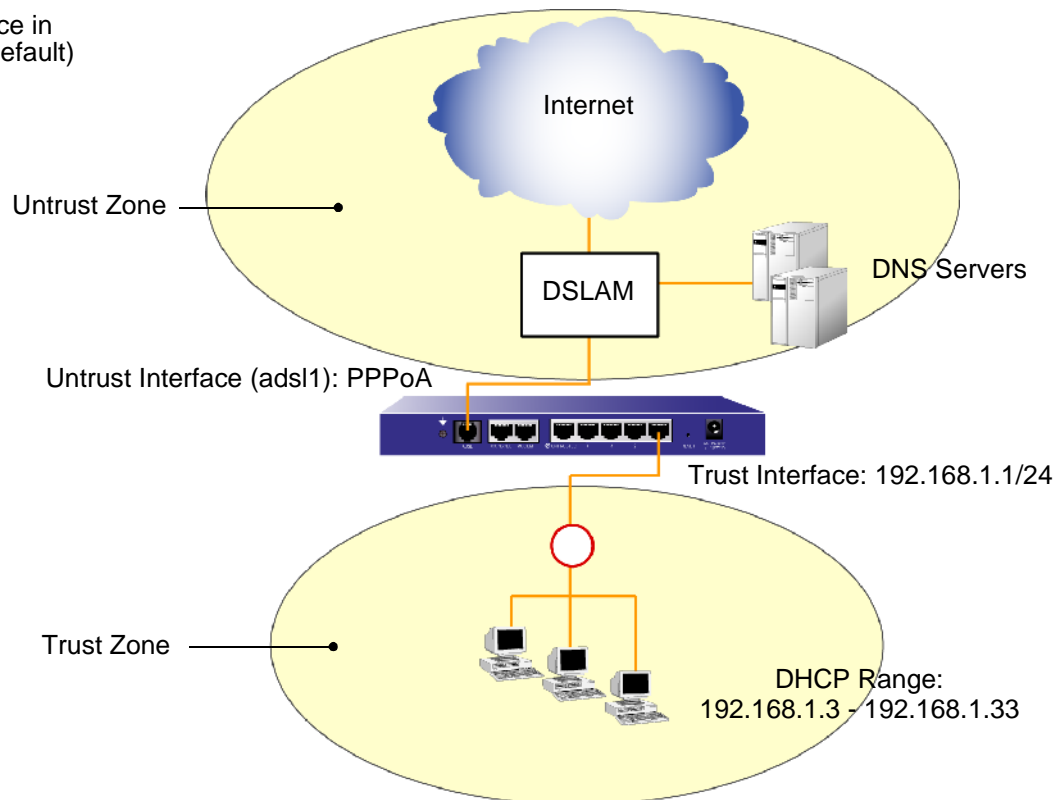
- (Small business or home user) Configure the NetScreen device as a firewall with an Internet connection through the ADSL interface, using one of the following transports:
 - PPPoA (or PPPoE). See [page 8](#).
 - RFC 1483 bridging. See [page 12](#).
- (Small business or home user) Configure the NetScreen device as a firewall with the primary Internet connection through the ADSL interface using PPPoE, and the following backup Internet connections:
 - Dialup connection through the serial Modem interface. See [page 16](#).
 - Ethernet connection. See [page 22](#).
- (Small business) Configure the NetScreen device as a firewall with an Internet connection through the ADSL interface. Allow Internet access to local web servers while protecting other internal hosts from being directly accessible from the Internet. See [page 26](#).
- (Branch office) Configure the NetScreen device as a firewall with a VPN tunnel to corporate headquarters through the ADSL interface. Allow Internet access to local web servers while protecting other internal hosts from being directly accessible from the Internet. See [page 31](#).
- (Branch office) Configure the NetScreen device as a firewall with both an Internet connection and a connection to corporate headquarters through the ADSL interface. Configure a VPN tunnel through the Internet to corporate headquarters as a secondary connection. See [page 38](#).
- (Branch office) Configure the NetScreen device as a firewall with an Internet connection through the ADSL interface, using RFC 1483 routing. See [page 48](#).

Example: (Small Business/Home) PPPoA on ADSL Interface

The following example shows how to configure the NetScreen device as a firewall with an Internet connection through the ADSL interface using PPPoA. In this example, you configure a PVC on the ADSL interface with the VPI/VCI pair value 0/35 that uses LLC encapsulation, and a PPPoA instance named "poa1" which is bound to the ADSL interface. In this example, the NetScreen device receives a dynamically assigned IP address for its ADSL interface (adsl1) from the service provider through PPPoA, and the NetScreen device also dynamically assigns IP addresses for the hosts in its Trust zone. In this example, the NetScreen device acts as both a PPPoA client and a DHCP server. When the NetScreen device receives the IP address for the ADSL interface, it also receives one or more IP addresses for DNS servers. When the NetScreen device assigns IP addresses to the hosts in the Trust zone, it also provides to the hosts the DNS server address obtained from the service provider.

Note: You can perform the configuration shown in this example using the Initial Configuration Wizard.

NetScreen device in
Trust-Untrust (default)
port mode



Note: This example shows PPPoA configuration on the ADSL interface. PPPoE configuration on the ADSL interface is very similar.

WebUI

1. Trust Interface and DHCP Server

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

Zone: Trust

Static IP: (select)

IP Address/Netmask: 192.168.1.1/24

Network > DHCP > Edit (for trust interface) > DHCP Server: Select **Apply**.

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

Dynamic: (select)

IP Address Start: 192.168.1.3

IP Address End: 192.168.1.33

2. ADSL Interface and PPPoA

Network > Interfaces > Edit (for adsl1 interface): Enter the following, and then click **OK**:

VPI/VCI: 0/35

Encapsulation: LLC (select)

Zone: Untrust

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

PPPoA Instance: poa1

Bound to Interface: adsl1 (selected)

Username: alex

Password: tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==

Automatic Update of DHCP Server's DNS Parameters: (select)

3. Activating PPPoA on the NetScreen Device

Turn off the power to the NetScreen device and the workstations in the Trust zone.

Turn on the NetScreen device.

The NetScreen device makes a PPPoA connection to the DSLAM, and obtains the IP address for the ADSL interface and the IP addresses for the DNS servers.

4. Activating DHCP on the Internal Network

Turn on the workstations.

The workstations automatically receive the IP address for the DNS server and obtain an IP address for themselves when they attempt a TCP/IP connection.

CLI

1. Trust Interface and DHCP Server

```
set interface trust zone trust
set interface trust ip 192.168.1.1/24
set interface trust dhcp server service
set interface trust dhcp server ip 192.168.1.3 192.168.1.33
```

2. ADSL Interface and PPPoA

```
set interface adsl1 pvc 0 35 mux llc zone untrust
set pppoa name poa1 username alex password tSOcbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
set pppoa name poa1 interface adsl1
set pppoa update-dhcpserver
save
```

3. Activating PPPoA on the NetScreen Device

Turn off the power to the NetScreen device and the workstations in the Trust zone.

Turn on the NetScreen device.

The NetScreen device makes a PPPoA connection to the DSLAM, and obtains the IP address for the ADSL interface and the IP addresses for the DNS servers.

4. Activating DHCP on the Internal Network

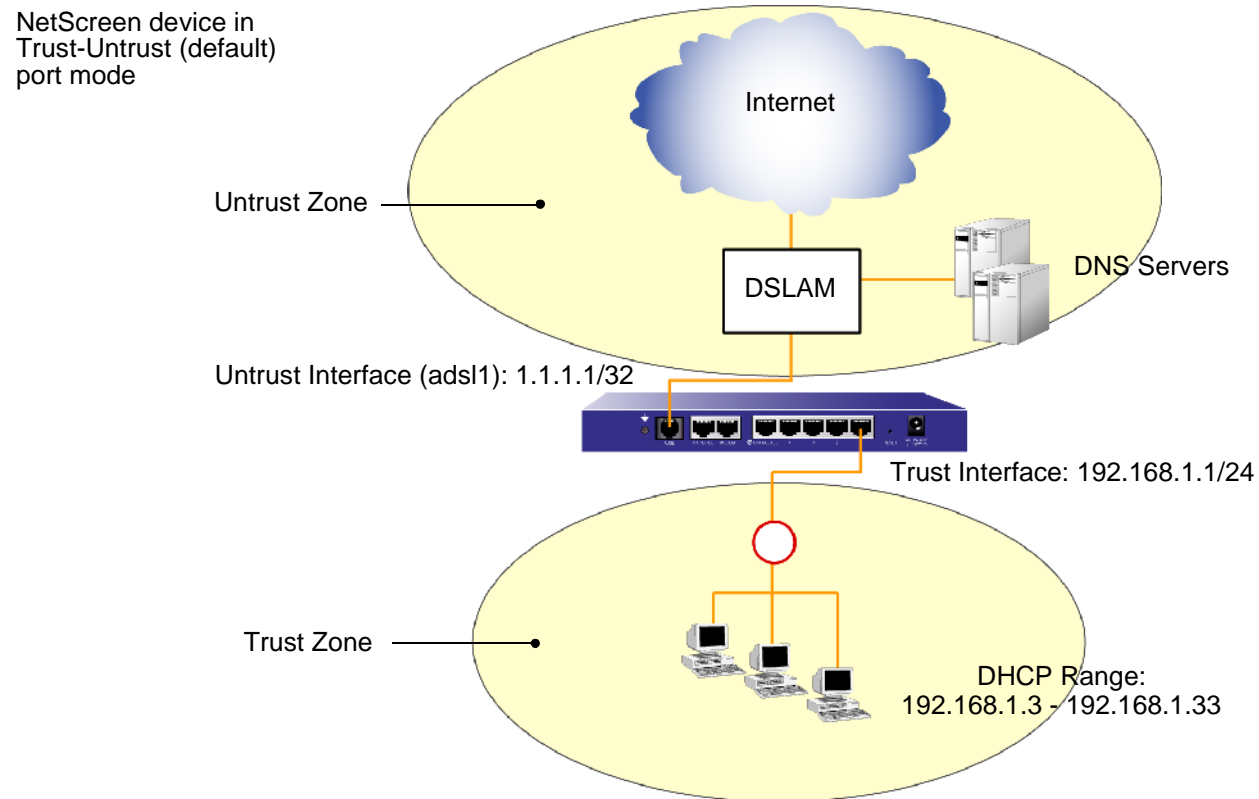
Turn on the workstations.

The workstations automatically receive the IP address for the DNS server and obtain an IP address for themselves when they attempt a TCP/IP connection.

Example: (Small Business/Home) 1483 Bridging on ADSL Interface

RFC 1483 describes methods of transporting bridged protocol data units (PDUs) over AAL5 links. The bridged PDUs do not require the overhead of IPSec processing, thus allowing more usable bandwidth to be available for data traffic. Such traffic is not secured at the IP packet layer and should only be used where you have a private virtual circuit (the service provider assigns you a static IP address for your ADSL interface).

The following example shows how to configure the NetScreen device as a firewall with an Internet connection through the ADSL interface using 1483 bridging. In this example, the service provider assigns the static IP address 1.1.1.1/32 for your network, as well as an IP address for the DNS server. You configure a PVC on the ADSL interface with the VPI/VCI pair 0/35 and the static IP address 1.1.1.1/32 assigned by the service provider. The NetScreen device also dynamically assigns IP addresses for the hosts in its Trust zone. When the NetScreen device assigns IP addresses to the hosts in the Trust zone, it also provides the DNS server address from the service provider.



WebUI

1. Trust Interface and DHCP Server

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

Zone: Trust

Static IP: (select)

IP Address/Netmask: 192.168.1.1/24

Interface Mode: NAT

Network > DHCP > Edit (for trust interface) > DHCP Server: Enter the following, and then click **Apply**.

Gateway: 1.1.1.1

Netmask: 255.255.255.255

DNS#1: 1.1.1.221

> Addresses > New: Enter the following, and then click OK

Dynamic: (select)

IP Address Start: 192.168.1.3

IP Address End: 192.168.1.33

2. ADSL Interface

Network > Interfaces > Edit (for adsl1 interface): Enter the following, and then click **Apply**:

VPI/VCI: 0/35

Zone Name: Untrust

Static IP: (select)

IP Address/Netmask: 1.1.1.1/32

3. Activating DHCP on the Internal Network

Turn off the workstations.

The workstations automatically receive the IP address for the DNS server and obtain an IP address for themselves when they attempt a TCP/IP connection.

CLI

1. Trust Interface and DHCP Server

```
set interface trust zone trust
set interface trust ip 192.168.1.1/24
set interface trust dhcp server service
set interface trust dhcp server ip 192.168.1.3 192.168.1.33
```

2. ADSL Interface

```
set interface adsl1 pvc 0 35 mux llc zone untrust
set interface adsl1 ip 1.1.1.1/32
save
```

3. Activating DHCP on the Internal Network

Turn off the workstations.

The workstations automatically receive the IP address for the DNS server and obtain an IP address for themselves when they attempt a TCP/IP connection.

Example: (Small Business/Home) Dialup Backup

The following example shows how to configure the NetScreen device as a firewall with the primary Internet connection through the ADSL interface using PPPoE, and a backup Internet connection through a dialup connection.

The port mode is the binding of physical ports, logical interfaces, and zones on the NetScreen device. The default port mode for the device is Trust-Untrust, where the adsl1 interface is bound to the Untrust zone, and the Trust interface (Ethernet ports 1-4 on the device) is bound to the Trust zone. You can change the port mode to use different port, interface and zone bindings on the device. For all port modes, the adsl1 interface is the only interface bound to the Untrust zone by default. You can configure a backup link using either the Untrusted Ethernet port or the Modem port on the device. You must bind the backup interface to the Untrust zone and configure the interface appropriately.

Note: You can configure only one backup interface.

The following example shows setting the NetScreen device into Home-Work port mode. This mode creates special Home and Work zones to segregate business and home users, while allowing users in both zones to access the Internet (the Untrust zone) through the ADSL interface⁶. In the Home-Work port mode, the following default policies apply:

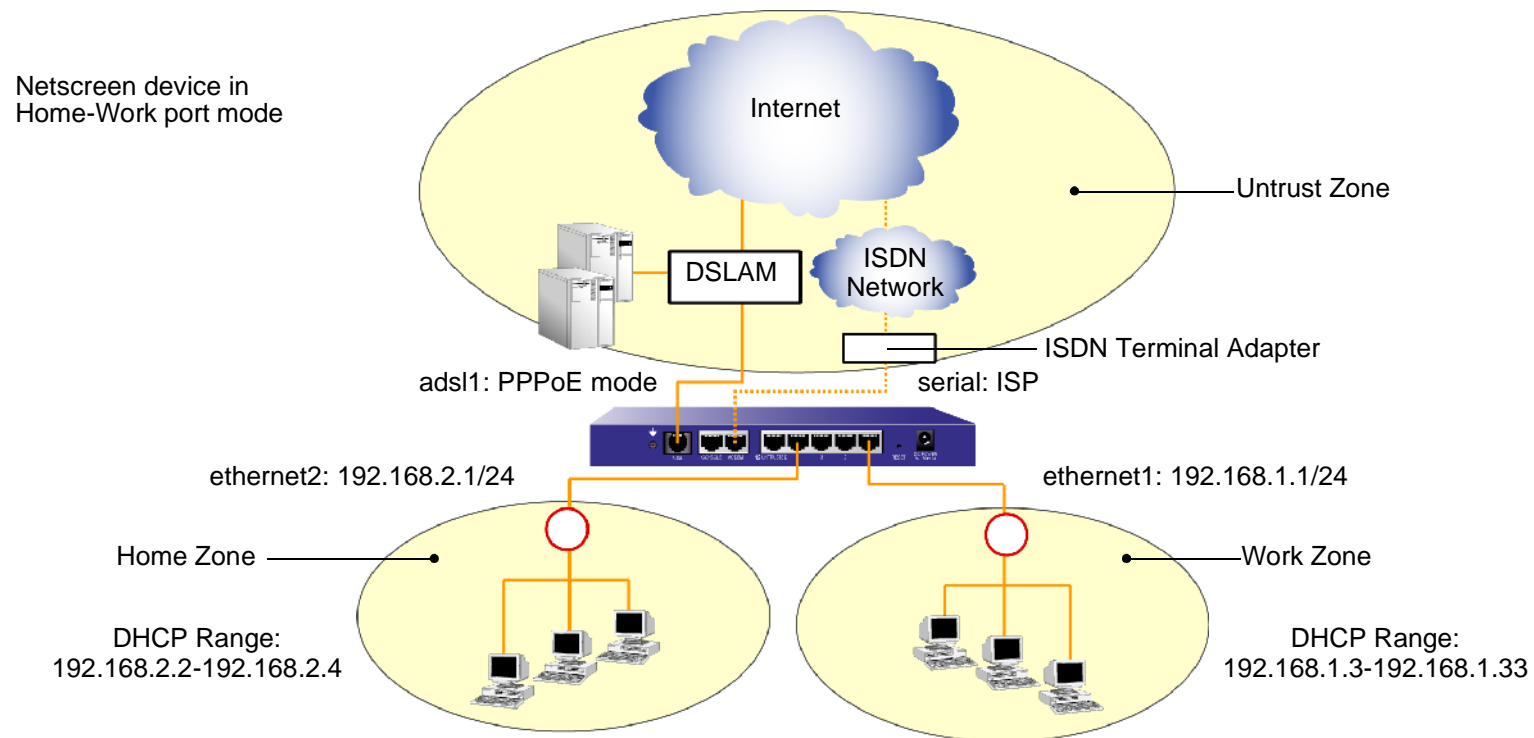
- Allow all traffic from the Work zone to the Untrust zone
- Allow all traffic from the Home zone to the Untrust zone
- Allow all traffic from the Work zone to the Home zone
- Block all traffic from the Home zone to the Work zone (you cannot remove this policy)

For more information about port modes, see the “Zones” chapter in the “Fundamentals” volume of the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

In this example, you configure a PVC on the ADSL interface with the VPI/VCI pair value 0/35 that uses LLC encapsulation, and a PPPoA instance named “poa1” which is bound to the ADSL interface. The NetScreen device also acts as DHCP servers to the Home and Work zones, assigning IP addresses to hosts in both zones.

6. In the Home-Work port mode, you configure the NetScreen device only from the Work zone using Telnet or WebUI. You cannot configure the device from the Home zone, nor can you use any management services on the Home zone interface. The default IP address of ethernet1, the Work zone interface, is 192.168.1.1/24.

This example also shows the configuration for a backup connection to the Internet using the serial interface on the Modem port. When the `adsl1` and serial interface are both bound to the Untrust zone, interface failover is automatically configured. This means that if the ADSL interface becomes unavailable, the NetScreen device automatically sends outgoing traffic to the serial interface, dialing through the ISDN terminal adapter or modem to your ISP account. When the ADSL interface is again available, the NetScreen device automatically sends outgoing traffic to the `adsl1` interface.



To configure the serial interface, you need the following information:

- Login and password for your account to the dialup service provider
- Primary phone connection for dialing into the account
- Modem initialization string

For more information about configuring the serial interface on a NetScreen device, see the “Interface Redundancy” chapter in the “High Availability” volume of the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

WebUI

1. Home-Work Port Mode

Configuration > Port Mode > Port Mode: Select Home-Work from the drop-down list, and then click **Apply**.

At the following prompt, click **OK**:

Operational mode change will erase current configuration and reset the device, continue?

2. ADSL Interface and PPPoE

Network > Interfaces > Edit (for adsl1 interface): Enter the following, and then click **OK**:

VPI/VCI: 0/35

Encapsulation: LLC (selected)

Zone: Untrust

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

PPPoE Instance: poe1

Bound to Interface: adsl1 (select)

Username: alex

Password: tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==

Automatic Update of DHCP Server's DNS Parameters: (select)

3. Backup Dialup Interface

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

Zone Name: Untrust (select)

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

ISP Name: isp1

Primary Number: 4085551111

Alternative Number: 4085552222

Login Name: kgreen

Login Password: 98765432

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

Modem Name: mod1

Init String: AT&FS7=255S32=6

Status: Enable

4. Work Interface

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

Zone: Work (already selected)

Static IP: (select)

IP Address/Netmask: 192.168.1.1/24

Interface Mode: NAT

Network > DHCP > Edit (for ethernet1 interface) > DHCP Server: Select **Apply**.

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

Dynamic: (select)

IP Address Start: 192.168.1.3

IP Address End: 192.168.1.33

5. Home Interface

Network > Interfaces > Edit (for ethernet2 interface): Enter the following, and then click **OK**:

Zone: Home (already selected)

Static IP: (select)

IP Address/Netmask: 192.168.2.1/24

Interface Mode: NAT

Network > DHCP > Edit (for ethernet2 interface) > DHCP Server: Select **Apply**.

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

Dynamic: (select)

IP Address Start: 192.168.2.2

IP Address End: 192.168.2.5

6. Activating DHCP on the Home and Work Zones

Turn off the workstations.

The workstations automatically receive the IP address for the DNS server and obtain an IP address for themselves when they attempt a TCP/IP connection.

CLI

1. Home-Work Port Mode

```
exec port-mode home-work
```

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] ?
```

2. ADSL Interface and PPPoE

```
set interface adsl1 pvc 0 35 mux llc zone untrust
set pppoe name poe1 username alex password tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
set pppoe name poe1 interface adsl1
```

3. Backup Dialup Interface

```
set interface serial zone untrust
set modem isp1 account login kgreen password 98765432
set modem isp1 primary-number 4085551111 alternative-number 4085552222
set modem settings mod1 init-strings AT&FS7=255S32=6
set modem settings mod1 active
```

4. Work Interface

```
set interface ethernet1 ip 192.168.1.1/247
set interface ethernet1 dhcp server service
set interface ethernet1 dhcp server ip 192.168.1.3 192.168.1.33
```

5. Home Interface

```
set interface ethernet2 ip 192.168.2.1/248
set interface ethernet2 dhcp server service
set interface ethernet2 dhcp server ip 192.168.2.2 192.168.2.5
save
```

6. Activating DHCP on the Home and Work Zones

Turn off the workstations.

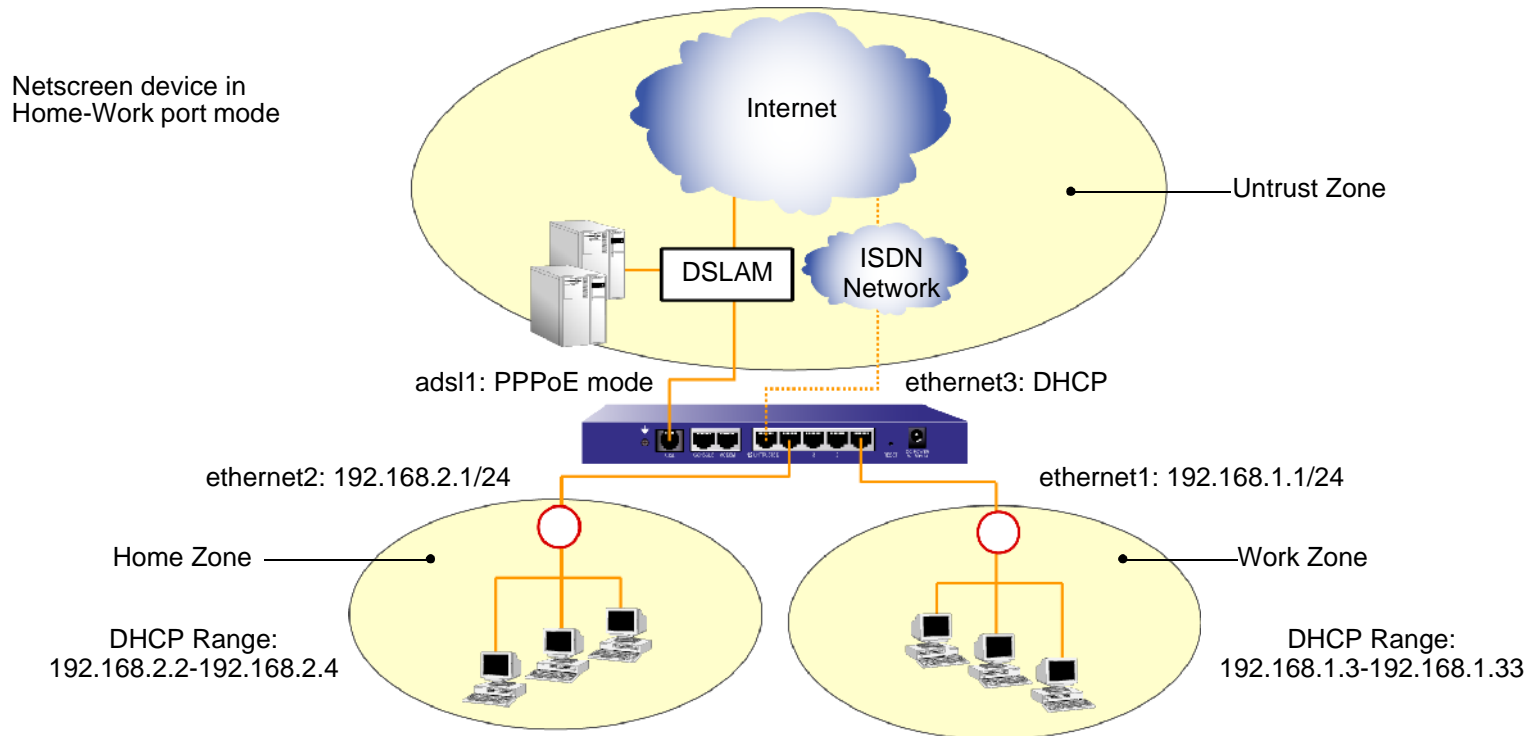
The workstations automatically receive the IP address for the DNS server and obtain an IP address for themselves when they attempt a TCP/IP connection.

7. The ethernet1 interface is prebound to the Work zone in the Home-Work port mode.

8. The ethernet2 interface is prebound to the Home zone in the Home-Work port mode.

Example: (Small Business/Home) Ethernet Backup

The following example shows how to configure the NetScreen device as a firewall with the primary Internet connection through the ADSL interface using PPPoE, and a backup Internet connection through an Ethernet connection. This example is similar to the configuration shown in “[Example: \(Small Business/Home\) Dialup Backup](#)” on page 16, except that the backup connection to the Internet is through the Untrusted Ethernet port, which is “ethernet3” in the Home-Work port mode.



WebUI

1. Home-Work Port Mode

Configuration > Port Mode > Port Mode: Select Home-Work from the drop-down list, and then click **Apply**.

At the following prompt, click **OK**:

Operational mode change will erase current configuration and reset the device, continue?

2. ADSL Interface and PPPoE

Network > Interfaces > Edit (for adsl1 interface): Enter the following, and then click **OK**:

VPI/VCI: 0/35

Encapsulation: LLC (selected)

Zone: Untrust

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

PPPoE Instance: poe1

Bound to Interface: adsl1 (select)

Username: alex

Password: tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==

Automatic Update of DHCP Server's DNS Parameters: (select)

3. Backup Ethernet Interface

Network > Interfaces > Edit (for ethernet3 interface): Enter the following, and then click **OK**:

Zone Name: Untrust (select)

Obtain IP using DHCP: (select)

Automatic update DHCP server parameters: (select)

4. Work Interface

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

Zone: Work (already selected)

Static IP: (select)

IP Address/Netmask: 192.168.1.1/24

Interface Mode: NAT

Network > DHCP > Edit (for ethernet1 interface) > DHCP Server: Select **Apply**.

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

Dynamic: (select)

IP Address Start: 192.168.1.3

IP Address End: 192.168.1.33

5. Home Interface

Network > Interfaces > Edit (for ethernet2 interface): Enter the following, and then click **OK**:

Zone: Home (already selected)

Static IP: (select)

IP Address/Netmask: 192.168.2.1/24

Interface Mode: NAT

Network > DHCP > Edit (for ethernet 2interface) > DHCP Server: Select **Apply**.

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

Dynamic: (select)

IP Address Start: 192.168.2.2

IP Address End: 192.168.2.5

CLI

1. Home-Work Port Mode

```
exec port-mode home-work
```

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] ?
```

2. ADSL Interface and PPPoE

```
set interface adsl1 pvc 0 35 mux llc zone untrust
set pppoe name poe1 username alex password tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
set pppoe name poe1 interface adsl1
```

3. Backup Ethernet Interface

```
set interface ethernet3 zone untrust
set interface ethernet3 dhcp client
set interface ethernet3 update-dhcpserver
```

4. Work Interface

```
set interface ethernet1 ip 192.168.1.1/249
set interface ethernet1 dhcp server service
set interface ethernet1 dhcp server ip 192.168.1.3 192.168.1.33
```

5. Home Interface

```
set interface ethernet2 ip 192.168.2.1/2410
set interface ethernet2 dhcp server service
set interface ethernet2 dhcp server ip 192.168.2.2 192.168.2.5
save
```

9. The ethernet1 interface is prebound to the Work zone in the Home-Work port mode.

10. The ethernet2 interface is prebound to the Home zone in the Home-Work port mode.

Example: (Small Business) Allow Access to Local Servers

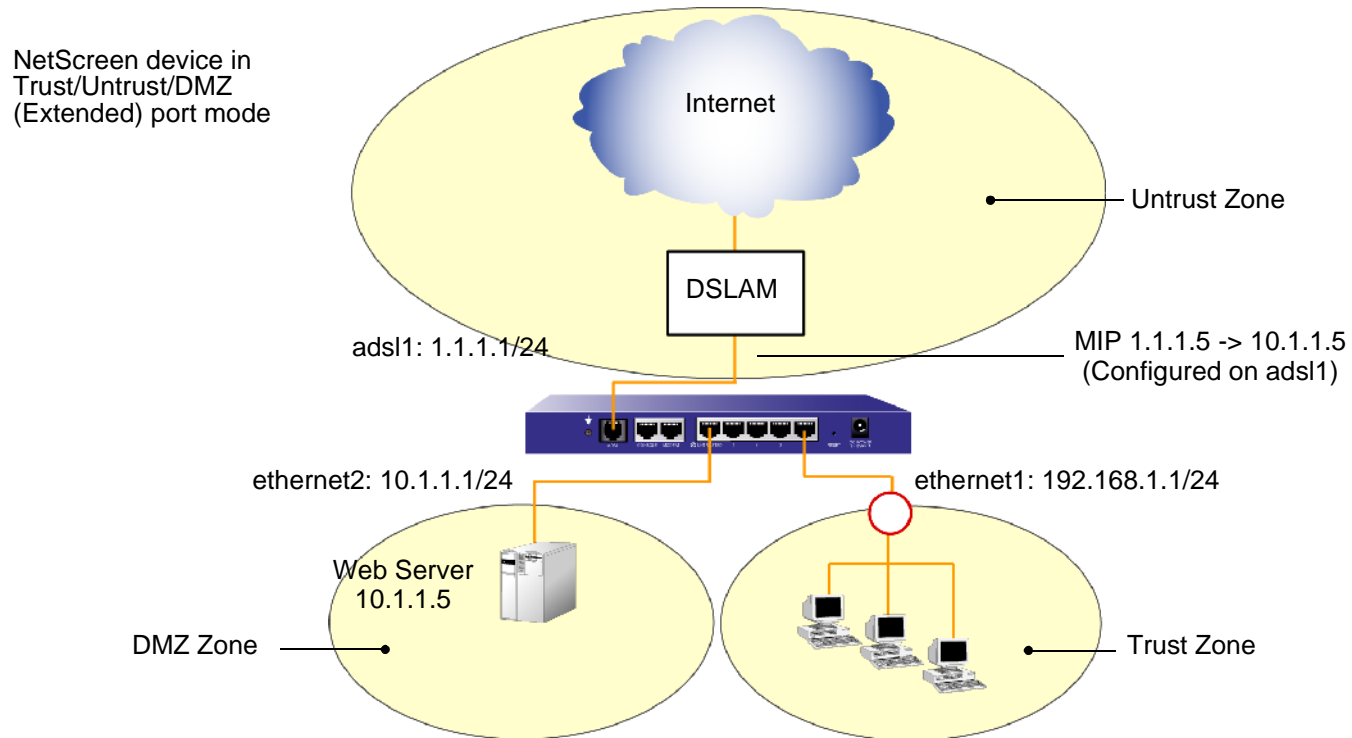
The following example shows how to configure the NetScreen device to allow internal hosts to access the Internet through the ADSL interface and allow Internet users to access a local web server while protecting other internal hosts. To segregate traffic flow to the web server from the rest of your internal network, you place the web server into a separate zone. You then create a policy to allow only HTTP traffic to the zone in which the web server resides.

The following example shows setting the NetScreen device into Trust/Untrust/DMZ port mode. This port mode creates an additional zone, the DMZ zone, which allows you to segregate web or other application servers from the internal network. This port mode provides the following port, interface, and zone bindings:

- Binds the Ethernet ports 1 and 2 to the ethernet1 interface, which is bound to the Trust security zone
- Binds the Ethernet ports 3 and 4 to the ethernet2 interface, which is bound to the DMZ security zone
- Binds the ADSL port to the adsl1 interface, which is bound to the Untrust security zone

Note: *The Trust/Untrust/DMZ port mode is supported only on the Extended version of the NetScreen-5GT ADSL device.*

In this example, you configure a PVC on the ADSL interface with the VPI/VCI pair 0/35 and the static IP address 1.1.1.1/24 assigned by the service provider. You bind the Trust interface to the Trust zone and assign it IP address 192.168.1.1/24. You configure a MIP to direct incoming HTTP traffic destined for the host 1.1.1.5 to the web server at 10.1.1.5 in the DMZ zone. You then need to create a policy that permits only HTTP traffic from any address in the Untrust zone to the MIP host (the web server) in the DMZ zone. (Default policies allow all traffic from the Trust zone to the Untrust Zone and block all traffic from the Untrust zone to the Trust zone.)



WebUI

1. Trust/Untrust/DMZ Port Mode

Configuration > Port Mode > Port Mode: Select Extended from the drop-down list, and then click **Apply**.

At the following prompt, click **OK**:

Operational mode change will erase current configuration and reset the device, continue?

2. Trust and DMZ Interfaces¹¹

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

Static IP: (select)

IP Address/Netmask: 192.168.1.1/24

Interface Mode: NAT

Network > DHCP > Edit (for ethernet1 interface) > DHCP Server: Select **Apply**.

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

Dynamic: (select)

IP Address Start: 192.168.1.3

IP Address End: 192.168.1.33

Network > Interfaces > Edit (for ethernet2 interface): Enter the following, and then click **OK**:

Static IP: (select)

IP Address/Netmask: 10.1.1.1/24

Interface Mode: NAT

3. ADSL Interface and MIP

Network > Interfaces > Edit (for adsl1 interface): Enter the following, and then click **Apply**:

VPI/VCI: 0/35

Zone Name: Untrust

Static IP: (select)

IP Address/Netmask: 1.1.1.1/24

11. In Trust/Untrust/DMZ port mode, the ethernet1 interface is automatically bound to the Trust zone, while ethernet2 is bound to the DMZ zone.

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

Mapped IP: 1.1.1.5

Netmask: 255.255.255.255

Host IP Address: 10.1.1.5

Host Virtual Router Name: trust-vr

4. Policy

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

Source Address:

Address Book Entry: (select) Any

Destination Address:

Address Book Entry: (select), MIP(1.1.1.5)

Service: HTTP

Action: Permit

CLI

1. Trust/Untrust/DMZ Port Mode

```
exec port-mode extend
```

At the following prompt, enter **y** (for yes):

```
Change port mode from <trust-untrust> to <extend> will erase system  
configuration and reboot box
```

```
Are you sure y/[n] ?
```

2. Trust and DMZ Interfaces¹²

```
set interface ethernet1 ip 192.168.1.1/24
set interface ethernet1 nat
set interface ethernet1 dhcp server service
set interface ethernet1 dhcp server ip 192.168.1.3 192.168.1.33
set interface ethernet2 ip 10.1.1.1/24
set interface ethernet2 nat
```

3. ADSL Interface and MIP

```
set interface adsl1 pvc 0 35 zone untrust
set interface adsl1 ip 1.1.1.1/24
set interface adsl1 mip 1.1.1.5 host 10.1.1.5 netmask 255.255.255.255 vrtr
trust-vr
```

4. Policy

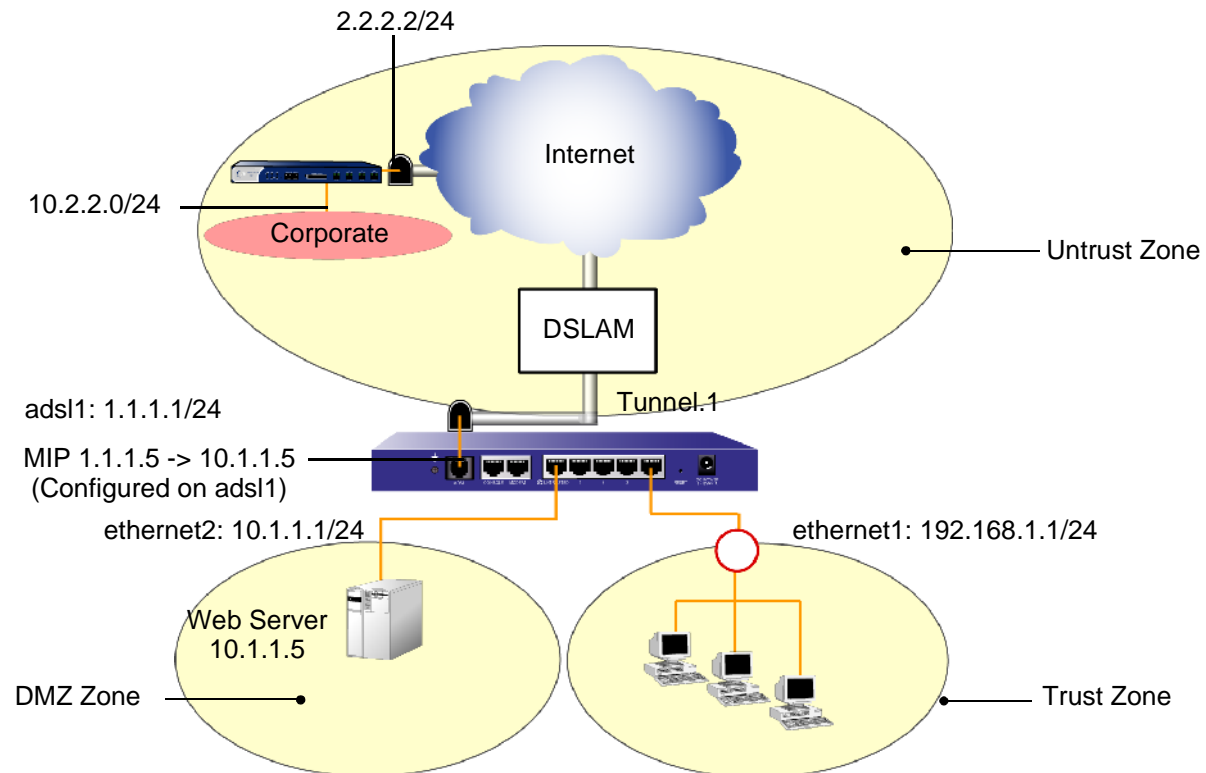
```
set policy from untrust to dmz any mip(1.1.1.5) http permit
save
```

12. In Trust/Untrust/DMZ port mode, the ethernet1 interface is automatically bound to the Trust zone, while ethernet2 is bound to the DMZ zone.

Example: (Branch Office) VPN Tunnel through ADSL

The following example shows how to configure a VPN tunnel to corporate headquarters through the ADSL interface on the NetScreen device. This example also shows how to allow Internet access to local web servers while protecting other internal hosts from being directly accessible from the Internet, as described in [“Example: \(Small Business\) Allow Access to Local Servers”](#) on page 26.

NetScreen device in Trust/Untrust/DMZ (Extended) port mode



In this example, you configure a route-based AutoKey IKE tunnel using a preshared secret.¹³ For the Phase 1 and 2 security levels, you configure pre-g2-3des-sha for the Phase 1 proposal and the predefined “Compatible” set of proposals for Phase 2. To configure the tunnel, you need to do the following:

1. Create a tunnel interface and bind it to the Untrust security zone. You configure the tunnel interface to borrow the IP address from the adsl1 interface, which is also bound to the Untrust security zone (this is known as an “unnumbered” interface).
2. Configure the VPN tunnel, designate the adsl1 interface as its outgoing interface in the Untrust zone, bind it to the tunnel interface, and configure its proxy-ID.
3. Enter a route to the Corporate LAN via the tunnel interface.
4. Set up policies for VPN traffic to pass between the branch office and corporate headquarters.

WebUI

1. Trust/Untrust/DMZ Port Mode

Configuration > Port Mode > Port Mode: Select Extended from the drop-down list, and then click **Apply**.

At the following prompt, click **OK**:

Operational mode change will erase current configuration and reset the device, continue?

2. Trust and DMZ Interfaces¹⁴

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

Static IP: (select)

IP Address/Netmask: 192.168.1.1/24

Interface Mode: NAT

Network > DHCP > Edit (for ethernet1 interface) > DHCP Server: Select **Apply**.

13. You need to configure the preshared secret at each end of the tunnel. This example shows the configuration on the NetScreen ADSL device only.

14. In Trust/Untrust/DMZ port mode, the ethernet1 interface is automatically bound to the Trust zone, while ethernet2 is bound to the DMZ zone.

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

Dynamic: (select)

IP Address Start: 192.168.1.3

IP Address End: 192.168.1.33

Network > Interfaces > Edit (for ethernet2 interface): Enter the following, and then click **OK**:

Static IP: (select)

IP Address/Netmask: 10.1.1.1/24

Interface Mode: NAT

3. ADSL Interface and MIP

Network > Interfaces > Edit (for adsl1 interface): Enter the following, and then click **Apply**:

VPI/VCI: 0/35

Zone Name: Untrust

Static IP: (select)

IP Address/Netmask: 1.1.1.1/24

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

Mapped IP: 1.1.1.5

Netmask: 255.255.255.255

Host IP Address: 10.1.1.5

Host Virtual Router Name: trust-vr

4. VPN Tunnel

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (select)

Interface: adsl1 (trust-vr)

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

Gateway Name: To_Corp

Security Level: Custom

Remote Gateway Type:

Static IP Address: (select), IP Address/Hostname: 2.2.2.2

Preshared Key: h1p8A24nG5

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: Branch1_Corp

Security Level: Compatible

Remote Gateway:

Predefined: (select), To_Corp

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

Security Level: Compatible

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (select)

Local IP/Netmask: 192.168.1.1/24

Remote IP/Netmask: 10.2.2.0/24

Service: ANY

Network > Routing > Routing Entries > trust vr > New: Enter the following, and then click **OK**:

Network Address/Netmask: 10.2.2.0/24

Gateway: (select)

Interface: Tunnel.1

5. Policies

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

Source Address:

Address Book Entry: (select) Any

Destination Address:

Address Book Entry: (select), MIP(1.1.1.5)

Service: HTTP

Action: Permit

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

Name: To_Corp

Source Address: 192.168.1.1/24

Destination Address: 10.2.2.0/24

Service: ANY

Action: Permit

Position at Top: (select)

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

Name: From_Corp
Source Address: 10.2.2.0/24
Destination Address: 192.168.1.1/24
Service: ALL
Action: Permit
Position at Top: (select)

CLI

1. Trust/Untrust/DMZ Port Mode

```
exec port-mode extend
```

At the following prompt, enter **y** (for yes):

```
Change port mode from <trust-untrust> to <extend> will erase system
configuration and reboot box
Are you sure y/[n] ?
```

2. Trust and DMZ Interfaces¹⁵

```
set interface ethernet1 ip 192.168.1.1/24
set interface ethernet1 nat
set interface ethernet1 dhcp server service
set interface ethernet1 dhcp server ip 192.168.1.3 192.168.1.33
set interface ethernet2 ip 10.1.1.1/24
set interface ethernet2 nat
```

15. In Trust/Untrust/DMZ port mode, the ethernet1 interface is automatically bound to the Trust zone, while ethernet2 is bound to the DMZ zone.

3. ADSL Interface and MIP

```
set interface adsl1 pvc 0 35 zone untrust
set interface adsl1 ip 1.1.1.1/24
set interface adsl1 mip 1.1.1.5 host 10.1.1.5 netmask 255.255.255.255 vrouter
trust-vr
```

4. VPN Tunnel

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface adsl1
set ike gateway To_Corp address 2.2.2.2 main outgoing-interface adsl1 preshare
hlp8A24nG5 proposal pre-g2-3des-sha
set vpn Branch1_Corp gateway To_Corp sec-level compatible
set vpn Branch1_Corp bind interface tunnel.1
set vpn Branch1_Corp proxy-id local-ip 192.168.1.1/24 remote-ip 10.2.2.0/24 any
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
```

5. Policies

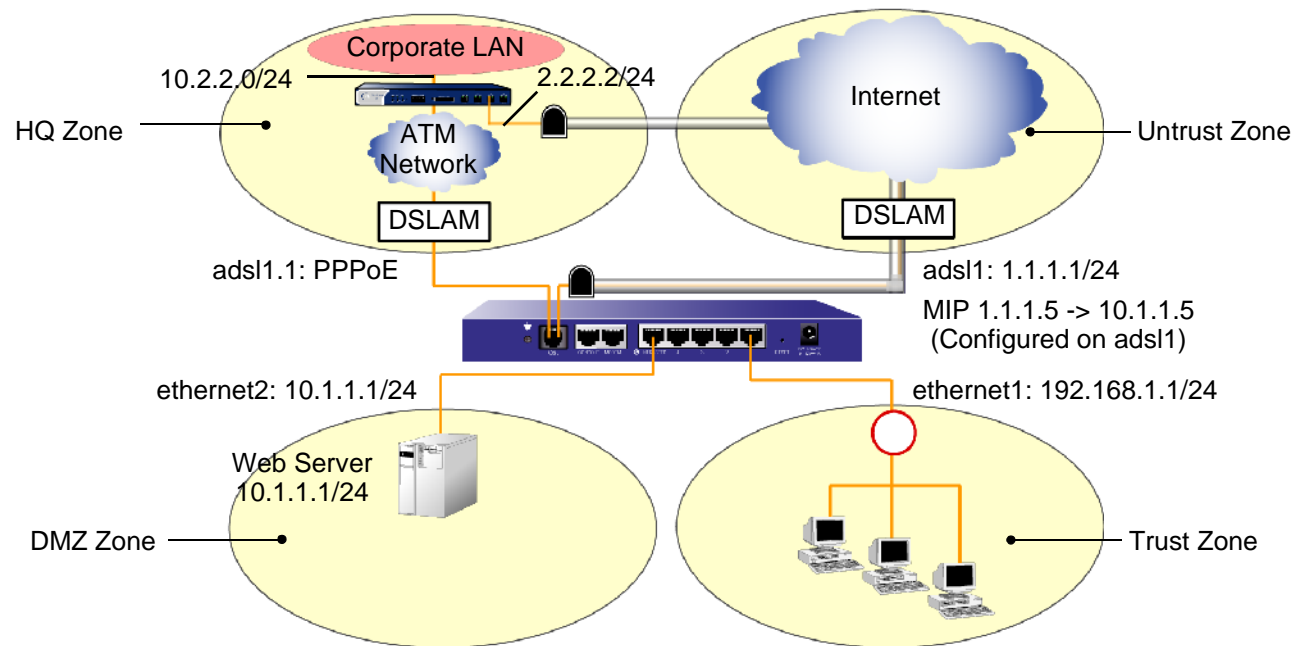
```
set policy from untrust to dmz any mip(1.1.1.5) http permit
set policy top name "To Corp" from trust to untrust 192.168.1.1/24 10.2.2.0/24
any permit
set policy top name "From Corp" from untrust to trust 10.2.2.0/24
192.168.1.1/24 any permit
save
```

Example: (Branch Office) Secondary VPN Tunnel

The following example shows how to configure the NetScreen device as a firewall with both an Internet connection and a connection to corporate headquarters through the ADSL interface. This example is similar to the configuration shown in “[Example: \(Branch Office\) VPN Tunnel through ADSL](#)” on page 31, but you create two PVCs: one to the Internet and another to corporate headquarters. You also configure a VPN tunnel through the Internet to corporate headquarters as a secondary connection.

You configure an additional PVC on the NetScreen device by creating the ADSL subinterface `adsl1.1`. You can bind the ADSL interface and each of its subinterfaces to different security zones; you bind the ADSL subinterface to a custom zone “HQ” (the main ADSL interface is bound to the Untrust zone by default). In this example, you configure the `adsl1.1` subinterface with the VPI/VCI pair value 1/35 that uses LLC encapsulation and a PPPoE instance named “`poe1`” which is bound to the subinterface. You then need to define policies to allow the flow of traffic to and from the HQ zone.

NetScreen device in
Trust/Untrust/DMZ
(Extended) port mode



Because you have two different routes between workstations in the Trust zone and corporate headquarters—one using the adsl1.1 interface and another using the VPN tunnel interface—you need to specify which route is “preferred”. This is done by setting the metric for the route through the VPN tunnel higher than the route through the adsl1.1 interface.

WebUI

1. Trust/Untrust/DMZ Port Mode

Configuration > Port Mode > Port Mode: Select Extended from the drop-down list, and then click **Apply**.

At the following prompt, click **OK**:

Operational mode change will erase current configuration and reset the device, continue?

2. Trust and DMZ Interfaces¹⁶

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

Static IP: (select)

IP Address/Netmask: 192.168.1.1/24

Interface Mode: NAT

Network > DHCP > Edit (for ethernet1 interface) > DHCP Server: Select **Apply**.

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

Dynamic: (select)

IP Address Start: 192.168.1.3

IP Address End: 192.168.1.33

16. In Trust/Untrust/DMZ port mode, the ethernet1 interface is automatically bound to the Trust zone, while ethernet2 is bound to the DMZ zone.

Network > Interfaces > Edit (for ethernet2 interface): Enter the following, and then click **OK**:

Static IP: (select)

IP Address/Netmask: 10.1.1.1/24

Interface Mode: NAT

3. ADSL Interface and MIP

Network > Interfaces > Edit (for adsl1 interface): Enter the following, and then click **Apply**:

VPI/VCI: 0/35

Zone Name: Untrust

Static IP: (select)

IP Address/Netmask: 1.1.1.1/24

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

Mapped IP: 1.1.1.5

Netmask: 255.255.255.255

Host IP Address: 10.1.1.5

Host Virtual Router Name: trust-vr

4. HQ Zone

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

Zone Name: HQ

Block Intra-Zone Traffic: (select)

5. ADSL Subinterface

Network > Interfaces > New ADSL Sub-IF: Enter the following, and then click OK:

Interface Name: adsl1.1

VPI/VCI: 1/35

Encapsulation: LLC (selected)

Zone: HQ (select)

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

PPPoE Instance: poe1

Bound to Interface: adsl1.1 (select)

Username: felix

Password: ioP936QNIwab48Rc

6. VPN Tunnel

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (select)

Interface: adsl1 (trust-vr)

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

Gateway Name: To_Corp

Security Level: Custom

Remote Gateway Type:

Static IP Address: (select), IP Address/Hostname: 2.2.2.2

Preshared Key: h1p8A24nG5

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: Branch1_Corp

Security Level: Compatible

Remote Gateway:

Predefined: (select), To_Corp

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

Security Level: Compatible

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (select)

Local IP/Netmask: 192.168.1.1/24

Remote IP/Netmask: 10.2.2.0/24

Service: ANY

7. Routes

Network > Routing > Routing Entries > trust vr > New: Enter the following, and then click **OK**:

Network Address/Netmask: 10.2.2.0/24

Gateway: (select)

Interface: adsl1.1

Metric: 1

Network > Routing > Routing Entries > trust vr > New: Enter the following, and then click **OK**:

Network Address/Netmask: 10.2.2.0/24

Gateway: (select)

Interface: Tunnel.1

Metric: 5

8. Policies

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

Source Address:

Address Book Entry: (select) Any

Destination Address:

Address Book Entry: (select) Any

Service: ANY

Action: Permit

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

Source Address:

Address Book Entry: (select) Any

Destination Address:

Address Book Entry: (select) Any

Service: ANY

Action: Permit

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

Source Address:

Address Book Entry: (select) Any

Destination Address:

Address Book Entry: (select) Any

Service: ANY

Action: Permit

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

Source Address:

Address Book Entry: (select) Any

Destination Address:

Address Book Entry: (select) Any

Service: ANY

Action: Permit

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

Source Address:

Address Book Entry: (select) Any

Destination Address:

Address Book Entry: (select), MIP(1.1.1.5)

Service: HTTP

Action: Permit

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

Name: To_Corp

Source Address: 192.168.1.1/24

Destination Address: 10.2.2.0/24

Service: ANY

Action: Permit
Position at Top: (select)
Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:
Name: From_Corp
Source Address: 10.2.2.0/24
Destination Address: 192.168.1.1/24
Service: ALL
Action: Permit
Position at Top: (select)

CLI

1. Trust/Untrust/DMZ Port Mode

```
exec port-mode extend
```

At the following prompt, enter **y** (for yes):

```
Change port mode from <trust-untrust> to <extend> will erase system  
configuration and reboot box  
Are you sure y/[n] ?
```

2. Trust and DMZ Interfaces¹⁷

```
set interface ethernet1 ip 192.168.1.1/24  
set interface ethernet1 nat  
set interface ethernet1 dhcp server service  
set interface ethernet1 dhcp server ip 192.168.1.3 192.168.1.33  
set interface ethernet2 ip 10.1.1.1/24  
set interface ethernet2 nat
```

17. In Trust/Untrust/DMZ port mode, the ethernet1 interface is automatically bound to the Trust zone, while ethernet2 is bound to the DMZ zone.

3. ADSL Interface and MIP

```
set interface adsl1 pvc 0 35 zone untrust
set interface adsl1 ip 1.1.1.1/24
set interface adsl1 mip 1.1.1.5 host 10.1.1.5 netmask 255.255.255.255 vrouter
trust-vr
```

4. HQ Zone

```
set zone name HQ
set zone HQ block
set zone HQ vrouter trust-vr
```

5. ADSL Subinterface

```
set interface adsl1.1 pvc 1 35 mux llc zone HQ
set pppoe name poel username felix password ioP936QNlwab48Rc
set pppoe name poel interface adsl1.1
```

6. VPN Tunnel

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface adsl1
set ike gateway To_Corp address 2.2.2.2 main outgoing-interface adsl1 preshare
hlp8A24nG5 proposal pre-g2-3des-sha
set vpn Branch1_Corp gateway To_Corp sec-level compatible
set vpn Branch1_Corp bind interface tunnel.1
set vpn Branch1_Corp proxy-id local-ip 192.168.1.1/24 remote-ip 10.2.2.0/24 any
```

7. Routes

```
set vrouter trust-vr route 10.2.2.0/24 interface adsl1.1 metric 1
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1 metric 5
```

8. Policies

```
set policy from trust to HQ any any any permit
set policy from HQ to trust any any any permit
```

```
set policy from dmz to HQ any any any permit
set policy from HQ to dmz any any any permit
set policy from untrust to dmz any mip(1.1.1.5) http permit
set policy top name "To Corp" from trust to untrust 192.168.1.1/24 10.2.2.0/24
    any permit
set policy top name "From Corp" from untrust to trust 10.2.2.0/24
    192.168.1.1/24 any permit
save
```

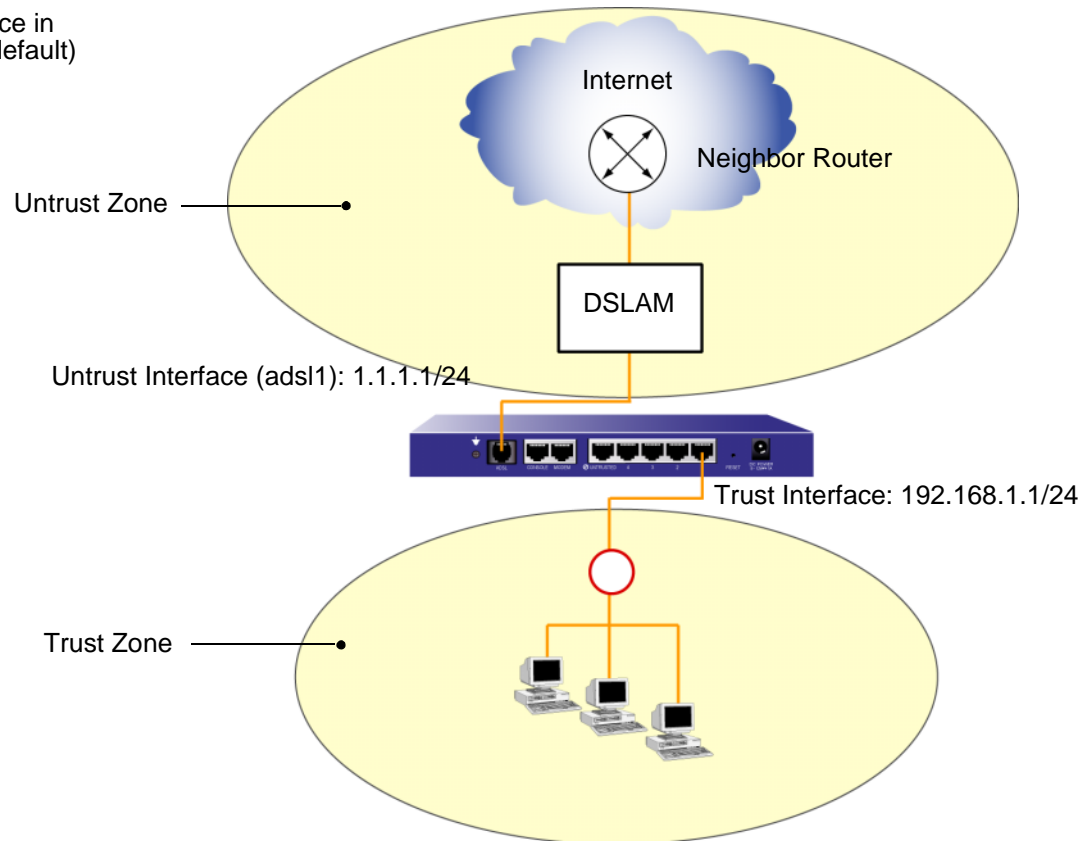
Example: 1483 Routing on ADSL Interface

(This configuration is only supported in the ScreenOS 5.0.0-1483 release for the NetScreen-5GT ADSL device.) RFC 1483 describes methods of transporting routed protocol data units (PDUs) over AAL5 links. Use this configuration to enable the NetScreen-5GT ADSL device to exchange routing information with another router through the ADSL interface.

The following example shows how to configure the NetScreen device as a firewall with an Internet connection through the ADSL interface using 1483 routing and LLC encapsulation. You configure a PVC on the ADSL interface with the VPI/VCI pair 0/35 and the static IP address 1.1.1.1/24. (In the ScreenOS 5.0.0-1483 release, you can also configure the ADSL interface to be a DHCP client which receives its IP address from a DHCP server running on the neighbor router.)

You enable the dynamic routing protocol—which can be either RIP, OSPF, or BGP—in the trust-vr virtual router and on the ADSL and trust interfaces; in the example, the dynamic routing protocol is RIP. The interface on the neighbor router is also configured for LLC encapsulation and 1483 routing.

NetScreen device in
Trust-Untrust (default)
port mode



WebUI

1. ADSL Interface

Network > Interfaces > Edit (for adsl1 interface): Enter the following, and then click **OK**:

VPI/VCI: 0/35

Multiplexing Method: LLC (select)

RFC1483 Protocol Mode: Routed (select)

Zone: Untrust
Static IP: (select)
IP Address/Netmask: 1.1.1.1/24

2. Trust Interface

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

Zone: Trust
Static IP: (select)
IP Address/Netmask: 192.168.1.1/24
Interface Mode: Route

3. Dynamic Routing Protocol

Network > Routing > Virtual Router (trust-vr) > Edit: Select Create RIP Instance.

Select Enable RIP, and then click **OK**.

Network > Interface > Edit (for adsl1 interface) > RIP: Select Protocol RIP Enable, and then click **Apply**.

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

CLI

1. ADSL Interface

```
set int adsl1 pvc 0 35 mux llc protocol routed zone untrust  
set int adsl1 ip 1.1.1.1/24
```

2. Trust Interface

```
set interface trust zone trust  
set interface trust ip 192.168.1.1/24  
set interface trust route
```

3. Dynamic Routing Protocol

```
set vr trust-vr protocol rip
set vr trust-vr protocol rip enable
set interface adsl1 protocol rip
set interface adsl1 protocol rip enable
set interface trust protocol rip
set interface trust protocol rip enable
```


New and Modified CLI Commands

This chapter introduces the following new commands:

- [pppoa on page 54](#)

In addition, it presents new changes to the following commands:

- [interface on page 60](#)

New command elements in the Syntax sections appear in **red**. For example, in the following command, **pvc** *id_num1 id_num2* is new in this release:

```
set interface interface pvc id_num1 id_num2
```

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* for ScreenOS 5.0.0.

pppoa

Description: Use the **pppoa** commands to configure PPPoA, or to display current PPPoA configuration parameters.

Point-to-Point Protocol over ATM (PPPoA) is usually used for PPP sessions that are to be terminated on a NetScreen device with an ADSL interface. PPPoA is primarily used for business class services as it does not require a desktop client (which is required for PPPoE termination).

Syntax

clear

```
clear [ cluster ] pppoa [ name name_str ]
```

exec

```
exec pppoa [ name name_str ] { connect | disconnect }
```

get

```
get pppoa { all | name name_str }
```

set

```
set pppoa [ name name_str ]  
  {  
    authentication { CHAP | PAP | any } |  
    auto-connect number |  
    clear-on-disconnect |  
    idle-interval number |  
    interface [ interface ] |  
    netmask [ mask ] |  
    ppp
```

```
    {  
      lcp-echo-retries number |  
      lcp-echo-timeout number  
    } |  
  static-ip |  
  update-dhcpserver |  
  username name_str password pswd_str  
}
```

unset

```
unset pppoa [ name name_str ]  
{  
  authentication { CHAP | PAP } |  
  auto-connect |  
  clear-on-disconnect |  
  idle-interval |  
  interface |  
  netmask |  
  ppp  
  {  
    lcp-echo-retries |  
    lcp-echo-timeout  
  } |  
  static-ip |  
  update-dhcpserver |  
  username  
}
```

Keywords and Variables

all

```
get pppoa all
```

all Displays information for all PPPoA instances.

authentication

```
set pppoa authentication { CHAP | PAP | any }
```

```
unset pppoa authentication { CHAP | PAP }
```

authentication Sets the authentication methods to **CHAP**, **PAP**, or **any**. (The **any** option gives preference to CHAP.) The default authentication is **any** (both CHAP and PAP). To set authentication to CHAP only, first execute **unset pppoa authentication PAP**.

auto-connect

```
set pppoa auto-connect number
```

```
unset pppoa auto-connect
```

auto-connect Specifies the number of seconds that elapse before automatic re-initiation of a previously-closed connection occurs. Valid range is 0-10000. (0 to disable.) This is disabled by default.

clear-on-disconnect

```
set pppoa [ name name_str ] clear-on-disconnect
```

unset pppoa clear-on-disconnect

clear-on-disconnect Directs the NetScreen device to clear the IP address and the gateway for the interface once PPPoA disconnects. By default, this is disabled; that is, the IP address and gateway for the interface remain when PPPoA disconnects.

If you do not specify **name**, ScreenOS sets the parameter for the default instance untrust.

connect / disconnect

exec pppoa [name *name_str*] { connect | disconnect }

connect Starts a PPPoA connection for an instance. (Each instance can be bound to an interface.)

disconnect Takes down a PPPoA connection.

idle-interval

set pppoa idle-interval *number*

unset pppoa idle-interval

idle-interval Sets the idle timeout, which is time elapsed (in minutes) before the NetScreen device terminates a PPPoA connection due to inactivity. Valid range is 0-10000 minutes. Specifying 0 turns off the idle timeout and the device never terminates the connection. The default is 30 minutes.

interface

set pppoa interface [*name_str*]

unset pppoa interface

interface Specifies the ADSL interface for PPPoA encapsulation.

name

```
exec pppoa [ name name_str ] { connect | disconnect }
get pppoa [ name name_str | all ]
set pppoa [ name name_str ] ...
unset pppoa [ name name_str ]
```

name Specifies or defines the name for a specific PPPoA instance. You can assign a username and password, interface, and other PPP/PPPoA parameters to the instance. If you do not specify **name**, ScreenOS automatically configures the parameters for the default instance untrust.

Example: The following commands define a name for a PPPoA instance.

- User name user1 and password 123456
- PPPoA instance pppoa-user-1 bound to the ethernet2 interface

```
set pppoa name pppoa-user-1 username user1 password 123456
set pppoa name pppoa-user-1 interface ethernet2
```

netmask

```
set pppoa netmask mask
unset pppoa netmask
```

netmask Specifies a PPPoA subnet mask that the device assigns to the interface bound to the PPPoA instance (after establishment of the connection). The default netmask is 255.255.255.0. When it is necessary for two or more interfaces to have overlapping subnets, use the following command:
set vrouter vrouter ignore-subnet-conflict

ppp

```
set pppoa ppp { ... }  
unset pppoa ppp { ... }
```

ppp Specifies PPP parameters.

- **lcp-echo-retries** the number of unacknowledged LCP Echo requests before connection is terminated. Valid range is 1-30. The default is 10.
- **lcp-echo-timeout** the time that elapses between transmission of two LCP Echo requests. Valid range is 1-1000 seconds. The default is 180 seconds.

static-ip

```
set pppoa static-ip  
unset pppoa static-ip
```

static-ip Specifies that your connection uses the static IP address assigned to your device's interface. This is disabled by default.

update-dhcpserver

```
set pppoa update-dhcpserver  
unset pppoa update-dhcpserver
```

update-dhcpserver Specifies that the DHCP server (on the device) automatically updates DNS parameters received through the PPPoA connection. This is enabled by default.

username

```
set pppoa username name_str password pswd_str
```

username Sets the user name and password for authentication.

interface

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

Syntax

get

```
get interface ...
```

set

```
set interface interface phy
  {
    annex-b-mode { dt | non-dt } |
    operating-mode { auto | ansi-dmt | itu-dmt | glite }
  }
set interface interface pvc id_num1 id_num2 [ mux { vc | llc } ]
[ protocol { routed | bridged } ] zone zone
```

unset

```
unset interface ...
```

Variable Parameter

```
set interface interface [ ... ]
```

interface **ads11** is the main ADSL interface on which you configure a virtual circuit. You can configure subinterfaces to **ads11**, such as **ads11.1**, **ads11.2**, etc., to support additional virtual circuits.

Keywords

mux

```
set interface interface ... [ mux { vc | llc } ]
```

mux

Specifies one of the following ATM multiplexing encapsulation methods for the ADSL interface:

- **vc** specifies VC encapsulation.
- **llc** specifies Logical Link Control/SubNetwork Attachment Point (LLC/SNAP) encapsulation (this is the default encapsulation method).

phy

```
set interface interface phy annex-b-mode { dt | non-dt }  
set interface interface phy operating-mode { auto | ansi-dmt | itu-dmt | glite}
```

annex-b-mode

(For Annex B device models only) Specifies one of the following modes for the main ADSL interface:

- **dt** specifies that the ADSL interface is connected to a Deutsch Telecom DSLAM. You must use this option if you are connecting an Annex B model of the NetScreen device to a Deutsch Telecom DSLAM.
- **non-dt** specifies that the ADSL interface is connected to a non-Deutsch Telecom DSLAM. This is the default mode.

- operating-mode** Specifies one of the following operating modes for the physical line for the ADSL interface:
- **auto** allows the ADSL interface to automatically negotiate the operating mode with the service provider's DSLAM. This is the default operating mode.
 - **ansi-dmt** specifies that the ADSL interface uses ANSI T1.413 Issue 2 mode.
 - **itu-dmt** specifies that the ADSL interface uses the International Telecommunications Union (ITU) G.992.1 (G.dmt) standard. This mode supports minimum data rates of 6.144 Mbps downstream and 640 kbps upstream.
 - **glite** specifies that the ADSL interface uses the ITU 992.2 (G.lite) standard. This mode supports maximum data rates of 1.536 Mbps downstream and 512 kbps upstream.

protocol

```
set interface interface ... [ protocol { routed | bridged } ]
```

- protocol** (This option is only supported on the ScreenOS 5.0.0-1483 release.) Specifies that one of the following types of protocol data units (PDUs) is used to carry network traffic through the ADSL interface:
- **routed** specifies routed PDUs, as described in RFC 1483, "Multiprotocol Encapsulation over ATM Adaption Layer 5".
 - **bridged** specifies bridged PDUs, as described in RFC 1483, "Multiprotocol Encapsulation over ATM Adaption Layer 5". This is the default.

pvc

```
set interface interface pvc id_num1 id_num2 ...
```

- pvc** Specifies a permanent virtual circuit (PVC), in the form of a virtual path identifier (VPI)/virtual channel identifier (VCI) pair, for the ADSL interface or subinterface. *id_num1* is the VPI number and *id_num2* is the VCI number. You must configure a VPI/VCI pair that corresponds to the PVC for each ADSL interface or subinterface.

zone

set interface *interface* ... **zone** *zone*

zone Specifies the zone to which the ADSL interface or subinterface is bound.

New Messages

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

- [“ADSL” on page 66](#)
- [“PPPoA” on page 69](#)

For a complete list of NetScreen log messages, refer to the *NetScreen Message Log Reference Guide* for ScreenOS 5.0.0.

ADSL

These messages relate to the ADSL line connection on the NetScreen device.

Notification (00555)

Message ADSL Line UP Fast and Interleave Channels.

Meaning The ADSL line is operational for fast-path and interleaved-path channels.

Action No recommended action

Message ADSL Line Waiting for Activating.

Meaning The ADSL line is awaiting activation.

Action No recommended action

Message ADSL Line Activating.

Meaning The ADSL line is activating.

Action No recommended action

Message ADSL Line DOWN.

Meaning There is no physical connection on the ADSL line.

Action Make sure that the ADSL cable is properly connected and that you have ADSL service on the line. If you continue to see this message, contact NetScreen technical support by visiting www.netscreen.com/cso. (Note: You must be a registered NetScreen customer.)

Message ADSL Line UP Fast Channel.

Meaning The ADSL line is operational for a fast-path channel.

Action No recommended action

Message ADSL Line UP Interleaved Channel.

Meaning The ADSL line is operational for an interleaved-path channel.

Action No recommended action

Message ADSL Line UP Fast Channel, change Utopia address to match it.

Meaning The ADSL line is operational for a fast-path channel, and the address on the ATM connection bus has changed.

Action No recommended action

Message ADSL Line UP Interleaved Channel, change Utopia address to match it.

Meaning The ADSL line is operational for an interleaved channel, and the address on the ATM connection bus has changed.

Action No recommended action

Message ADSL Line in an unknown state.

Meaning An internal error occurred

Action Contact NetScreen technical support by visiting www.netscreen.com/cso. (Note: You must be a registered NetScreen customer.)

PPPoA

These messages relate to the configuration of Point-to-Point Protocol over Asynchronous Transfer Mode (ATM) virtual circuits.

Notification (00055)

Message PPPoA is enabled on <interface> interface.

Meaning The PPPoA client on the NetScreen device is enabled on the specified interface.

Action No recommended action.

Message PPPoA is disabled on <interface> interface.

Meaning The PPPoA client on the NetScreen device is disabled on the specified interface.

Action No recommended action.

Notification (00556)

Message PPPoA <name> has started negotiation.

Meaning The PPPoA client on the NetScreen device began to initiate a session with the PPPoA server.

Action No recommended action.

Message PPPoA <name> connected successfully.

Meaning The PPPoA client on the NetScreen device successfully established a session with the PPPoA server.

Action No recommended action.

Message PPPoA <name> connection attempt failed <reason>.

Meaning The NetScreen device was unsuccessful in its attempt to establish a session with a PPPoA server for the reason given.

Action Check the PPPoA configuration.

Message PPPoA <name> idle timeout.

Meaning The NetScreen device terminated the PPPoA connection due to inactivity. The default idle timeout is 30 minutes.

Action Specify a higher idle timeout value (valid range is up to 10000 minutes), or set the idle timeout to 0, which turns off the timeout.

Message PPPoA <name> shutdown.

Meaning The NetScreen device shut down the PPPoA session.

Action No recommended action

Message PPPoA <name> failed to modify the IP for the interface.

Meaning During the PPPoA session, a new IP address was assigned to the interface but failed to update on the device.

Action Reboot the device.

Message PPPoA <name> failed to negotiate IP for the interface.

Meaning No IP address was assigned to the interface during the PPPoA session.

Action Check the PPPoA configuration on the device. Recheck the PPPoA configuration parameters on the service provider's server.

Message PPPoA <name> failed to modify the gateway for the interface.

Meaning During the PPPoA session, a new IP address was assigned to the default gateway for the interface but failed to update on the device.

Action Reboot the device.

Index

Symbols

1483 bridging, example configuration 12
1483 routing, example configuration 48

A

AAL5 encapsulations 3
ADSL
 connecting the cable 3
 messages 66
 overview 2
ATM 3

C

CLI
 interface commands 60
 pppoa commands 54
configuration
 1483 bridging 12
 1483 routing 48
 dial backup 16
 Ethernet backup 22
 local server access 26
 PPPoA 8
 VPN tunnel 31, 38
conventions
 WebUI iv

D

dial backup, example configuration 16
DMT 4

E

Ethernet backup, example configuration 22
example configuration
 1483 bridging 12
 1483 routing 48
 dial backup 16
 Ethernet backup 22
 local server access 26
 PPPoA 8
 VPN tunnel 31, 38

H

Home-Work port mode, example configuration 16

I

interface CLI commands 60

L

local server access, example configuration 26

O

overview of ADSL 2

P

PPP 4
PPPoA 4, 5
 example configuration 8
 messages 69
pppoa CLI commands 54
PPPoE 4

S

service provider, information from 3

T

Trust/Untrust/DMZ port mode
 example configuration 26

V

VCI 3
VPI 3
VPN tunnel
 example configuration 31, 38

W

WebUI, conventions iv

