

NETSCREEN-5GT WIRELESS

User's Guide

*in English, French, German, Spanish, Japanese,
Simplified Chinese and Traditional Chinese*

Version 5.0.0

P/N 093-1481-000

Rev. A



Copyright Notice

Copyright © 2005 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 JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Languages Contents

English	1
French	41
German	83
Spanish	123
Japanese	163
Simplified Chinese	201
Traditional Chinese	239

Contents

Preface	3
Organization	3
WebUI Conventions	4
CLI Conventions	4
NetScreen Publications	5
Chapter 1 Connecting the Device	7
Connecting the NetScreen Device to Your Networks	7
Connecting the Device to an Untrusted Network	7
Connecting the ADSL Port	7
Connecting the Untrusted Port	9
Connecting the Device to Your Internal Network or Workstations.....	9
Connecting Trusted Ethernet Ports	9
Using the Wireless Interface	9
Connecting the Power	10
Rack Mounting (Optional)	10
Chapter 2 Configuring the Device	13
Accessing the Device	13
Using the WebUI.....	13
Using Telnet	14
Using a Console Connection.....	15
Required Configuration	15
Changing the Admin Name and Password.....	16
Setting the Date and Time.....	16
Wireless Configuration	17
Configuring the Wireless Network	18
ADSL Configuration	19
Configuring the ADSL Interface	20
Adding Virtual Circuits to an ADSL Interface	21
VPI/VCI and Multiplexing Method	21
PPPoE or PPPoA	22
Annex B Mode	23
Static IP Address and Netmask	23
Optional Configuration	24
Restricting Management.....	25
Configuring Additional Policies.....	25
Operational Mode	25
Changing the Port Mode.....	26
Configuring a Backup Untrust Zone Interface.....	28

Changing the Trust or Wireless2 Interface Address	29
Verifying External Connectivity	29
Resetting the Device to Factory Defaults	29
Using the Reset Pinhole.....	30
Chapter 3 Hardware Descriptions.....	31
Port and Power Connectors	31
Status LEDs	32
Main Status LEDs for the Device.....	33
Port Status LEDs	33
Specifications	35
Index.....	39

Preface

The Juniper Networks NetScreen-5GT Wireless device provides IPsec Virtual Private Network (VPN) and firewall services for a branch office or a retail outlet that uses an integrated wireless 802.11b/g interface. The NetScreen-5GT Wireless device uses the same firewall, VPN, antivirus, deep inspection, and traffic management technology as NetScreen's high-end central site products.

Juniper Networks offers three models of the NetScreen-5GT Wireless device:

- **NetScreen-5GT Wireless:** The Wireless only model.
- **NetScreen-5GT Wireless ADSL A:** The Wireless with Annex A model supports ADSL over standard telephone lines (POTS).
- **NetScreen-5GT Wireless ADSL B:** The Wireless with Annex B model supports ADSL over Integrated Services Digital Network (ISDN).

All models support up to four wireless security zones. Both ADSL models support ANSI T1.413 Issue 2, ITU G.992.1 (G.dmt), and ITU 992.2 (G.lite) standards.

Each model supports three software versions:

- The 10-user version supports up to 10 users.
- The Plus version supports an unrestricted number of users.
- The Extended version provides the same capabilities as the Plus version, with additional features: High Availability (NSRP Lite), the DMZ security zone, and additional sessions and tunnel capacity.

ORGANIZATION

This manual has three chapters and one appendix.

[Chapter 1, “Connecting the Device”](#) describes how to connect the device to your network, connect the power and an antenna, and install the NetScreen-5GT Wireless device in a rack.

[Chapter 2, “Configuring the Device”](#) describes the default settings and operation of the NetScreen-5GT Wireless (ADSL) and the configuration required to use the device.

[Chapter 3, “Hardware Descriptions”](#) provides an overview of NetScreen-5GT Wireless ports, LEDs, and power requirements.

[Appendix A, “Specifications”](#) provides a list of physical specifications about the NetScreen-5GT Wireless device.

WEBUI CONVENTIONS

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

Example: Objects > Addresses > List > New

To access the new address configuration dialog box:

1. Click **Objects** in the menu column.
The Objects menu option expands to reveal a subset of options for Objects.
2. (Applet menu¹) 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 name1 password xyz
```

1. You can choose either the applet or DHTML menu types by clicking the **Toggle Menu** option at the bottom of the menu column.

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 PUBLICATIONS

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

Connecting the Device

This chapter describes how to connect the NetScreen-5GT Wireless device to the network, connect the power, and connect an antenna. If you are using the optional NetScreen-5GT Wireless rack mount kit, use the rack mounting instructions that are included at the end of this chapter.

Note: For safety warnings and instructions, refer to the NetScreen Safety Guide. The instructions in this guide warn you about situations that could cause bodily injury. Before working on any equipment, be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.

CONNECTING THE NETSCREEN DEVICE TO YOUR NETWORKS

The NetScreen device provides firewall and general security for your networks when it is placed between your internal networks and the Untrusted network. This section describes the physical connections.

Connecting the Device to an Untrusted Network

Depending upon which model of the NetScreen-5GT Wireless device you have, you can connect to the Untrusted network in one of the following ways:

- Through an ADSL connection from the ADSL port on the NetScreen device
- Through an Ethernet connection from the Untrusted port on the NetScreen device

Connecting the ADSL Port

Connect the provided ADSL cable from the ADSL port on the NetScreen-5GT Wireless ADSL device to your telephone outlet. The ADSL port on the Annex A version of the device uses an RJ-11 connector, while the Annex B version uses an RJ-45 connector. In the case of Annex B models, the cable you connect from the ADSL port to the telephone outlet is identical in appearance and wiring to a straight-through 10 Base-T Ethernet cable.

Warning: Make sure that you do not inadvertently connect the Console, Modem, or Ethernet ports on the NetScreen device to the telephone outlet.

On the NetScreen-5GT Wireless ADSL device, the ADSL line is your *primary* connection to an outside network. For a backup data link to an outside network, you can either connect an Ethernet cable from the Untrusted port on the NetScreen-5GT Wireless ADSL device to an external router or a DSL, or cable modem, or you can connect a serial cable from the Modem port on the device to an external modem.

Warning: You cannot connect both the Untrusted port and the Modem port on the device to an outside network at the same time.

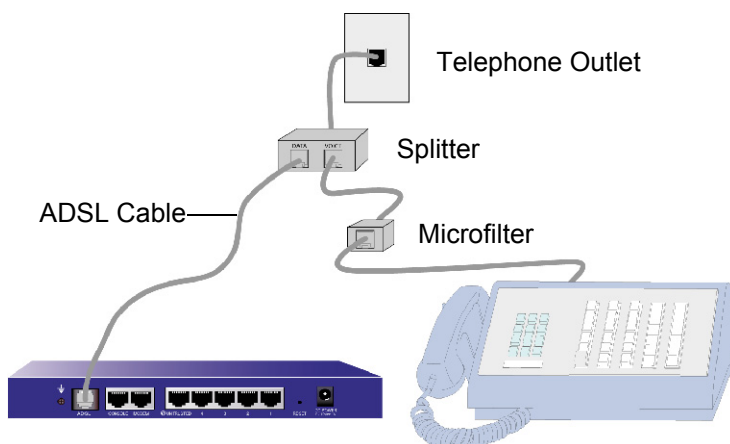
Connecting Splitters and Microfilters

A *signal splitter* divides the telephone signal into low-frequency voice signals for voice calls and high-frequency data signals for data traffic. Your service provider usually installs the splitter as part of the equipment that connects your site telephone lines to the provider network.

There are also splitters that you may be able to install yourself, depending upon your service provider equipment. If you are installing such a splitter yourself, connect the ADSL cable from the NetScreen device and the telephone line to the appropriate connectors (for example, “data” or “voice”) on the splitter. You connect the other end of the splitter to the telephone outlet.

You may need to install a *microfilter* on each telephone, fax machine, answering machine, or analog modem that connects to the ADSL line. The microfilter filters out high-frequency noise on the telephone line. You install the microfilter on the telephone line between the telephone, fax machine, answering machine, or analog modem and the voice connector on the splitter.

The following shows an example of a microfilter and a splitter that you install on your site. (You must obtain the appropriate microfilters or splitters from your service provider.)



Connecting the Untrusted Port

You can establish an Internet connection to an external router or a DSL, or cable modem and provide firewall and general security for your network. To establish a high-speed connection, connect the provided Ethernet cable from the Untrusted interface on the NetScreen-5GT Wireless device to the external router or modem. The NetScreen-5GT Wireless device autosenses the correct speed, duplex, and polarity settings.

If you are using the NetScreen-5GT Wireless ADSL device, refer to [“Connecting the ADSL Port” on page 7](#) and [“Connecting Splitters and Microfilters” on page 8](#) for ADSL connection instructions.

Connecting the Device to Your Internal Network or Workstations

You can connect your local area network (LAN) or workstation using one or both of the following methods:

- Connecting through one or more of the Trusted Ethernet ports on the NetScreen device
- Using a wireless interface on the NetScreen device

Connecting Trusted Ethernet Ports

The NetScreen-5GT Wireless device contains four Trust Ethernet ports. You can use one or more of these ports to connect to LANs via switches or hubs. You can also connect one or all of the ports directly to workstations, eliminating the need for a hub or switch. You can use either cross-over or straight-through cables to connect the Ethernet ports to other devices.

Using the Wireless Interface

If you are using the wireless interface, you need to connect the provided antennae on the device. If you have the standard 2dB omnidirectional antennae, then screw them onto the posts marked A and B at the back of the device, please refer to [“Port and Power Connectors” on page 31](#). Bend the antennae at their elbows, making sure not to put pressure on the bulkhead connector.

CONNECTING THE POWER

To connect the power to the NetScreen-5GT Wireless device:

1. Plug the DC connector end of the power cable into the DC power receptacle on the back of the device.
2. Plug the AC adapter end of the power cable into an AC power source.

Warning: We recommend using a surge protector for the power connection.

RACK MOUNTING (OPTIONAL)

With a NetScreen-5GT Wireless rack-mount kit, you can mount one or two NetScreen-5GT Wireless devices in a standard 19-inch equipment rack. The NetScreen-5GT Wireless rack-mount kit includes installation instructions and a rack-mounting tray. The dimensions of the tray are as follows:

Width:	48.26 cm.	19 in.
Height:	4.013 cm.	1-5/8 in. (1 rack unit)
Depth:	33.655 cm.	13-1/4 in.

In addition to the NetScreen-5GT Wireless device(s), rack-mount kit, and equipment rack, you will need the following:

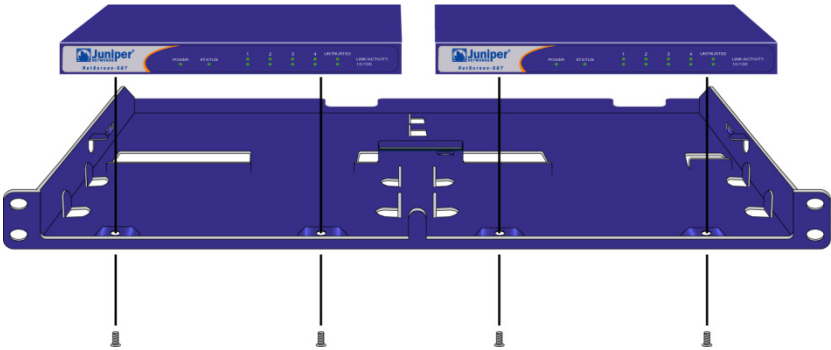
- Phillips-head screwdriver
- Four screws that match the thread size of the equipment rack

To mount the device in a rack:

1. Use the Phillips-head screwdriver to remove the two screws from the underside of each NetScreen-5GT Wireless device that you intend to mount. (Keep the screws for use in the next step.) The screws are located on the underside of the device near the front panel.



2. Insert each device on the rack-mount tray and attach it to the tray with the screws that you removed in step 1.



- 3. Attach the left and right tray plates to the equipment rack using the remaining screws.



You can run power cords and Ethernet cables through the openings in the floor of the tray or out the depressions in the back wall. You can also use the space behind the devices to hold power supplies.

Configuring the Device

This chapter describes how to configure a NetScreen-5GT Wireless device after you have connected it to your network. If you are accessing the device for the first time using the ScreenOS WebUI graphical interface, then you can use the Initial Configuration Wizard to guide you through the basic configuration. To use this wizard, refer to the *Juniper Networks NetScreen-5GT Wireless Getting Started Guide* or the *Juniper Networks NetScreen-5GT Wireless ADSL Getting Started Guide*.

Topics explained in this chapter include:

- [Accessing the Device](#)
- [Required Configuration](#)
- [Wireless Configuration](#)
- [ADSL Configuration](#)
- [Optional Configuration](#)
- [Verifying External Connectivity](#)
- [Resetting the Device to Factory Defaults](#)

Note: After you configure the NetScreen device and verify connectivity to the Internet, you must register your product at www.juniper.net/support/ so that certain ScreenOS services, such as internal antivirus or Deep Inspection Signature Service, can be activated on the device. After registering your product, use the WebUI to obtain the subscription for the service. For more information about registering your product and obtaining subscriptions for specific services, see the “System Parameters” chapter in the “Fundamentals” volume of the NetScreen Concepts & Examples ScreenOS Reference Guide for ScreenOS 5.0.0.

ACCESSING THE DEVICE

This section describes how to access your NetScreen device using the WebUI, Telnet, or a Console connection.

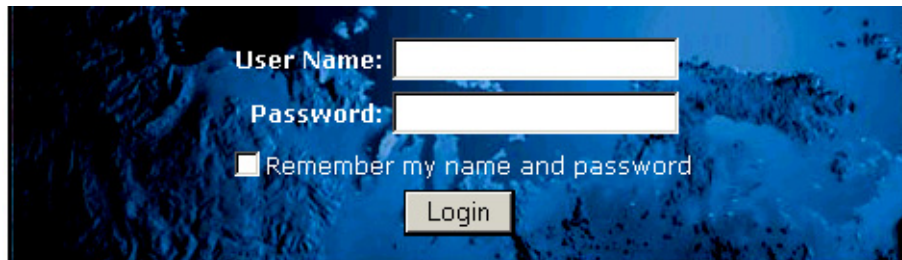
Using the WebUI

The ScreenOS WebUI is a graphical interface that is available through a web browser. To use the WebUI, you must be on the same subnetwork as the Trust or wireless2 interface. To access the NetScreen-5GT Wireless device with the WebUI management application:

1. Launch your browser, enter the IP address for the Trust or wireless2 interface in the URL field, and press Enter. For example, enter the following in the URL field:

192.168.1.1

The NetScreen WebUI software displays the login prompt.



***Note:** If you choose to skip the Initial Configuration Wizard, the WebUI login prompt automatically appears.*

2. If you have not yet changed the default user name and password, enter **netscreen** in both the **User Name** and **Password** fields and click **Login**. (Use lowercase letters only. The User Name and Password fields are both case-sensitive.)

Using Telnet

Telnet is an application that allows you to access devices through an Internet Protocol (IP) network.

***Note:** You can also access NetScreen devices using Secure Shell (SSH) applications. For more information, refer to the “Administration” chapter in the “Administration” volume of the NetScreen Concepts & Examples ScreenOS Reference Guide for ScreenOS 5.0.0.*

To configure the device using Telnet, you enter ScreenOS Command Line Interface (CLI) commands in a Telnet session from your workstation.

1. Start a Telnet client application to the IP address for the Trust or wireless2 interface. For example, enter the following:

```
telnet 192.168.1.1
```
2. If you have not yet changed the default user name and password, enter **netscreen** at both the **login** and **password** prompts. (Use lowercase letters only. The login and password prompts are both case-sensitive.)

Using a Console Connection

The Console port on the NetScreen-5GT Wireless device allows you to access the device through a serial cable connected to your workstation or terminal. To configure the device using a console connection, you enter ScreenOS CLI commands on your terminal or in a terminal emulation program on your workstation.

Note: For the console connection, use a serial cable with a male RJ-45 connector on one end and female DB-9 connector on the other end. See [Appendix A, “Specifications”](#) for the connector pinouts for the serial cable.

To establish a console connection:

1. Plug the female DB-9 end of the serial cable into the serial port of your computer. (Be sure that the DB-9 connector is seated properly in the port.)
2. Plug the male RJ-45 end of the serial cable into the Console port of the NetScreen-5GT Wireless device. (Be sure that the RJ-45 connector is seated properly in the port.)
3. Launch a serial terminal emulation program. (A commonly used terminal program is Hilgreave HyperTerminal.) The required settings to launch a console session with your NetScreen-5GT Wireless device are as follows:
 - Baud Rate: 9600
 - Parity: No
 - Data Bits: 8
 - Stop Bit: 1
 - Flow Control: None
4. If you have not yet changed the default user name and password, enter **netscreen** in both the **login** and **password** prompts. (Use lowercase letters only. The login and password fields are both case-sensitive.)

REQUIRED CONFIGURATION

This section describes the configurations that you need to complete to use the device.

Note: If at any point you need to restore the device to its default settings, see [“Resetting the Device to Factory Defaults”](#) on page 29.

Changing the Admin Name and Password

Because all NetScreen products use the same default admin name and password (**netscreen**), it is highly advisable to change your admin name and password immediately. To change the administrator name and password from “netscreen” and “netscreen” to “darwin1” and “1240jes”:

WebUI

Configuration > Admin > Administrators > Edit (for the NetScreen administrator name): Enter the following, and click **OK**:

Administrator Name: darwin1

Old Password: netscreen

Note: Passwords do not display in the WebUI when you type them in.

New Password: 1240jes

Confirm New Password: 1240jes

CLI

```
set admin name darwin1
set admin password 1240jes
save
```

For information about creating different levels of administrators, see the “Administration” chapter in the “Administration” volume of the *NetScreen Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.0.0.

Setting the Date and Time

The time set on the NetScreen device affects events such as the setup of VPN tunnels and the timing of schedules. The easiest way to set the date and time on the NetScreen device is to synchronize the system clock on the NetScreen device with the clock on your computer. To do this in the WebUI:

1. Configuration > Date/Time: Click the **Sync Clock with Client** button.
A pop-up message prompts you to specify if you have enabled the daylight saving time (DTS) option on your computer clock.
2. Click **Yes** to synchronize the system clock and adjust it according to DTS or **No** to synchronize the system clock without adjusting it for DTS.

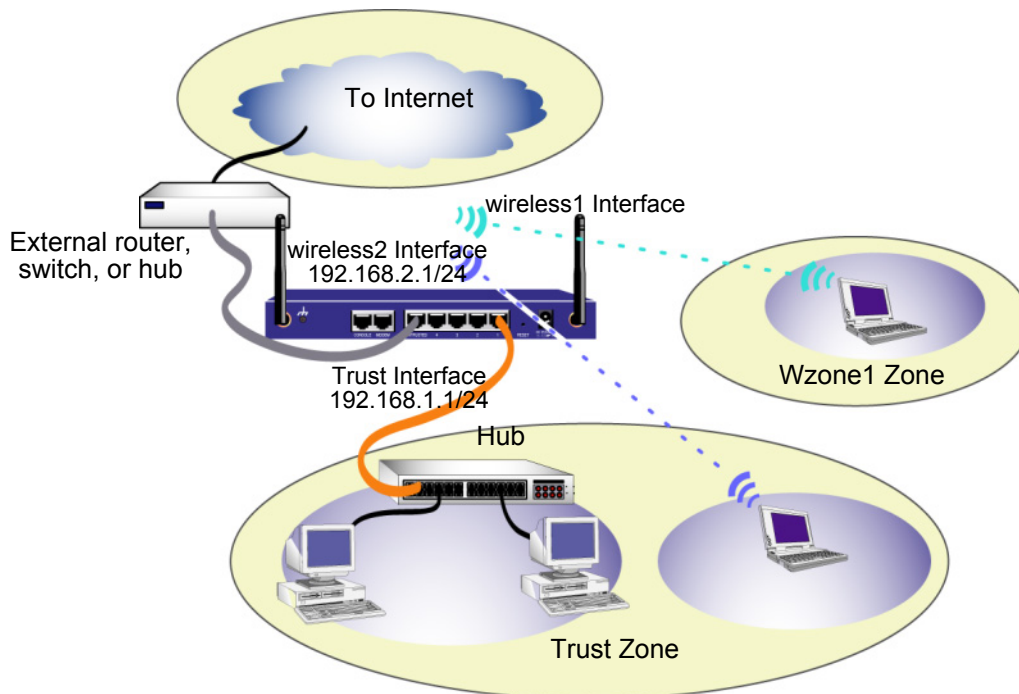
You can also use the CLI **set clock** command in a Telnet or Console session to manually set the date and time.

WIRELESS CONFIGURATION

This section provides information for configuring the wireless interface on the NetScreen device. Depending on the type of license you have installed, you can configure up to four wireless security zones on a NetScreen-5GT Wireless device. The interface to zone bindings are predefined and are dependent on the port mode you configure, and you cannot assign wireless interfaces to the Untrust zone. You must configure at least one wireless interface on the NetScreen device to create a wireless local area network (WLAN).

Note: If you are operating the NetScreen-5GT Wireless device in a country other than the United States or Japan, then you must use the `set wlan country-code` command before a WLAN connection can be established. This command sets the selectable channel range and transmit power level.

The figure below shows the default configuration for the NetScreen-5GT Wireless device.



The default wireless interface has the predefined name “wireless2”. The Trust and wireless2 interfaces are bound to the Trust zone and are configured with the subnetwork addresses 192.168.1.1/24 and 192.168.2.1/24, respectively. This means that all devices that you connect to in the Trust zone must be in the same subnetwork as either the Trust or wireless2 interface and have IP addresses in one of the two subnetworks. The NetScreen device is also configured to assign IP addresses for the 192.168.1.1/24 and 192.168.2.1/24 subnetworks to your devices. For more information, refer to [“Changing the Trust or Wireless2 Interface Address”](#) on page 29.

By default, the wireless1 interface is bound to the Wzone1 zone and does not have an IP address assigned to it. If you want to use the wireless1 interface, you must configure an IP address for it. Refer to the *NetScreen-5GT Wireless Reference Guide* for more information.

The NetScreen device allows any type of traffic to the Internet that originates from devices in your Trust zone, but it does not allow any traffic that originates in the Internet to reach your network. You can configure additional restrictions; refer to [“Configuring Additional Policies” on page 25](#).

Configuring the Wireless Network

Wireless networks consist of names referred to as Service Set Identifiers (SSIDs). Specifying an SSID allows you to have multiple wireless networks residing in the same location. You can have a maximum of eight SSIDs configured on each device. Once the SSID name is set, you can configure SSID attributes.

To set the SSID name **netscreen open**, allow wireless network connectivity, and activate the wireless2 interface:

WebUI

Wireless > SSID > New: Enter the following, and click **OK**:

SSID: “netscreen open”

Wireless Interface Binding: wireless2 (select)

Activate Changes > click the **Activate Changes** button

CLI

```
set ssid name "netscreen open"
set ssid "netscreen open" authentication open encryption
none
set ssid "netscreen open" interface wireless2
exec wlan reactivate
```

Once you have set an SSID to the wireless2 interface, you can access the device using the default wireless2 interface IP address in the steps provided with [“Accessing the Device” on page 13](#) to configure the device. Refer to the *NetScreen-5GT Wireless Reference Guide* for configuration examples, SSID attributes, and CLI commands relating to wireless security configurations.

ADSL CONFIGURATION

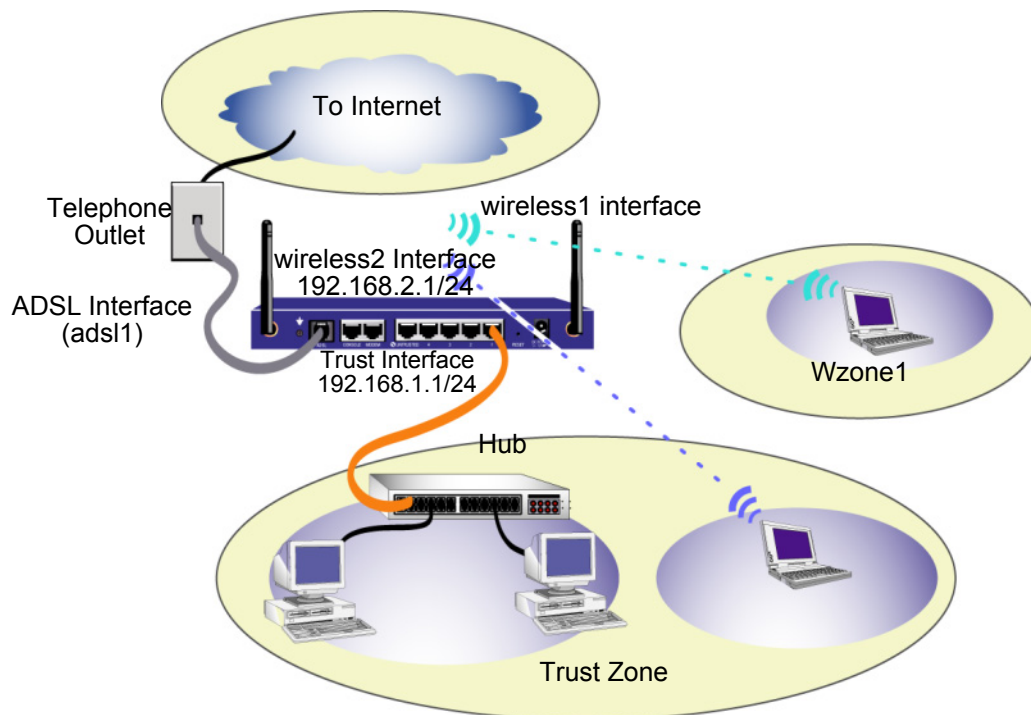
This section describes the default settings and operation of the NetScreen-5GT Wireless ADSL Annex A and B devices as they are shipped from the factory. These default settings are such that, in most cases, there are only a few items that you must configure.

This section describes the following configurations for the Untrust zone interface:

- [Configuring the ADSL Interface](#)
- [Adding Virtual Circuits to an ADSL Interface](#)
- [VPI/VCI and Multiplexing Method](#)
- [PPPoE or PPPoA](#)
- [Annex B Mode](#)
- [Static IP Address and Netmask](#)

Note: If at any point you need to restore the device to its default settings, see [“Resetting the Device to Factory Defaults”](#) on page 29.

The figure below shows the default configuration for the NetScreen-5GT Wireless ADSL device.



The ADSL interface has the predefined name “adsl1” and is the main connection from your network to the Internet. To allow the NetScreen device (and the devices on your network) to connect to the Internet, you must configure the adsl1 interface according to information obtained from your service provider. Refer to [“Configuring the ADSL Interface” on page 20](#).

The NetScreen device allows any type of traffic to the Internet that originates from devices in your Trust zone, but it does not allow any traffic that originates in the Internet to reach your network. You can configure additional restrictions; refer to [“Configuring Additional Policies” on page 25](#).

Configuring the ADSL Interface

Your network uses the ADSL interface “adsl1” on the NetScreen device to connect to the service provider’s network through an Asynchronous Transfer Mode (ATM) virtual circuit. You can configure additional virtual circuits by creating ADSL subinterfaces (for more information, see [“Adding Virtual Circuits to an ADSL Interface” on page 21](#)).

In the WebUI, navigate to the Network > Interfaces page to see a list of the current interfaces on the NetScreen device. If you are using a Telnet or Console session, enter the CLI command **get interface**. You should see that the adsl1 interface is bound to the Untrust zone. If you used the ICW to configure the device, there may be an IP address and netmask already assigned to the adsl1 interface.

***Note:** If you do not want to use the ADSL interface, you can bind it to the Null zone with the **set interface adsl1 zone null** command. If you use the ICW to configure the device, you can choose an interface other than the ADSL interface as the default interface to the Untrust zone.*

You must configure the adsl1 interface to enable the NetScreen device to connect to the service provider’s network. To do this, you must obtain the following information from your service provider:

- Virtual Path Identifier and Virtual Channel Identifier (VPI/VCI) values
- ATM Adaptation Layer 5 (AAL5) multiplexing method, which can be one of the following:
 - Virtual Circuit (VC)-based multiplexing, in which each protocol is carried over a separate ATM VC
 - Logical Link Control (LLC) encapsulation, which allows several protocols to be carried on the same ATM VC (the default multiplexing method)
- User name and password assigned by the service provider for connection to the service provider’s network using either the Point-to-Point Protocol over Ethernet (PPPoE) or Point-to-Point Protocol over ATM (PPPoA)
- Authentication method, if any, provided for the PPPoE or PPPoA connection
- Optionally, a static IP address and netmask value for your network

Adding Virtual Circuits to an ADSL Interface

To add virtual circuits, you create subinterfaces to the ADSL interface. You can create up to 10 ADSL subinterfaces. For example, to create a new subinterface named `adsl1.1` that is bound to the user-defined zone named “Corp1”:

WebUI

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

Interface Name: `adsl1.1`

VPI/VCI: `0/35`

Zone Name: Corp1 (select)

CLI

```
set interface adsl1.1 pvc 0 35 zone corp1
save
```

You need to configure an ADSL subinterface in the same way as the main ADSL interface, including setting the VPI/VCI values, as described in [“Configuring the ADSL Interface” on page 20](#). You configure an ADSL subinterface independently of the main ADSL interface; that is, you can configure a different multiplexing method, VPI/VCI, and PPP client on the subinterface than the main ADSL interface. You can also configure a static IP address on a subinterface, even if the main ADSL interface does not have a static IP address. Note that a subinterface and the main ADSL interface can use the same VPI/VCI values if one interface is configured for PPPoA and the other for PPPoE and they both use LLC multiplexing.

VPI/VCI and Multiplexing Method

Your service provider assigns a VPI/VCI pair for each VC connection. For example, you may receive the VPI/VCI pair 1/1, which means a VPI value of 1 and a VCI value of 1. These values must match the values that the service provider has configured on the subscriber’s side of the Digital Subscriber Line Access Multiplexer (DSLAM).

To configure the VPI/VCI pair 1/1 on the `adsl1` interface:

WebUI

Network > Interfaces > Edit (for the `adsl1` interface): Enter 1/1 in the VPI/VCI field, and then click **Apply**.

CLI

```
set interface adsl1 pvc 1 1
save
```

By default, the NetScreen-5GT Wireless ADSL device uses LLC-based multiplexing for each VC. To configure the VPI/VCI 1/1 on the `adsl1` interface and use LLC encapsulation on the VC:

WebUI

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

VPI/VCI: 1 / 2

Multiplexing Method: LLC (selected)

CLI

```
set interface adsl1 pvc 1 1 mux llc
save
```

PPPoE or PPPoA

The NetScreen device includes both PPPoE and PPPoA clients to connect to the service provider's network over the ADSL link. PPPoE is the most common form of ADSL encapsulation and is intended for termination on each host on your network. PPPoA is used primarily for business class service as PPP sessions can be terminated on the NetScreen device. To allow the NetScreen device to connect to the service provider's network, you need to configure the user name and password assigned by the service provider. The configuration for PPPoA is similar to the configuration for PPPoE.

Note: *The NetScreen device supports only one PPPoE session on each virtual circuit.*

To configure the user name "roswell" and password "area51" for PPPoE and bind the PPPoE configuration to the adsl1 interface:

WebUI

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

PPPoE Instance: poe1

Bound to Interface: adsl1 (select)

Username: roswell

Password: area51

CLI

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1
save
```

There are other PPPoE or PPPoA parameters that you can configure on the NetScreen device, including method of authentication (by default, the NetScreen device supports either Challenge Handshake Authentication Protocol or Password Authentication Protocol), idle timeout (default is 30 minutes), and so on. Ask your service provider if there are additional PPPoE or PPPoA parameters that you need to configure to enable proper communications with the service provider's server.

Annex B Mode

If you connect the Annex B model of the NetScreen-5GT Wireless ADSL device to a Deutsch Telecom ADSL line, then you must configure the physical interface on the ADSL port for operation with this equipment. To do this:

WebUI

Network > Interfaces > Edit (for the adsl1 interface): Select **DT** for the Annex B Mode, and click **Apply**.

CLI

```
set interface adsl1 phy annex-b-mode dt
save
```

You do not need to configure this setting if you are using the Annex A model of the device or if you are connecting the device to non-Deutsch Telecom equipment.

Static IP Address and Netmask

If your ISP gave you a specific, fixed IP address and netmask for your network, then configure the IP address and netmask for the network and the IP address of the router port connected to the NetScreen device. You need to also specify that the device is to use the static IP address. (By default, the NetScreen device acts as a PPPoE or PPPoA client and receives an IP address for the ADSL interface through negotiations with the PPPoE or PPPoA server.)

To configure the static IP address 1.1.1.1/24 for the network:

WebUI

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

IP Address/Netmask: 1.1.1.1/24

Static IP: (select)

Note: You need to configure a PPPoE or PPPoA instance and bind it to the adsl1 interface, as described in the previous section. Make sure that you select “Obtain IP using PPPoE” or “Obtain IP using PPPoA” and the name of the PPPoE or PPPoA instance.

CLI

```
set interface adsl1 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

or

```
set interface adsl1 ip 1.1.1.1/24
set pppoa name poa1 static-ip
save
```

To use Domain Name System (DNS) for domain name and address resolution, the computers in your network need to have the IP address of at least one DNS server. If the NetScreen device receives an IP address for the ADSL interface through PPPoE or PPPoA, then it also automatically receives IP addresses for the DNS server(s). If the computers in your network obtain their IP addresses from the DHCP server on the NetScreen device, then the computers also obtain these DNS server address(es).

If you assign a static IP address to the ADSL interface, then the service provider must give you the IP address(es) of the DNS server(s). You can either configure the DNS server address on each computer in your network or configure the DHCP server on the Trust zone interface so that it provides the DNS server address to each computer.

To configure the DHCP server on the Trust interface to provide the DNS server address 1.1.1.152 to computers in your network:

WebUI

Network > DHCP > Edit (for the Trust interface) > DHCP Server: Enter 1.1.1.152 for DNS1, and click **Apply**.

CLI

```
set interface trust dhcp server option dns1 1.1.1.152
save
```

OPTIONAL CONFIGURATION

This section describes the following features on the NetScreen-5GT Wireless devices that you may want to configure:

- [Restricting Management](#)
- [Configuring Additional Policies](#)
- [Operational Mode](#)
- [Changing the Port Mode](#)
- [Configuring a Backup Untrust Zone Interface](#)
- [Changing the Trust or Wireless2 Interface Address](#)

Note: *Not all of the optional configurations are described in detail in this manual. For more information, refer to the appropriate chapters in the NetScreen Concepts & Examples ScreenOS Reference Guide for ScreenOS 5.0.0.*

Restricting Management

By default, anyone in your network can manage the NetScreen device if they know the login and password. You can configure the NetScreen device to be managed only from one or more specific hosts on your network. (You can choose which services — for example, WebUI, Telnet, ping — you want enabled on the NetScreen device.)

For more information, refer to the “Administration” chapter in the “Administration” volume of the *NetScreen Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.0.0.

Configuring Additional Policies

The NetScreen-5GT Wireless devices are configured with a default policy that permits workstations in the Trust zone of your network to access any kind of service with outside computers, while outside computers are not allowed to access or start sessions with your workstations. You can configure policies that direct the NetScreen device to permit outside computers to start specific kinds of sessions with your computers. To create or modify policies, refer to the “Policies” chapter in the “Fundamentals” volume of the *NetScreen Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.0.0.

Operational Mode

The *operational mode* is the way an interface on a NetScreen device processes traffic between zones. By default, the NetScreen-5GT Wireless devices operates in Route mode with Network Address Translation (NAT) enabled on the Trust interface. This means that when devices in the Trust zone send traffic to the Internet, the NetScreen device replaces the original source IP addresses with the IP address of the Untrust interface. While the NetScreen device assigns private IP addresses to the devices in your network, these addresses remain hidden to computers outside your network.

If all devices in your network have public IP addresses, then you can configure the NetScreen device for Route mode without NAT enabled. In Route mode without NAT enabled, the NetScreen device routes traffic by checking IP addresses. For more information about configuring the device for Route mode without NAT enabled, refer to the “Interface Modes” chapter in the “Fundamentals” volume of the *NetScreen Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.0.0.

Changing the Port Mode

The *port mode* is the binding of physical ports, logical interfaces, and zones.

Warning: *Changing the port mode removes any existing configurations on the NetScreen device. Therefore, you should change the port mode before you configure the device.*

The following table summarizes the port, interface, and zone bindings for the port modes that are available on the NetScreen-5GT Wireless devices:

Port Name ^a	Trust-Untrust Port Mode ^b		Home-Work Port Mode		Trust/Untrust/DMZ (Extended) Mode		Dual Untrust Port Mode		Combined Port Mode	
	Interface	Zone	Interface	Zone	Interface	Zone	Interface	Zone	Interface	Zone
1	trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet1	Trust	ethernet1	Work
2	trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet1	Trust	ethernet2	Home
3	trust	Trust	ethernet2	Home	ethernet2	DMZ	ethernet1	Trust	ethernet2	Home
4	trust	Trust	ethernet2	Home	ethernet2	DMZ	ethernet2	Untrust	ethernet3	Untrust
Untrusted Modem ^c	untrust	Untrust	ethernet3	Untrust	ethernet3	Untrust	ethernet3	Untrust	untrust	Untrust
	serial	Null	serial	Null	serial	Null	serial	Null	serial	Null
	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1
	wireless2	Trust	wireless2	Work	wireless2	Trust	wireless2	Trust	wireless2	Work
			wireless3	Home	wireless3	DMZ			wireless3	Home
					wireless4	Wzone2				

- As labeled on the NetScreen appliance chassis.
- Default port mode.
- You can configure a backup interface to the Untrust zone using the Modem port. See [“Configuring a Backup Untrust Zone Interface”](#) on page 28.

The following table summarizes the port, interface, and zone bindings for the port modes that are available on the NetScreen-5GT Wireless ADSL devices:

Port Name ^a	Trust-Untrust Port Mode ^b		Home-Work Port Mode		Trust/Untrust/DMZ (Extended) Mode	
	Interface	Zone	Interface	Zone	Interface	Zone
1	trust	Trust	ethernet1	Work	ethernet1	Trust
2	trust	Trust	ethernet1	Work	ethernet1	Trust
3	trust	Trust	ethernet2	Home	ethernet2	DMZ
4	trust	Trust	ethernet2	Home	ethernet2	DMZ
Untrusted	untrust	Null ^c	ethernet3	Null ^c	ethernet3	Null ^c
Modem	serial	Null ^c	serial	Null ^c	serial	Null ^c
ADSL	adsl1	Untrust	adsl1	Untrust	adsl1	Untrust
	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1
	wireless2	Trust	wireless2	Work	wireless2	Trust
			wireless3	Home	wireless3	DMZ
				wireless4	Wzone2	

a. As labeled on the NetScreen appliance chassis.

b. Default port mode.

c. You can configure a backup interface to the Untrust zone, using either the Untrusted Ethernet port or the Modem port. See [“Configuring a Backup Untrust Zone Interface”](#) on page 28.

To change the NetScreen device to the Home-Work port mode:

WebUI

Configuration > 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?

CLI

```
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]? y
```

Configuring a Backup Untrust Zone Interface

By default, on NetScreen-5GT Wireless ADSL device, the `adsl1` interface is the primary connection to an outside network. Each port mode available on the NetScreen-5GT Wireless ADSL device allows you the option of connecting either the Untrusted Ethernet port or the Modem port as a backup connection to the outside network (see “[Changing the Port Mode](#)” on page 26). You must bind the backup interface to the Untrust zone and configure the interface appropriately.

Note: You can configure only one backup interface, using either the Untrusted Ethernet port or Modem port connection. If you use the Untrusted port for the backup connection, configure the Untrust interface in Trust-Untrust port mode or the `ethernet3` interface for other port modes. If you use the Modem port for the backup connection, configure the serial interface for all port modes.

For example, to bind the Untrust interface to the Untrust zone:

WebUI

Network > Interfaces > Edit (for the untrust interface): Select Untrust from the Zone Name drop-down list, and click **OK**.

CLI

```
set interface untrust zone untrust
save
```

You also need to set a static IP address for the Untrust interface or to specify whether the IP address for the interface is obtained via either DHCP or PPPoE. See the “Interfaces” chapter in the “Fundamentals” volume of the *NetScreen Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.0.0 for more information about configuring interface parameters.

When the `adsl1` interface and either the Ethernet interface (named `untrust` or `ethernet3`, depending upon the port mode) or the serial interface is bound to the Untrust zone, interface failover is automatically configured. That is, if the `adsl1` interface becomes unavailable, the NetScreen device automatically sends traffic to the backup interface. The device automatically sends traffic to the `adsl1` interface when the `adsl1` interface is again available.

Note: Only the `adsl1` interface is affected by failover. That is, if you have also configured ADSL subinterfaces, the subinterfaces do not fail over to the backup interface.

You can also manually force failover and failback on the `adsl1` interface. For more information, see the “Interface Redundancy” chapter in the “High Availability” volume of the *NetScreen Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.0.0.

Changing the Trust or Wireless2 Interface Address

You can change the IP address and netmask of the Trust and wireless interfaces if necessary. (Remember that when the Trust or wireless2 interface is in NAT mode, the IP addresses of devices in your network are never seen by computers outside your network; outside computers see only the IP address of the Untrust interface.) For example, you might need to change the Trust or wireless2 interface to match the IP addresses that already exist on your network. If you change the IP address and netmask of the Trust or wireless2 interface, then you also need to change either the range of addresses that the NetScreen device assigns via DHCP to devices in the network or disable the DHCP server on the Trust or wireless2 interfaces.

If the computers in your network obtain their IP addresses from the DHCP server on the NetScreen device, then the computers also obtain their default gateway from the NetScreen device. If a computer has a statically assigned IP address, then you must manually set its default gateway to the IP address of the Trust or wireless2 interface on the NetScreen device.

To assign a different IP address and netmask to the Trust or wireless2 interface, refer to the “Interfaces” chapter in the “Fundamentals” volume of the *NetScreen Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.0.0.

To change the DHCP settings for the NetScreen device, refer to the “System Parameters” chapter in the “Fundamentals” volume of the *NetScreen Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.0.0.

VERIFYING EXTERNAL CONNECTIVITY

To verify that workstations in your network can access resources on the Internet, start a Web browser from any workstation in the network and enter the following URL:
www.juniper.net.

RESETTING THE DEVICE TO FACTORY DEFAULTS

If you lose the admin password, you can reset the NetScreen device to its default settings. This destroys any existing configurations but restores access to the device.

Warning: *Resetting the device deletes all existing configuration settings and renders existing firewall and VPN service inoperative.*

You can restore the device to its default settings in one of the following ways:

- Using a Console connection. For further information, see the “Administration” chapter in the “Administration” volume of the *NetScreen Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.0.0.
- Using the reset pinhole on the rear panel of the device, as described in the next section.

Using the Reset Pinhole

You can reset the device and restore the factory default settings by pressing the reset pinhole. To perform this operation, you need to either view the device status LEDs on the front panel or start a Console session as described in [“Using a Console Connection” on page 15](#).

1. Locate the reset pinhole on the rear panel. Using a thin, firm wire (such as a paper clip), push the pinhole for four to six seconds and then release.



The Status LED blinks amber. A message on the Console states that erasure of the configuration has started and the system sends an SNMP/SYSLOG alert.

2. Wait for one to two seconds.

After the first reset, the Status LED blinks green; the device is now waiting for the second reset. The Console message now states that the device is waiting for a second confirmation.

3. Push the reset pinhole again for four to six seconds.

The Console message verifies the second confirmation. The Status LED lights amber for one-half second and then returns to the blinking green state.

The device then resets to its original factory settings. When the device resets, the Status LED turns amber for one-half second and then glows green. The Console displays device bootup messages. The system generates SNMP and SYSLOG alerts to configured SYSLOG or SNMP trap hosts.

After the device has rebooted, the Console displays the login prompt for the device. The status LED now blinks green.

If you do not follow the complete sequence, the reset process cancels without any configuration change and the console message states that the erasure of the configuration is aborted. The Status LED returns to blinking green. If the device did not reset, an SNMP alert is sent to confirm the failure.

Hardware Descriptions

This chapter provides detailed descriptions of the NetScreen-5GT Wireless chassis.

PORT AND POWER CONNECTORS

The rear panel of the NetScreen-5GT Wireless device contains port and power connectors.

Antenna B

Antenna A



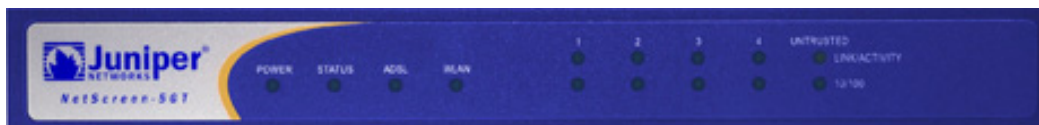
The DC power receptacle is for connecting power to the NetScreen-5GT Wireless device. The reset pinhole allows you to reset the device and restore its factory default settings. The NetScreen-5GT Wireless device includes the following ports:

Port	Description	Connector	Speed/Protocol
ADSL	When applicable, enables an Internet connection through an ADSL data link.	RJ-11 (Annex A) RJ-45 (Annex B)	ANSI T1.413 Issue 2 ITU G.992.1 (G.dmt) ITU 992.2 (G.lite)
Console	Enables a serial connection with the system. Used for launching Command Line Interface (CLI) sessions.	RJ-45	9600 bps/ RS-232
Modem	Enables a dial backup serial Internet connection through an external modem.	RJ-45	9600 bps-115 Kbps/ RS-232
Untrusted	Enables a primary or backup Internet or untrusted network connection through an external router or a DSL or cable modem.	RJ-45	10/100 Mbps/ Ethernet Autosensing duplex and polarity
Ports 1-4	Enables direct connections to workstations or a LAN connection through a switch or hub. This connection also allows you to manage the device through a Telnet session or the WebUI management application.	RJ-45	10/100 Mbps/ Ethernet Autosensing duplex and polarity
Antenna A & B	Enables direct connection to workstations in vicinity of a wireless radio connection. This connection allows you to manage the device through a Telnet session or the WebUI management application.	RPSMA	802.11b 802.11g

Warning: Do not connect a phone line or ISDN line directly to the Modem port on the NetScreen-5GT Wireless device. You must first connect the device to a modem, using an RS-232 port, and then connect the modem to the line.

STATUS LEDs

The front panel of the NetScreen-5GT Wireless device has power and status LEDs for the device and port status LEDs for the interfaces.



Main Status LEDs for the Device

The device status LEDs indicate whether the device is operating properly. The following table describes the status for each LED.

LED	Status	Meaning
POWER	green	Indicates the system is receiving power.
	off	Indicates the system is not receiving power.
STATUS	blinking green	Indicates the system is functioning.
	green	Indicates the system is starting up.
	red	Indicates a diagnostics or system initialization error.
	off	Indicates the system is not operational.
ADSL (on the Wireless ADSL only)	green	Indicates the ADSL loop is up.
	off	Indicates the ADSL loop is down.
WLAN	slow blinking green	Indicates that a Wireless connection is established but there is no link activity.
	fast blinking green	Indicates that a Wireless connection is established. The blink rate is proportional to the link activity.
	off	Indicates there is no Wireless connection established.

Port Status LEDs

The port status LEDs indicate whether the ports on the device are operating properly. The following table describes the possible status for the ports.

LED	LED Color	Meaning of the LED
Link/Activity	blinking green	Indicates the device detects Ethernet traffic for the port.
	off	Indicates the port has not established a link with another device.
	green	Indicates the port has established a link with another device.
10/100	green	Indicates the port is connected to a 100 Base-T device.
	off	Indicates the port is connected to a 10 Base-T device.



Specifications

This appendix provides general system specifications for the NetScreen-5GT Wireless device.

Attributes

Height	2.93 centimeters	1.15 inches
Depth	18.45 centimeters	7.26 inches
Width	20.8 centimeters	8.19 inches
Weight	.9 kilograms	1.98 pounds

Electrical

Switching Regulator	AC Adaptor: 100V-240VAC +/- 10% 50/60 Hz, 15-18 Watts DC Input: 12 Volts 1.25-1.5 Amps
---------------------	--

Environmental

Normal altitude	0°-40° C, 32-105°F
Relative humidity	10-90%
Non-condensing	10-90%

The maximum normal altitude is 2,000 meters (6,562 feet)

Certifications

Safety	UL, CUL, TUV, CE, CB
EMI	FCC Part 15 class B, VCCI, CE

Ethernet Connectors

Standard	100Base-TX
Media Type	Category 5 and higher Unshielded Twisted Pair (UTP) Cable
Maximum Distance	100 meters (328.08 feet)

The RJ-45 twisted-pair ports are compatible with the IEEE 802.3 Type 10/100 Base-T standard

ADSL Connector

Types	6-pin RJ-11 connector for Annex A RJ-45 connector for Annex B
Media Type	Standard telephone cable

CONSOLE AND MODEM ADAPTER CONNECTIONS

The following table lists the RJ-45 connector definitions. To employ a standard UART port, both the console and the modem ports use this configuration.

RJ-45	Signal	Abbreviation	DCE
1	Request To Send	RTS	In
2	Data Terminal Ready	DTR	In
3	Transmitted Data	TD	In
4, 5	Signal Ground	SGND	N/A
6	Received Data	RD	Out
7	Not Connected		
8	Clear To Send	CTS	Out

The table below lists the RJ-45 to DB-9 adapter connection definitions. To employ a standard UART port, both the console and the modem ports must use this configuration.

DB9	Signal	Abbreviation	DTE	DCE	RJ45
1	Data Carrier Detect	DCD	In	Out	NC
2	Received Data	RD	In	Out	3
3	Transmitted Data	TD	Out	In	6
4	Data Terminal Ready	DTR	Out	In	7
5	Signal Ground	SGND	N/A	N/A	4
6	Data Set Ready	DSR	In	Out	2
7	Request To Send	RTS	Out	In	8
8	Clear To Send	CTS	In	Out	1
9	Ring Indicator	RI	In	Out	NC

Note: If you use the Console cable that is provided with the NetScreen device to connect to a modem, you need to obtain and install a null modem adapter on the modem connector.

INDUSTRY CANADA STATEMENT

Operation is subject to the following two conditions:

1. this device may not cause interference and
2. this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 4 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding.

Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Juniper Networks declared that the 5GT-ADSL Wireless device is limited in CH1~11 from 2400 to 2483.5 MHz by specified firmware controlled in the USA.

Index

A

- AAL5 multiplexing [20](#)
- adding virtual circuit [21](#)
- address of Trust zone interface [29](#)
- admin name, changing [16](#)
- ADSL
 - configuring interface [20](#)
 - connecting the cable [7](#)
 - connecting the port [7](#)
- Annex A [7](#)
- Annex B [7](#)
 - configuring for Deutsch Telecom [23](#)
- antennae [9](#)
- ATM Adaptation Layer 5 [20](#)

B

- backup interface to Untrust zone [28](#)

C

- changing login name and password [16](#)
- changing the port mode [26](#)
- configuration
 - default settings [19](#)
 - optional [24](#)
 - required [15](#), [19](#)
 - SSID [18](#)
 - wireless network [17](#)
- connecting power [10](#)
- connectors
 - port [31](#)
 - power [31](#)
- Console, using [15](#)
- conventions [13](#)
 - CLI [4](#)
 - WebUI [4](#)

D

- date, setting [16](#)
- DB-9 connector [36](#)
- default settings [19](#)
 - restoring [29](#)

- Deutsch Telecom, configuring Annex B [23](#)

G

- Guide Organization [3](#)

L

- LEDs
 - port status [33](#)
 - status [32](#)

M

- managing device from specific host [25](#)
- microfilter [8](#)
- mounting device in rack [10](#)
- multiplexing, configuring [21](#)

N

- NetScreen Publications [5](#)

P

- password, changing [16](#)
- Point-to-Point Protocol over ATM
 - See* PPPoA
- Point-to-Point Protocol over Ethernet
 - See* PPPoE
- policies, configuring additional [25](#)
- port connectors [31](#)
- port mode, changing [26](#)
- port status LEDs [33](#)
- power connectors [31](#)
- power, connecting [10](#)
- PPPoA [20](#)
 - configuring [22](#)
- PPPoE [20](#)
 - configuring [22](#)

R

- rack mounting the device [10](#)
- registering the device [13](#)
- reset pinhole, using [30](#)

restoring default settings [29](#)
restricting management from specific host [25](#)
RJ-45 connector [36](#)
Route mode [25](#)

S

Service Set Identifier
 See SSID
setting device clock [16](#)
signal splitter [8](#)
SSID, Service Set Identifier [18](#)
static IP address [20](#)
 configuring [23](#)
status LEDs [32](#)

T

time, setting [16](#)
Transparent mode [25](#)
Trust Ethernet Ports [9](#)

U

Untrust zone, configuring backup interface [28](#)
Untrusted port [9](#)

V

verifying connectivity [29](#)
virtual circuit, adding [21](#)
Virtual Path Identifier/Virtual Channel Identifier
 See VPI/VCI
VPI/VCI [20](#)
 configuring [21](#)

W

WebUI
 accessing [13](#)
WebUI, conventions [4](#)
Wireless
 antennae [9](#)
 configuration [17](#)
 connecting [7, 9](#)
 Trust zone [17](#)
 using the default interface [9](#)
 Wzone1 zone [18](#)
wireless1 interface [18](#)
wireless2 interface
 accessing [13](#)
 binding zones [17](#)
 changing interface address [29](#)
 setting SSID for [18](#)
 Trust zone [17](#)

Table des matières

Préface	43
Organisation	43
Conventions WebUI	44
Conventions CLI	44
Publications NetScreen	45
Chapitre 1 Connexion de l'appareil	47
Connexion de l'appareil NetScreen à vos réseaux	47
Connexion de l'appareil à un réseau non sécurisé	47
Connexion du port ADSL	47
Connexion du port Untrusted	49
Connexion de l'appareil à votre réseau interne ou à vos postes de travail ..	49
Connexion des ports Ethernet sécurisés	49
Utilisation de l'interface sans fil	49
Connexion d'une source d'alimentation	50
Montage en baie (facultatif)	50
Chapitre 2 Configuration de l'appareil	53
Accès à l'appareil	53
Utilisation de l'interface utilisateur Web (WebUI)	53
Utilisation de Telnet	54
Utilisation d'une connexion de console	55
Configuration requise	55
Modification du nom et du mot de passe d'administrateur	56
Réglage de la date et de l'heure	56
Configuration sans fil	57
Configuration du réseau sans fil	58
Configuration ADSL	59
Configuration de l'interface ADSL	60
Ajout de circuits virtuels à une interface ADSL	61
VPI/VCI et méthode de multiplexage	61
PPPoE ou PPPoA	62
Mode Annexe B	63
Adresse IP statique et masque de réseau	63
Configuration facultative	65
Restriction de la gestion	65
Configuration de règles de sécurité supplémentaires	65
Mode de fonctionnement	66
Modification du mode de port	67
Configuration d'une interface « de secours » de zone Untrust	69

Modification de l'adresse de l'interface sécurisée ou wireless2.....	70
Contrôle de la connectivité externe	71
Restauration des paramètres par défaut de l'appareil	71
Utilisation du trou d'épingle de réinitialisation	71
Chapitre 3 Description du matériel.....	73
Connecteurs de ports et d'alimentation	73
DEL d'état	74
Principales DEL d'état de l'appareil.....	75
DEL d'état des ports.....	75
Annexe A Spécifications	77
Index.....	81

Préface

L'appareil NetScreen-5GT sans fil de Juniper Networks fournit des services de réseau privé virtuel (VPN) et de pare-feu IPSec pour des succursales ou points de vente qui utilisent une interface sans fil intégrée 802.11b/g. L'appareil NetScreen-5GT sans fil utilise des technologies de pare-feu, de VPN, d'antivirus, Deep Inspection et de gestion du trafic identiques à celles des produits haut de gamme pour sites centraux de NetScreen.

Juniper Networks propose trois modèles d'appareils NetScreen-5GT sans fil :

- **NetScreen-5GT sans fil** : le modèle de base sans fil.
- **NetScreen-5GT ADSL A sans fil** : le modèle Annexe A de l'appareil sans fil prend en charge l'ADSL sur des lignes téléphoniques standard (STT).
- **NetScreen-5GT ADSL B sans fil** : le modèle Annexe B de l'appareil sans fil prend en charge l'ADSL sur les réseaux numériques à intégration de services (RNIS).

Tous ces modèles prennent en charge jusqu'à quatre zones de sécurité sans fil. Les deux modèles ADSL sont compatibles avec les normes ANSI T1.413 Issue 2, ITU G.992.1 (G.dmt) et ITU 992.2 (G.lite).

Chaque modèle prend en charge trois versions logicielles :

- La version « 10-user » accepte jusqu'à 10 utilisateurs.
- La version « Plus » accepte un nombre illimité d'utilisateurs.
- La version « Extended » propose des caractéristiques identiques à celles de la version Plus, agrémentées des fonctions supplémentaires suivantes : haute disponibilité (NSRP Lite), zone de sécurité DMZ et davantage de sessions et de tunnels.

ORGANISATION

Ce manuel comporte trois chapitres et une annexe.

Le [Chapitre 1, « Connexion de l'appareil »](#), décrit comment connecter l'appareil NetScreen-5GT sans fil à votre réseau, ainsi qu'à une source d'alimentation et à une antenne, et comment l'installer dans une baie.

Le [Chapitre 2, « Configuration de l'appareil »](#), décrit les paramètres par défaut et le fonctionnement de l'appareil NetScreen-5GT sans fil (ADSL), ainsi que la configuration requise pour utiliser cet appareil.

Le [Chapitre 3, « Description du matériel »](#), offre un aperçu des ports, des DEL et de l'alimentation électrique nécessaire pour l'appareil NetScreen-5GT sans fil.

L'[Annexe A, « Spécifications »](#), fournit la liste des spécifications physiques concernant l'appareil NetScreen-5GT sans fil.

CONVENTIONS WEBUI

Dans ce manuel, un chevron (>) indique la procédure de navigation au sein de l'interface utilisateur Web suivie en cliquant sur les options de menus et les liens.

Exemple : **Objects** (Objets) > **Addresses** (Adresses) > **List** (Liste) > **New** (Nouveau)

Pour accéder à la boîte de dialogue de configuration des nouvelles adresses :

1. Cliquez sur **Objects** (Objets) dans la colonne de menus.
L'option de menu **Objects** (Objets) se développe pour révéler un sous-ensemble d'options d'objets.
2. (Menu de type « mini-application »¹) Placez le pointeur de la souris sur l'option **Addresses** (Adresses).
(Menu de type « DHTML ») Cliquez sur **Addresses** (Adresses).
L'option **Addresses** (Adresses) se développe pour révéler un sous-ensemble d'options d'adresses.
3. Cliquez sur **List** (Liste).
Le tableau du carnet d'adresses s'affiche.
4. Cliquez sur le lien **New** (Nouveau) dans le coin supérieur droit.
La boîte de dialogue de configuration des nouvelles adresses s'affiche.

CONVENTIONS CLI

Les conventions adoptées pour présenter la syntaxe des commandes de l'interface de ligne de commande (CLI) sont les suivantes :

- Les informations présentées entre crochets [] sont facultatives.
- Les informations présentées entre accolades { } sont obligatoires.
- Si plusieurs choix sont possibles, ils sont séparés par un trait vertical (|). Par exemple :

```
set interface { ethernet1 | ethernet2 | ethernet3 }  
manage
```

signifie « définir les options de gestion pour l'interface ethernet1, ethernet2 ou ethernet3 ».

- Les variables sont en *italique*. Par exemple :

```
set admin user name1 password xyz
```

1. Vous pouvez choisir des menus de type « mini-application » ou DHTML en cliquant sur l'option **Toggle Menu** (Changer de menu), en bas de la colonne de menus.

Lorsqu'une commande CLI est insérée dans une phrase du corps du texte, elle apparaît en **gras** (à l'exception des variables qui sont systématiquement en *italique*). Par exemple : « Pour afficher le numéro de série d'un appareil NetScreen, utilisez la commande **get system**. »

***Remarque :** Lors de la saisie d'un mot-clé, vous pouvez ne saisir que ses premiers caractères, à condition qu'ils permettent d'identifier le mot de manière unique. Par exemple, pour entrer la commande **set admin user joe j12fmt54**, il vous suffit de saisir **set adm u joe j12fmt54**. Vous pouvez utiliser ce système de saisie rapide pour les commandes. Les commandes détaillées dans cette documentation sont cependant proposées dans leur version complète.*

PUBLICATIONS NETSCREEN

Pour obtenir de la documentation technique relative à un des produits Juniper Networks NetScreen, consultez le site Internet www.juniper.net/techpubs/.

Si vous souhaitez obtenir une assistance technique, ouvrez un dossier d'assistance à l'aide du lien Case Manager disponible sous <http://www.juniper.net/support/> ou contactez le 1-888-314-JTAC (aux États-Unis) ou le 1-408-745-9500 (hors États-Unis).

Si vous trouvez des informations erronées ou incomplètes dans cette documentation, merci de nous les signaler en nous envoyant un courrier électronique à l'adresse suivante :

techpubs-comments@juniper.net

Connexion de l'appareil

Ce chapitre décrit la procédure de connexion de l'appareil NetScreen-5GT sans fil à un réseau, ainsi qu'à une source d'alimentation et à une antenne. Si vous utilisez le kit de montage en baie optionnel pour le modèle NetScreen-5GT sans fil, reportez-vous aux instructions de montage correspondantes fournies à la fin de ce chapitre.

Remarque : pour connaître les instructions et consignes de sécurité, reportez-vous au manuel NetScreen Safety Guide. Ces instructions vous informent sur les situations susceptibles d'entraîner des lésions corporelles. Avant de travailler sur les équipements, renseignez-vous sur les risques présentés par les circuits électriques sur les pratiques standard de prévention des accidents.

CONNEXION DE L'APPAREIL NETSCREEN À VOS RÉSEAUX

Lorsqu'il est placé entre vos réseaux internes et le réseau non sécurisé, l'appareil NetScreen assure les fonctions de pare-feu et de sécurité générale pour vos réseaux. Cette section décrit les connexions physiques.

Connexion de l'appareil à un réseau non sécurisé

Selon le modèle de l'appareil NetScreen-5GT sans fil utilisé, vous pouvez la connecter au réseau non sécurisé en procédant de l'une des manières suivantes :

- Par l'intermédiaire d'une connexion ADSL à l'aide du port ADSL de l'appareil NetScreen
- Par l'intermédiaire d'une connexion Ethernet à l'aide du port Untrusted de l'appareil NetScreen

Connexion du port ADSL

Connectez le câble ADSL fourni au port ADSL de l'appareil NetScreen-5GT ADSL sans fil et à votre prise de téléphone. Le port ADSL de la version Annexe A de l'appareil utilise un connecteur RJ-11, tandis que la version Annexe B utilise un connecteur RJ-45. Dans le cas des modèles Annexe B, le câble devant être connecté au port ADSL et à la prise de téléphone est identique, par son aspect et son câblage, à un câble Ethernet 10 Base-T direct.

Avertissement : veillez à ne pas connecter par inadvertance les ports Console, Modem ou Ethernet de l'appareil NetScreen à la prise de téléphone.

Sur l'appareil NetScreen-5GT ADSL sans fil, la ligne ADSL constitue votre connexion *principale* à un réseau extérieur. Pour bénéficier d'une liaison de données « de secours » avec un réseau extérieur, vous pouvez soit connecter un câble Ethernet au port Untrusted de l'appareil NetScreen-5GT ADSL sans fil et à un routeur externe, à un modem DSL ou à un modem câble, soit connecter un câble série entre le port Modem de l'appareil et un modem externe.

Avertissement : vous ne pouvez pas connecter simultanément le port *Untrusted* et le port *Modem* de l'appareil à un réseau extérieur.

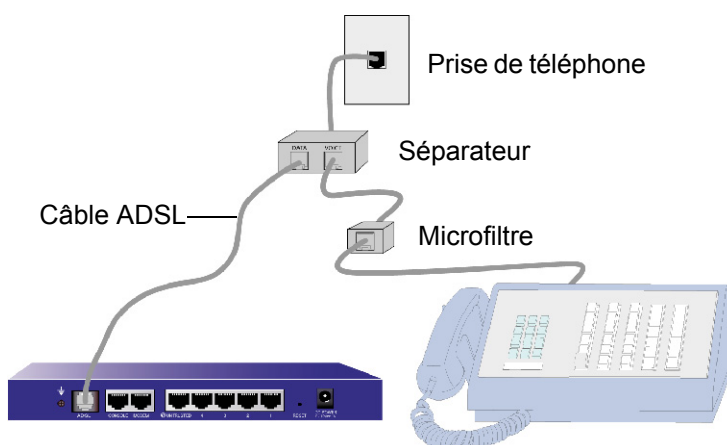
Connexion de séparateurs et de microfiltres

Un *séparateur de signaux* scinde le signal téléphonique en signaux vocaux à basse fréquence pour les communications vocales et en signaux de données à haute fréquence pour le trafic des données. Votre fournisseur d'accès installe généralement le séparateur en même temps que l'équipement permettant de raccorder les lignes téléphoniques de votre site au réseau de votre fournisseur.

Il existe également des séparateurs que vous pouvez installer vous-même, selon le matériel utilisé par votre fournisseur d'accès. Si vous installez vous-même un séparateur de ce type, connectez le câble ADSL aux connecteurs adéquats (par exemple, « données » ou « voix ») de l'appareil NetScreen et du séparateur. Connectez l'autre extrémité du séparateur à la prise de téléphone.

Vous devrez peut-être installer un *microfiltre* sur chaque téléphone, fax, répondeur ou modem analogique connecté à la ligne ADSL. Les microfiltres filtrent les parasites à haute fréquence sur la ligne téléphonique. Installez le microfiltre sur la ligne téléphonique reliant le téléphone, le fax, le répondeur ou le modem analogique au connecteur « voix » du séparateur.

L'illustration suivante représente un exemple d'installation de microfiltre et de séparateur sur votre site. (Vous devez vous procurer les microfiltres ou séparateurs adéquats auprès de votre fournisseur d'accès.)



Connexion du port Untrusted

Vous pouvez établir une connexion Internet avec un routeur externe, un modem DSL ou un modem câble, et fournir des fonctions de pare-feu et de sécurité générale à votre réseau. Pour établir une connexion à haut débit, connectez le câble Ethernet fourni à l'interface non sécurisée de l'appareil NetScreen-5GT sans fil d'une part, et au routeur externe ou modem d'autre part. L'appareil NetScreen-5GT sans fil détecte automatiquement les paramètres corrects de vitesse, de duplex et de polarité.

Si vous utilisez l'appareil NetScreen-5GT ADSL sans fil, reportez-vous aux sections « [Connexion du port ADSL](#) », page 47 et « [Connexion de séparateurs et de microfiltres](#) », page 48 pour obtenir des instructions de connexion ADSL.

Connexion de l'appareil à votre réseau interne ou à vos postes de travail

Vous pouvez connecter l'appareil à votre réseau local (LAN) ou à votre poste de travail en utilisant l'une ou les deux procédures suivantes :

- Par l'intermédiaire d'un ou plusieurs ports Ethernet sécurisés de l'appareil NetScreen
- À l'aide d'une interface sans fil sur l'appareil NetScreen

Connexion des ports Ethernet sécurisés

L'appareil NetScreen-5GT sans fil comporte quatre ports Ethernet sécurisés. Vous pouvez utiliser un ou plusieurs de ces ports pour connecter l'appareil à des réseaux locaux via des commutateurs ou des hubs. Vous pouvez également connecter directement l'un ou la totalité des ports aux postes de travail, et éliminer ainsi la nécessité d'utiliser un hub ou un commutateur. Pour connecter les ports Ethernet à d'autres appareils, vous pouvez utiliser des câbles de raccord croisés ou des câbles directs.

Utilisation de l'interface sans fil

Si vous utilisez l'interface sans fil, vous devez connecter les antennes fournies à l'appareil. Si vous disposez d'antennes omnidirectionnelles 2 dB standard, fixez-les sur les montants A et B à l'arrière de l'appareil à l'aide de vis (reportez-vous à la section « [Connecteurs de ports et d'alimentation](#) », page 73). Courbez les antennes au niveau des coudes, en veillant à ne pas appuyer sur le répartiteur de câblage.

CONNEXION D'UNE SOURCE D'ALIMENTATION

Pour relier l'appareil NetScreen-5GT sans fil à une source d'alimentation :

1. Insérez le connecteur CC situé à l'extrémité du câble d'alimentation dans la prise d'alimentation CC située à l'arrière de l'appareil.
2. Branchez l'adaptateur CA situé à l'autre extrémité du câble d'alimentation à une source d'alimentation CA.

Avertissement : *il est conseillé d'installer un parasurtenseur sur votre branchement électrique.*

MONTAGE EN BAIE (FACULTATIF)

Le kit de montage en baie pour le modèle NetScreen-5GT sans fil vous permet de monter un ou deux appareils NetScreen-5GT sans fil dans une baie de matériel standard de 19 pouces. Le kit de montage en baie pour NetScreen-5GT sans fil comprend des instructions d'installation et un plateau de montage en baie. Les dimensions du plateau sont les suivantes :

Largeur :	48,26 cm	19 po
Hauteur :	4,013 cm	1-5/8 po (1 appareil de baie)
Profondeur :	33,655 cm	13-1/4 po

Outre un ou plusieurs appareils NetScreen-5GT sans fil, du kit de montage en baie et de la baie de matériel, vous devez également disposer du matériel suivant :

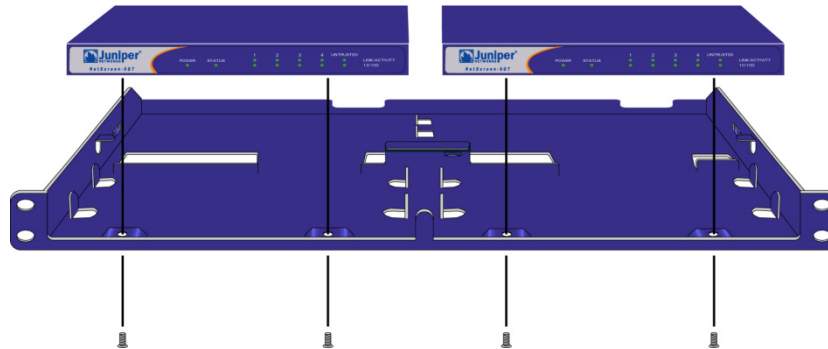
- Tournevis cruciforme
- Quatre vis dont le filetage correspond à celui de la baie de matériel

Pour monter l'appareil dans une baie :

1. Utilisez le tournevis cruciforme pour retirer les deux vis de la face inférieure de chaque appareil NetScreen-5GT sans fil que vous souhaitez monter dans la baie. (Conservez ces vis ; vous les utiliserez à l'étape suivante.) Les vis sont situées sur la face inférieure de l'appareil, près du panneau avant.



2. Positionnez chacun des appareils sur un plateau de montage en baie et fixez-les à ce plateau à l'aide des vis que vous avez retirées à l'étape 1.



3. Fixez les plaques gauche et droite des plateaux de montage sur la baie de matériel à l'aide des vis restantes.



Les ouvertures pratiquées dans le fond du plateau et les gouttières situées au niveau de la paroi arrière du plateau autorisent le passage des câbles d'alimentation et des câbles Ethernet. Vous pouvez également utiliser l'espace libre situé derrière les appareils pour stocker les blocs d'alimentation.

Configuration de l'appareil

Ce chapitre décrit la procédure de configuration d'un appareil NetScreen-5GT sans fil après sa connexion à votre réseau. Si vous accédez à l'appareil pour la première fois par l'intermédiaire de l'interface utilisateur graphique Web de ScreenOS (WebUI), l'Initial Configuration Wizard (Assistant de configuration initiale) vous guidera au fil du processus de configuration de base. Pour utiliser cet assistant, reportez-vous au manuel *Juniper Networks NetScreen-5GT Wireless Getting Started Guide* ou *Juniper Networks NetScreen-5GT Wireless ADSL Getting Started Guide*.

Les sujets abordés dans ce chapitre sont les suivants :

- [Accès à l'appareil](#)
- [Configuration requise](#)
- [Configuration sans fil](#)
- [Configuration ADSL](#)
- [Configuration facultative](#)
- [Contrôle de la connectivité externe](#)
- [Restauration des paramètres par défaut de l'appareil](#)

Remarque : après avoir configuré l'appareil NetScreen et vous être assuré du bon fonctionnement de votre connexion Internet, vous devez enregistrer votre produit sur le site www.juniper.net/support/ (site en anglais) afin que certains services ScreenOS, tels que l'antivirus interne ou le service de signatures Deep Inspection, puissent être activés sur l'appareil. Une fois votre produit enregistré, utilisez l'interface utilisateur Web pour obtenir un abonnement au service de votre choix. Pour plus d'informations sur l'enregistrement de votre produit et l'obtention d'abonnements à des services spécifiques, reportez-vous au chapitre « System Parameters » du volume « Fundamentals » du manuel NetScreen Concepts & Examples ScreenOS Reference Guide de ScreenOS 5.0.0.

ACCÈS À L'APPAREIL

Cette section décrit la procédure d'accès à l'appareil NetScreen à l'aide d'une connexion WebUI, Telnet ou de console.

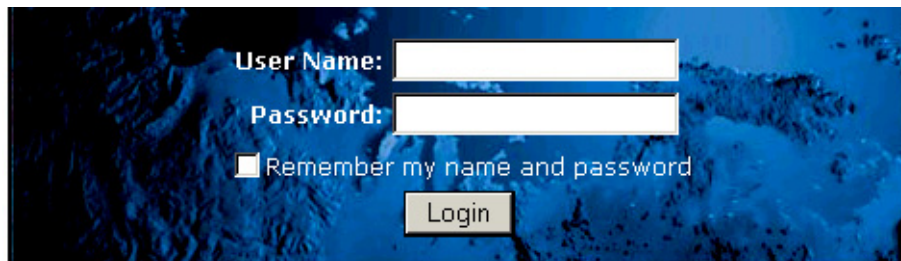
Utilisation de l'interface utilisateur Web (WebUI)

L'interface utilisateur Web de ScreenOS est une interface graphique accessible par l'intermédiaire d'un navigateur Web. Pour utiliser l'IU Web, vous devez être connecté au même sous-réseau que l'interface Trust ou wireless2. Pour accéder à l'appareil NetScreen-5GT sans fil par l'intermédiaire de l'application de gestion WebUI :

1. Lancez le navigateur, entrez l'adresse IP par défaut pour l'interface Trust dans le champ URL, puis appuyez sur Entrée. Par exemple, complétez le champ URL à l'aide des informations suivantes :

192.168.1.1

Le logiciel de l'interface utilisateur Web de NetScreen affiche l'invite de connexion.



***Remarque :** si vous choisissez de sauter l'Initial Configuration Wizard (Assistant de configuration initiale), l'invite de commande de connexion de l'interface utilisateur Web s'affiche automatiquement.*

2. Si vous n'avez pas encore modifié le nom d'utilisateur et mot de passe par défaut, saisissez **netscreen** dans les champs **User Name** (Nom d'utilisateur) et **Password** (Mot de passe), puis cliquez sur **Login** (Connexion). (N'utilisez que des lettres minuscules. Les champs User Name (Nom d'utilisateur) et Password (Mot de passe) sont tous les deux sensibles à la casse.)

Utilisation de Telnet

Telnet est une application qui vous permet d'accéder à des appareils par l'intermédiaire d'un réseau IP (Internet Protocol).

***Remarque :** vous pouvez également accéder aux appareils NetScreen à l'aide d'applications utilisant le protocole Secure Shell (SSH). Pour plus d'informations, reportez-vous au chapitre « Administration » du volume « Administration » du manuel NetScreen Concepts & Examples ScreenOS Reference Guide de ScreenOS 5.0.0.*

Pour configurer l'appareil à l'aide de Telnet, vous devez saisir des commandes CLI de ScreenOS dans une session Telnet depuis votre poste de travail.

1. Exécutez une application cliente Telnet sur l'adresse IP de l'interface sécurisée ou wireless2. Par exemple, saisissez les informations suivantes :

```
telnet 192.168.1.1
```

2. Si vous n'avez pas encore modifié le nom d'utilisateur et mot de passe par défaut, saisissez **netscreen** aux invites de connexion **Login** et de mot de passe **Password**. (N'utilisez que des lettres minuscules. Les invites de connexion et de mot de passe sont toutes deux sensibles à la casse.)

Utilisation d'une connexion de console

Le port Console de l'appareil NetScreen-5GT sans fil vous permet d'accéder à l'appareil par l'intermédiaire d'un câble série connecté à votre poste de travail ou terminal. Pour configurer l'appareil à l'aide d'une connexion de console, saisissez des commandes CLI de ScreenOS sur votre terminal ou dans un programme d'émulation de terminal exécuté sur votre poste de travail.

Remarque : pour établir une connexion de console, utilisez un câble série comportant un connecteur mâle RJ-45 à une extrémité et un connecteur femelle DB-9 à l'autre extrémité. Pour consulter les schémas de brochage des connecteurs du câble série, reportez-vous à l'Annexe A, *Spécifications*.

Pour établir une connexion de console :

1. Connectez l'extrémité femelle DB-9 du câble série au port série de votre ordinateur. (Assurez-vous que le connecteur DB-9 est correctement enfiché dans le port.)
2. Branchez l'autre extrémité du connecteur DB-9 sur le port DB-9 du connecteur RJ-45. (Assurez-vous que le connecteur DB-9 est correctement enfiché dans le port DB-9 du connecteur RJ-45.)
3. Connectez l'extrémité mâle RJ-45 du câble série au port Console de l'appareil NetScreen-5GT sans fil. (Assurez-vous que le connecteur RJ-45 est correctement enfiché dans le port.)
4. Démarrez un programme d'émulation de terminal série. (Hilgreave HyperTerminal est un programme de terminal fréquemment utilisé.) Les paramètres requis pour initier une session de console avec l'appareil NetScreen-5GT sans fil sont les suivants :
 - Baud Rate: 9600
 - Parity: No
 - Data Bits: 8
 - Stop Bit: 1
 - Flow Control: None
5. Si vous n'avez pas encore modifié les nom d'utilisateur et mot de passe par défaut, saisissez **netscreen** aux invites de connexion **Login** et de mot de passe **Password**. (N'utilisez que des lettres minuscules. Les champs de connexion et de mot de passe sont tous deux sensibles à la casse.)

CONFIGURATION REQUISE

Cette section décrit les configurations à respecter pour utiliser cet appareil.

Remarque : si vous devez à un moment ou à un autre rétablir les paramètres par défaut de l'appareil, reportez-vous à la section « *Restauration des paramètres par défaut de l'appareil* », page 71.

Modification du nom et du mot de passe d'administrateur

Étant donné que tous les produits NetScreen utilisent les mêmes nom d'administrateur et mot de passe (**netscreen**), nous vous recommandons vivement de les modifier immédiatement. Pour remplacer le nom et le mot de passe d'administrateur « netscreen » par « darwin1 » et « 1240jes » :

WebUI

Configuration > Admin > Administrators (Administrateurs) > Edit (Modifier)
(pour le nom d'administrateur Netscreen) : entrez les informations suivantes, puis cliquez sur **OK** :

Administrator Name (Nom d'administrateur) : darwin1

Old Password (Ancien mot de passe) : netscreen

***Remarque** : les mots de passe ne s'affichent pas sur l'interface utilisateur Web lors de la saisie.*

New Password (Nouveau mot de passe) : 1240jes

Confirm New Password (Confirmer le nouveau mot de passe) : 1240jes

CLI

```
set admin name darwin1
set admin password 1240jes
save
```

Pour plus d'informations sur la création de différents niveaux d'administrateurs, reportez-vous au chapitre « Administration » du volume « Administration » du manuel *NetScreen Concepts & Examples ScreenOS Reference Guide* de ScreenOS 5.0.0.

Réglage de la date et de l'heure

L'heure définie sur l'appareil NetScreen affecte les événements tels que la configuration des tunnels VPN et la planification des calendriers. La manière la plus simple de régler la date et l'heure sur l'appareil NetScreen consiste à synchroniser l'horloge système de l'appareil NetScreen avec l'horloge de votre ordinateur. Pour effectuer cette opération dans l'interface utilisateur Web :

1. Configuration > Date/Time (la date et l'heure) : Cliquez sur le bouton **Sync Clock with Client** (Synch. horloge avec client).

Un message s'affiche, vous invitant à préciser si l'option de passage à l'heure d'été a été activée sur l'horloge de votre ordinateur.

2. Cliquez sur **Yes** (Oui) pour synchroniser l'horloge système et la régler en tenant compte de l'heure d'été ou sur **No** (Non) pour synchroniser l'horloge système sans tenir compte de l'heure d'été.

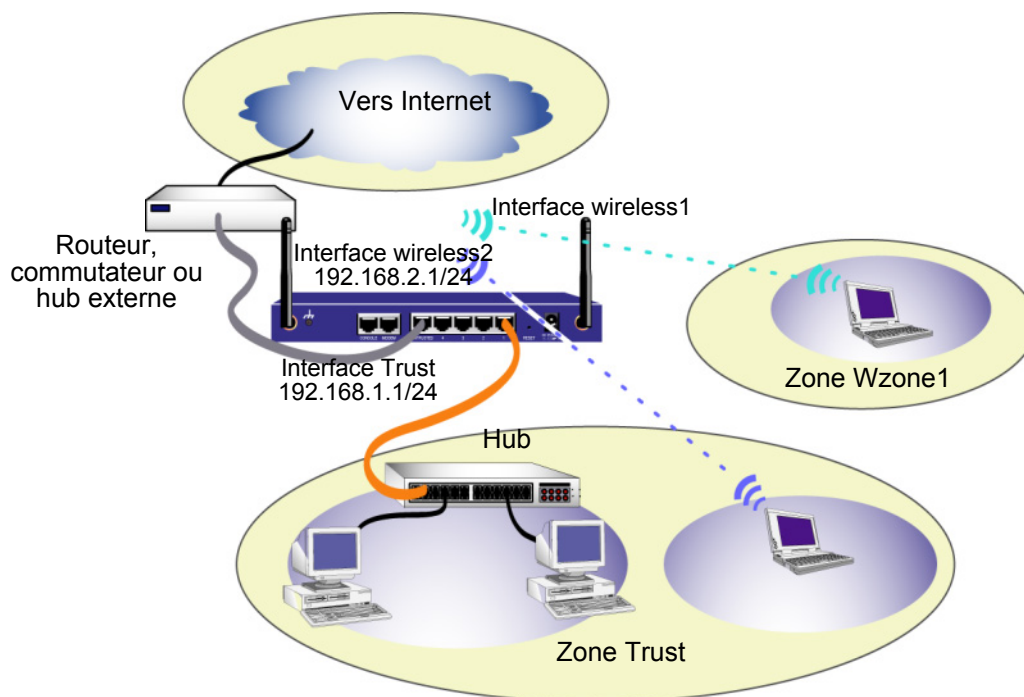
Vous pouvez également utiliser la commande CLI **set clock** dans une session Telnet ou de console afin de saisir manuellement la date et l'heure.

CONFIGURATION SANS FIL

Cette section fournit des informations pour la configuration de l'interface sans fil de l'appareil NetScreen. Selon le type de licence installée, vous pouvez configurer jusqu'à quatre zones de sécurité sans fil sur un appareil NetScreen-5GT sans fil. Les liaisons entre l'interface et les zones sont prédéfinies et dépendent du mode de port que vous configurez ; en outre, vous ne pouvez pas associer des interfaces sans fil à une zone Untrust. Pour créer un réseau local sans fil (WLAN), vous devez configurer au moins une interface sans fil sur l'appareil NetScreen.

Remarque : si vous utilisez l'appareil NetScreen-5GT sans fil dans un autre pays que les États-Unis ou le Japon, vous devez utiliser la commande **set wlan country-code** avant d'établir une connexion WLAN. Cette commande définit la plage de canaux disponibles et le niveau de puissance émise.

L'illustration suivante représente la configuration par défaut de l'appareil NetScreen-5GT sans fil.



L'interface sans fil par défaut porte le nom prédéfini « wireless2 ». Les interfaces sécurisées et wireless2 sont liées à la zone Trust ; elles sont respectivement configurées avec les adresses de sous-réseau 192.168.1.1/24 et 192.168.2.1/24. Cela signifie que tous les appareils que vous connectez dans la zone Trust doivent se trouver dans le même sous-réseau que l'interface sécurisée ou wireless2, et qu'ils doivent posséder une adresse IP

comprise dans l'un de ces deux sous-réseaux. L'appareil NetScreen est également configuré de manière à attribuer à vos appareils des adresses IP comprises dans les sous-réseaux 192.168.1.1/24 et 192.168.2.1/24. Pour plus d'informations, reportez-vous à la section « [Modification de l'adresse de l'interface sécurisée ou wireless2](#) », page 70.

Par défaut, l'interface wireless1 est liée à la zone Wzone1 et aucune adresse IP ne lui est assignée. Pour utiliser l'interface wireless1, vous devez configurer l'adresse IP correspondante. Pour plus d'informations, reportez-vous au manuel *NetScreen-5GT Wireless Reference Guide*.

L'appareil NetScreen autorise la transmission vers Internet de tous les types de trafic provenant de votre zone Trust, mais n'autorise pas le trafic provenant d'Internet sur votre réseau. Vous pouvez également configurer des restrictions supplémentaires ; reportez-vous à la section « [Configuration de règles de sécurité supplémentaires](#) », page 65.

Configuration du réseau sans fil

Les réseaux sans fil sont désignés par des noms SSID (Service Set Identifiers). La spécification d'un SSID vous permet d'avoir plusieurs réseaux sans fil résidant sur un même emplacement. Vous pouvez avoir un maximum de huit SSID configurés sur chaque appareil. Une fois le nom SSID défini, vous pouvez configurer les attributs SSID.

Pour définir le nom SSID **netscreen open**, autorisez une connexion réseau sans fil et activez l'interface wireless2 :

WebUI

Wireless (Sans fil) > SSID > New (Nouveau) : entrez les informations suivantes, puis cliquez sur **OK** :

SSID : « netscreen open »

Wireless Interface Binding (Liaison d'interface sans fil) : wireless2 (sélection)

Activate Changes > cliquez sur le bouton **Activate Changes** (Activer les modifications).

CLI

```
set ssid name "netscreen open"  
set ssid "netscreen open" authentication open encryption  
none  
set ssid "netscreen open" interface wireless2  
exec wlan reactivate
```

Une fois un SSID défini sur l'interface wireless2, vous pouvez accéder à l'appareil à l'aide de l'adresse IP de l'interface wireless2 par défaut (voir les étapes de la section « [Accès à l'appareil](#) », page 53 pour configurer l'appareil). Pour obtenir des exemples de configuration, ainsi que des informations sur les attributs SSID et les commandes CLI en relation avec les configurations de sécurité sans fil, reportez-vous au manuel *NetScreen-5GT Wireless Reference Guide*.

CONFIGURATION ADSL

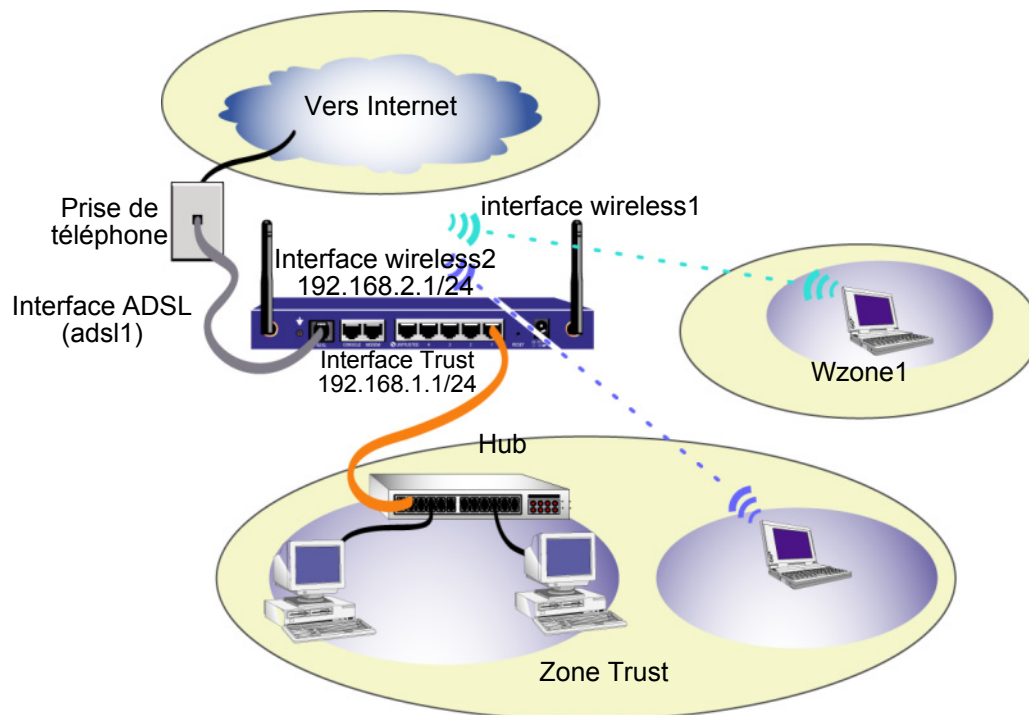
Cette section décrit les paramètres par défaut et le fonctionnement des appareils NetScreen-5GT ADSL sans fil Annexe A et B, tels qu'ils sont configurés à la sortie d'usine. Ces paramètres par défaut ont été définis de telle manière que, dans la plupart des cas, vous n'avez que quelques éléments à configurer.

Cette section décrit les configurations suivantes pour l'interface de zone Untrust :

- [Configuration de l'interface ADSL](#)
- [Ajout de circuits virtuels à une interface ADSL](#)
- [VPI/VCI et méthode de multiplexage](#)
- [PPPoE ou PPPoA](#)
- [Mode Annexe B](#)
- [Adresse IP statique et masque de réseau](#)

Remarque : si vous devez à un moment ou à un autre restaurer les paramètres par défaut de l'appareil, reportez-vous à la section « [Restauration des paramètres par défaut de l'appareil](#) », page 71.

L'illustration suivante représente la configuration par défaut de l'appareil NetScreen-5GT ADSL sans fil.



L'interface ADSL porte le nom prédéfini « `adsl1` » et constitue la connexion principale entre votre réseau et Internet. Pour permettre à l'appareil NetScreen (et aux appareils de votre réseau) de se connecter à Internet, vous devez configurer l'interface `adsl1` conformément aux informations obtenues auprès de votre fournisseur d'accès. Reportez-vous à la section « [Configuration de l'interface ADSL](#) », page 60.

L'appareil NetScreen permet la transmission vers Internet de tous les types de trafic provenant de votre zone Trust, mais n'autorise pas le trafic provenant d'Internet sur votre réseau. Vous pouvez également configurer des restrictions supplémentaires ; reportez-vous à la section « [Configuration de règles de sécurité supplémentaires](#) », page 65.

Configuration de l'interface ADSL

Votre réseau utilise l'interface ADSL « `adsl1` » de l'appareil NetScreen pour se connecter au réseau de votre fournisseur d'accès par l'intermédiaire d'un circuit virtuel configuré en mode de transfert asynchrone (ATM). Vous pouvez configurer des circuits virtuels supplémentaires en créant des sous-interfaces ADSL (pour plus d'informations, voir la section « [Ajout de circuits virtuels à une interface ADSL](#) », page 61).

Dans l'interface utilisateur Web, accédez à la page Network > Interfaces (Interfaces réseau) pour afficher une liste des interfaces actuellement définies sur l'appareil NetScreen. Si vous utilisez une session Telnet ou de console, entrez la commande CLI **get interface**. Vous devriez constater que l'interface `adsl1` est liée à la zone Untrust. Si vous avez utilisé l'Initial Configuration Wizard (Assistant de configuration initiale) pour configurer l'appareil, il est possible qu'une adresse IP et un masque de réseau soient déjà attribués à l'interface `adsl1`.

***Remarque :** si vous ne souhaitez pas utiliser l'interface ADSL, vous pouvez la lier à la zone Null (nulle) à l'aide de la commande **set interface adsl1 zone null**. Si vous utilisez l'Initial Configuration Wizard (Assistant de configuration initiale) pour configurer l'appareil, vous pouvez choisir d'utiliser une autre interface que l'interface ADSL en tant qu'interface par défaut de la zone Untrust.*

Vous devez configurer l'interface `adsl1` afin de permettre à l'appareil NetScreen de se connecter au réseau de votre fournisseur d'accès. Pour cela, vous devez vous procurer les informations suivantes auprès de votre fournisseur d'accès :

- Les valeurs Virtual Path Identifier (Identificateur de trajet virtuel) et Virtual Channel Identifier (Identificateur de canal virtuel) (VPI/VCI)
- La méthode de multiplexage Couche d'adaptation 5 (AAL5) au mode de transfert asynchrone (ATM), qui peut être l'une des méthodes suivantes :
 - Le multiplexage utilisant un circuit virtuel (VC), dans lequel chaque protocole est transporté sur un circuit virtuel ATM distinct
 - L'encapsulation par commande de liaison logique (LLC), qui autorise le transport de plusieurs protocoles sur le même circuit virtuel ATM (méthode de multiplexage par défaut)

- Les nom d'utilisateur et mot de passe attribués par votre fournisseur d'accès pour vous connecter au réseau de votre fournisseur d'accès à l'aide des protocoles « Point-to-Point Protocol over Ethernet » (PPPoE) ou « Point-to-Point Protocol over ATM » (PPPoA)
- La méthode d'authentification fournie pour la connexion PPPoE ou PPPoA, le cas échéant
- En option, une adresse IP statique et une valeur de masque de réseau pour votre réseau

Ajout de circuits virtuels à une interface ADSL

Pour ajouter des circuits virtuels, vous devez créer des sous-interfaces avec l'interface ADSL. Vous pouvez créer jusqu'à dix sous-interfaces ADSL. Par exemple, pour créer une nouvelle sous-interface adsl1.1 liée à la zone définie par l'utilisateur intitulée « Corp1 » :

WebUI

Network (Réseau) > Interfaces > New ADSL Sub-IF (Nouvelle sous-IF ADSL) :
entrez les informations suivantes, puis cliquez sur **Apply** (Appliquer) :

Interface Name (Nom de l'interface) : adsl1.1

VPI/VCI : 0/35

Zone Name (Nom de la zone) : Corp1 (sélection)

CLI

```
set interface adsl1.1 pvc 0 35 zone corp1
save
```

Vous devez configurer une sous-interface ADSL de la même manière que l'interface ADSL principale, en définissant notamment les valeurs VPI/VCI comme décrit à la section « Configuration de l'interface ADSL », page 60. La configuration d'une sous-interface ADSL s'effectue indépendamment de l'interface ADSL principale ; cela signifie que vous pouvez configurer, pour la sous-interface, une méthode de multiplexage, des valeurs VPI/VCI et un client PPP différents de ceux de l'interface ADSL principale. Vous pouvez également configurer une adresse IP statique sur une sous-interface, même si l'interface ADSL principale ne comporte pas d'adresse IP statique. Notez qu'une sous-interface peut utiliser les mêmes valeurs VPI/VCI que l'interface ADSL principale si l'une des interfaces est configurée pour le protocole PPPoA et l'autre pour le protocole PPPoE, et si toutes deux utilisent le multiplexage LLC.

VPI/VCI et méthode de multiplexage

Votre fournisseur d'accès attribue une paire VPI/VCI pour chaque connexion à un circuit virtuel. Vous pouvez, par exemple, recevoir la paire VPI/VCI 1/1, qui signifie une valeur de VPI de 1 et une valeur de VCI de 1. Ces valeurs doivent correspondre aux valeurs configurées par votre fournisseur d'accès du côté abonné du multiplexeur d'accès de lignes numériques d'abonnés (DSLAM).

Pour configurer la paire VPI/VCI 1/1 sur l'interface adsl1 :

WebUI

Network (Réseau) > Interfaces > Edit (Modifier) (pour l'interface adsl1) : Entrez 1/1 dans le champ VPI/VCI, puis cliquez sur **Apply** (Appliquer).

CLI

```
set interface adsl1 pvc 1 1
save
```

Par défaut, l'appareil NetScreen-5GT ADSL sans fil utilise le multiplexage LLC pour chaque circuit virtuel. Pour configurer la paire VPI/VCI 1/1 sur l'interface adsl1 et utiliser l'encapsulation LLC sur le circuit virtuel :

WebUI

Network (Réseau) > Interfaces > Edit (Modifier) (pour l'interface adsl1) : entrez les informations suivantes, puis cliquez sur **Apply** (Appliquer) :

VPI/VCI : 1 / 2

Multiplexing Method (Méthode de multiplexage) : LLC (sélectionné)

CLI

```
set interface adsl1 pvc 1 1 mux llc
save
```

PPPoE ou PPPoA

L'appareil NetScreen inclut à la fois des clients PPPoE et PPPoA pour se connecter au réseau du fournisseur d'accès par l'intermédiaire de la liaison ADSL. Le protocole PPPoE est la forme d'encapsulation ADSL la plus répandue, et il est conçu pour se terminer au niveau de chaque hôte connecté à votre réseau. Le protocole PPPoA est principalement utilisé pour le service de classe entreprise, car les sessions PPP peuvent se terminer au niveau de l'appareil NetScreen. Pour permettre à l'appareil NetScreen de se connecter au réseau de votre fournisseur d'accès, vous devez configurer le nom d'utilisateur et le mot de passe qui vous ont été attribués par votre fournisseur d'accès. La configuration pour le protocole PPPoA est semblable à celle du protocole PPPoE.

Remarque : *l'appareil NetScreen n'accepte qu'une seule session PPPoE sur chaque circuit virtuel.*

Pour configurer le nom d'utilisateur « roswell » et le mot de passe « area51 » pour le protocole PPPoE et lier la configuration PPPoE à l'interface adsl1 :

WebUI

Network (Réseau) > PPPoE > New (Nouveau) : entrez les informations suivantes, puis cliquez sur **OK** :

PPPoE Instance (Instance PPPoE) : poe1

Bound to Interface (Lier à l'interface) : adsl1 (sélection)

Username (Nom d'utilisateur) : roswell

Password (Mot de passe) : area51

CLI

```
set pppoe name poel username roswell password area51
set pppoe name poel interface adsl1
save
```

Il existe d'autres paramètres PPPoE ou PPPoA pouvant être configurés au niveau de l'appareil NetScreen, tels que la méthode d'authentification (par défaut, l'appareil NetScreen accepte aussi bien les protocoles Challenge Handshake Authentication Protocol (CHAP) que Password Authentication Protocol (PAP)), le délai d'inactivité avant déconnexion (la valeur par défaut est de 30 minutes), etc. Demandez à votre fournisseur d'accès si des paramètres PPPoE ou PPPoA supplémentaires doivent être configurés afin de permettre à l'appareil de communiquer correctement avec le serveur du fournisseur d'accès.

Mode Annexe B

Si vous connectez le modèle Annexe B de l'appareil NetScreen-5GT ADSL sans fil à une ligne ADSL de Deutsch Telecom, vous devez configurer l'interface physique au niveau du port ADSL afin qu'elle fonctionne avec ce matériel. Pour ce faire :

WebUI

Network (Réseau) > Interfaces > Edit (Modifier) (pour l'interface adsl1) : sélectionnez **DT** pour le paramètre Annex B Mode (Mode Annexe B), puis cliquez sur **Apply** (Appliquer).

CLI

```
set interface adsl1 phy annex-b-mode dt
save
```

Il n'est pas nécessaire de configurer ce paramètre si vous utilisez le modèle Annexe A de l'appareil ou si vous connectez l'appareil à un équipement ne provenant pas de Deutsch Telecom.

Adresse IP statique et masque de réseau

Si votre FAI vous a fourni une adresse IP fixe et un masque de réseau propres à votre réseau, configurez l'adresse IP et le masque de réseau en fonction du réseau et de l'adresse IP du port de routeur connecté à l'appareil NetScreen. Vous devez également spécifier que l'appareil utilisera l'adresse IP statique. (Par défaut, l'appareil NetScreen se comporte en tant que client PPPoE ou PPPoA et reçoit une adresse IP pour l'interface ADSL par l'intermédiaire de négociations avec le serveur PPPoE ou PPPoA.)

Pour configurer l'adresse IP statique 1.1.1.1/24 pour le réseau :

WebUI

Network (Réseau) > Interfaces > Edit (Modifier) (pour l'interface adsl1) : entrez les informations suivantes, puis cliquez sur **Apply** (Appliquer) :

IP Address/Netmask (Adresse IP/Masque de réseau) : 1.1.1.1/24

Static IP (Adresse IP statique) : (sélection)

Remarque : vous devez configurer une instance PPPoE ou PPPoA et la lier à l'interface `adsl1`, comme décrit dans la section précédente. Vous devez sélectionner « Obtain IP using PPPoE » (Obtenir une adresse IP par PPPoE) ou « Obtain IP using PPPoA » (Obtenir une adresse IP par PPPoA), ainsi que le nom de l'instance PPPoE ou PPPoA concernée.

CLI

```
set interface adsl1 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

ou

```
set interface adsl1 ip 1.1.1.1/24
set pppoa name poa1 static-ip
save
```

Pour utiliser la méthode Domain Name System (DNS) afin de résoudre les noms et adresses de domaines, les ordinateurs connectés à votre réseau doivent disposer de l'adresse IP d'au moins un serveur DNS. Si l'appareil NetScreen reçoit une adresse IP pour l'interface ADSL par l'intermédiaire des protocoles PPPoE ou PPPoA, il reçoit également automatiquement les adresses IP du ou des serveurs DNS. Si les ordinateurs connectés à votre réseau obtiennent leurs adresses IP auprès du serveur DHCP sur l'appareil NetScreen, les ordinateurs obtiennent également ces adresses de serveurs DNS.

Si vous devez attribuer une adresse IP statique à l'interface ADSL, votre fournisseur d'accès doit vous fournir l'adresse (ou les adresses) IP du (ou des) serveur(s) DNS. Vous pouvez soit configurer l'adresse du serveur DNS sur chaque ordinateur connecté à votre réseau, soit configurer le serveur DHCP dans l'interface de zone Trust afin qu'il fournisse l'adresse du serveur DNS à chaque ordinateur.

Pour configurer le serveur DHCP dans l'interface sécurisée de façon à fournir l'adresse de serveur DNS 1.1.1.152 aux ordinateurs connectés à votre réseau :

WebUI

Network (Réseau) > DHCP > Edit (Modifier) (pour l'interface sécurisée) > DHCP Server (Serveur DHCP) : saisissez 1.1.1.152 dans le champ DNS1, puis cliquez sur **Apply** (Appliquer).

CLI

```
set interface trust dhcp server option dns1 1.1.1.152
save
```

CONFIGURATION FACULTATIVE

Cette section décrit les fonctions suivantes des appareils NetScreen-5GT sans fil que vous pouvez ou non choisir de configurer :

- [Restriction de la gestion](#)
- [Configuration de règles de sécurité supplémentaires](#)
- [Mode de fonctionnement](#)
- [Modification du mode de port](#)
- [Configuration d'une interface « de secours » de zone Untrust](#)
- [Modification de l'adresse de l'interface sécurisée ou wireless2](#)

Remarque : *les configurations facultatives ne sont pas toutes décrites de façon détaillée dans ce manuel. Pour plus d'informations, reportez-vous aux chapitres adéquats du manuel NetScreen Concepts & Exemples ScreenOS Reference Guide de ScreenOS 5.0.0.*

Restriction de la gestion

Par défaut, tous les utilisateurs connectés à votre réseau peuvent gérer l'appareil NetScreen dès lors qu'ils connaissent le nom de connexion et le mot de passe. Vous pouvez configurer l'appareil NetScreen de façon à ce qu'il ne puisse être géré que depuis un ou plusieurs hôtes spécifiques de votre réseau. (Vous pouvez également sélectionner les services - par exemple WebUI, Telnet, ping - que vous souhaitez activer au niveau de l'appareil NetScreen.)

Pour plus d'informations, reportez-vous au chapitre « Administration » du volume « Administration » du manuel *NetScreen Concepts & Exemples ScreenOS Reference Guide* de ScreenOS 5.0.0.

Configuration de règles de sécurité supplémentaires

Vos appareils NetScreen-5GT sans fil sont configurées avec des règles de sécurité par défaut qui permettent aux postes de travail situés dans la zone Trust de votre réseau d'accéder à tous les types de services utilisant des ordinateurs extérieurs au réseau tandis que les ordinateurs extérieurs au réseau ne peuvent pas accéder à vos postes de travail ou initier des sessions avec eux. Vous pouvez configurer des règles de sécurité de façon à ce que l'appareil NetScreen autorise les ordinateurs extérieurs à votre réseau à initier des sessions de type spécifique avec vos ordinateurs. Pour plus d'informations sur la création ou la modification des règles de sécurité, reportez-vous au chapitre « Politiques » du volume « Fundamentals » du manuel *NetScreen Concepts & Exemples ScreenOS Reference Guide* de ScreenOS 5.0.0.

Mode de fonctionnement

Le *mode de fonctionnement* représente la manière dont une interface sur un appareil NetScreen traite le trafic entre différentes zones. Par défaut, les appareils NetScreen-5GT sans fil fonctionnent en mode Route, la fonction de traduction des adresses réseau (NAT) étant activée dans l'interface sécurisée. Cela signifie que lorsque les appareils dans la zone Trust transmettent du trafic vers Internet, l'appareil NetScreen remplace les adresses IP source originales par l'adresse IP de l'interface non sécurisée. Lorsque l'appareil NetScreen attribue des adresses IP privées aux appareils connectés à votre réseau, ces adresses restent invisibles aux ordinateurs extérieurs à votre réseau.

Si tous les appareils connectés à votre réseau disposent d'adresses IP publiques, vous pouvez configurer l'appareil NetScreen en mode Route sans activer la fonction NAT. En mode Route, la fonction NAT étant désactivée, l'appareil NetScreen route le trafic en contrôlant les adresses IP. Pour plus d'informations sur la configuration de l'appareil en mode Route sans activer la fonction NAT, reportez-vous au chapitre « Interface Modes » du volume « Fundamentals » du manuel *NetScreen Concepts & Examples ScreenOS Reference Guide* de ScreenOS 5.0.0.

Modification du mode de port

Le *mode de port* définit la liaison des ports physiques, des interfaces logiques et des zones.

Avertissement : la modification du mode de port supprime les éventuelles configurations existantes sur l'appareil NetScreen. Vous devez donc modifier le mode de port avant de configurer l'appareil.

Le tableau suivant récapitule les liaisons de port, d'interface et de zone fournies par les modes de port disponibles sur les appareils NetScreen-5GT sans fil :

Nom du port ^a	Mode de port Trust-Untrust (sécurisé-non sécurisé) ^b		Mode de port Home-Work (Domicile-Travail)		Mode (étendu) Trust/Untrust/DMZ (sécurisé/non sécurisé/DMZ)		Dual Untrust Port Mode		Combined Port Mode	
	Interface	Zone	Interface	Zone	Interface	Zone	Interface	Zone	Interface	Zone
1	trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet1	Trust	ethernet1	Work
2	trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet1	Trust	ethernet2	Home
3	trust	Trust	ethernet2	Home	ethernet2	DMZ	ethernet1	Trust	ethernet2	Home
4	trust	Trust	ethernet2	Home	ethernet2	DMZ	ethernet2	Untrust	ethernet3	Untrust
Untrusted	untrust	Untrust	ethernet3	Untrust	ethernet3	Untrust	ethernet3	Untrust	untrust	Untrust
Modem ^c	série	Null	série	Null	série	Null	série	Null	série	Null
	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1
	wireless2	Trust	wireless2	Work	wireless2	Trust	wireless2	Trust	wireless2	Work
			wireless3	Home	wireless3	DMZ			wireless3	Home
					wireless4	Wzone2				

- Selon l'étiquette apposée sur le châssis de l'appareil NetScreen.
- Mode de port par défaut.
- Vous pouvez configurer une interface « de secours » avec la zone Untrust en utilisant le port Ethernet Untrusted ou le port Modem. Reportez-vous à la section « Configuration d'une interface « de secours » de zone Untrust », page 69.

Le tableau suivant récapitule les liaisons de port, d'interface et de zone fournies par les modes de port disponibles sur les appareils NetScreen-5GT ADSL sans fil :

Nom du port ^a	Mode de port Trust-Untrust (sécurisé-non sécurisé) ^b		Mode de port Home-Work (Domicile-Travail)		Mode (étendu) Trust/Untrust/DMZ (sécurisé/non sécurisé/DMZ)	
	Interface	Zone	Interface	Zone	Interface	Zone
1	trust	Trust	ethernet1	Work	ethernet1	Trust
2	trust	Trust	ethernet1	Work	ethernet1	Trust
3	trust	Trust	ethernet2	Home	ethernet2	DMZ
4	trust	Trust	ethernet2	Home	ethernet2	DMZ
Untrusted	untrust	Null ^c	ethernet3	Null ^c	ethernet3	Null ^c
Modem	série	Null ^c	série	Null ^c	série	Null ^c
ADSL	adsl1	Untrust	adsl1	Untrust	adsl1	Untrust
	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1
	wireless2	Trust	wireless2	Work	wireless2	Trust
			wireless3	Home	wireless3	DMZ
				wireless4	Wzone2	

- a. Selon l'étiquette apposée sur le châssis de l'appareil NetScreen.
- b. Mode de port par défaut.
- c. Vous pouvez configurer une interface « de secours » avec la zone Untrust en utilisant le port Ethernet Untrusted ou le port Modem. Reportez-vous à la section « Configuration d'une interface « de secours » de zone Untrust », page 69.

Pour configurer l'appareil NetScreen en mode de port Home-Work (Domicile-Travail) :

WebUI

Configuration > Port Mode (Mode de port) : sélectionnez Home-Work (Domicile-Travail) dans la liste déroulante, puis cliquez sur **Apply** (Appliquer).

À l'invite suivante, cliquez sur **OK** :

« Operational mode change will erase current configuration and reset the device, continue? » (La modification du mode de fonctionnement efface la configuration actuelle et réinitialise l'appareil, continuer ?)

CLI

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

À l'invite suivante, entrez **y** (pour « yes ») :

```
Change port mode from <trust-untrust> to <home-work> will
erase system configuration and reboot box (Modifier le mode
du port de <sécurisé-non sécurisé> en <domicile-travail>
efface la configuration du système et réinitialise
l'appareil)
```

```
Are you sure y/[n] ? y (Êtes-vous sûr) ? o/[n])
```

Configuration d'une interface « de secours » de zone Untrust

Par défaut, sur les appareils NetScreen-5GT ADSL sans fil, l'interface `adsl1` constitue la connexion principale vers un réseau externe. Chaque mode de port disponible sur l'appareil NetScreen-5GT ADSL sans fil vous permet d'établir une connexion « de secours » avec le réseau externe, soit par l'intermédiaire du port Ethernet Untrusted, soit par l'intermédiaire du port Modem (voir la section « [Modification du mode de port](#) », page 67). Vous devez lier l'interface de secours à la zone Untrust et configurer l'interface de façon adéquate.

Remarque : vous ne pouvez configurer qu'une seule interface de secours, en utilisant soit une connexion au port Ethernet Untrusted, soit une connexion au port Modem. Si vous utilisez le port Untrusted afin d'établir une connexion de secours, configurez l'interface Untrusted en mode de port Trust-Untrust (sécurisé-non sécurisé), ou utilisez l'interface `ethernet3` pour accéder aux autres modes de port. Si vous utilisez le port Modem pour établir la connexion de secours, configurez l'interface série pour tous les modes de port.

Par exemple, pour lier l'interface non sécurisée à la zone Untrust :

WebUI

Network (Réseau) > Interfaces > Edit (Modifier) (pour l'interface non sécurisée) : sélectionnez Untrust (Non sécurisée) dans la liste déroulante Zone Name (Nom de la zone), puis cliquez sur **OK**.

CLI

```
set interface untrust zone untrust
save
```

Vous devez également définir une adresse IP statique pour l'interface non sécurisée ou spécifier si l'adresse IP de l'interface est obtenue par l'intermédiaire du protocole DHCP ou PPPoE. Pour plus d'informations sur la configuration des paramètres des interfaces, reportez-vous au chapitre « Interfaces » du volume « Fundamentals » du manuel *NetScreen Concepts & Examples ScreenOS Reference Guide* de ScreenOS 5.0.0.

Lorsque l'interface `adsl1` et l'une des interfaces Ethernet (nommée interface non sécurisée ou `ethernet3`, en fonction du mode de port) ou l'interface série sont liées à la zone Untrust, la commutation de l'interface en cas de défaillance est automatiquement configurée. Cela signifie que si l'interface `adsl1` est indisponible, l'appareil NetScreen route automatiquement le trafic vers l'interface de secours. L'appareil route automatiquement le trafic vers l'interface `adsl1` dès que l'interface `adsl1` redevient disponible.

Remarque : *seule l'interface `adsl1` est affectée par la commutation en cas de défaillance. Cela signifie que si vous avez également configuré des sous-interfaces ADSL, les sous-interfaces ne basculeront pas vers l'interface de secours en cas de défaillance.*

Vous pouvez manuellement forcer les fonctions de reprise et de retour à l'interface principale sur l'interface `adsl1`. Pour plus d'informations, reportez-vous au chapitre « Interface Redundancy » du volume « High Availability » du manuel *NetScreen Concepts & Examples ScreenOS Reference Guide* de ScreenOS 5.0.0.

Modification de l'adresse de l'interface sécurisée ou wireless2

Au besoin, vous pouvez modifier l'adresse IP et le masque de réseau des interfaces sécurisée et sans fil. (N'oubliez pas que lorsque l'interface sécurisée ou `wireless2` se trouve en mode NAT, les adresses IP des appareils connectés à votre réseau ne sont jamais visibles par les ordinateurs extérieurs à votre réseau ; les ordinateurs extérieurs voient uniquement l'adresse IP de l'interface non sécurisée.) Par exemple, vous pouvez avoir besoin de modifier l'interface sécurisée ou `wireless2` afin que celle-ci corresponde aux adresses IP existant déjà sur votre réseau. Si vous modifiez l'adresse IP et le masque de réseau de l'interface sécurisée ou `wireless2`, vous devez également soit modifier l'étendue des adresses attribuées par l'appareil NetScreen aux appareils connectés au réseau, par l'intermédiaire du protocole DHCP, soit désactiver le serveur DHCP dans l'interface sécurisée ou `wireless2`.

Si les ordinateurs connectés à votre réseau obtiennent leurs adresses IP par l'intermédiaire du serveur DHCP sur l'appareil NetScreen, les ordinateurs obtiendront également leur passerelle par l'intermédiaire de l'appareil NetScreen. Si un ordinateur possède une adresse IP attribuée de façon statique, vous devez définir sa passerelle par défaut manuellement, en fonction de l'adresse IP de l'interface sécurisée ou `wireless2` sur l'appareil NetScreen.

Pour attribuer une adresse IP et un masque de réseau différents à l'interface sécurisée ou `wireless2`, reportez-vous au chapitre « Interfaces » du volume « Fundamentals » du manuel *NetScreen Concepts & Examples ScreenOS Reference Guide* de ScreenOS 5.0.0.

Pour modifier les paramètres DHCP de l'appareil NetScreen, reportez-vous au chapitre « System Parameters » du volume « Fundamentals » du manuel *NetScreen Concepts & Examples ScreenOS Reference Guide* de ScreenOS 5.0.0.

CONTRÔLE DE LA CONNECTIVITÉ EXTERNE

Afin de vérifier que les postes de travail connectés à votre réseau sont en mesure d'accéder aux ressources sur Internet, lancez un navigateur Web sur n'importe quel poste de travail connecté à votre réseau et entrez l'URL suivante : www.juniper.net.

RESTAURATION DES PARAMÈTRES PAR DÉFAUT DE L'APPAREIL

Si vous égarez votre mot de passe d'administrateur, vous pouvez réinitialiser l'appareil NetScreen et en restaurer les paramètres par défaut. Cela écrase les configurations existantes mais rétablit l'accès à l'appareil.

Avvertissement : réinitialiser l'appareil supprime tous les paramètres de configuration existants et désactive les services de pare-feu et de VPN.

Procédez de l'une des manières suivantes pour restaurer les paramètres par défaut de l'appareil :

- À l'aide d'une connexion de console. Pour plus d'informations, reportez-vous au chapitre « Administration » du volume « Administration » du manuel *NetScreen Concepts & Examples ScreenOS Reference Guide* de ScreenOS 5.0.0.
- En utilisant le trou d'épingle de réinitialisation situé sur le panneau arrière de l'appareil, comme décrit dans la section suivante.

Utilisation du trou d'épingle de réinitialisation

Vous pouvez réinitialiser l'appareil et en restaurer les paramètres par défaut en appuyant sur le bouton situé dans le trou d'épingle de réinitialisation. Pour effectuer cette opération, vous devez soit consulter les DEL d'état situées sur le panneau avant de l'appareil, soit ouvrir une session de console comme décrit dans la section « [Utilisation d'une connexion de console](#) », page 55.

1. Repérez le trou d'épingle de réinitialisation situé sur le panneau arrière de l'appareil. En utilisant un fil de fer fin et rigide (un trombone, par exemple), appuyez sur le bouton situé dans le trou d'épingle pendant quatre à six secondes, puis relâchez.



Trou d'épingle de réinitialisation

La DEL d'état affiche une lumière orange clignotante. Un message s'affiche sur la console, indiquant que la suppression de la configuration a commencé, et le système transmet une alerte SNMP/SYSLOG.

2. Patientez une à deux secondes.

Après la première réinitialisation, la DEL d'état affiche une lumière verte clignotante ; l'appareil attend maintenant la deuxième réinitialisation. Le message de la console indique maintenant que l'appareil attend une deuxième confirmation.

3. Appuyez à nouveau sur le bouton situé dans le trou d'épingle de réinitialisation pendant quatre à six secondes.

Le message de la console valide la seconde confirmation. La DEL d'état affiche une lumière orange clignotante pendant une demi-seconde, puis retourne à l'état clignotant vert.

L'appareil est maintenant réinitialisé et ses paramètres par défaut restaurés. Lorsque l'appareil se réinitialise, la DEL d'état affiche une lumière orange clignotante pendant une demi-seconde, puis affiche une lumière verte clignotante. La console affiche les messages d'amorçage de l'appareil. Le système génère des alertes SNMP et SYSLOG aux hôtes de déROUTement SYSLOG ou SNMP configurés.

Une fois l'appareil redémarré, la console affiche l'invite de connexion à l'appareil. La DEL d'état affiche une lumière clignotante verte.

Si vous ne suivez pas la procédure entière, le processus de réinitialisation s'interrompt et le message affiché sur la console indique que l'effacement de la configuration est annulé. La DEL d'état clignote en vert. Si l'appareil n'a pas été réinitialisé, une alerte SNMP est transmise afin de confirmer l'échec de la procédure.

Description du matériel

Ce chapitre fournit la description détaillée du châssis de l'appareil NetScreen-5GT sans fil.

CONNECTEURS DE PORTS ET D'ALIMENTATION

Le panneau arrière de l'appareil NetScreen-5GT sans fil est équipé de connecteurs de ports et d'alimentation.

Antenne B

Antenne A



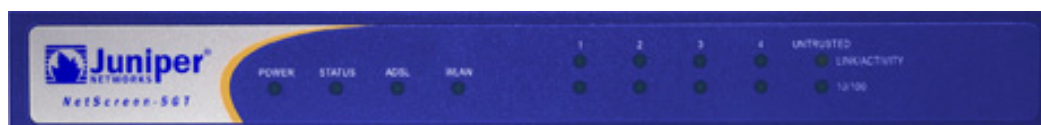
La prise d'alimentation CC permet de raccorder une source d'alimentation à l'appareil NetScreen-5GT sans fil. Le trou d'épingle de réinitialisation vous permet de réinitialiser l'appareil et de restaurer ses paramètres par défaut définis en usine. L'appareil NetScreen-5GT sans fil comporte les ports suivants :

Port	Description	Connecteur	Vitesse/Protocole
ADSL	Le cas échéant, permet d'établir une connexion à Internet au moyen d'une liaison de données ADSL.	RJ-11 (Annexe A) RJ-45 (Annexe B)	ANSI T1.413 Issue 2 ITU G.992.1 (G.dmt) ITU 992.2 (G.lite)
Console	Permet d'établir une connexion série avec le système. Utilisé pour le lancement des sessions d'interface de ligne de commande (CLI).	RJ-45	9600 bits/s ; RS-232
Modem	Permet d'établir une connexion série de secours à Internet par l'intermédiaire d'un modem externe.	RJ-45	9600 bits/s- 115 Kbits/s ; RS-232
Untrusted (Non sécurisé)	Permet d'établir une connexion principale ou de secours à Internet ou à un réseau non sécurisé par l'intermédiaire d'un routeur externe, d'un modem DSL ou d'un modem câble.	RJ-45	10/100 Mbits/s ; Ethernet Détection automatique du mode duplex et de la polarité
Ports 1 à 4	Permet d'établir une connexion directe avec des postes de travail ou une connexion à un réseau local par l'intermédiaire d'un commutateur ou d'un hub. Cette connexion vous permet également de gérer l'appareil par l'intermédiaire d'une session Telnet ou de l'application de gestion WebUI.	RJ-45	10/100 Mbits/s ; Ethernet Détection automatique du mode duplex et de la polarité
Antenne A et B	Permet d'établir une connexion directe avec des postes de travail se trouvant à proximité d'une connexion radio sans fil. Cette connexion vous permet de gérer l'appareil par l'intermédiaire d'une session Telnet ou de l'application de gestion WebUI.	RPSMA	802.11b 802.11g

Avertissement : ne connectez pas de ligne téléphonique ou RNIS directement au port Modem de l'appareil NetScreen-5GT sans fil. Vous devez d'abord connecter l'appareil à un modem par l'intermédiaire d'un port RS-232, puis connecter le modem à la ligne téléphonique.

DEL D'ÉTAT

Le panneau avant de l'appareil NetScreen-5GT sans fil comporte des DEL d'alimentation et d'état spécifiques à l'appareil, et des DEL d'état des ports spécifiques aux interfaces.



Principales DEL d'état de l'appareil

Les DEL d'état de l'appareil permettent d'indiquer si l'appareil fonctionne correctement. Le tableau suivant décrit les différents états possibles pour chaque DEL.

DEL	État	Signification
POWER (ALIMENTATION)	verte	Indique que le système est sous tension.
	éteinte	Indique que le système n'est pas sous tension.
STATUS (ÉTAT)	verte clignotante	Indique que le système est opérationnel.
	verte	Indique que le système est en phase de démarrage.
	rouge	Indique une erreur de diagnostic ou d'initialisation du système.
	éteinte	Indique que le système n'est pas opérationnel.
ADSL (sur les modèles ADSL sans fil uniquement)	verte	Indique que la boucle ADSL est active.
	éteinte	Indique que la boucle ADSL est inactive.
WLAN	verte clignotante lente	Indique qu'une connexion sans fil est établie, mais qu'il n'y a pas d'activité de liaison.
	verte clignotante rapide	Indique qu'une connexion sans fil est établie. La rapidité du clignotement est proportionnelle à l'activité de la liaison.
	éteinte	Indique qu'aucune connexion sans fil n'a été établie.

DEL d'état des ports

Les DEL d'état des ports indiquent si les ports de l'appareil fonctionnent correctement. Le tableau suivant décrit les différents états possibles pour chaque port.

DEL	Couleur de la DEL	Signification de la DEL
Liaison/ Activité	verte clignotante	Indique que l'appareil détecte un trafic Ethernet sur le port.
	éteinte	Indique que le port n'a pas encore établi de liaison avec un autre appareil.
	verte	Indique que le port a établi une liaison avec un autre appareil.
10/100	verte	Indique que le port est connecté à un appareil 100Base-T.
	éteinte	Indique que le port est connecté à un appareil 10Base-T.



Spécifications

Cette annexe contient les spécifications système générales de l'appareil NetScreen-5GT sans fil.

Attributs

Hauteur	2,93 centimètres	1,15 pouces
Profondeur	18,45 centimètres	7,26 pouces
Largeur	20,8 centimètres	8,19 pouces
Poids	0,9 kilogramme	1,98 livres

Spécifications électriques

Régulateur à découpage	Adaptateur CA : 100 V-240 V CA +/- 10 % 50/60 Hz, 15-18 watts Entrée CC : 12 volts, 1,25-1,5 A
------------------------	--

Spécifications environnementales

Altitude normale	0-40° C, 32-105° F
Humidité relative	10-90 %
Sans condensation	10-90 %

L'altitude normale maximale est de 2 000 mètres (6 562 pieds).

Certifications

Sécurité	UL, CUL, TUV, CE, CB
IEM	Chapitre 15 des FCC, classe B, VCCI, CE

Connecteurs Ethernet

Norme	100Base-TX
Type de support	Catégorie 5 et supérieure Câble à paire torsadée non blindée (UTP)
Distance maximale	100 mètres (328,08 pieds)

Les ports RJ-45 à paire torsadée sont compatibles avec la norme IEEE 802.3 Type 10/100 Base-T

Connecteur ADSL

Types	Connecteur RJ-11 à 6 broches pour la version Annexe A Connecteur RJ-45 pour la version Annexe B
Type de support	Câble téléphonique standard

CONNEXIONS AVEC ADAPTATEUR POUR CONSOLE ET MODEM

Le tableau suivant décrit les définitions de connecteur RJ-45. Lorsque vous utilisez un port UART standard, les ports Console et Modem utilisent tous deux cette configuration.

RJ-45	Signal	Abréviation	DCE
1	Request To Send (Demande d'émission)	RTS	In
2	Data Terminal Ready (Terminal prêt)	DTR	In
3	Transmitted Data (Données transmises)	TD	In
4, 5	Signal Ground (Mise à la terre du signal)	SGND	N/A
6	Received Data (Données reçues)	RD	Out
7	Not Connected (Non connecté)		
8	Clear To Send (Prêt à émettre)	CTS	Out

Le tableau suivant décrit les définitions des adaptateurs de connexion RJ-45 à DB-9. Lorsque vous utilisez un port UART standard, les ports Console et Modem doivent tous deux utiliser cette configuration.

DB9	Signal	Abréviation	DTE	DCE	RJ45
1	Data Carrier Detect (Détection de porteuse de données)	DCD	In	Out	NC
2	Received Data (Données reçues)	RD	In	Out	3
3	Transmitted Data (Données transmises)	TD	Out	In	6
4	Data Terminal Ready (Terminal prêt)	DTR	Out	In	7
5	Signal Ground (Mise à la terre du signal)	SGND	N/A	N/A	4
6	Data Set Ready (Modem prêt)	DSR	In	Out	2

7	Request To Send (Demande d'émission)	RTS	Out	In	8
8	Clear To Send (Prêt à émettre)	CTS	In	Out	1
9	Ring Indicator (Indicateur d'appel)	RI	In	Out	NC

Remarque : si vous utilisez le câble de console fourni avec l'appareil NetScreen pour la connecter à un modem, vous devez vous procurer un adaptateur simulateur de modem et l'installer sur le connecteur du modem.

Index

A

- AAL5, multiplexage 60
- adresse de l'interface de zone Trust 70
- adresse IP statique 61
 - configuration 63
- ADSL
 - configuration de l'interface 60
 - connexion du câble 47
 - connexion du port 47
- ajout d'un circuit virtuel 61
- Annexe A 47
- Annexe B 47
 - configuration pour Deutsch Telecom 63
- antennes 49
- appareil, montage en baie 50
- ATM, Couche d'adaptation 5 60

C

- circuit virtuel, ajout 61
- configuration
 - facultative 65
 - paramètres par défaut 59
 - requis 55, 59
 - réseau sans fil 57
 - SSID 58
- connecteur DB-9 78
- connecteur RJ-45 78
- connecteurs
 - alimentation 73
 - port 73
- connexion d'une source d'alimentation 50
- Console, utilisation 55
- contrôle de la connectivité 71
- conventions 53
 - CLI 44
 - WebUI 44

D

- date, réglage 56
- DEL
 - état 74

- DEL d'état des ports 75
- Deutsch Telecom, configuration Annexe B 63

E

- enregistrement de l'appareil 53

G

- gestion de l'appareil depuis un hôte spécifique 65

H

- heure, réglage 56

I

- interface de secours avec une zone Untrust 69
- interface wireless1 58
- interface wireless2
 - accès 53
 - modification de l'adresse de l'interface 70
 - paramétrage pour un SSID 58
 - zone Trust 57
 - zones de liaison 57

M

- microfiltre 48
- modification du mode de port 67
- modification du nom de connexion et du mot de passe 56
- montage en baie de l'appareil 50
- mot de passe, modification 56
- multiplexage, configuration 61

N

- nom d'administrateur, modification 56

O

- Organisation du manuel 43

P

- paramètres par défaut 59

- restauration 71
 - Point-to-Point Protocol over ATM
 - Voir* PPPoA
 - Point-to-Point Protocol over Ethernet
 - Voir* PPPoE
 - port Untrusted 49
 - ports Ethernet sécurisés 49
 - PPPoA 61
 - configuration 62
 - PPPoE 61
 - configuration 62
 - Publications NetScreen 45
- R**
- réglage de l'horloge de l'appareil 56
 - règles de sécurité supplémentaires, configuration 65
 - restauration des paramètres par défaut 71
 - restriction de la gestion depuis un hôte spécifique 65
 - Route, mode 66
- S**
- sans fil
 - antennes 49
 - configuration 57
 - connexion 47, 49
 - utilisation de l'interface par défaut 49
 - zone Trust 57
 - zone Wzone1 58
- séparateur de signaux 48
 - Service Set Identifier
 - Voir* SSID
 - source d'alimentation, connexion 50
 - SSID (Service Set Identifier) 58
- T**
- Telnet, utilisation 54
 - Transparent, mode 66
 - trou d'épingle de réinitialisation, utilisation 71
- V**
- Virtual Path Identifier (Identificateur de trajet virtuel)/Virtual Channel Identifier (Identificateur de canal virtuel)
 - Voir* VPI/VCI
 - VPI/VCI 60
 - configuration 61
- W**
- WebUI
 - accès 53
 - conventions 44
- Z**
- zone Untrust, configuration d'une interface de secours 69

Inhalt

Vorwort.....	85
Organisation	85
WebUI-Konventionen	86
CLI-Konventionen	86
NetScreen-Publikationen	87
Kapitel 1 Anschließen des Geräts.....	89
Anschließen des NetScreen-Geräts an Ihre Netzwerke	89
Anschluss des Geräts an ein Untrusted-Netzwerk	89
Anschließen des ADSL-Anschlusses	89
Anschließen des Untrusted-Anschlusses	91
Anschließen des Geräts an Ihr internes Netzwerk oder Arbeitsstationen	91
Verbindung von Trusted Ethernet-Anschlüssen	91
Verwenden der Wireless-Schnittstelle	91
Anschließen der Stromversorgung	92
Gestellmontage (optional)	92
Kapitel 2 Konfigurieren des Geräts	95
Zugriff auf das Gerät	95
Verwenden der WebUI.....	95
Verwenden von Telnet.....	96
Verwenden einer Konsolenverbindung	97
Erforderliche Konfiguration	97
Ändern des Administratorsnamens und -kennworts	97
Einstellen des Datums und der Uhrzeit	98
Wireless-Konfiguration	99
Konfigurieren des Wireless-Netzwerks	100
ADSL-Konfiguration	101
Konfigurieren der ADSL-Schnittstelle.....	102
Hinzufügen von virtuellen Verbindungen zu einer ADSL-Schnittstelle	103
VPI/VCI und Multiplexingmethode	103
PPPoE oder PPPoA.....	104
Annex B-Modus.....	105
Statische IP-Adresse und Netzmaske	105
Optionale Konfiguration	106
Beschränken der Verwaltung	107
Konfigurieren zusätzlicher Richtlinien	107
Betriebsmodus	107
Ändern des Anschlussmodus	108
Konfigurieren einer Untrust Sicherungszonenschnittstelle	110

Ändern der Trust- oder Wireless2-Schnittstellenadresse	111
Überprüfen der externen Verbindung	111
Zurücksetzen des Geräts auf die werkseitigen Standardeinstellungen ...	111
Verwenden des Reset-Stiftlochs	112
Kapitel 3 Hardwarebeschreibungen.....	115
Verbindungs- und Netzanschlüsse	115
Status-LEDs	116
Hauptstatus-LEDs für das Gerät.....	117
Anschlussstatus-LEDs	117
Technische Daten	119
Index.....	121

Vorwort

Das Juniper Networks NetScreen-5GT Wireless-Gerät bietet über eine integrierte drahtlose 802.11b/g-Schnittstelle IPSec Virtual Private Network (VPN)- und Firewalldienste für Zweigniederlassungen oder Einzelhandelsgeschäfte. Das NetScreen-5GT Wireless-Gerät verwendet dieselbe Firewall-, VPN-, Antiviren-, Deep Inspection- und Verkehrsverwaltungstechnologie wie die hochwertigen NetScreen-Produkte für zentrale Standorte.

Juniper Networks bietet drei Modelle des NetScreen-5GT Wireless-Geräts an:

- **NetScreen-5GT Wireless:** Das Wireless-Modell.
- **NetScreen-5GT Wireless ADSL A:** Das Wireless mit Annex A-Modell unterstützt ADSL über standardmäßige Telefonleitungen (POTS).
- **NetScreen-5GT Wireless ADSL B:** Das Wireless mit Annex B-Modell unterstützt ADSL über ISDN (Integrated Services Digital Network).

Alle Modelle unterstützen bis zu vier Wireless-Sicherheitszonen. Beide ADSL-Modelle unterstützen die Standards gemäß ANSI T1.413 Ausgabe 2, ITU G.992.1 (G.dmt) und ITU 992.2 (G.lite).

Jedes Modell unterstützt drei Softwareversionen:

- Die 10-Benutzerversion unterstützt bis zu 10 Benutzer.
- Die Plus-Version unterstützt eine unbeschränkte Anzahl von Benutzern.
- Die Extended-Version bietet neben den Funktionen der Plus-Version einige zusätzliche Features: hohe Verfügbarkeit (NSRP Lite), DMZ-Sicherheitszone sowie zusätzliche Sitzungs- und Tunnelkapazität.

ORGANISATION

Dieses Handbuch besteht aus drei Kapiteln und einem Anhang.

[Kapitel 1, „Anschließen des Geräts“](#), beschreibt den Anschluss des Geräts an Ihr Netzwerk, den Stromnetz- und Antennenanschluss sowie die Installation des NetScreen-5GT Wireless-Geräts in einem Gestell.

[Kapitel 2, „Konfigurieren des Geräts“](#), beschreibt die Standardeinstellungen und den Betrieb des NetScreen-5GT Wireless (ADSL) sowie die zur Verwendung des Geräts erforderlichen Konfigurationsschritte.

[Kapitel 3, „Hardwarebeschreibungen“](#), bietet einen Überblick über die Anschlüsse und LEDs sowie die Anforderungen für die Stromversorgung des NetScreen-5GT Wireless.

[Anhang A, „Technische Daten“](#), enthält eine Liste der technischen Daten des NetScreen-5GT Wireless-Geräts.

WEBUI-KONVENTIONEN

In diesem Handbuch wird ein Rechtspfeil (>) als Symbol für das Navigieren in der WebUI durch Auswahl von Menüoptionen und Links verwendet.

Beispiel: Objects > Addresses > List > New

Gehen Sie wie folgt vor, um auf das Konfigurationsdialogfeld für neue Adressen zuzugreifen:

1. Klicken Sie in der Menüspalte auf **Objects**.
Die Menüoption Objects wird erweitert, und eine Reihe von Unteroptionen wird angezeigt.
2. (Applet-Menü¹) Platzieren Sie die Maus auf **Addresses**.
(DHTML-Menü) Klicken Sie auf **Addresses**.
Die Menüoption Addresses wird erweitert, und eine Reihe von Unteroptionen wird angezeigt.
3. Klicken Sie auf **List**.
Die Adressbuchtabelle wird angezeigt.
4. Klicken Sie oben rechts auf den Link **New**.
Das Konfigurationsdialogfeld für neue Adressen wird angezeigt.

CLI-KONVENTIONEN

Die folgenden Konventionen gelten für die Darstellung der Syntax von CLI-Befehlen (CLI = Command Line Interface = Befehlszeilenschnittstelle):

- Alle Angaben in eckigen Klammern [] sind optional.
- Alle Angaben in geschwungenen Klammern { } sind erforderlich.
- Wenn mehreren Optionen möglich sind, sind diese durch einen senkrechten Strich (|) voneinander getrennt. Beispiel:

```
set interface { ethernet1 | ethernet2 | ethernet3 }  
manage
```

Dies bedeutet „Verwaltungsoptionen für die Schnittstelle ethernet1, ethernet2 oder ethernet3 einstellen“.

- Variablen werden *kursiv* dargestellt. Beispiel:

```
set admin user name1 password xyz
```

1. Sie können zwischen dem Applet- und DHTML-Menütyp wechseln, indem Sie unten in der Menüspalte auf die Option **Toggle Menu** klicken.

Im Kontext eines Satzes werden CLI-Befehle **fett** formatiert (mit Ausnahme der Variablen, die immer *kursiv* dargestellt werden). Beispiel: „Verwenden Sie den Befehl **get system**, um die Seriennummer eines NetScreen-Geräts anzuzeigen.“

***Hinweis:** Beim Eingeben eines Schlüsselworts müssen Sie nur so viele Buchstaben eingeben wie zur eindeutigen Identifizierung des Wortes erforderlich sind. Die Eingabe **set adm u joe j12fmt54** ist z.B. ausreichend für den Befehl **set admin user joe j12fmt54**. Obwohl solche Abkürzungen zum Eingeben von Befehlen verwendet werden können, sind alle in diesem Handbuch dokumentierten Befehle vollständig dargestellt.*

NETSCREEN-PUBLIKATIONEN

Technische Dokumentation für Juniper Networks NetScreen-Produkte steht Ihnen auf unserer Website unter www.juniper.net/techpubs/ zur Verfügung.

Um technischen Support anzufordern, eröffnen Sie einen Support-Fall (Support Case) mit Hilfe des Links „Case Manager“ unter <http://www.juniper.net/support/>, oder rufen Sie uns unter 1-888-314-JTAC (innerhalb der Vereinigten Staaten) oder unter +001-408-745-9500 (außerhalb der Vereinigten Staaten) an.

Sollten Sie Fehler oder Auslassungen in diesem Handbuch feststellen, schreiben Sie uns an die folgende E-Mail-Adresse:

techpubs-comments@juniper.net

Anschließen des Geräts

In diesem Kapitel wird beschrieben, wie Sie das NetScreen-5GT Wireless-Gerät an das Netzwerk und die Stromversorgung sowie die Antenne an das Gerät anschließen. Wenn Sie das optionale NetScreen-5GT Wireless-Gestellmontagekit verwenden, finden Sie die entsprechenden Montageanweisungen am Ende dieses Kapitels.

Hinweis: Sicherheitshinweise und Anweisungen finden Sie im NetScreen-Sicherheitshandbuch. Dieses Handbuch enthält Informationen über Situationen, die zu Verletzungen führen können. Bevor Sie mit der Arbeit an Geräten beginnen, informieren Sie sich über die Gefahren, die beim Umgang mit elektrischen Komponenten bestehen. Machen Sie sich außerdem mit den gängigen Vorkehrungen zur Vermeidung von Unfällen vertraut.

ANSCHLIEßEN DES NETSCREEN-GERÄTS AN IHRE NETZWERKE

Das NetScreen-Gerät bietet eine Firewall und allgemeine Sicherheitsfunktionen für Ihre Netzwerke, wenn es zwischen den internen Netzwerken und dem ungesicherten (Untrusted) Netzwerk platziert wird. In diesem Abschnitt werden die physischen Verbindungen beschrieben.

Anschluss des Geräts an ein Untrusted-Netzwerk

Je nachdem, welches Modell des NetScreen-5GT Wireless-Geräts Sie verwenden, können Sie die Verbindung zum Untrusted-Netzwerk auf eine der folgenden Weisen herstellen:

- Durch eine ADSL-Verbindung über den ADSL-Anschluss am NetScreen-Gerät
- Durch eine Ethernet-Verbindung über den Untrusted-Anschluss am NetScreen-Gerät

Anschließen des ADSL-Anschlusses

Schließen Sie das mitgelieferte ADSL-Kabel vom ADSL-Anschluss des NetScreen-5GT Wireless ADSL-Geräts an die Telefonanschlussdose an. Der ADSL-Anschluss der Annex A-Version des Geräts verwendet einen RJ-11-Stecker, während die Annex B-Version mit einem RJ-45-Stecker ausgestattet ist. Das zum Verbinden des ADSL-Anschlusses mit dem Telefonanschluss verwendete Kabel für Annex B-Modelle sieht identisch aus, und für die Verkabelung wird ein Straight-Through-10 Base-T Ethernet-Kabel verwendet.

Warnung: Schließen Sie nicht versehentlich die Konsolen-, Modem- oder Ethernet-Anschlüsse des NetScreen-Geräts an der Telefonanschlussdose an.

Auf dem NetScreen-5GT Wireless ADSL-Gerät ist die ADSL-Leitung Ihre *primäre* Verbindung mit einem externen Netzwerk. Wenn Sie eine Sicherungsdatenverbindung mit einem externen Netzwerk einrichten möchten, können Sie ein Ethernet-Kabel vom Untrusted-Anschluss des NetScreen-5GT Wireless ADSL-Geräts mit einem externen Router oder einem DSL- bzw. Kabelmodem verbinden oder ein seriell Kabel vom Modemanschluss des Geräts an ein externes Modem anschließen.

Warnung: Es ist nicht möglich, den Untrusted-Anschluss und den Modemanschluss des Geräts gleichzeitig mit einem externen Netzwerk zu verbinden.

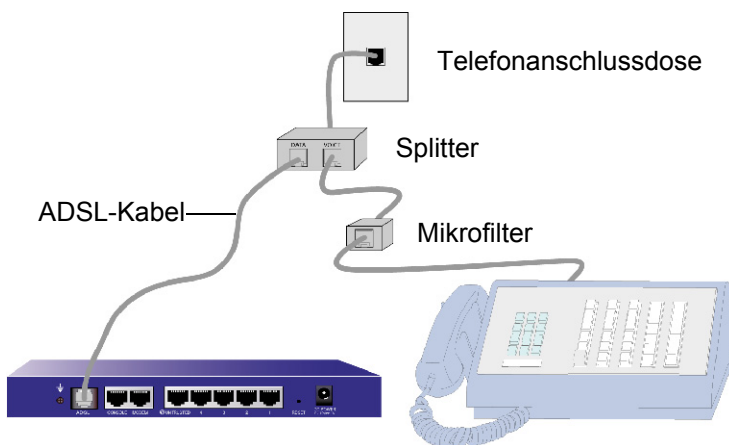
Anschließen von Splitttern und Mikrofiltern

Ein *Signalsplitter* teilt das Telefonsignal in niederfrequente Sprachsignale für Telefonate und hochfrequente Datensignale für Datenverkehr auf. Der Dienstanbieter installiert den Splitter normalerweise zusammen mit dem Gerät, über das die Telefonleitungen an Ihrem Standort mit dem Netzwerk des Anbieters verbunden werden.

Abhängig von den vom Dienstanbieter bereitgestellten Geräten können Sie möglicherweise selbst Splitter installieren. In diesem Fall schließen Sie das ADSL-Kabel vom NetScreen-Gerät und die Telefonleitung an die entsprechenden Stecker (z.B. „Daten“ oder „Sprache“) am Splitter an. Das andere Ende des Splitters wird mit der Telefonanschlusssdose verbunden.

Möglicherweise müssen Sie für alle mit der ADSL-Leitung verbundenen Telefone, Faxgeräte, Anrufbeantworter oder analogen Modems einen *Mikrofilter* installieren. Der Mikrofilter filtert hochfrequentes Rauschen in der Telefonleitung. Der Mikrofilter kann in der Telefonleitung zwischen dem Telefon, Faxgerät, Anrufbeantworter bzw. analogen Modem und dem Sprachstecker des Splitters installiert werden.

Die folgende Abbildung zeigt ein Beispiel für die Installation eines Mikrofilters und Splitters am Standort. (Die entsprechenden Mikrofilter oder Splitter erhalten Sie von Ihrem Dienstanbieter.)



Anschließen des Untrusted-Anschlusses

Sie haben die Möglichkeit, eine Internetverbindung zu einem externen Router oder einem DSL- oder Kabelmodem herzustellen und eine Firewall sowie allgemeine Sicherheitsfunktionen für Ihr Netzwerk bereitzustellen. Für eine Hochgeschwindigkeitsverbindung schließen Sie das mitgelieferte Ethernet-Kabel an die Untrusted-Schnittstelle am NetScreen-5GT Wireless-Gerät und an den externen Router oder das Modem an. Das NetScreen-5GT Wireless-Gerät erkennt dann automatisch die korrekten Übertragungsgeschwindigkeits-, Duplex- und Polaritätseinstellungen.

Wenn Sie das NetScreen-5GT Wireless ADSL-Gerät verwenden, finden Sie Anweisungen zum Herstellen einer ADSL-Verbindung unter [„Anschließen des ADSL-Anschlusses“](#) auf Seite 89 und [„Anschließen von Splittern und Mikrofiltern“](#) auf Seite 90.

Anschließen des Geräts an Ihr internes Netzwerk oder Arbeitsstationen

Sie können Ihr lokales Netz (LAN) oder Ihre Arbeitsstation mit einer oder beiden der folgenden Methoden anschließen:

- Verbindung über mindestens einen der Trusted Ethernet-Anschlüsse am NetScreen-Gerät
- Verwenden einer Wireless-Schnittstelle am NetScreen-Gerät

Verbindung von Trusted Ethernet-Anschlüssen

Das NetScreen-5GT Wireless-Gerät enthält vier Trusted Ethernet-Anschlüsse. Sie können diese Anschlüsse für die Verbindung mit LANs über Switches oder Hubs verwenden. Die Anschlüsse können jedoch auch ohne Hubs oder Switches direkt mit Arbeitsstationen verbunden werden. Zum Anschließen der Ethernet-Anschlüsse an andere Geräte können Crossover- oder Straight-Through-Kabel verwendet werden.

Verwenden der Wireless-Schnittstelle

Wenn Sie die Wireless-Schnittstelle verwenden, müssen Sie die mitgelieferten Antennen am Gerät anschließen. Wenn Sie über die standardmäßigen omnidirektionalen 2dB-Antennen verfügen, schrauben Sie sie an die mit A und B gekennzeichneten Halterungen auf der Geräterückseite an. Weitere Hinweise finden Sie unter [„Verbindungs- und Netzanschlüsse“](#) auf Seite 115. Biegen Sie die Antennen jeweils am Gelenk, ohne dabei Druck auf die Stecker auszuüben.

ANSCHLIEßEN DER STROMVERSORGUNG

So schließen Sie das NetScreen-5GT Wireless-Gerät an die Stromversorgung an:

1. Schließen Sie den Gleichstromstecker des Netzkabels an die Gleichstromnetzbuchse an der Rückseite des Geräts an.
2. Schließen Sie den Wechselstromadapter des Netzkabels an eine Wechselstromquelle an.

Warnung: Wir empfehlen die Verwendung eines Überspannungsschutzes für die Stromverbindung.

GESTELLMONTAGE (OPTIONAL)

Mit einem NetScreen-5GT Wireless-Gestellmontagekit können Sie ein oder zwei NetScreen-5GT Wireless-Geräte in einem standardmäßigen 19-Zoll-Gerätegestell montieren. Das NetScreen-5GT Wireless-Gestellmontagekit enthält Installationsanweisungen und eine Gestellmontagehalterung. Die Abmessungen der Halterung lauten wie folgt:

Breite:	48,26 cm	19 Zoll
Höhe:	4,013 cm	1 5/8 Zoll (1 Gestelleinheit)
Tiefe:	33,655 cm	13 1/4 Zoll

Neben den NetScreen-5GT Wireless-Geräten, dem Gestellmontagekit und dem Gerätegestell benötigen Sie auch Folgendes:

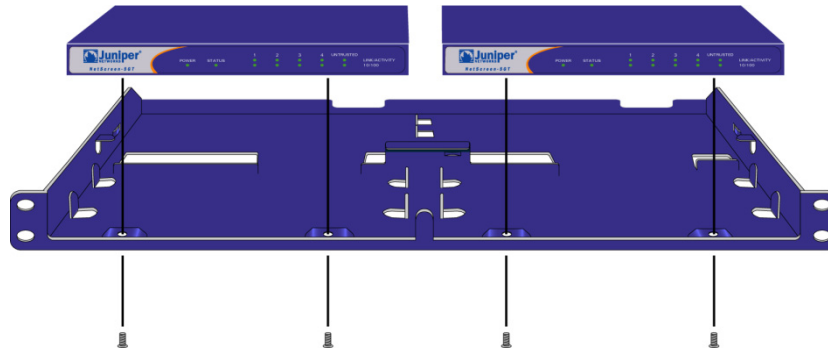
- Kreuzschlitzschraubendreher
- Vier Schrauben entsprechender Größe für das Gerätegestell

So montieren Sie das Gerät in einem Gestell:

1. Entfernen Sie mit dem Kreuzschlitzschraubendreher die beiden Schrauben an der Unterseite jedes zu montierenden NetScreen-5GT Wireless-Geräts. (Bewahren Sie die Schrauben für den nächsten Schritt auf.) Die Schrauben befinden sich an der Unterseite des Geräts neben dem Bedienfeld.



2. Setzen Sie jedes Gerät in die Gestellmontagehalterung ein, und befestigen Sie es mit den in Schritt 1 entfernten Schrauben an der Halterung.



3. Schrauben Sie die linke und rechte Halterungsplatte am Gerätegestell mit den verbleibenden Schrauben fest.



Netzkabel und Ethernet-Kabel können durch die Öffnungen im Halterungsboden oder durch die Vertiefungen an der Rückseite verlegt werden. Der Platz hinter den Geräten kann ebenfalls zum Unterbringen von Kabeln usw. verwendet werden.

Konfigurieren des Geräts

In diesem Kapitel wird beschrieben, wie Sie ein NetScreen-5GT Wireless-Gerät konfigurieren, nachdem Sie es mit dem Netzwerk verbunden haben. Wenn Sie erstmals über die grafische ScreenOS-Webbenutzerschnittstelle (WebUI) auf das Gerät zugreifen, können Sie den Assistenten für die Anfangskonfiguration verwenden, der Sie durch die grundlegende Konfiguration führt. Informationen zur Verwendung dieses Assistenten finden Sie im *Juniper Networks NetScreen-5GT Wireless Getting Started Guide* oder im *Juniper Networks NetScreen-5GT Wireless ADSL Getting Started Guide*.

Folgende Themen werden in diesem Kapitel behandelt:

- [Zugriff auf das Gerät](#)
- [Erforderliche Konfiguration](#)
- [Wireless-Konfiguration](#)
- [ADSL-Konfiguration](#)
- [Optionale Konfiguration](#)
- [Überprüfen der externen Verbindung](#)
- [Zurücksetzen des Geräts auf die werkseitigen Standardeinstellungen](#)

Hinweis: Nachdem Sie das NetScreen-Gerät konfiguriert und die Internetverbindung überprüft haben, müssen Sie das Produkt unter www.juniper.net/support/ registrieren, damit bestimmte ScreenOS-Dienste wie der interne Virenschutz oder der Deep Inspection-Signaturdienst im Gerät aktiviert werden. Nach der Registrierung des Produkts abonnieren Sie den Dienst über die WebUI. Weitere Informationen zum Registrieren des Produkts und Abonnieren bestimmter Dienste finden Sie im Kapitel „Systemparameter“ im Band „Grundlagen“ des ScreenOS-Referenzhandbuchs NetScreen-Konzepte und Beispiele für ScreenOS 5.0.0.

ZUGRIFF AUF DAS GERÄT

In diesem Abschnitt wird beschrieben, wie Sie auf Ihr NetScreen-Gerät mithilfe der WebUI, Telnet oder einer Konsolenverbindung zugreifen.

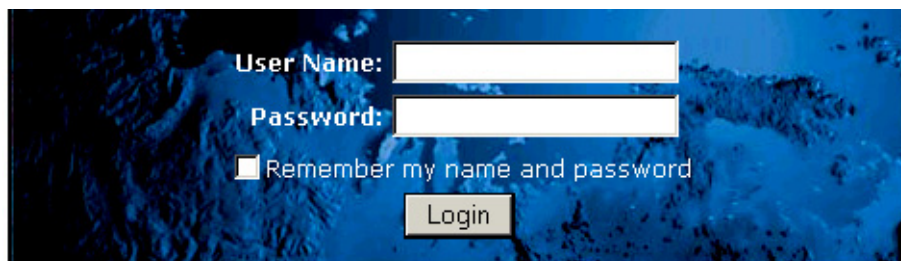
Verwenden der WebUI

Die ScreenOS-WebUI ist eine über einen Webbrowser verfügbare grafische Schnittstelle. Zur Verwendung der WebUI müssen Sie sich im selben Subnetz befinden wie die Trust- oder wireless2-Schnittstelle. Gehen Sie folgendermaßen vor, um mit der WebUI-Verwaltungsanwendung auf das NetScreen-5GT Wireless-Gerät zuzugreifen:

1. Starten Sie den Browser, geben Sie die IP-Adresse für die Trust- oder wireless2-Schnittstelle ins URL-Feld ein, und drücken Sie die EINGABETASTE. Geben Sie z.B. die folgende Adresse in das URL-Feld ein:

192.168.1.1

Die NetScreen-WebUI-Software zeigt die Anmeldeaufforderung an.



Hinweis: Wenn Sie den Assistenten für die Anfangskonfiguration nicht verwenden, wird die WebUI-Anmeldeaufforderung automatisch angezeigt.

2. Wenn Sie den Standardbenutzernamen und das Standardkennwort noch nicht geändert haben, geben Sie **netscreen** in die Felder **User Name** und **Password** ein, und klicken Sie auf **Login**. (Verwenden Sie nur Kleinbuchstaben. Für die Felder „User Name“ und „Password“ muss die Groß-/Kleinschreibung beachtet werden.)

Verwenden von Telnet

Telnet ist eine Anwendung, die Ihnen den Zugriff auf Geräte über ein Internet Protocol (IP)-Netzwerk ermöglicht.

Hinweis: Sie können auch mit SSH-Anwendungen (Secure Shell) auf NetScreen-Geräte zugreifen. Weitere Informationen finden Sie im Kapitel „Verwaltung“ im Band „Verwaltung“ des ScreenOS-Referenzhandbuchs NetScreen-Konzepte und Beispiele für ScreenOS 5.0.0.

Zum Konfigurieren des Geräts mittels Telnet geben Sie in einer Telnet-Sitzung an Ihrer Arbeitsstation ScreenOS-CLI-Befehle (CLI = Befehlszeilenschnittstelle) ein.

1. Starten Sie eine Telnet-Clientanwendung mit der IP-Adresse für die Trust- oder wireless2-Schnittstelle. Geben Sie z.B. Folgendes ein:

```
telnet 192.168.1.1
```

2. Wenn Sie den Standardbenutzernamen und das Standardkennwort noch nicht geändert haben, geben Sie **netscreen** an den Eingabeaufforderungen **Login** und **Password** ein. (Verwenden Sie nur Kleinbuchstaben. Für die Felder „login“ und „password“ muss die Groß-/Kleinschreibung beachtet werden.)

Verwenden einer Konsolenverbindung

Der Konsolenanschluss am NetScreen-5GT Wireless-Gerät ermöglicht Ihnen den Zugriff auf das Gerät über ein serielles mit der Arbeitsstation oder dem Terminal verbundenes Kabel. Zum Konfigurieren des Geräts mithilfe einer Konsolenverbindung geben Sie am Terminal oder in einem Terminalemulationsprogramm auf Ihrer Arbeitsstation ScreenOS-CLI-Befehle ein.

Hinweis: Verwenden Sie für die Konsolenverbindung ein serielles Kabel mit einem RJ-45-Stecker an einem Ende und einem DB-9-Buchsenstecker am anderen Ende. Die Kontaktanordnung der Stecker für das serielle Kabel finden Sie in [Anhang A](#), „Technische Daten“.

So richten Sie eine Konsolenverbindung ein:

1. Schließen Sie den DB-9-Buchsenstecker des seriellen Kabels an den seriellen Anschluss des Computers an. (Vergewissern Sie sich, dass der DB-9-Stecker fest im Anschluss sitzt.)
2. Schließen Sie den RJ-45-Stecker des seriellen Kabels an den Konsolenanschluss des NetScreen-5GT Wireless-Geräts an. (Vergewissern Sie sich, dass der RJ-45-Stecker fest im Anschluss sitzt.)
3. Starten Sie ein serielles Terminalemulationsprogramm. (Ein häufig verwendetes Terminalprogramm ist Hilgreave HyperTerminal.) Die erforderlichen Einstellungen zum Starten einer Konsolensitzung mit Ihrem NetScreen-5GT Wireless-Gerät lauten folgendermaßen:
 - Baudrate: 9600
 - Parität: Nein
 - Datenbits: 8
 - Stoppbit: 1
 - Flusststeuerung: Keine
4. Wenn Sie den Standardbenutzernamen und das Standardkennwort noch nicht geändert haben, geben Sie **netscreen** an den Eingabeaufforderungen **login** und **password** ein. (Verwenden Sie nur Kleinbuchstaben. Für die Felder „login“ und „password“ muss die Groß-/Kleinschreibung beachtet werden.)

ERFORDERLICHE KONFIGURATION

In diesem Abschnitt werden die Konfigurationsschritte beschrieben, die Sie zur Verwendung des Geräts ausführen müssen.

Hinweis: Sollten Sie die Standardeinstellungen des Geräts wiederherstellen müssen, finden Sie Informationen hierzu unter „Zurücksetzen des Geräts auf die werkseitigen Standardeinstellungen“ auf Seite 111.

Ändern des Administratornamens und -kennworts

Da alle NetScreen-Produkte denselben standardmäßigen Administratorknamen und dasselbe Kennwort verwenden (**netscreen**), sollten der Administratorname und das Kennwort sofort geändert werden. So ändern Sie den Administratorknamen und das Kennwort von „netscreen“ und „netscreen“ zu „darwin1“ und „1240jes“:

WebUI

Configuration > Admin > Administrators > Edit (für den NetScreen-Administratorknamen): Geben Sie Folgendes ein, und klicken Sie dann auf **OK**:

Administratorname: darwin1

Altes Kennwort: netscreen

Hinweis: Kennwörter werden während der Eingabe nicht in der WebUI angezeigt.

Neues Kennwort: 1240jes

Neues Kennwort bestätigen: 1240jes

CLI

```
set admin name darwin1
set admin password 1240jes
save
```

Informationen zum Erstellen unterschiedlicher Administratorebenen finden Sie im Kapitel „Verwaltung“ im Band „Verwaltung“ des *ScreenOS-Referenzhandbuchs NetScreen-Konzepte und Beispiele* für ScreenOS 5.0.0.

Einstellen des Datums und der Uhrzeit

Die auf dem NetScreen-Gerät eingestellte Uhrzeit beeinflusst Ereignisse wie die Einrichtung von VPN-Tunneln und die zeitliche Steuerung von Plänen. Die einfachste Methode zum Einstellen des Datums und der Uhrzeit auf dem NetScreen-Gerät ist die Synchronisierung der Systemuhr im NetScreen-Gerät mit der Uhr des Computers. Führen Sie hierzu in der WebUI die folgenden Schritte aus:

1. Configuration > Date/Time: Klicken Sie auf die Schaltfläche **Sync Clock with Client**.
Sie werden gefragt, ob Sie die Sommer-/Winterzeitoption (DTS) auf Ihrem Computer aktiviert haben.
2. Klicken Sie auf **Yes**, um die Systemuhr zu synchronisieren und entsprechend der Sommer-/Winterzeit anzupassen, oder klicken sie auf **No**, um die Systemuhr ohne Anpassung für die Sommer-/Winterzeit zu synchronisieren.

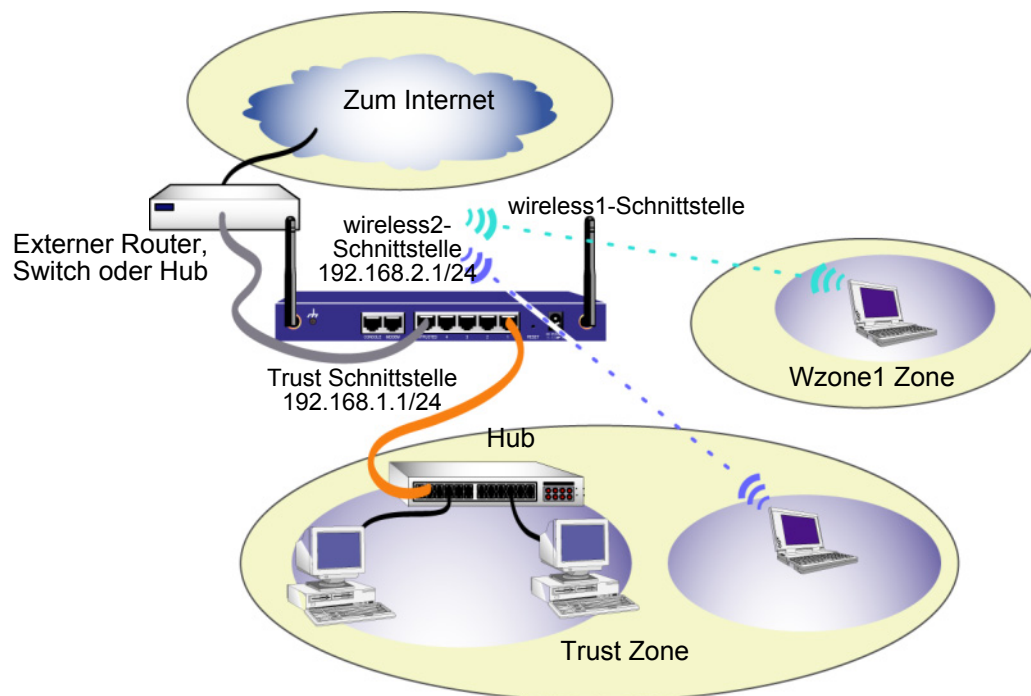
Sie können auch den CLI-Befehl **set clock** in einer Telnet- oder Konsolensitzung verwenden, um das Datum und die Uhrzeit manuell einzugeben.

WIRELESS-KONFIGURATION

In diesem Abschnitt finden Sie Informationen zur Konfiguration der Wireless-Schnittstelle am NetScreen-Gerät. Abhängig vom installierten Lizenztyp können Sie auf einem NetScreen-5GT Wireless-Gerät bis zu vier Wireless-Sicherheitszonen konfigurieren. Die Schnittstellen-zu-Zonen-Bindungen sind vordefiniert und abhängig vom konfigurierten Anschlussmodus; Sie können der nicht vertrauten (untrust) Zone keine Wireless-Schnittstellen zuweisen. Sie müssen mindestens eine Wireless-Schnittstelle auf dem NetScreen-Gerät konfigurieren, damit ein drahtloses lokales Netz (WLAN) erstellt werden kann.

Hinweis: Wenn Sie das NetScreen-5GT Wireless-Gerät außerhalb der Vereinigten Staaten oder Japan verwenden, müssen Sie den Befehl **set wlan country-code** ausführen, bevor eine WLAN-Verbindung hergestellt werden kann. Dieser Befehl stellt den wählbaren Kanalbereich und die Übertragungsleistung ein.

Die folgende Abbildung zeigt die Standardkonfiguration des NetScreen-5GT Wireless-Geräts.



Die standardmäßige Wireless-Schnittstelle hat den vordefinierten Namen „wireless2“. Die Trust- und wireless2-Schnittstellen sind an die Trust Zone gebunden und entsprechend mit den Subnetzadressen 192.168.1.1/24 und 192.168.2.1/24 konfiguriert. Dies bedeutet, dass alle in der Trust Zone verbundenen Geräte sich in demselben Subnetz wie die Trust- bzw. wireless2-Schnittstelle befinden und IP-Adressen in einem der beiden

Subnetze besitzen müssen. Das NetScreen-Gerät ist zudem so konfiguriert, dass es Ihren Geräten IP-Adressen für die Subnetze 192.168.1.1/24 und 192.168.2.1/24 zuordnet. Weitere Informationen hierzu finden Sie unter [„Ändern der Trust- oder Wireless2-Schnittstellenadresse“ auf Seite 111](#).

Standardmäßig ist die wireless1-Schnittstelle an die Wzone1 Zone gebunden und besitzt keine zugewiesene IP-Adresse. Wenn Sie die wireless1-Schnittstelle verwenden wollen, müssen Sie für sie eine IP-Adresse konfigurieren. Weitere Informationen hierzu finden Sie im *NetScreen-5GT Wireless Reference Guide*.

Das NetScreen-Gerät lässt jeden von Geräten in der Trust Zone ausgehenden Verkehrstyp zum Internet zu, aus dem Internet stammender Verkehr kann Ihr Netzwerk jedoch nicht erreichen. Sie können bei Bedarf weitere Beschränkungen konfigurieren. Informationen hierzu finden Sie unter [„Konfigurieren zusätzlicher Richtlinien“ auf Seite 107](#).

Konfigurieren des Wireless-Netzwerks

Wireless-Netzwerke (Drahtlosnetzwerke) bestehen aus Namen, die als Service Set Identifiers (SSIDs) bezeichnet werden. Durch das Festlegen eines SSID haben Sie die Möglichkeit, mehrere drahtlose Netzwerke am selben Standort zu betreiben. An jedem Gerät können maximal acht SSIDs konfiguriert werden. Sobald der SSID-Name eingerichtet ist, können Sie die SSID-Attribute konfigurieren.

Gehen Sie wie folgt vor, um den SSID-Namen **netscreen open** festzulegen, drahtlose Netzwerkverbindungen zu ermöglichen und die wireless2-Schnittstelle zu aktivieren:

WebUI

Wireless > SSID > New: Geben Sie Folgendes ein, und klicken Sie dann auf **OK**:

SSID: „netscreen open“

Wireless Interface Binding: wireless2 (ausgewählt)

Activate Changes > Klicken Sie auf die Schaltfläche **Activate Changes**.

CLI

```
set ssid name "netscreen open"  
set ssid "netscreen open" authentication open encryption  
none  
set ssid "netscreen open" interface wireless2  
exec wlan reactivate
```

Sobald Sie einen SSID für die wireless2-Schnittstelle eingerichtet haben, können Sie auf das Gerät zur Konfiguration mithilfe der standardmäßigen IP-Adresse der wireless2-Schnittstelle zugreifen (schrittweise Anleitungen hierzu finden Sie unter [„Zugriff auf das Gerät“ auf Seite 95](#)). Im *NetScreen-5GT Wireless Reference Guide* finden Sie Konfigurationsbeispiele, SSID-Attribute und CLI-Befehle bzgl. Wireless-Sicherheitskonfigurationen.

ADSL-KONFIGURATION

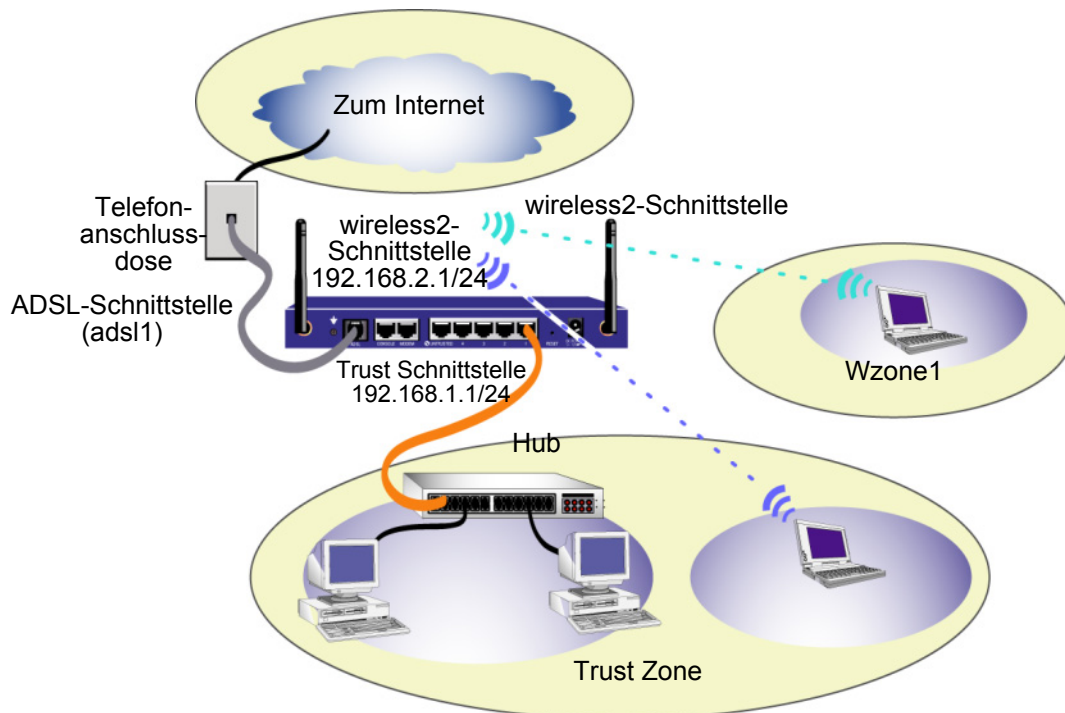
In diesem Abschnitt werden die werkseitigen Standardeinstellungen und der Betrieb der NetScreen-5GT Wireless ADSL Annex A- und Annex B-Geräte in dieser Standardkonfiguration beschrieben. In der Regel sind diese Standardeinstellungen ausreichend, und nur wenige Elemente müssen konfiguriert werden.

In diesem Abschnitt werden die folgenden Konfigurationsschritte für die Schnittstelle der Untrust Zone beschrieben:

- [Konfigurieren der ADSL-Schnittstelle](#)
- [Hinzufügen von virtuellen Verbindungen zu einer ADSL-Schnittstelle](#)
- [VPI/VCI und Multiplexingmethode](#)
- [PPPoE oder PPPoA](#)
- [Annex B-Modus](#)
- [Statische IP-Adresse und Netzmaske](#)

Hinweis: Sollten Sie die Standardeinstellungen des Geräts wiederherstellen müssen, finden Sie Informationen hierzu unter „Zurücksetzen des Geräts auf die werkseitigen Standardeinstellungen“ auf Seite 111.

Die folgende Abbildung zeigt die Standardkonfiguration des NetScreen-5GT Wireless ADSL-Geräts.



Die ADSL-Schnittstelle besitzt den vordefinierten Namen „adsl1“ und ist die Hauptverbindung zwischen dem Netzwerk und dem Internet. Damit das NetScreen-Gerät (und die Geräte im Netzwerk) eine Verbindung mit dem Internet herstellen können, müssen Sie die adsl1-Schnittstelle gemäß den Informationen von Ihrem Dienstanbieter konfigurieren. Siehe [„Konfigurieren der ADSL-Schnittstelle“ auf Seite 102](#).

Das NetScreen-Gerät lässt jeden von Geräten in der Trust Zone ausgehenden Verkehrstyp zum Internet zu, aus dem Internet stammender Verkehr kann Ihr Netzwerk jedoch nicht erreichen. Sie können bei Bedarf weitere Beschränkungen konfigurieren. Informationen hierzu finden Sie unter [„Konfigurieren zusätzlicher Richtlinien“ auf Seite 107](#).

Konfigurieren der ADSL-Schnittstelle

Ihr Netzwerk verwendet die ADSL-Schnittstelle „adsl1“ im NetScreen-Gerät, um über eine virtuelle ATM-Verbindung (ATM = Asynchronous Transfer Mode) eine Verbindung mit dem Netzwerk des Dienstanbieters herzustellen. Sie können weitere virtuelle Verbindungen konfigurieren, indem Sie ADSL-Subschnittstellen erstellen (weitere Informationen finden Sie unter [„Hinzufügen von virtuellen Verbindungen zu einer ADSL-Schnittstelle“ auf Seite 103](#)).

Wechseln Sie in der WebUI zur Seite „Network > Interfaces“, um eine Liste der aktuellen Schnittstellen im NetScreen-Gerät anzuzeigen. Wenn Sie eine Telnet- oder Konsolensitzung verwenden, geben Sie den CLI-Befehl **get interface** ein. Die adsl1-Schnittstelle sollte an die Untrust Zone gebunden sein. Wenn Sie den Assistenten für die Anfangskonfiguration (ICW) zum Konfigurieren des Geräts verwendet haben, sind der adsl1-Schnittstelle u.U. bereits eine IP-Adresse und eine Netzmaske zugeordnet.

***Hinweis:** Wenn Sie die ADSL-Schnittstelle nicht verwenden möchten, können Sie sie mit dem Befehl **set interface adsl1 zone null** an die Null Zone binden. Beim Konfigurieren des Geräts mithilfe des ICW können Sie als Standardschnittstelle zur Untrust Zone eine andere als die ADSL-Schnittstelle festlegen.*

Sie müssen die adsl1-Schnittstelle konfigurieren, um dem NetScreen-Gerät das Herstellen einer Verbindung mit dem Netzwerk des Dienstanbieters zu ermöglichen. Hierzu benötigen Sie zunächst die folgenden Informationen von Ihrem Dienstanbieter:

- VPI- und VCI-Werte (virtuelle Pfad-ID/virtuelle Kanal-ID)
- ATM AAL5-Multiplexingmethode (Asynchronous Transfer Mode Adaptation Layer 5), hierbei kann es sich um Folgendes handeln:
 - Auf eine virtuelle Verbindung (VC) gestütztes Multiplexing. Hierbei wird jedes Protokoll über eine separate virtuelle ATM-Verbindung gesendet.
 - LLC-Einkapselung (Logical Link Control). Hierbei können mehrere Protokolle über dieselbe virtuelle ATM-Verbindung gesendet werden (dies ist die standardmäßige Multiplexingmethode).
- Vom Dienstanbieter zugeordneter Benutzername und Kennwort zum Herstellen einer Verbindung mit dem Netzwerk des Dienstanbieters mittels des PPPoE-Protokolls (Point-to-Point-Protokoll über Ethernet) oder PPPoA-Protokolls (Point-to-Point-Protokoll über ATM)
- Ggf. Authentifizierungsmethode für die PPPoE- oder PPPoA-Verbindung
- Optional eine statische IP-Adresse und ein Netzmaskenwert für Ihr Netzwerk

Hinzufügen von virtuellen Verbindungen zu einer ADSL-Schnittstelle

Zum Hinzufügen von virtuellen Verbindungen erstellen Sie Subschnittstellen für die ADSL-Schnittstelle. Sie können bis zu zehn ADSL-Subschnittstellen erstellen. Zum Erstellen einer neuen an die benutzerdefinierte Zone „Corp1“ gebundene Subschnittstelle namens „adsl1.1“ gehen Sie z.B. folgendermaßen vor:

WebUI

Network > Interfaces > New ADSL Sub-IF: Geben Sie Folgendes ein, und klicken Sie dann auf **Apply**:

Interface Name: adsl1.1

VPI/VCI: 0/35

Zone Name: Corp1 (ausgewählt)

CLI

```
set interface adsl1.1 pvc 0 35 zone corp1
save
```

Eine ADSL-Subschnittstelle muss auf die gleiche Weise konfiguriert werden wie die ADSL-Hauptschnittstelle, d.h., Sie müssen auch wie unter „[Konfigurieren der ADSL-Schnittstelle](#)“ auf Seite 102 beschrieben, die VPI/VCI-Werte einstellen. ADSL-Subschnittstellen können unabhängig von der ADSL-Hauptschnittstelle konfiguriert werden, d.h., Sie können für die Subschnittstelle eine andere Multiplexingmethode, andere VPI/VCI-Werte und einen anderen PPP-Client festlegen. Zudem können Sie auch dann eine statische IP-Adresse für eine Subschnittstelle konfigurieren, wenn die ADSL-Hauptschnittstelle nicht über eine statische IP-Adresse verfügt. Eine Subschnittstelle und die ADSL-Hauptschnittstelle können dieselben VPI/VCI-Werte verwenden, wenn eine Schnittstelle für PPPoA und die andere für PPPoE konfiguriert ist und beide Schnittstellen die LLC-Multiplexingmethode verwenden.

VPI/VCI und Multiplexingmethode

Ihr Dienstanbieter ordnet für jede virtuelle Verbindung ein VPI/VCI-Wertepaar zu. Sie können z.B. das VPI/VCI-Paar 1/1 erhalten. Dies bedeutet, dass der VPI-Wert und der VCI-Wert 1 lauten. Diese Werte müssen mit den Werten übereinstimmen, die der Dienstanbieter auf der Abonentenseite des DSLAM (Digital Subscriber Line Access Multiplexer) konfiguriert hat.

So konfigurieren Sie das VPI/VCI-Paar 1/1 in der adsl1-Schnittstelle:

WebUI

Network > Interfaces > Edit (für die adsl1-Schnittstelle): Geben Sie 1/1 ins VPI/VCI-Feld ein, und klicken Sie dann auf **Apply**.

CLI

```
set interface adsl1 pvc 1 1
save
```

Standardmäßig verwendet das NetScreen-5GT Wireless ADSL-Gerät die LLC-gestützte Multiplexingmethode für jede virtuelle Verbindung. So konfigurieren Sie das VPI/VCI-Paar 1/1 in der adsl1-Schnittstelle, und verwenden Sie die LLC-Einkapselung für die virtuelle Verbindung:

WebUI

Network > Interfaces > Edit (für die adsl1-Schnittstelle): Geben Sie Folgendes ein, und klicken Sie auf **Apply**:

VPI/VCI: 1 / 2

Multiplexing Method: LLC (ausgewählt)

CLI

```
set interface adsl1 pvc 1 1 mux llc
save
```

PPPoE oder PPPoA

Das NetScreen-Gerät enthält sowohl PPPoE- als auch PPPoA-Clients zum Herstellen einer Verbindung mit dem Netzwerk des Diensteanbieters über die ADSL-Verbindung. PPPoE ist die am häufigsten verwendete Form der ADSL-Einkapselung und für die Beendigung an jedem Host im Netzwerk konzipiert. PPPoA wird in erster Linie für Geschäftsklassendienste verwendet, da PPP-Sitzungen am NetScreen-Gerät beendet werden können. Damit das NetScreen-Gerät eine Verbindung mit dem Netzwerk des Diensteanbieters herstellen kann, müssen Sie den vom Diensteanbieter zugeordneten Benutzernamen und das zugehörige Kennwort konfigurieren. Die Konfiguration für PPPoA ähnelt der Konfiguration für PPPoE.

Hinweis: Das NetScreen-Gerät unterstützt nur eine PPPoE-Sitzung für jede virtuelle Verbindung.

So konfigurieren Sie den Benutzernamen „roswell“ und das Kennwort „area51“ für PPPoE und binden Sie die PPPoE-Konfiguration an die adsl1-Schnittstelle:

WebUI

Network > PPPoE > New: Geben Sie Folgendes ein, und klicken Sie dann auf **OK**:

PPPoE Instance: poe1

Bound to Interface: adsl1 (ausgewählt)

Username: roswell

Kennwort: area51

CLI

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1
save
```

Sie können weitere PPPoE- oder PPPoA-Parameter im NetScreen-Gerät konfigurieren, z.B. die Authentifizierungsmethode (standardmäßig unterstützt das NetScreen-Gerät entweder CHAP, Challenge Handshake Authentication-Protokoll, oder PAP, Password Authentication-Protokoll), das Zeitlimit für Inaktivität (Standard ist 30 Minuten) usw. Fragen Sie Ihren Diensteanbieter, ob Sie weitere PPPoE- oder PPPoA-Parameter konfigurieren müssen, um eine einwandfreie Kommunikation mit dem Server des Diensteanbieters zu gewährleisten.

Annex B-Modus

Wenn Sie das Annex B-Modell des NetScreen-5GT Wireless ADSL-Geräts an eine ADSL-Leitung der deutschen Telekom anschließen, müssen Sie die physische Schnittstelle am ADSL-Anschluss für den Betrieb mit diesem Gerät konfigurieren. Gehen Sie hierfür folgendermaßen vor:

WebUI

Network > Interfaces > Edit (für die adsl1-Schnittstelle): Wählen Sie **DT** für den Annex B-Modus, und klicken Sie dann auf **Apply**.

CLI

```
set interface adsl1 phy annex-b-mode dt
save
```

Sie müssen diese Einstellung nicht konfigurieren, wenn Sie das Annex A-Modell des Geräts verwenden oder das Gerät nicht an Geräte der deutschen Telekom anschließen.

Statische IP-Adresse und Netzmaske

Wenn Sie von Ihrem Internetdiensteanbieter eine spezifische statische IP-Adresse und eine Netzmaske für Ihr Netzwerk erhalten haben, dann konfigurieren Sie die IP-Adresse und die Netzmaske für das Netzwerk und die IP-Adresse des mit dem NetScreen-Gerät verbundenen Routeranschlusses. Zudem müssen Sie festlegen, dass das Gerät die statische IP-Adresse verwenden soll. (Das NetScreen-Gerät agiert standardmäßig als PPPoE- oder PPPoA-Client und erhält durch Verhandlungen mit dem PPPoE- oder PPPoA-Server eine IP-Adresse für die ADSL-Schnittstelle.)

So konfigurieren Sie die statische IP-Adresse 1.1.1.1/24 für das Netzwerk:

WebUI

Network > Interfaces > Edit (für die adsl1-Schnittstelle): Geben Sie Folgendes ein, und klicken Sie auf **Apply**:

IP Address/Netmask: 1.1.1.1/24

Static IP: (ausgewählt)

Hinweis: Sie müssen wie im vorhergehenden Abschnitt beschrieben eine PPPoE- oder PPPoA-Instanz konfigurieren und an die adsl1-Schnittstelle binden. Achten Sie darauf, dass Sie „Obtain IP using PPPoE“ oder „Obtain IP using PPPoA“ sowie den Namen der PPPoE- oder PPPoA-Instanz auswählen.

CLI

```
set interface adsl1 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save

oder

set interface adsl1 ip 1.1.1.1/24
set pppoa name poa1 static-ip
save
```

Wenn Sie das DNS (Domain Name System) für die Auflösung von Domännennamen und Adressen verwenden möchten, müssen die Computer in Ihrem Netzwerk die IP-Adresse von mindestens einem DNS-Server enthalten. Wenn dem NetScreen-Gerät über PPPoE oder PPPoA eine IP-Adresse für die ADSL-Schnittstelle zugewiesen wird, erhält es automatisch auch IP-Adressen für die DNS-Server. Weist der DHCP-Server im NetScreen-Gerät den Computern im Netzwerk ihre IP-Adressen zu, erhalten die Computer auch diese DNS-Serveradresse(n).

Wenn Sie der ADSL-Schnittstelle eine statische IP-Adresse zuordnen, muss Ihnen der Dienstanbieter die IP-Adressen der DNS-Server zur Verfügung stellen. Sie können entweder die DNS-Serveradresse auf jedem Computer im Netzwerk konfigurieren, oder Sie können den DHCP-Server in der Trust Zonenschnittstelle so konfigurieren, dass er die DNS-Serveradressen für jeden Computer bereitstellt.

So konfigurieren Sie den DHCP-Server in der Trust Schnittstelle zum Bereitstellen der DNS-Serveradresse 1.1.1.152 für Computer im Netzwerk:

WebUI

Network > DHCP > Edit (für die Trust Schnittstelle) > DHCP Server: Geben Sie 1.1.1.152 für DNS1 ein, und klicken Sie dann auf **Apply**.

CLI

```
set interface trust dhcp server option dns1 1.1.1.152
save
```

OPTIONALE KONFIGURATION

In diesem Abschnitt werden die folgenden bei Bedarf konfigurierbaren Funktionen des NetScreen-5GT Wireless-Geräts beschrieben:

- [Beschränken der Verwaltung](#)
- [Konfigurieren zusätzlicher Richtlinien](#)
- [Betriebsmodus](#)
- [Ändern des Anschlussmodus](#)
- [Konfigurieren einer Untrust Sicherungszonenschnittstelle](#)
- [Ändern der Trust- oder Wireless2-Schnittstellenadresse](#)

Hinweis: In diesem Handbuch werden nicht alle der optionalen Konfigurationsverfahren ausführlich beschrieben. Weitere Informationen finden Sie in den entsprechenden Kapiteln des ScreenOS-Referenzhandbuchs NetScreen-Konzepte und Beispiele für ScreenOS 5.0.0.

Beschränken der Verwaltung

Standardmäßig kann jeder Benutzer im Netzwerk das NetScreen-Gerät verwalten, sofern er den Anmeldenamen und das Kennwort kennt. Sie können das NetScreen-Gerät so konfigurieren, dass es nur über einen oder mehrere bestimmte Hosts im Netzwerk verwaltet werden kann. (Sie können die im NetScreen-Gerät zu aktivierenden Dienste auswählen, z.B. WebUI, Telnet und Ping.)

Weitere Informationen finden Sie im Kapitel „Verwaltung“ im Band „Verwaltung“ des *ScreenOS-Referenzhandbuchs NetScreen-Konzepte und Beispiele* für ScreenOS 5.0.0.

Konfigurieren zusätzlicher Richtlinien

Die NetScreen-5GT Wireless-Geräte sind mit einer Standardrichtlinie konfiguriert, die Arbeitsstationen in der Trust Zone Ihres Netzwerks den Zugriff auf jeden Dienstyp mit externen Computern erlaubt, während externe Computer nicht auf Sitzungen mit Ihren Arbeitsstationen zugreifen oder solche Sitzungen starten können. Sie können Richtlinien konfigurieren, damit das NetScreen-Gerät externen Computern das Starten bestimmter Sitzungstypen mit Ihren Computern erlaubt. Informationen zum Erstellen oder Ändern von Richtlinien finden Sie im Kapitel zu Richtlinien im Band „Grundlagen“ des *ScreenOS-Referenzhandbuchs NetScreen-Konzepte und Beispiele* für ScreenOS 5.0.0.

Betriebsmodus

Der *Betriebsmodus* ist die Art und Weise, wie eine Schnittstelle in einem NetScreen-Gerät Verkehr zwischen Zonen verarbeitet. Standardmäßig arbeiten die NetScreen-5GT Wireless-Geräte im Routemodus, und die Netzwerkadressübersetzung (NAT) ist in der Trust-Schnittstelle aktiviert. Dies bedeutet, dass das NetScreen-Gerät die ursprünglichen Quell-IP-Adressen durch die IP-Adresse der Untrust-Schnittstelle ersetzt, wenn Geräte in der Trust Zone Verkehr an das Internet senden. Das NetScreen-Gerät ordnet den Geräten im Netzwerk private IP-Adressen zu, die für Computer außerhalb Ihres Netzwerks verborgen bleiben.

Wenn alle Geräte im Netzwerk öffentliche IP-Adressen besitzen, können Sie das NetScreen-Gerät für den Routemodus ohne aktivierte NAT konfigurieren. Im Routemodus ohne aktivierte NAT leitet das NetScreen-Gerät Verkehr weiter, indem es IP-Adressen überprüft. Weitere Informationen zum Konfigurieren des Geräts für den Routemodus ohne aktivierte NAT finden Sie im Kapitel „Schnittstellenmodi“ im Band „Grundlagen“ des *ScreenOS-Referenzhandbuchs NetScreen-Konzepte und Beispiele* für ScreenOS 5.0.0.

Ändern des Anschlussmodus

Unter dem *Anschlussmodus* ist die Bindung von physischen Anschlüssen, logischen Schnittstellen und Zonen zu verstehen.

Warnung: Durch das Ändern des Anschlussmodus werden alle vorhandenen Konfigurationen im NetScreen-Gerät entfernt. Der Anschlussmodus sollte daher vor der Konfiguration des Geräts geändert werden.

Die folgende Tabelle enthält eine Zusammenfassung der Anschluss-, Schnittstellen- und Zonenbindungen der auf NetScreen-5GT Wireless-Geräten verfügbaren Anschlussmodi:

Anschlussname ^a	Trust-Untrust Anschlussmodus ^b		Home-Work Anschlussmodus		Trust/Untrust/DMZ (erweiterter) Modus		Dual Untrust-Anschlussmodus		Kombinierter Anschlussmodus	
	Schnittstelle	Zone	Schnittstelle	Zone	Schnittstelle	Zone	Schnittstelle	Zone	Schnittstelle	Zone
1	trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet1	Trust	ethernet1	Work
2	trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet1	Trust	ethernet2	Home
3	trust	Trust	ethernet2	Home	ethernet2	DMZ	ethernet1	Trust	ethernet2	Home
4	trust	Trust	ethernet2	Home	ethernet2	DMZ	ethernet2	Untrust	ethernet3	Untrust
Untrusted	untrust	Untrust	ethernet3	Untrust	ethernet3	Untrust	ethernet3	Untrust	untrust	Untrust
Modem ^c	seriell	Null	seriell	Null	seriell	Null	seriell	Null	seriell	Null
	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1
	wireless2	Trust	wireless2	Work	wireless2	Trust	wireless2	Trust	wireless2	Work
			wireless3	Home	wireless3	DMZ			wireless3	Home
					wireless4	Wzone2				

- Gemäß der Angabe auf dem NetScreen-Gerätechassis
- Standardanschlussmodus.
- Sie können mit dem Ethernet-Anschluss „Untrusted“ oder dem Modemanschluss eine Sicherungsschnittstelle für die Untrust Zone konfigurieren. Siehe „Konfigurieren einer Untrust Sicherungszonenschnittstelle“ auf Seite 110.

Die folgende Tabelle enthält eine Zusammenfassung der Anschluss-, Schnittstellen- und Zonenbindungen der auf NetScreen-5GT Wireless-Geräten ADSL verfügbaren Anschlussmodi:

Anschluss-name ^a	Trust-Untrust Anschlussmodus ^b		Home-Work Anschlussmodus		Trust/Untrust/DMZ (erweiterter) Modus	
	Schnittstelle	Zone	Schnittstelle	Zone	Schnittstelle	Zone
1	trust	Trust	ethernet1	Work	ethernet1	Trust
2	trust	Trust	ethernet1	Work	ethernet1	Trust
3	trust	Trust	ethernet2	Home	ethernet2	DMZ
4	trust	Trust	ethernet2	Home	ethernet2	DMZ
Untrusted	untrust	Null ^c	ethernet3	Null ^c	ethernet3	Null ^c
Modem	seriell	Null ^c	seriell	Null ^c	seriell	Null ^c
ADSL	adsl1	Untrust	adsl1	Untrust	adsl1	Untrust
	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1
	wireless2	Trust	wireless2	Work	wireless2	Trust
			wireless3	Home	wireless3	DMZ
				wireless4	Wzone2	

a. Gemäß der Angabe auf dem NetScreen-Gerätechassis

b. Standardanschlussmodus.

c. Sie können mit dem Ethernet-Anschluss „Untrusted“ oder dem Modemanschluss eine Sicherungsschnittstelle für die Untrust Zone konfigurieren. Siehe „Konfigurieren einer Untrust Sicherungszonenschnittstelle“ auf Seite 110.

So stellen Sie das NetScreen-Gerät auf den Home-Work Anschlussmodus ein:

WebUI

Configuration > Port Mode: Wählen Sie in der Dropdown-Liste die Option „Home-Work“, und klicken Sie dann auf **Apply**.

Klicken Sie an der folgenden Eingabeaufforderung auf **OK**:

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

CLI

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

Geben Sie an der folgenden Eingabeaufforderung **y** (für yes) ein:

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

Konfigurieren einer Untrust Sicherungszonenschnittstelle

Standardmäßig ist auf einem NetScreen-5GT Wireless ADSL-Gerät die adsl1-Schnittstelle die primäre Verbindung mit einem externen Netzwerk. Jeder im NetScreen-5GT Wireless ADSL-Gerät verfügbare Anschlussmodus ermöglicht Ihnen das Anschließen des Ethernet-Anschlusses „Untrusted“ oder des Modemanschlusses als Sicherungsverbindung mit dem externen Netzwerk (siehe „[Ändern des Anschlussmodus](#)“ auf Seite 108). Sie müssen die Sicherungsschnittstelle an die Untrust Zone binden und entsprechend konfigurieren.

Hinweis: Sie können nur eine Sicherungsschnittstelle unter Verwendung des Ethernet-Anschlusses „Untrusted“ oder des Modemanschlusses konfigurieren. Wenn Sie den Anschluss „Untrusted“ für die Sicherungsverbindung verwenden, konfigurieren Sie die Untrust-Schnittstelle im Anschlussmodus „Trust-Untrust“ oder die ethernet3-Schnittstelle für andere Anschlussmodi. Bei Verwendung des Modemanschlusses für die Sicherungsverbindung konfigurieren Sie die Serial-Schnittstelle für alle Anschlussmodi.

So binden Sie z.B. die Untrust-Schnittstelle an die Untrust Zone:

WebUI

Network > Interfaces > Edit (für die Untrust-Schnittstelle): Wählen Sie in der Dropdown-Liste „Zone Name“ den Eintrag **Untrust** aus, und klicken Sie dann auf **OK**.

CLI

```
set interface untrust zone untrust
save
```

Sie müssen auch eine statische IP-Adresse für die Untrust-Schnittstelle angeben oder festlegen, ob die IP-Adresse für die Schnittstelle über DHCP oder PPPoE abgerufen wird. Weitere Informationen zum Konfigurieren von Schnittstellenparametern finden Sie im Kapitel „Schnittstellen“ im Band „Grundlagen“ des *ScreenOS-Referenzhandbuchs NetScreen-Konzepte und Beispiele* für ScreenOS 5.0.0.

Wenn die adsl1-Schnittstelle und die Ethernet-Schnittstelle („untrust“ oder „ethernet3“, je nach Anschlussmodus) oder die serial-Schnittstelle an die Untrust Zone gebunden sind, wird die Failover-Funktion für Schnittstellen automatisch konfiguriert. Dies bedeutet, dass das NetScreen-Gerät den Verkehr automatisch an die Sicherungsschnittstelle sendet, wenn die adsl1-Schnittstelle nicht verfügbar ist. Wenn die adsl1-Schnittstelle wieder verfügbar ist, sendet das Gerät den Verkehr automatisch wieder an die adsl1-Schnittstelle.

Hinweis: Nur die adsl1-Schnittstelle ist vom Failover betroffen. Konfigurierte ADSL-Subschnittstellen werden daher nicht per Failover auf die Sicherungsschnittstelle umgeschaltet.

Sie können ein Failover auch manuell erzwingen und dann mittels Failback wieder auf die adsl1-Schnittstelle umschalten. Weitere Informationen finden Sie im Kapitel über die Schnittstellenredundanz im Band „Hohe Verfügbarkeit“ des *ScreenOS-Referenzhandbuchs NetScreen-Konzepte und Beispiele* für ScreenOS 5.0.0.

Ändern der Trust- oder Wireless2-Schnittstellenadresse

Sie können die IP-Adresse und die Netzmaske der Trust- und Wireless-Schnittstelle bei Bedarf ändern. (Bedenken Sie, dass die IP-Adressen von Geräten im Netzwerk niemals für Computer außerhalb des Netzwerks sichtbar sind, wenn die Trust- oder Wireless-Schnittstelle im NAT-Modus betrieben wird. Externe Computer sehen nur die IP-Adresse der Untrust-Schnittstelle.) Möglicherweise müssen Sie die Trust- oder wireless2-Schnittstelle ändern, um die Übereinstimmung mit den bereits im Netzwerk vorhandenen IP-Adressen zu gewährleisten. Wenn Sie die IP-Adresse und Netzmaske der Trust- oder wireless2-Schnittstelle ändern, müssen Sie auch den vom NetScreen-Gerät über DHCP für Geräte im Netzwerk zugewiesenen Adressbereich ändern oder den DHCP-Server in der Trust- oder wireless2-Schnittstelle deaktivieren.

Wenn der DHCP-Server im NetScreen-Gerät den Computern im Netzwerk ihre IP-Adressen zuweist, erhalten die Computer auch ihr Standardgateway vom NetScreen-Gerät. Besitzt ein Computer eine statisch zugeordnete IP-Adresse, müssen Sie sein Standardgateway manuell auf die IP-Adresse der Trust- oder wireless2-Schnittstelle im NetScreen Gerät einstellen.

Informationen zum Zuordnen einer anderen IP-Adresse und Netzmaske zur Trust- oder wireless2-Schnittstelle finden Sie im Kapitel „Schnittstellen“ im Band „Grundlagen“ des *ScreenOS-Referenzhandbuchs NetScreen-Konzepte und Beispiele* für ScreenOS 5.0.0.

Informationen zum Ändern der DHCP-Einstellungen für das NetScreen-Gerät finden Sie im Kapitel „Systemparameter“ im Band „Grundlagen“ des *ScreenOS-Referenzhandbuchs NetScreen-Konzepte und Beispiele* für ScreenOS 5.0.0.

ÜBERPRÜFEN DER EXTERNEN VERBINDUNG

Um zu überprüfen, ob die Arbeitsstationen in Ihrem Netzwerk auf Ressourcen im Internet zugreifen können, starten Sie auf einer Arbeitsstation im Netzwerk einen Webbrowser, und geben Sie den folgenden URL ein: www.juniper.net.

ZURÜCKSETZEN DES GERÄTS AUF DIE WERKSEITIGEN STANDARDEINSTELLUNGEN

Wenn Sie das Administratorkennwort verlieren oder vergessen, können Sie das NetScreen-Gerät auf die Standardeinstellungen zurücksetzen. Dadurch gehen alle vorhandenen Konfigurationen verloren, der Zugriff auf das Gerät ist jedoch wieder möglich.

Warnung: Durch das Zurücksetzen des Geräts werden alle vorhandenen Konfigurationseinstellungen gelöscht, und die vorhandene Firewall und der VPN-Dienst funktionieren nicht mehr.

Zum Wiederherstellen der Standardeinstellungen des Geräts stehen Ihnen folgende Methoden zur Auswahl:

- Verwenden einer Konsolenverbindung. Weitere Informationen finden Sie im Kapitel „Verwaltung“ im Band „Verwaltung“ des *ScreenOS-Referenzhandbuchs NetScreen-Konzepte und Beispiele* für ScreenOS 5.0.0.
- Verwenden des Reset-Stiftlochs an der Rückseite des Geräts wie im folgenden Abschnitt beschrieben.

Verwenden des Reset-Stiftlochs

Sie können das Gerät zurücksetzen und die werkseitigen Standardeinstellungen wiederherstellen, indem Sie das Reset-Stiftloch betätigen. Hierzu müssen Sie entweder die Gerätestatus-LEDs am Bedienfeld überprüfen oder wie in [„Verwenden einer Konsolenverbindung“ auf Seite 97](#) beschrieben eine Konsolensitzung starten.

1. Machen Sie das Reset-Stiftloch an der Rückseite des Geräts ausfindig. Drücken Sie einen dünnen festen Draht (z.B. eine Büroklammer) vier bis sechs Sekunden lang in das Stiftloch.



Die Status-LED blinkt gelb. Durch eine Meldung auf der Konsole wird angezeigt, dass die Löschung der Konfiguration gestartet wurde, und das System sendet eine SNMP/SYSLOG-Benachrichtigung.

2. Warten Sie ein bis zwei Sekunden.

Nach dem ersten Zurücksetzen blinkt die Status-LED grün. Das Gerät wartet jetzt auf das zweite Zurücksetzen. In der Konsolenmeldung werden Sie nun darauf hingewiesen, dass das Gerät auf eine zweite Bestätigung wartet.

3. Betätigen Sie das Reset-Stiftloch erneut vier bis sechs Sekunden lang.

Die Konsolenmeldung verifiziert die zweite Bestätigung. Die Status-LED leuchtet kurz gelb auf und blinkt dann wieder grün.

Das Gerät wird dann auf seine ursprünglichen Werkseinstellungen zurückgesetzt. Beim Zurücksetzen des Geräts leuchtet die Status-LED kurz gelb auf und leuchtet dann wieder grün. Die Konsole zeigt Gerätestartmeldungen an. Das System sendet SNMP- und SYSLOG-Benachrichtigungen an konfigurierte SYSLOG- oder SNMP-Trap-Hosts.

Nachdem das Gerät neu gestartet wurde, zeigt die Konsole die Anmeldeaufforderung für das Gerät an. Die Status-LED blinkt nun grün.

Wenn Sie nicht die vollständige Zurücksetzsequenz ausführen, wird der Vorgang ohne Konfigurationsänderung abgebrochen, und in der Konsolenmeldung werden Sie darauf hingewiesen, dass die Löschung der Konfiguration abgebrochen wird. Die Status-LED blinkt dann wieder grün. Wenn das Gerät nicht zurückgesetzt wurde, wird zur Bestätigung dieses Fehlers eine SNMP-Benachrichtigung gesendet.

Hardwarebeschreibungen

Dieses Kapitel enthält Beschreibungen des NetScreen-5GT Wireless-Chassis.

VERBINDUNGS- UND NETZANSCHLÜSSE

An der Rückseite des NetScreen-5GT Wireless-Geräts befinden sich Verbindungs- und Netzanschlüsse.

Antenne B

Antenne A



Die Gleichspannungsbuchse dient zur Verbindung des NetScreen-5GT Wireless-Geräts mit einer Stromquelle. Das Reset-Stiftloch ermöglicht Ihnen das Zurücksetzen des Geräts und Wiederherstellen der werkseitigen Standardeinstellungen. Das NetScreen-5GT Wireless-Gerät enthält die folgenden Anschlüsse:

Anschluss	Beschreibung	Stecker	Geschwindigkeit/ Protokoll
ADSL	Falls zutreffend, ermöglicht eine Internetverbindung über eine ADSL-Datenverbindung.	RJ-11 (Annex A) RJ-45 (Annex B)	ANSI T1.413 Ausgabe 2 ITU G.992.1 (G.dmt) ITU 992.2 (G.lite)
Console	Ermöglicht eine serielle Verbindung mit dem System. Dient zum Starten von CLI-Sitzungen (Befehlszeilenschnittstelle).	RJ-45	9600 Bit/s RS-232
Modem	Ermöglicht eine serielle Sicherungs-DFÜ-Internetverbindung über ein externes Modem.	RJ-45	9600 Bit/s - 115 kBit/s RS-232
Untrusted	Ermöglicht eine primäre oder Sicherungs-Internet- oder ungesicherte Netzwerkverbindung über einen externen Router oder ein DSL- oder Kabelmodem.	RJ-45	10/100 MBit/s Ethernet Automatische Erkennung von Duplex und Polarität
Anschlüsse 1 – 4	Ermöglichen direkte Verbindungen mit Arbeitsstationen oder eine LAN-Verbindung über einen Switch oder ein Hub. Mithilfe dieser Verbindung kann das Gerät auch über eine Telnet-Sitzung oder die WebUI-Verwaltungsanwendung verwaltet werden.	RJ-45	10/100 MBit/s Ethernet Automatische Erkennung von Duplex und Polarität
Antenne A und B	Ermöglichen direkte Verbindungen mit Arbeitsstationen in der Nähe einer drahtlosen Funkverbindung. Mithilfe dieser Verbindung kann das Gerät über eine Telnet-Sitzung oder die WebUI-Verwaltungsanwendung verwaltet werden.	RPSMA	802.11b 802.11g

Warnung: Schließen Sie keine Telefonleitung oder ISDN-Leitung direkt an den Modemanschluss des NetScreen-5GT Wireless-Geräts an. Sie müssen das Gerät zuerst mittels eines RS-232-Anschlusses mit einem Modem verbinden, bevor Sie das Modem an die Leitung anschließen.

STATUS-LEDs

Das Bedienfeld des NetScreen-5GT Wireless-Geräts enthält Strom- und Status-LEDs für das Gerät sowie Anschlussstatus-LEDs für die Schnittstellen.



Hauptstatus-LEDs für das Gerät

Die Gerätestatus-LEDs zeigen an, ob das Gerät korrekt funktioniert. Die folgende Tabelle beschreibt den Status für jede LED.

LED	Status	Bedeutung
POWER	Grün	Das System wird mit Strom versorgt.
	Aus	Das System wird nicht mit Strom versorgt.
STATUS	Blinkt grün	Das System funktioniert einwandfrei.
	Grün	Das System wird gestartet.
	Rot	Ein Diagnose- oder Systeminitialisierungsfehler liegt vor.
	Aus	Das System ist nicht betriebsbereit.
ADSL (nur bei Wireless ADSL)	Grün	Die ADSL-Schleife ist aktiv.
	Aus	Die ADSL-Schleife ist inaktiv.
WLAN	Blinkt langsam grün	Die Wireless-Verbindung ist hergestellt, aber es liegt keine Verbindungsaktivität vor.
	Blinkt schnell grün	Eine Wireless-Verbindung ist hergestellt. Die Blinkrate verhält sich proportional zur Verbindungsaktivität.
	Aus	Es ist keine Wireless-Verbindung hergestellt.

Anschlussstatus-LEDs

Die Anschlussstatus-LEDs zeigen an, ob die Anschlüsse des Geräts korrekt funktionieren. Die folgende Tabelle beschreibt die möglichen Statusoptionen für die Anschluss-LEDs.

LED	LED-Farbe	Bedeutung der LED
Link/Activity	Blinkt grün	Das Gerät erkennt Ethernet-Verkehr zum Anschluss.
	Aus	Der Anschluss hat keine Verbindung mit einem anderen Gerät hergestellt.
	Grün	Der Anschluss hat eine Verbindung mit einem anderen Gerät hergestellt.
10/100	Grün	Der Anschluss ist mit einem 100 Base-T-Gerät verbunden.
	Aus	Der Anschluss ist mit einem 10 Base-T-Gerät verbunden.



Technische Daten

Dieser Anhang enthält allgemeine technische Systemdaten für das NetScreen-5GT Wireless-Gerät.

Attribute

Höhe	2,93 cm	1,15 Zoll
Tiefe	18,45 cm	7,26 Zoll
Breite	20,8 cm	8,19 Zoll
Gewicht	0,9 kg	1,98 US-Pounds

Elektrik

Schaltregler	Wechselstromadapter: 100 V - 240 V +/- 10 % 50/60 Hz, 15-18 Watt Gleichstromeingang: 12 Volt 1,25 - 1,5 Amp
--------------	---

Umgebung

Normale Höhe	0-40° C, 32-105° F
Relative Luftfeuchtigkeit	10-90%
Nicht kondensierend	10-90%

Die maximale normale Höhe ü.M. beträgt 2.000 m (6.562 Fuß)

Zertifizierungen

Sicherheit	UL, CUL, TUV, CE, CB
EMI	FCC Teil 15 Klasse B, VCCI, CE

Ethernet-Stecker

Standard	100Base-TX
Medientyp	Kategorie 5 und höher Nicht abgeschirmtes Twisted-Pair-Kabel (UTP)
Maximaler Abstand	100 m (328,08 Fuß)

Die Twisted-Pair-RJ-45-Anschlüsse sind mit dem Standard IEEE 802.3 Typ 10/100 Base-T kompatibel.

ADSL-Stecker

Typen	RJ-11-Stecker mit 6 Pins für Annex A RJ-45-Stecker für Annex B
Medientyp	Standardmäßiges Telefonkabel

KONSOLEN- UND MODEMADAPTERVERBINDUNGEN

Die folgende Tabelle enthält die Definitionen der RJ-45-Anschlüsse. Zur Verwendung eines Standard-UART-Anschlusses wird diese Konfiguration sowohl für den Konsolen- als auch den Modemanschluss verwendet.

RJ-45	Signal	Abkürzung	DCE
1	Request To Send	RTS	In
2	Data Terminal Ready	DTR	In
3	Transmitted Data	TD	In
4, 5	Signal Ground	SGND	Nicht zutreffend
6	Received Data	RD	Out
7	Not Connected		
8	Clear To Send	CTS	Out

Die folgende Tabelle enthält die Definitionen für die RJ-45-nach-DB-9-Adapterverbindungen. Zur Verwendung eines Standard-UART-Anschlusses muss diese Konfiguration sowohl für den Konsolen- als auch den Modemanschluss verwendet werden.

DB9	Signal	Abkürzung	DTE	DCE	RJ45
1	Data Carrier Detect (Datenträgererkennung)	DCD	In	Out	NC
2	Received Data	RD	In	Out	3
3	Transmitted Data	TD	Out	In	6
4	Data Terminal Ready	DTR	Out	In	7
5	Signal Ground	SGND	Nicht zutreffend	Nicht zutreffend	4
6	Data Set Ready (Datensatz bereit)	DSR	In	Out	2
7	Request To Send	RTS	Out	In	8
8	Clear To Send	CTS	In	Out	1
9	Ring Indicator (Anrufanzeige)	RI	In	Out	NC

Hinweis: Wenn Sie das mit dem NetScreen-Gerät gelieferte Konsolenkabel zum Anschließen eines Modems verwenden, müssen Sie am Modemanschluss einen Nullmodemadapter installieren.

Index

A

- AAL5-Multiplexing 102
- Administratorname, ändern 98
- Adresse der Trust Zonenschnittstelle 111
- ADSL
 - Anschluss verbinden 89
 - Kabel anschließen 89
 - Schnittstelle konfigurieren 102
- Ändern des Anmeldenamens und Kennworts 98
- Ändern des Anschlussmodus 108
- Annex A 89
- Annex B 89
 - für die deutsche Telekom konfigurieren 105
- Anschließen der Stromversorgung 92
- Anschlüsse
 - Port 115
 - Stromversorgung 115
- Anschlussmodus, ändern 108
- Anschlussstatus-LEDs 117
- Antennen 91
- ATM Adaptation Layer 5 102
- Aufbau des Handbuchs 85

B

- Beschränken der Verwaltung auf einen spezifischen Host 107

D

- Datum, einstellen 98
- DB-9-Anschluss 120
- Deutsche Telekom, Konfigurieren von Annex B 105

E

- Einstellen der Geräteuhr 98

G

- Gestellmontage des Geräts 92

H

- Hinzufügen von Virtuellen Verbindungen 103

K

- Kennwort, ändern 98
- Konfiguration
 - Drahtloses Netzwerk 99
 - erforderlich 97, 101
 - optional 106
 - SSID 100
 - Standardeinstellungen 101
- Konsole, verwenden 97
- Konventionen 95
 - CLI 86
 - WebUI 86

L

- LEDs
 - Anschlussstatus 117
 - Status 116

M

- Mikrofilter 90
- Montieren des Geräts im Gestell 92
- Multiplexing, konfigurieren 103

N

- NetScreen-Publikationen 87
- Netzanschlüsse 115

P

- Point-to-Point-Protokoll über ATM
 - Siehe* PPPoA
- Point-to-Point-Protokoll über Ethernet
 - Siehe* PPPoE
- PPPoA 102
 - konfigurieren 104
- PPPoE 102
 - konfigurieren 104

R

- Registrieren des Geräts 95
- Reset-Stiftloch, Verwenden 112

Richtlinien, Konfigurieren zusätzlicher [107](#)

RJ-45-Anschluss [120](#)

Routenmodus [107](#)

S

Service Set Identifier

siehe [SSID](#)

Sicherungsschnittstelle für die Untrust Zone [110](#)

Signalsplitter [90](#)

SSID, Service Set Identifier [100](#)

Standardeinstellungen [101](#)

Wiederherstellen [111](#)

statische IP-Adresse [102](#)

konfigurieren [105](#)

Status-LEDs [116](#)

Stromversorgung, Anschließen [92](#)

T

Telnet, verwenden [96](#)

transparenter Modus [107](#)

Trust Ethernet-Anschlüsse [91](#)

U

Überprüfen der Verbindung [111](#)

Uhrzeit, einstellen [98](#)

Untrust Zone, Konfigurieren einer

Sicherungsschnittstelle [110](#)

Untrusted-Anschluss [91](#)

V

Verbindungsanschlüsse [115](#)

Verwalten des Geräts über einen spezifischen

Host [107](#)

Virtuelle Pfad-ID/Virtuelle Kanal-ID

Siehe [VPI/VCI](#)

Virtuelle Verbindung, Hinzufügen [103](#)

VPI/VCI [102](#)

konfigurieren [103](#)

W

WebUI

Zugriff auf [95](#)

WebUI, Konventionen [86](#)

Wiederherstellen der Standardeinstellungen [111](#)

Wireless

Anschließen [89, 91](#)

Antennen [91](#)

Konfiguration [99](#)

Trust Zone [100](#)

Verwenden der Standardschnittstelle [91](#)

Wzone1 Zone [100](#)

wireless2-Schnittstelle [100](#)

Ändern von Schnittstellenadressen [111](#)

Bindungen an Zonen [100](#)

Einstellen des SSID für [100](#)

Trust Zone [100](#)

Zugriff auf [95](#)

Z

Zugriffspunkte [99](#)

Contenido

Prefacio	125
Organización	125
Convenciones de la interfaz gráfica (WebUI)	126
Convenciones de la interfaz de línea de comandos (CLI)	126
Publicaciones de NetScreen	127
Capítulo 1 Conexión del dispositivo	129
Conexión del dispositivo NetScreen a la red	129
Conexión del dispositivo a una red sin confianza	129
Conexión del puerto ADSL	129
Conexión del puerto sin confianza	131
Conexión del dispositivo a la red interna o a estaciones de trabajo	131
Conexión de los puertos Ethernet de confianza	131
Utilización de la interfaz inalámbrica	131
Conexión de la alimentación	132
Montaje en bastidor (opcional)	132
Capítulo 2 Configuración del dispositivo	135
Acceso al dispositivo	135
Utilización de la interfaz WebUI	136
Utilización de Telnet.....	136
Utilización de una conexión de consola.....	137
Configuración requerida	137
Cambio de nombre y contraseña del administrador	138
Ajuste de la fecha y la hora.....	138
Configuración inalámbrica	139
Configuración de la red inalámbrica	140
Configuración de ADSL	141
Configuración de la interfaz ADSL.....	142
Inclusión de circuitos virtuales en una interfaz ADSL	143
Método VPI/VCI y multiplexado	143
PPPoE o PPPoA	144
Modo de Anexo B.....	145
Dirección IP estática y máscara de red.....	145
Configuración opcional	146
Restricción de administración	147
Configuración de directivas adicionales.....	147
Modo de funcionamiento	147
Cambio del modo de puerto.....	148
Configuración de una interfaz de zona Untrust de respaldo	150

Cambio de la dirección de interfaz Trust o Wireless2	151
Verificación de la conectividad externa	151
Restauración de los ajustes predeterminados de fábrica	151
Utilización del orificio de restablecimiento.....	152
Capítulo 3 Descripciones del hardware	155
Conector de alimentación y puertos	155
Diodos LED de estado	156
Diodos LED de estado principales del dispositivo	157
Diodos LED de estado de los puertos.....	157
Apéndice A Ficha técnica.....	159
Índice	161

Prefacio

El dispositivo NetScreen-5GT Wireless de Juniper Networks ofrece servicios de red privada virtual (VPN) IPsec y de cortafuegos para sucursales o establecimientos minoristas que utilizan una interfaz inalámbrica integrada 802.11b/g. El dispositivo NetScreen-5GT Wireless utiliza el mismo cortafuegos, la misma VPN, el mismo antivirus, la misma inspección minuciosa (“deep inspection”) y la misma tecnología de gestión del tráfico que los productos de gama alta para estaciones centrales de NetScreen.

Juniper Networks ofrece tres modelos del dispositivo NetScreen-5GT Wireless:

- **NetScreen-5GT Wireless:** El modelo sólo Wireless.
- **NetScreen-5GT Wireless ADSL A:** El modelo Wireless con Anexo A acepta la tecnología ADSL en líneas telefónicas estándar (POTS).
- **NetScreen-5GT Wireless ADSL B:** El modelo Wireless con Anexo B acepta la tecnología ADSL en redes digitales de servicios integrados (ISDN).

Todos los modelos admiten hasta cuatro zonas de seguridad inalámbrica. Los dos modelos ADSL admiten las normas ANSI T1.413 Issue 2, ITU G.992.1 (G.dmt) e ITU 992.2 (G.lite).

Cada modelo admite tres versiones de software:

- La versión para 10 usuarios admite un máximo de 10 usuarios.
- La versión Plus admite un número ilimitado de usuarios.
- La versión Extended ofrece las mismas funciones que la versión Plus y estas otras características: alta disponibilidad (NSRP Lite), zona de seguridad DMZ, y capacidad de sesiones y túneles adicionales.

ORGANIZACIÓN

Este manual se compone de tres capítulos y un apéndice.

Capítulo 1, En “[Conexión del dispositivo](#)” se describe cómo conectar el dispositivo a la red, cómo conectar la alimentación y la antena y cómo instalar el dispositivo NetScreen-5GT Wireless en un bastidor.

Capítulo 2, En “[Configuración del dispositivo](#)” se describen los ajustes predeterminados y el manejo del NetScreen-5GT Wireless (ADSL), así como la configuración necesaria para utilizar el dispositivo.

Capítulo 3, En “[Descripciones del hardware](#)” se ofrece una vista general de los puertos, los diodos LED y los requisitos de alimentación del NetScreen-5GT Wireless.

Apéndice A, En “[Apéndice A Ficha técnica](#)” se proporciona una lista de las especificaciones físicas del dispositivo NetScreen-5GT Wireless.

CONVENCIONES DE LA INTERFAZ GRÁFICA (WEBUI)

En este manual se utilizan ángulos (>) para indicar las rutas de navegación de la WebUI por las que se pasa al seleccionar opciones de menú y vínculos.

Ejemplo: Objects > Addresses > List > New

Para acceder al cuadro de diálogo de configuración de nuevas direcciones:

1. Haga clic en **Objects** en la columna de menú.
La opción de menú Objects se desplegará para mostrar las opciones subordinadas que contiene.
2. (Menú Applet¹) Sitúe el mouse sobre **Addresses**.
(Menú DHTML) Haga clic en **Addresses**.
La opción de menú Addresses se desplegará para mostrar las opciones subordinadas que contiene.
3. Haga clic en **List**.
Aparecerá la tabla de libretas de direcciones.
4. Haga clic en el vínculo **New** situado en la esquina superior derecha.
Aparecerá el cuadro de diálogo de configuración de nuevas direcciones.

CONVENCIONES DE LA INTERFAZ DE LÍNEA DE COMANDOS (CLI)

Para presentar la sintaxis de los comandos de la interfaz de línea de comandos (CLI) se utilizan las siguientes convenciones:

- Los elementos entre corchetes [] son opcionales.
- Los elementos entre llaves { } son obligatorios.
- Si existen dos o más opciones alternativas, aparecerán separadas entre sí por barras verticales (|). Por ejemplo:

```
set interface { ethernet1 | ethernet2 | ethernet3 }  
manage
```

significa “establecer las opciones de administración de la interfaz ethernet1, ethernet2 o ethernet3”.

- Las variables aparecen en *cursiva*. Por ejemplo:

```
set admin user name1 password xyz
```

1. Podrá seleccionar el tipo de menú Applet o DHTML haciendo clic en la opción **Toggle Menu** situada en la parte inferior de la columna de menú.

Los comandos CLI insertados en el contexto de una frase aparecen en **negrita** (salvo en el caso de las variables, que siempre aparecen en *cursiva*). Por ejemplo: “Utilice el comando **get system** para mostrar el número de serie de un dispositivo NetScreen”.

***Nota:** Para escribir palabras clave, basta con introducir los primeros caracteres que permitan al sistema reconocer de forma inequívoca la palabra que se está introduciendo. Por ejemplo, es suficiente escribir **set adm u joe j12fmt54** para que el sistema reconozca el comando **set admin user joe j12fmt54**. Aunque este método se puede utilizar para introducir comandos, en la presente documentación todos ellos se representan con sus palabras completas.*

PUBLICACIONES DE NETSCREEN

Para obtener documentación técnica sobre cualquier producto NetScreen de Juniper Networks, visite www.juniper.net/techpubs/.

Para obtener soporte técnico, abra un expediente de soporte utilizando el vínculo “Case Manager” en la página web <http://www.juniper.net/support/> o llame al teléfono 1-888-314-JTAC (si llama desde los EE.UU.) o al +1-408-745-9500 (si llama desde fuera de los EE.UU.).

Si encuentra algún error u omisión en esta documentación, póngase en contacto con nosotros a través de la siguiente dirección de correo electrónico:

techpubs-comments@juniper.net

Conexión del dispositivo

En este capítulo se describe la conexión del dispositivo NetScreen-5GT Wireless a la red, a la fuente de alimentación y la conexión de una antena. Para utilizar el juego opcional de montaje en bastidor de NetScreen-5GT Wireless, consulte las instrucciones para el montaje en bastidor que se incluyen al final de este capítulo.

***Nota:** Para obtener información sobre las advertencias e instrucciones de seguridad, consulte el Manual de seguridad de NetScreen. Las instrucciones incluidas en este manual advierten sobre situaciones que podrían provocar lesiones físicas. Antes de utilizar cualquier equipo, tenga en cuenta los peligros que entraña el sistema de circuitos eléctricos y familiarícese con las prácticas habituales de prevención de accidentes.*

CONEXIÓN DEL DISPOSITIVO NETSCREEN A LA RED

El dispositivo NetScreen proporciona protección de cortafuegos y seguridad general para las redes cuando se coloca entre las redes internas y la red sin confianza. En esta sección se describen las conexiones físicas.

Conexión del dispositivo a una red sin confianza

Según el modelo que tenga del dispositivo NetScreen-5GT Wireless, puede conectarse a una red sin confianza de una de las siguientes maneras:

- Mediante una conexión ADSL desde el puerto ADSL del dispositivo NetScreen
- Mediante una conexión Ethernet desde el puerto sin confianza del dispositivo NetScreen

Conexión del puerto ADSL

Conecte el cable ADSL suministrado desde el puerto ADSL del dispositivo NetScreen-5GT Wireless ADSL a la toma de teléfono. El puerto ADSL de la versión de Anexo A del dispositivo utiliza un conector RJ-11. Sin embargo, la versión de Anexo B utiliza un conector RJ-45. Para los modelos de Anexo B, el cable de conexión desde el puerto ADSL a la toma de teléfono tiene la misma apariencia y el mismo tipo de cables que un cable directo Ethernet 10 Base-T.

***Aviso:** Tenga cuidado de no conectar los puertos de la consola, el módem o Ethernet del dispositivo NetScreen a la toma de teléfono.*

En el dispositivo NetScreen-5GT Wireless ADSL, la línea ADSL es la conexión *principal* a una red exterior. Para realizar una conexión de datos de respaldo a una red exterior, puede conectar un cable Ethernet desde el puerto sin confianza del dispositivo NetScreen-5GT Wireless ADSL a un enrutador externo, módem DSL o módem de cable, o bien puede conectar un cable serie desde el puerto del módem a un módem externo.

Aviso: No será posible conectar tanto el puerto sin confianza como el puerto del módem del dispositivo a una red exterior al mismo tiempo.

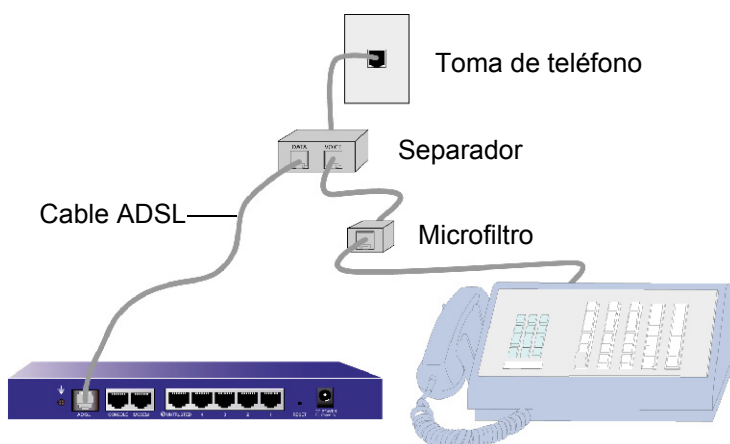
Conexión de separadores y microfiltros

Un *separador de señal* divide la señal telefónica en señales de voz de baja frecuencia para las llamadas de voz y en señales de datos de alta frecuencia para el tráfico de datos. Los proveedores de telefonía normalmente instalan los separadores (“splitters”) como parte del equipo que conecta las líneas telefónicas del lugar a la red del proveedor.

Hay separadores que los usuarios pueden instalar por sí mismos, según los equipos de los proveedores del servicio. Si instala un separador de este tipo por sí mismo, conecte el cable ADSL desde el dispositivo NetScreen y la línea telefónica a los conectores correspondientes (por ejemplo, “datos” o “voz”) del separador. Conecte el otro extremo del separador a la toma de teléfono.

También resulta necesario instalar un *microfiltro* en cada teléfono, fax, contestador automático o módem analógico que se conecte a la línea ADSL. El microfiltro filtra los ruidos de alta frecuencia en la línea telefónica. Instale el microfiltro en la línea telefónica entre el teléfono, fax, contestador automático o módem analógico y el conector de voz del separador.

La siguiente ilustración muestra un ejemplo de instalación de un microfiltro y un separador. El proveedor de telefonía debe proporcionarle los microfiltros o separadores adecuados.



Conexión del puerto sin confianza

Puede establecer una conexión Internet a un enrutador externo, un módem DSL o un módem de cable, proporcionando protección de cortafuegos y garantizando la seguridad general en toda la red. Para establecer una conexión de alta velocidad, conecte el cable Ethernet proporcionado desde la interfaz Untrusted del dispositivo NetScreen-5GT Wireless al enrutador o módem externo. El dispositivo NetScreen-5GT Wireless detectará automáticamente los ajustes correctos de velocidad, dúplex y polaridad.

Si va a utilizar el dispositivo NetScreen-5GT Wireless ADSL, consulte [“Conexión del puerto ADSL”](#), en la página 129 y [“Conexión de separadores y microfiltros”](#), en la página 130 para obtener instrucciones sobre la conexión ADSL.

Conexión del dispositivo a la red interna o a estaciones de trabajo

Puede conectar la red de área local (LAN) o la estación de trabajo mediante los siguientes métodos:

- Conexión a través de uno o varios de los puertos Ethernet de confianza del dispositivo NetScreen
- Uso de una interfaz inalámbrica en el dispositivo NetScreen

Conexión de los puertos Ethernet de confianza

El dispositivo NetScreen-5GT Wireless contiene cuatro puertos Ethernet de confianza. Puede utilizar uno o varios de estos puertos para conectarse a redes LAN mediante conmutadores o concentradores. También es posible conectar uno o todos los puertos directamente a estaciones de trabajo, sin tener que utilizar un conmutador (“switch”) o un concentrador (“hub”). Puede utilizar cables cruzados o rectos para conectar los puertos Ethernet a otros dispositivos.

Utilización de la interfaz inalámbrica

Si utiliza la interfaz inalámbrica, deberá conectar la antena proporcionada con el dispositivo. Si dispone de antenas omnidireccionales 2dB estándar, atorníllelas a los puestos marcados A y B en la parte posterior del dispositivo. Para obtener más información, consulte [“Conector de alimentación y puertos”](#), en la página 155. Doble las antenas por su parte curva, teniendo cuidado de no ejercer presión sobre el conector de obturación.

CONEXIÓN DE LA ALIMENTACIÓN

Para conectar la alimentación al dispositivo NetScreen-5GT Wireless:

1. Enchufe el conector de CC del cable de alimentación al conector de CC de la parte posterior del dispositivo.
2. Conecte el adaptador de CA (corriente alterna) del cable de alimentación a la fuente de alimentación de CA (corriente alterna).

Aviso: Recomendamos utilizar un protector contra sobretensiones en la conexión de alimentación.

MONTAJE EN BASTIDOR (OPCIONAL)

El juego de montaje en bastidor para el NetScreen-5GT Wireless permite montar uno o dos dispositivos NetScreen-5GT Wireless en un bastidor estándar de 48,25 cm (19 pulgadas). El juego de montaje en bastidor para el NetScreen-5GT Wireless incluye instrucciones de instalación y una bandeja de montaje en bastidor. Las dimensiones de la bandeja son:

Anchura:	48,26 cm	19 pulg.
Altura:	4,013 cm	1-5/8 pulg. (1 bastidor)
Fondo:	33,655 cm	13-1/4 pulg.

Además del dispositivo NetScreen-5GT Wireless, el juego de montaje y el bastidor, necesitará el siguiente material:

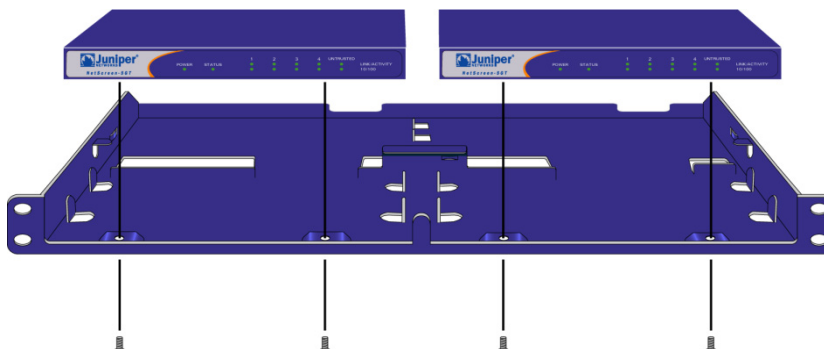
- Destornillador Phillips
- Cuatro tornillos con el tamaño adecuado para los orificios del bastidor

Para montar el dispositivo en un bastidor:

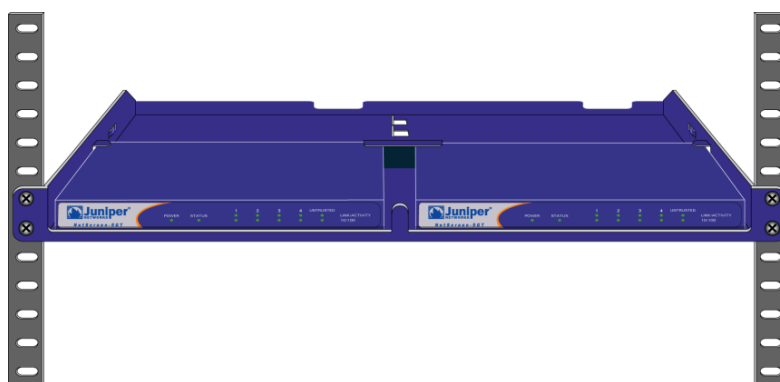
1. Utilice el destornillador Phillips para extraer los dos tornillos de la parte inferior de cada dispositivo NetScreen-5GT Wireless que desee montar. Conserve los tornillos para utilizarlos en el siguiente paso. Los tornillos se encuentran situados en la base del dispositivo, cerca del panel frontal.



2. Inserte cada dispositivo en la bandeja de montaje en bastidor y atorníllelos a la bandeja con los tornillos que extrajo en el paso 1.



3. Atornille las lengüetas derecha e izquierda de la bandeja al bastidor con los tornillos restantes.



Puede pasar los cables de alimentación y los cables Ethernet a través de las aberturas situadas en la base de la bandeja o de las hendiduras de la parte posterior del bastidor. También puede utilizar el espacio situado detrás de los dispositivos para colocar fuentes de alimentación.

Configuración del dispositivo

En este capítulo se describe cómo configurar un dispositivo NetScreen-5GT Wireless después de conectarlo a la red. Si accede al dispositivo por primera vez mediante la interfaz gráfica ScreenOS WebUI, el asistente de configuración inicial (Initial Configuration Wizard) le mostrará los pasos necesarios para realizar la configuración básica. Para utilizar esta asistente, consulte la guía rápida *Juniper Networks NetScreen-5GT Wireless Getting Started Guide* o la guía rápida *Juniper Networks NetScreen-5GT Wireless ADSL Getting Started Guide*.

Los temas que se explican en este capítulo son:

- [Acceso al dispositivo](#)
- [Configuración requerida](#)
- [Configuración inalámbrica](#)
- [Configuración de ADSL](#)
- [Configuración opcional](#)
- [Verificación de la conectividad externa](#)
- [Restauración de los ajustes predeterminados de fábrica](#)

Nota: Después de configurar el dispositivo NetScreen y comprobar la conexión a Internet, debe registrar el producto en www.juniper.net/support/ para que se puedan activar determinados servicios de ScreenOS en el dispositivo, como son el antivirus interno o el servicio de inspección minuciosa de firmas. Después de registrar el producto, utilice la interfaz WebUI para obtener la suscripción al servicio. Si desea obtener más información sobre el registro del producto y adquirir suscripciones a servicios particulares, consulte el capítulo “Parámetros del sistema” en el volumen “Fundamentos” del Manual de referencia de ScreenOS NetScreen: conceptos y ejemplos para ScreenOS 5.0.0.

ACCESO AL DISPOSITIVO

En esta sección se describe la forma de acceder al dispositivo NetScreen mediante la interfaz WebUI, Telnet o una conexión de consola.

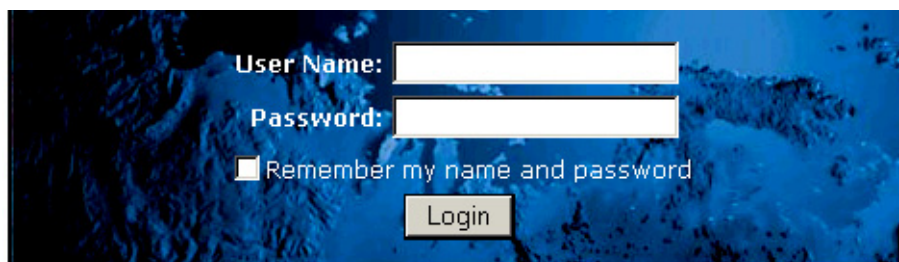
Utilización de la interfaz WebUI

ScreenOS WebUI es una interfaz gráfica que está disponible a través de un explorador web. Para poder utilizar la interfaz WebUI, debe encontrarse en la misma subred que la interfaz Trust o wireless2. Para acceder al dispositivo NetScreen-5GT Wireless con la aplicación de administración WebUI:

1. Inicie el explorador web, introduzca la dirección IP de la interfaz Trust o wireless2 en el campo de la URL y pulse Enter. Por ejemplo, introduzca la siguiente dirección en el campo de URL:

192.168.1.1

El software NetScreen WebUI mostrará el mensaje de inicio de sesión.



***Nota:** Si omite el asistente de configuración inicial (ICW), aparecerá automáticamente el mensaje de inicio de sesión de la WebUI.*

2. Si todavía no ha modificado el nombre de usuario y la contraseña predeterminados, escriba **netscreen** en los campos **User Name** y **Password** y haga clic en **Login** (utilice sólo letras en minúscula. Los campos User Name y Password distinguen entre mayúsculas y minúsculas).

Utilización de Telnet

Telnet es una aplicación que permite acceder a dispositivos a través de una red de protocolo Internet (IP).

***Nota:** También puede acceder a dispositivos NetScreen mediante aplicaciones de Shell seguro (SSH). Para obtener más información, consulte el capítulo “Administración” en el volumen “Administración” del Manual de referencia de ScreenOS NetScreen: conceptos y ejemplos para ScreenOS 5.0.0.*

Para configurar el dispositivo mediante Telnet, se introducen comandos de la interfaz de línea de comandos (CLI) de ScreenOS en una sesión Telnet desde la estación de trabajo.

1. Inicie una aplicación de cliente Telnet en la dirección IP de la interfaz Trust o wireless2. Por ejemplo, introduzca lo siguiente:

telnet 192.168.1.1

2. Si todavía no ha modificado el nombre de usuario y la contraseña predeterminados, escriba **netscreen** en los campos **Login** y **Password** (utilice sólo letras en minúscula. Los campos login y password distinguen entre mayúsculas y minúsculas).

Utilización de una conexión de consola

El puerto de consola del dispositivo NetScreen-5GT Wireless permite acceder al dispositivo a través de un cable serie conectado a la estación de trabajo o el terminal. Para configurar el dispositivo mediante una conexión de consola, se introducen comandos ScreenOS CLI en el terminal o en un programa de emulación de terminal de la estación de trabajo.

Nota: Para la conexión de consola utilice un cable serie con un conector macho RJ-45 en un extremo y un conector hembra DB-9 en el otro. Consulte el [Apéndice A, “Apéndice A Ficha técnica”](#) para obtener información acerca de las patillas de salida del conector del cable serie.

Para establecer una conexión de consola:

1. Inserte el conector hembra DB-9 del cable serie en el puerto serie del equipo (asegúrese de que el conector DB-9 esté correctamente alojado en el puerto).
2. Inserte el conector macho RJ-45 del cable serie en el puerto de consola del dispositivo NetScreen-5GT Wireless (asegúrese de que el conector RJ-45 esté correctamente alojado en el puerto).
3. Inicie un programa de emulación de terminal serie (uno de los programas de terminal que más se utiliza es HyperTerminal de Hilgreave). A continuación se enumeran los ajustes requeridos para iniciar una sesión de consola con el dispositivo NetScreen-5GT Wireless:
 - Velocidad de transferencia: 9600
 - Paridad: No
 - Bits de datos: 8
 - Bit de parada: 1
 - Control de flujo: Ninguno
4. Si todavía no ha modificado el nombre de usuario y la contraseña predeterminados, escriba **netscreen** en los campos **Login** y **Password** (utilice sólo letras en minúscula. Los campos login y password distinguen entre mayúsculas y minúsculas).

CONFIGURACIÓN REQUERIDA

En esta sección se describe la configuración necesaria para utilizar el dispositivo.

Nota: Si en algún momento necesita restaurar la configuración predeterminada del dispositivo, consulte [“Restauración de los ajustes predeterminados de fábrica”, en la página 151](#).

Cambio de nombre y contraseña del administrador

Como todos los productos de NetScreen tienen predeterminados el mismo nombre del administrador y la misma contraseña (**netscreen**), es altamente recomendable modificar el nombre del administrador y la contraseña inmediatamente. Para cambiar el nombre del administrador “netscreen” y la contraseña “netscreen” a “darwin1” y “1240jes”:

WebUI

Configuration > Admin > Administrators > Edit (para el nombre de administrador de Netscreen): Introduzca los siguientes datos y haga clic en **OK**:

Administrator Name: darwin1

Old Password: netscreen

***Nota:** La interfaz WebUI no muestra las contraseñas cuando se están introduciendo.*

New Password: 1240jes

Confirm New Password: 1240jes

CLI

```
set admin name darwin1
set admin password 1240jes
save
```

Para obtener información sobre cómo crear diferentes niveles de administradores, consulte el capítulo “Administración” en el volumen “Administración” del *Manual de referencia de ScreenOS NetScreen: conceptos y ejemplos* para ScreenOS 5.0.0.

Ajuste de la fecha y la hora

La hora ajustada en el dispositivo NetScreen afecta a acciones como la configuración de los túneles VPN y a la sincronización de programaciones. La forma más sencilla de ajustar la fecha y la hora en el dispositivo NetScreen es sincronizando el reloj del sistema del dispositivo NetScreen con el reloj del equipo informático. Para hacerlo con la interfaz WebUI:

1. Configuration > Date/Time: Haga clic en el botón **Sync Clock with Client**. Aparecerá un mensaje preguntándole si tiene habilitada la opción del horario de verano en el reloj del sistema.
2. Haga clic en **Yes** para sincronizar el reloj del sistema y ajustarlo según el horario de verano, o bien en **No** para sincronizarlo sin el ajuste de horario de verano.

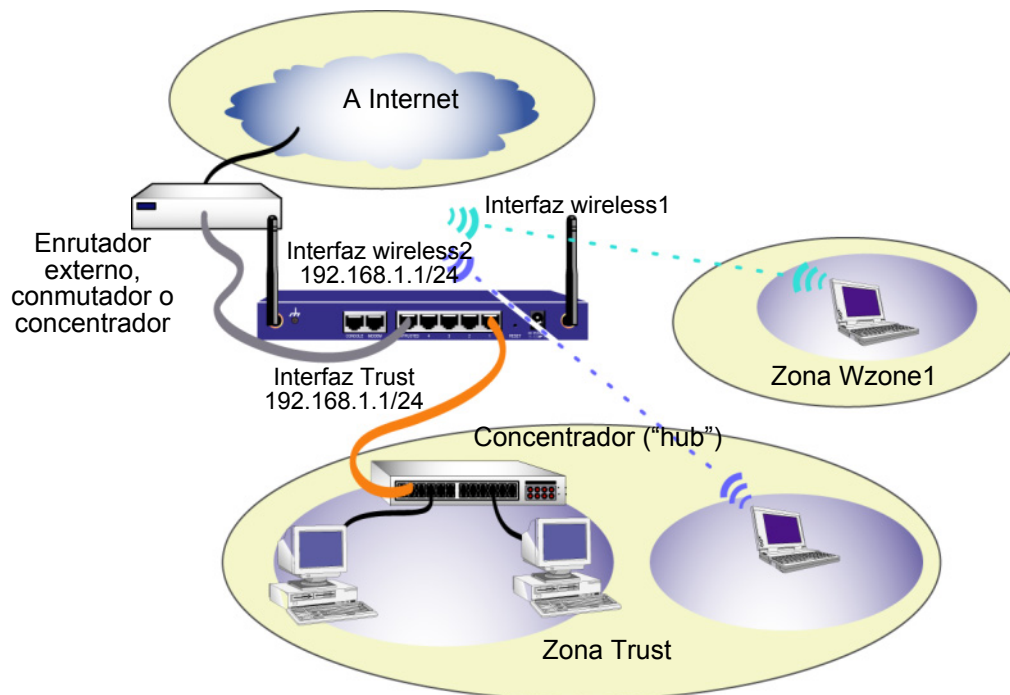
También puede utilizar el comando **set clock** CLI en una sesión Telnet o de consola para introducir manualmente la fecha y la hora.

CONFIGURACIÓN INALÁMBRICA

En esta sección se proporciona información para la configuración de la interfaz inalámbrica del dispositivo NetScreen. En función del tipo de licencia que haya instalado, podrá configurar hasta cuatro zonas de seguridad inalámbrica en los dispositivos NetScreen-5GT Wireless. Los enlaces de interfaz a zona están predefinidos y dependen del modo de puerto que configure. Además, no puede asignar interfaces inalámbricas a la zona Untrust. Debe configurar al menos una interfaz inalámbrica en el dispositivo NetScreen para crear una red de área local inalámbrica (WLAN).

Nota: Si no va a utilizar el dispositivo NetScreen-5GT Wireless en Estados Unidos o Japón, deberá utilizar el comando **set wlan country-code** para poder establecer una conexión WLAN. Este comando ajusta el intervalo de canales que se pueden seleccionar y el nivel de potencia de la transmisión.

La siguiente ilustración muestra la configuración predeterminada del dispositivo NetScreen-5GT Wireless.



La interfaz inalámbrica predeterminada tiene el nombre predefinido de “wireless2”. Las interfaces Trust y wireless2 están vinculadas a la zona Trust y configuradas con las direcciones de subred 192.168.1.1/24 y 192.168.2.1/24, respectivamente. Esto significa que todos los dispositivos a los que se conecte en la zona Trust deben estar en la misma subred que la interfaz Trust o wireless2 y tener direcciones IP en una de las dos subredes. El dispositivo NetScreen también está configurado para asignar a los dispositivos direcciones IP para las subredes 192.168.1.1/24 y 192.168.2.1/24. Para obtener más información, consulte [“Cambio de la dirección de interfaz Trust o Wireless2”](#), en la página 151.

De manera predeterminada, la interfaz wireless1 está vinculada a la zona Wzone1 y no tiene asignada una dirección IP. Si desea utilizar la interfaz wireless1, debe configurar una dirección IP para ella. Para obtener más información, consulte el *NetScreen-5GT Wireless Reference Guide*.

El dispositivo NetScreen permite cualquier tipo de tráfico hacia Internet originado en los dispositivos de la zona Trust, pero no permite que ningún tipo de tráfico originado en Internet acceda a la red. Puede configurar restricciones adicionales; consulte [“Configuración de directivas adicionales”, en la página 147](#).

Configuración de la red inalámbrica

Las redes inalámbricas están formadas por nombres conocidos como identificadores del conjunto de servicios (Service Set Identifiers, SSID). La especificación de un SSID permite contar con varias redes inalámbricas en la misma ubicación. Es posible tener hasta un máximo de ocho SSID configurados en cada dispositivo. Una vez definido el nombre SSID, puede configurar atributos SSID.

Para definir el nombre SSID **netscreen open**, permita que haya conectividad de red inalámbrica y active la interfaz wireless2:

WebUI

Wireless > SSID > New: Introduzca los siguientes datos y haga clic en **OK**:

SSID: “netscreen open”

Wireless Interface Binding: wireless2 (seleccionar)

Activate Changes > haga clic en el botón **Activate Changes**

CLI

```
set ssid name "netscreen open"
set ssid "netscreen open" authentication open encryption
none
set ssid "netscreen open" interface wireless2
exec wlan reactivate
```

Una vez que ha definido un SSID para la interfaz wireless2, puede acceder al dispositivo mediante la dirección IP de la interfaz wireless2 predeterminada descrita en los pasos proporcionados con [“Acceso al dispositivo”, en la página 135](#), para configurar el dispositivo. Consulte el *NetScreen-5GT Wireless Reference Guide* para ver ejemplos de configuración, atributos SSID y comandos CLI relacionados con las configuraciones de seguridad inalámbrica.

CONFIGURACIÓN DE ADSL

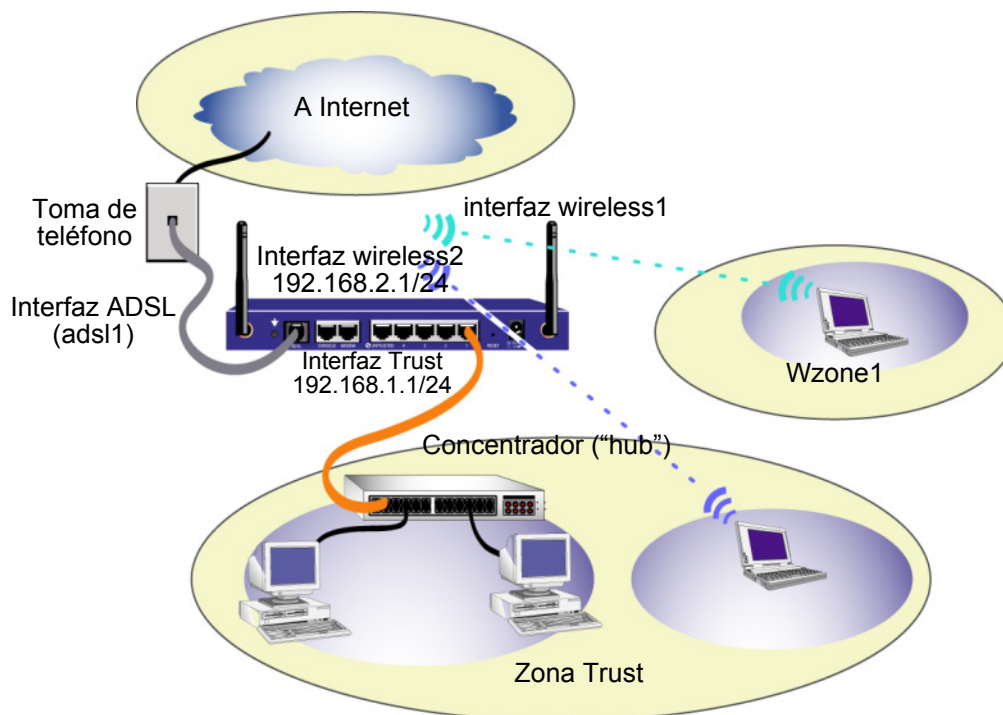
En esta sección se describen los ajustes predeterminados y el manejo de los dispositivos de Anexo A y B NetScreen-5GT Wireless ADSL tal y como se suministran de fábrica. Estos ajustes predeterminados están definidos de tal forma que, en la mayoría de los casos, el usuario sólo tiene que configurar pequeños detalles.

En esta sección se describen las siguientes configuraciones para la interfaz de zona Untrust:

- [Configuración de la interfaz ADSL](#)
- [Inclusión de circuitos virtuales en una interfaz ADSL](#)
- [Método VPI/VCI y multiplexado](#)
- [PPPoE o PPPoA](#)
- [Modo de Anexo B](#)
- [Dirección IP estática y máscara de red](#)

Nota: Si en algún momento necesita restaurar la configuración predeterminada del dispositivo, consulte [“Restauración de los ajustes predeterminados de fábrica”](#), en la [página 151](#).

La siguiente ilustración muestra la configuración predeterminada del dispositivo NetScreen-5GT Wireless ADSL.



La interfaz ADSL tiene el nombre predeterminado “adsl1” y se trata de la conexión principal de la red a Internet. Para permitir la conexión a Internet desde el dispositivo NetScreen (y los dispositivos de la red), deberá configurar la interfaz adsl1 de acuerdo con la información que le haya proporcionado su proveedor de servicios. Consulte [“Configuración de la interfaz ADSL”, en la página 142.](#)

El dispositivo NetScreen permite cualquier tipo de tráfico hacia Internet originado en los dispositivos de la zona Trust, pero no permite que ningún tipo de tráfico originado en Internet acceda a la red. Puede configurar restricciones adicionales; consulte [“Configuración de directivas adicionales”, en la página 147.](#)

Configuración de la interfaz ADSL

La red utiliza la interfaz ADSL “adsl1” del dispositivo NetScreen para conectarlo a la red del proveedor de servicios mediante un circuito virtual ATM (del inglés “Asynchronous Transfer Mode”). Puede configurar circuitos virtuales adicionales creando subinterfases ADSL (para obtener más información, consulte [“Inclusión de circuitos virtuales en una interfaz ADSL”, en la página 143.](#))

En la interfaz WebUI, acceda a la página Network > Interfaces para ver una lista de las interfaces disponibles en el dispositivo NetScreen. Si está utilizando una sesión Telnet o de consola, introduzca el comando CLI **get interface**. Comprobará que la interfaz adsl1 está asociada a la zona Untrust. Si ha utilizado el ICW para configurar el dispositivo, es posible que ya haya asignadas una dirección IP y una máscara de red a la interfaz adsl1.

***Nota:** Si no desea utilizar la interfaz ADSL, puede vincularla a la zona Null mediante el comando **set interface adsl1 zone null**. Si utiliza el ICW para configurar el dispositivo, puede seleccionar otra interfaz que no sea ADSL como interfaz predeterminada para la zona Untrust.*

Debe configurar la interfaz adsl1 para que el dispositivo NetScreen se conecte a la red del proveedor de servicios. Para ello, el proveedor de servicios le tiene que proporcionar la siguiente información:

- Valores del identificador de trayecto virtual (Virtual Path Identifier) y del identificador de canal virtual (Virtual Channel Identifier) (VPI/VCI)
- Método de multiplexado de capa de adaptación ATM 5 (AAL5) de modo de transferencia asíncrona (ATM), que puede ser una de las siguientes opciones:
 - Multiplexado basado en circuito virtual (VC), en el que cada protocolo se transporta a través de un circuito virtual ATM independiente.
 - Encapsulado de control de enlaces lógico (LLC), que permite transportar varios protocolos en el mismo circuito virtual ATM (el método de multiplexado predeterminado).
- Nombre de usuario y contraseña asignados por el proveedor del servicio para conectarse a la red del proveedor mediante el protocolo punto a punto sobre Ethernet (“Point-to-Point Protocol over Ethernet” o “PPPoE”) o el protocolo punto a punto sobre ATM (“Point-to-Point Protocol over ATM” o “PPPoA”)
- Método de autenticación, si hubiera, proporcionado para la conexión PPPoE o PPPoA
- Opcionalmente, una dirección IP estática y un valor de máscara de red para la red

Inclusión de circuitos virtuales en una interfaz ADSL

Para agregar circuitos virtuales, debe crear subinterfaces en la interfaz ADSL. Se pueden crear un máximo de 10 subinterfaces. Por ejemplo, para crear una nueva subinterfaz llamada adsl1.1 que esté vinculada a la zona definida por el usuario llamada “Corp1”:

WebUI

Network > Interfaces > New ADSL Sub-IF: Introduzca los siguientes datos y haga clic en **Apply**:

Interface Name: adsl1.1

VPI/VCI: 0/35

Zone Name: Corp1 (seleccionar)

CLI

```
set interface adsl1.1 pvc 0 35 zone corp1
save
```

Es necesario configurar una subinterfaz ADSL de la misma manera que la interfaz ADSL principal, incluyendo el ajuste de los valores VPI/VCI, tal y como se muestra en [“Configuración de la interfaz ADSL”, en la página 142](#). La configuración de la subinterfaz ADSL se realiza independientemente de la interfaz ADSL principal. Esto quiere decir que va a configurar un método de multiplexado, VPI/VCI, y un cliente PPP diferentes de los de la interfaz ADSL principal. También puede configurar una dirección IP estática en las subinterfaces, a pesar de que la interfaz ADSL principal no disponga de una dirección IP estática. Tenga en cuenta que una subinterfaz y la interfaz ADSL principal podrán utilizar los mismos valores VPI/VCI si una interfaz se configura para PPPoA y la otra para PPPoE y las dos utilizan el método de multiplexado LLC.

Método VPI/VCI y multiplexado

El proveedor de servicios asigna un par VPI/VCI a cada conexión de circuito virtual. Por ejemplo, puede obtener el valor 1/1 para el par VPI/VCI, lo que asigna un valor VPI de 1 y un valor VCI de 1. Estos valores deben coincidir con los que el proveedor de servicios ha configurado en la parte del abonado del multiplexador de acceso de línea de abonado digital (DSLAM).

Para configurar el par 1/1 VPI/VCI en la interfaz adsl1:

WebUI

Network > Interfaces > Edit (para la interfaz adsl1): introduzca 1/1 en el campo VPI/VCI y haga clic en **Apply**.

CLI

```
set interface adsl1 pvc 1 1
save
```

De forma predeterminada, el dispositivo NetScreen-5GT Wireless ADSL utiliza un multiplexado basado en LLC en cada circuito virtual. Para configurar el par VPI/VCI 1/1 en la interfaz adsl1 y utilizar el encapsulado LLC en el circuito virtual:

WebUI

Network > Interfaces > Edit (para la interfaz adsl1): Introduzca los siguientes datos y haga clic en **Apply**:

VPI/VCI: 1 / 2

Método de multiplexado: LLC (seleccionado)

CLI

```
set interface adsl1 pvc 1 1 mux llc
save
```

PPPoE o PPPoA

El dispositivo NetScreen incluye los clientes PPPoE y PPPoA para conectarse a la red del proveedor de servicios mediante ADSL. PPPoE es la manera más habitual de encapsulado ADSL y está diseñado para su finalización en cada anfitrión (“host”) de la red. PPPoA se utiliza principalmente para servicios empresariales, ya que las sesiones PPP se pueden finalizar en el dispositivo NetScreen. Para permitir conectar el dispositivo NetScreen a la red del proveedor de servicios, hay que configurar el nombre de usuario y la contraseña asignados por el proveedor. La configuración para PPPoA es parecida a la configuración para PPPoE.

Nota: El dispositivo NetScreen sólo admite una sesión PPPoE en cada circuito virtual.

Para configurar el nombre de usuario “roswell” y la contraseña “area51” para PPPoE y vincular esta configuración a la interfaz adsl1:

WebUI

Network > PPPoE > New: Introduzca los siguientes datos y haga clic en **OK**:

PPPoE Instance: poe1

Bound to Interface: adsl1 (seleccionar)

Username: roswell

Password: area51

CLI

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1
save
```

Hay otros parámetros PPPoE o PPPoA que se pueden configurar en el dispositivo NetScreen, incluyendo el método de autenticación (de forma predeterminada, el dispositivo NetScreen admite el protocolo de autenticación de establecimiento de conexión por desafío, CHAP, o bien el protocolo de autenticación mediante contraseña, PAP), el tiempo de espera (el valor predeterminado es de 30 minutos), etc. Pregunte al proveedor si hay otros parámetros PPPoE o PPPoA que debe configurar para establecer correctamente la comunicación con el servidor del proveedor de servicios.

Modo de Anexo B

Si conecta el modelo de Anexo B del dispositivo NetScreen-5GT Wireless ADSL a una línea ADSL de Deutsch Telecom, tendrá que configurar la interfaz física del puerto ADSL para que funcione con este equipamiento. Para ello:

WebUI

Network > Interfaces > Edit (para la interfaz adsl1): seleccione **DT** para el modo de Anexo B y haga clic en **Apply**.

CLI

```
set interface adsl1 phy annex-b-mode dt
save
```

No será necesario configurar este ajuste si utiliza el modelo de Anexo A del dispositivo o si conecta el dispositivo a un equipo que no pertenezca a Deutsch Telecom.

Dirección IP estática y máscara de red

Si su ISP (proveedor de servicios de Internet) le ha proporcionado una máscara de red y una dirección IP fija y específica para la red, configure la máscara de red y la dirección IP de la red y la dirección IP del puerto del enrutador conectado al dispositivo NetScreen. También deberá especificar que el dispositivo utiliza una dirección IP estática. De manera predeterminada, el dispositivo NetScreen actúa a modo de cliente PPPoE o PPPoA y recibirá una dirección IP para la interfaz ADSL mediante negociaciones con el servidor PPPoE o PPPoA.

Para configurar la dirección IP estática 1.1.1.1/24 para la red:

WebUI

Network > Interfaces > Edit (para la interfaz adsl1): Introduzca los siguientes datos y haga clic en **Apply**:

IP Address/Netmask: 1.1.1.1/24

Static IP: (seleccione)

Nota: Es necesario configurar una instancia PPPoE o PPPoA y vincularla a la interfaz adsl1, tal y como se muestra en la sección anterior. Asegúrese de que selecciona "Obtain IP using PPPoE" u "Obtain IP using PPPoA" y el nombre de la instancia PPPoE o PPPoA.

CLI

```
set interface adsl1 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

o bien

```
set interface adsl1 ip 1.1.1.1/24
set pppoa name poa1 static-ip
save
```

Para utilizar el sistema de nombres e dominios (“Domain Name System” o “DNS”) para la resolución de los nombres de dominio y direcciones, los equipos conectados a la red tendrán que disponer de la dirección IP de al menos un servidor DNS. Si el dispositivo NetScreen recibe una dirección IP para la interfaz ADSL mediante PPPoE o PPPoA, recibirá automáticamente las direcciones IP para los servidores DNS. Si los equipos conectados a la red obtienen sus direcciones IP del servidor DHCP del dispositivo NetScreen, estos equipos también obtendrán las direcciones de estos servidores DNS.

Si asigna una dirección IP estática a la interfaz ADSL, el proveedor de servicios debe proporcionarle las direcciones IP de los servidores DNS. Puede configurar la dirección del servidor DNS en todos los equipos de la red, o bien configurar el servidor DHCP en la interfaz de la zona Trust (de confianza) para que proporcione la dirección del servidor DNS a cada equipo.

Para configurar el servidor DHCP en la interfaz Trust para que proporcione la dirección 1.1.1.152 del servidor DNS a los equipos de la red:

WebUI

Network > DHCP > Edit (para la interfaz Trust) > DHCP Server: introduzca 1.1.1.152 para DNS1 y haga clic en **Apply**.

CLI

```
set interface trust dhcp server option dns1 1.1.1.152
save
```

CONFIGURACIÓN OPCIONAL

En esta sección se describen las siguientes características de los dispositivos NetScreen-5GT Wireless cuya configuración es opcional:

- [Restricción de administración](#)
- [Configuración de directivas adicionales](#)
- [Modo de funcionamiento](#)
- [Cambio del modo de puerto](#)
- [Configuración de una interfaz de zona Untrust de respaldo](#)
- [Cambio de la dirección de interfaz Trust o Wireless2](#)

Nota: No todas las operaciones de configuración opcionales se describen detalladamente en este manual. Para obtener más información, consulte los capítulos adecuados del Manual de referencia de ScreenOS NetScreen: conceptos y ejemplos para ScreenOS 5.0.0.

Restricción de administración

De forma predeterminada, todos los usuarios de la red pueden administrar el dispositivo NetScreen siempre que conozcan el nombre de usuario y la contraseña. Puede configurar el dispositivo NetScreen para que sólo puedan administrarlo uno o varios anfitriones específicos de la red (también puede elegir qué servicios, por ejemplo WebUI, Telnet o ping, van a estar activados en el dispositivo NetScreen).

Para obtener más información, consulte el capítulo “Administración” en el volumen “Administración” del *Manual de referencia de ScreenOS NetScreen: conceptos y ejemplos* para ScreenOS 5.0.0.

Configuración de directivas adicionales

Los dispositivos NetScreen-5GT Wireless están configurados con una directiva predeterminada que permite que las estaciones de trabajo de la zona Trust de la red accedan a cualquier tipo de servicio proporcionado por equipos externos, mientras que a los equipos externos se les prohíbe el acceso o el inicio de sesión en las estaciones de trabajo. Es posible configurar directivas que obliguen al dispositivo NetScreen a permitir que los equipos externos inicien determinado tipo de sesiones en los equipos de la red. Para crear o modificar directivas, consulte el capítulo “Directivas” en el volumen “Fundamentos” del *Manual de referencia de ScreenOS NetScreen: conceptos y ejemplos* para ScreenOS 5.0.0.

Modo de funcionamiento

El *modo de funcionamiento* es el modo en el que una interfaz de un dispositivo NetScreen procesa el tráfico entre las diversas zonas. De forma predeterminada, los dispositivos NetScreen-5GT Wireless operan en modo de ruta con la traducción de direcciones de red (NAT) activada en la interfaz Trust. Esto quiere decir que, cuando los dispositivos de la zona trust (de confianza) envían tráfico a Internet, el dispositivo NetScreen reemplaza la dirección IP de origen inicial por la dirección IP de la interfaz untrust (sin confianza). Mientras el dispositivo NetScreen asigne direcciones IP privadas a los dispositivos de la red, estas direcciones permanecerán ocultas a los equipos externos que no formen parte de dicha red.

Si todos los dispositivos de la red tienen direcciones IP públicas, puede configurar el dispositivo NetScreen para que funcione en modo de ruta con NAT desactivada. En el modo de ruta con NAT desactivada, el dispositivo NetScreen enruta el tráfico comprobando las direcciones IP. Para obtener más información sobre la configuración del dispositivo en modo de ruta con NAT desactivada, consulte el capítulo “Modos de interfaz” en el volumen “Fundamentos” del *Manual de referencia de ScreenOS NetScreen: conceptos y ejemplos* para ScreenOS 5.0.0.

Cambio del modo de puerto

El *modo de puerto* es la unión de puertos físicos, interfaces lógicas y zonas.

Aviso: Si se modifica el modo de puerto, se eliminará la configuración existente en el dispositivo NetScreen. Por lo tanto, se debe cambiar el modo de puerto antes de configurar el dispositivo.

La tabla siguiente resume los enlaces de puerto, interfaz y zona proporcionados por los modos de puerto disponibles en los dispositivos NetScreen 5-GT Wireless

Nombre del puerto ^a	Modo de puerto Trust-Untrust ^b		Modo de puerto Home-Work		Modo Trust/Untrust/DMZ (extendido)		Modo de puerto Dual Untrust		Modo de puerto combinado	
	Interfaz	Zona	Interfaz	Zona	Interfaz	Zona	Interfaz	Zona	Interfaz	Zona
1	trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet1	Trust	ethernet1	Work
2	trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet1	Trust	ethernet2	Home
3	trust	Trust	ethernet2	Home	ethernet2	DMZ	ethernet1	Trust	ethernet2	Home
4	trust	Trust	ethernet2	Home	ethernet2	DMZ	ethernet2	Untrust	ethernet3	Untrust
Untrusted	untrust	Untrust	ethernet3	Untrust	ethernet3	Untrust	ethernet3	Untrust	untrust	Untrust
Modem ^c	serial	Null	serial	Null	serial	Null	serial	Null	serial	Null
	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1
	wireless2	Trust	wireless2	Work	wireless2	Trust	wireless2	Trust	wireless2	Work
			wireless3	Home	wireless3	DMZ			wireless3	Home
					wireless4	Wzone2				

- Según la etiqueta adherida a los chasis del dispositivo NetScreen.
- Modo de puerto predeterminado.
- Puede configurar una interfaz de respaldo en la zona Untrust mediante el puerto Ethernet Untrusted o el puerto del módem. Consulte [“Configuración de una interfaz de zona Untrust de respaldo”](#), en la página 150.

La tabla siguiente resume los enlaces de puerto, interfaz y zona proporcionados por los modos de puerto disponibles en los dispositivos NetScreen 5-GT Wireless ADSL:

Nombre del puerto ^a	Modo de puerto Trust-Untrust ^b		Modo de puerto Home-Work		Modo Trust/Untrust/DMZ (extendido)	
	Interfaz	Zona	Interfaz	Zona	Interfaz	Zona
1	trust	Trust	ethernet1	Work	ethernet1	Trust
2	trust	Trust	ethernet1	Work	ethernet1	Trust
3	trust	Trust	ethernet2	Home	ethernet2	DMZ
4	trust	Trust	ethernet2	Home	ethernet2	DMZ
Untrusted	untrust	Null ^c	ethernet3	Null ^c	ethernet3	Null ^c

Nombre del puerto ^a	Modo de puerto Trust-Untrust ^b		Modo de puerto Home-Work		Modo Trust/Untrust/DMZ (extendido)	
	Interfaz	Zona	Interfaz	Zona	Interfaz	Zona
Modem	serial	Null ^c	serial	Null ^c	serial	Null ^c
ADSL	adsl1	Untrust	adsl1	Untrust	adsl1	Untrust
	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1
	wireless2	Trust	wireless2	Work	wireless2	Trust
			wireless3	Home	wireless3	DMZ
				wireless4	Wzone2	

- Según la etiqueta adherida a los chasis del dispositivo NetScreen.
- Modo de puerto predeterminado.
- Puede configurar una interfaz de respaldo en la zona Untrust mediante el puerto Ethernet Untrusted o el puerto del módem. Consulte [“Configuración de una interfaz de zona Untrust de respaldo”](#), en la página 150.

Para modificar el dispositivo NetScreen al modo de puerto Home-Work:

WebUI

Configuration > Port Mode: Seleccione “Home-Work” en la lista desplegable y haga clic en **Apply**.

Cuando aparezca la pregunta siguiente, haga clic en **OK**:

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

CLI

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

Cuando aparezca la pregunta siguiente, pulse la tecla **y** (respuesta afirmativa):

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

Configuración de una interfaz de zona Untrust de respaldo

De forma predeterminada, en el dispositivo NetScreen-5GT Wireless ADSL, la interfaz `adsl1` es la conexión principal a una red exterior. Cada modo de puerto disponible en el dispositivo NetScreen-5GT Wireless ADSL permite disponer de la opción de conectar el puerto Ethernet Untrusted o el puerto de módem a modo de conexión de respaldo a la red exterior (consulte [“Cambio del modo de puerto”, en la página 148](#)). Hay que vincular la interfaz de respaldo a la zona Untrust y configurar la interfaz según estos cambios.

Nota: Sólo podrá configurar una interfaz de respaldo mediante la conexión del puerto Ethernet Untrusted o del puerto de módem. Si utiliza el puerto Untrusted para la conexión de respaldo, configure la interfaz Untrust en el modo de puerto Trust-Untrusted de la interfaz `ethernet3` para los otros modos de puerto. Si utiliza el puerto de módem para la conexión de respaldo, configure la interfaz serie para todos los modos de puerto.

Por ejemplo, para vincular la interfaz Untrust a la zona Untrust:

WebUI

Network > Interfaces > Edit (para la interfaz Untrust): seleccione Untrust en la lista desplegable Zone Name y haga clic en **OK**.

CLI

```
set interface untrust zone untrust
save
```

También debe establecer una dirección IP estática para la interfaz Untrust o especificar si la dirección IP de la interfaz se obtiene mediante DHCP o PPPoE. Si desea obtener más información sobre la configuración de los parámetros de la interfaz, consulte el capítulo “Interfaces” en el volumen “Fundamentos” del *Manual de referencia de ScreenOS NetScreen: conceptos y ejemplos* para ScreenOS 5.0.0.

Cuando la interfaz `adsl1` y la interfaz Ethernet (denominada `untrust` o `ethernet3`, según el modo de puerto) o la interfaz serie está vinculada a la zona Untrust, se configurará automáticamente la conmutación en caso de error de la interfaz. Es decir, si la interfaz `adsl1` deja de estar disponible, el dispositivo NetScreen envía automáticamente el tráfico a la interfaz de respaldo. El dispositivo volverá a enviar automáticamente el tráfico a la interfaz `adsl1` cuando esté disponible.

Nota: La conmutación en caso de error sólo afecta a la interfaz `adsl1`. Por ello, si también ha configurado las subinterfaces ADSL, éstas no se conmutarán a la interfaz de respaldo.

También se puede provocar manualmente la conmutación y la recuperación en caso de error en la interfaz `adsl1`. Para obtener más información, consulte el capítulo “La redundancia de interfaces” en el volumen “Alta disponibilidad” del *Manual de referencia de ScreenOS NetScreen: conceptos y ejemplos* para ScreenOS 5.0.0.

Cambio de la dirección de interfaz Trust o Wireless2

Puede modificar la dirección IP y la máscara de red de las interfaces Trust y wireless si es necesario. (Recuerde que cuando la interfaz Trust o wireless2 está en modo NAT, las direcciones IP de los dispositivos de la red nunca están visibles para los equipos externos; los equipos que no forman parte de la red sólo pueden ver la dirección IP de la interfaz Untrust). Por ejemplo, tal vez necesite cambiar la interfaz Trust o wireless2 para que coincida con las direcciones IP ya existentes en la red. Si modifica la dirección IP y la máscara de red de la interfaz Trust o wireless2, deberá cambiar también el intervalo de direcciones que el dispositivo NetScreen asigna a los dispositivos de la red a través de DHCP o deshabilitar el servidor DHCP de la interfaces Trust o wireless2.

Si los equipos conectados a la red obtienen sus direcciones IP del servidor DHCP del dispositivo NetScreen, estos equipos también obtendrán su puerta de enlace predeterminada del dispositivo NetScreen. Si un equipo dispone de una dirección IP asignada de forma estática, debe configurar manualmente su puerta de enlace predeterminada en la dirección IP de la interfaz Trust o wireless2 del dispositivo NetScreen.

Para asignar una dirección IP y una máscara de red distintas a la interfaz Trust o wireless2, consulte el capítulo “Interfaces” en el volumen “Fundamentos” del *Manual de referencia de ScreenOS NetScreen: conceptos y ejemplos* para ScreenOS 5.0.0.

Para modificar los ajustes DHCP del dispositivo NetScreen, consulte el capítulo “Parámetros del sistema” en el volumen “Fundamentos” del *Manual de referencia de ScreenOS NetScreen: conceptos y ejemplos* para ScreenOS 5.0.0.

VERIFICACIÓN DE LA CONECTIVIDAD EXTERNA

Para verificar que las estaciones de trabajo de la red pueden acceder a los recursos de Internet, inicie un explorador web desde cualquier estación de la red e introduzca la siguiente URL: www.juniper.net.

RESTAURACIÓN DE LOS AJUSTES PREDETERMINADOS DE FÁBRICA

Si pierde la contraseña de administrador, puede restaurar los ajustes predeterminados del dispositivo NetScreen. De este modo destruirá la configuración existente, pero restablecerá el acceso al dispositivo.

Aviso: Si restablece los ajustes de fábrica del dispositivo, se eliminarán todos los ajustes de configuración existentes y se inutilizarán el servicio de cortafuegos y la red VPN existentes.

Puede restaurar los ajustes predeterminados del dispositivo mediante uno de los siguientes procedimientos:

- Utilizando una conexión de consola. Para obtener más información, consulte el capítulo “Administración” en el volumen “Administración” del *Manual de referencia de ScreenOS NetScreen: conceptos y ejemplos* para ScreenOS 5.0.0.
- Utilizando el orificio de restablecimiento situado en el panel posterior del dispositivo, tal como se describe en la sección siguiente.

Utilización del orificio de restablecimiento

Puede restablecer el dispositivo y restaurar los ajustes predeterminados de fábrica insertando un objeto punzante en el orificio de restablecimiento y presionando ligeramente. Para realizar esta operación, es necesario ver los diodos LED de estado del dispositivo situados en el panel frontal o iniciar una sesión de consola tal como se describe en [“Utilización de una conexión de consola”, en la página 137](#).

1. Localice el orificio de restablecimiento situado en el panel posterior. Inserte un alambre rígido y fino (como un clip) en el orificio de restablecimiento, presione hacia dentro entre cuatro y seis segundos y retire el alambre.



Orificio de restablecimiento

El LED de estado parpadea con luz ámbar. Aparece un mensaje en la consola que indica que se ha iniciado el borrado de la configuración. El sistema envía una alerta SNMP/SYSLOG.

2. Espere entre uno y dos segundos.

Después del primer restablecimiento, el LED de estado parpadea con luz verde; el dispositivo está a la espera de la segunda pulsación. El mensaje de la consola ahora indica que el dispositivo está a la espera de una segunda confirmación.

3. Introduzca el objeto punzante de nuevo en el orificio y presione hacia dentro entre cuatro y seis segundos.

El mensaje de la consola verifica la segunda confirmación. El LED de estado se enciende con luz ámbar durante medio segundo y, a continuación, la luz pasa a verde intermitente.

A continuación, se restablecen los ajustes originales de fábrica del dispositivo. Cuando el dispositivo se restablece, el LED de estado se enciende con luz ámbar durante medio segundo y, a continuación, la luz pasa a verde. La consola muestra los mensajes de arranque del dispositivo. El sistema genera alarmas SNMP y SYSLOG y las envía a los anfitriones de captura SNMP o SYSLOG configurados.

Una vez reiniciado el dispositivo, la consola muestra el mensaje de inicio de sesión del dispositivo. El LED de estado parpadea ahora con luz verde.

Si no sigue la secuencia completa, el proceso de restablecimiento se cancelará sin que se realice ningún cambio en la configuración. El mensaje de la consola indicará que se ha cancelado el borrado de la configuración. El LED de estado pasará a verde intermitente. Si el dispositivo no se restablece, se enviará una alerta SNMP para confirmar el error.

Descripciones del hardware

En este capítulo se describe de forma detallada el chasis del NetScreen-5GT Wireless.

CONECTOR DE ALIMENTACIÓN Y PUERTOS

El panel posterior del dispositivo NetScreen-5GT Wireless contiene un conector de alimentación y varios puertos.

Antena B

Antena A



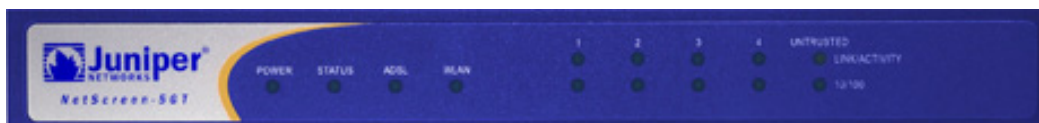
El conector DC POWER (alimentación de CC) sirve para conectar el dispositivo NetScreen-5GT Wireless a la fuente de alimentación. El orificio RESET (restablecimiento) permite reiniciar el dispositivo y restablecer sus ajustes de fábrica. El dispositivo NetScreen-5GT Wireless incluye los siguientes puertos:

Puerto	Descripción	Conector	Velocidad/ protocolo
ADSL	Si es aplicable, permite la conexión a Internet a través de una conexión de datos ADSL.	RJ-11 (Anexo A) RJ-45 (Anexo B)	ANSI T1.413 Issue 2 ITU G.992.1 (G.dmt) ITU 992.2 (G.lite)
Consola	Permite la conexión serie con el sistema. Se utiliza para lanzar sesiones de la interfaz de línea de comandos (CLI).	RJ-45	9.600 bps/ RS-232
Módem	Permite una conexión a Internet serie de acceso telefónico de respaldo a través de un módem externo.	RJ-45	9.600 bps-115 kbps/ RS-232
Untrusted	Permite la conexión a una red sin confianza o a Internet principal o de respaldo mediante un enrutador externo o un módem de cable o módem DSL.	RJ-45	10/100 Mbps/ Ethernet Detección automática de dúplex y polaridad
Puertos 1-4	Permite conectar directamente estaciones de trabajo o una LAN a través de un conmutador ("switch") o concentrador ("hub"). Esta conexión también permite manejar el dispositivo a través de una sesión Telnet o de la aplicación de gestión por la interfaz WebUI.	RJ-45	10/100 Mbps/ Ethernet Detección automática de dúplex y polaridad
Antenas A y B	Permite conectar directamente estaciones de trabajo próximas a una conexión de radio inalámbrica. Esta conexión también permite manejar el dispositivo a través de una sesión Telnet o de la aplicación de administración WebUI.	RPSMA	802.11b 802.11g

Aviso: Nunca conecte una línea telefónica o RDSI directamente al puerto de módem del dispositivo NetScreen-5GT Wireless. En primer lugar debe conectar el dispositivo a un módem utilizando uno de los puertos RS-232 y, a continuación, conectar el módem a la línea.

DIODOS LED DE ESTADO

El panel frontal del dispositivo NetScreen-5GT Wireless presenta unos diodos LED de alimentación y estado para el dispositivo y diodos LED de estado de los puertos para las interfaces.



Diodos LED de estado principales del dispositivo

Los diodos LED de estado del dispositivo indican si éste funciona correctamente. La siguiente tabla describe el estado de cada LED:

LED	Estado	Significado
POWER (alimentación)	verde	Indica que el sistema recibe alimentación.
	apagado	Indica que el sistema no recibe alimentación.
STATUS (estado)	verde intermitente	Indica que el sistema está en funcionamiento.
	verde	Indica que el sistema se está iniciando.
	rojo	Indica un error de diagnóstico o de inicio del sistema.
	apagado	Indica que el sistema no está en funcionamiento.
ADSL (sólo en el Wireless ADSL)	verde	Indica que el bucle ADSL está activo.
	apagado	Indica que el bucle ADSL está inactivo.
WLAN	verde intermitente lento	Indica que se ha establecido una conexión inalámbrica pero no hay actividad.
	verde intermitente rápido	Indica que se ha establecido una conexión inalámbrica. La velocidad de intermitencia es proporcional a la actividad de la conexión.
	apagado	Indica que no se ha establecido una conexión inalámbrica.

Diodos LED de estado de los puertos

Los diodos LED de estado de los puertos indican si los puertos del dispositivo funcionan correctamente. La siguiente tabla describe las posibilidades de cada uno de ellos.

LED	Color	Significado
LINK/ ACTIVITY (enlace/ actividad)	verde intermitente	Indica que el dispositivo ha detectado tráfico Ethernet en el puerto.
	apagado	Indica que el puerto no ha establecido ninguna conexión a otro dispositivo.
	verde	Indica que el puerto ha establecido una conexión a otro dispositivo.
10/100	verde	Indica que el puerto está conectado a un dispositivo 100 Base-T.
	apagado	Indica que el puerto está conectado a un dispositivo 10 Base-T.



Apéndice A Ficha técnica

En este apéndice se muestran las especificaciones generales del dispositivo NetScreen-5GT Wireless.

Dimensiones

Altura	2,93 cm	1,15 pulg.
Fondo	18,45 cm	7,26 pulg.
Anchura	20,8 cm	8,19 pulg.
Peso	0,9 kg	1,98 libras

Características eléctricas

Regulador conmutado	Adaptador de CA: 100 V a 240 V CA +/- 10% 50/60 Hz, 15 a 18 W Entrada de CC: 12 voltios, 1,25 a 1,5 amperios
---------------------	--

Condiciones ambientales

Altitud normal	0-40° C, 32-105° F
Humedad relativa	10-90%
Sin condensación	10-90%

La altitud normal máxima es de 2.000 metros (6.562 pies).

Certificaciones

Seguridad	UL, CUL, TUV, CE, CB
EMI	FCC Parte 15 Clase B, VCCI, CE

Conectores Ethernet

Estándar	100 Base-TX
Tipo de medio	Cable de par trenzado sin blindaje (UTP) de categoría 5 o superior
Distancia máxima	100 metros (328,08 pies)

Los puertos RJ-45 para cable de par trenzado son compatibles con la norma IEEE 802.3 Tipo 10/10 Base-T

Conector ADSL

Tipos	Conector RJ-11 de 6 patillas para el Anexo A Conector RJ-45 para el Anexo B
Tipo de medio	Cable telefónico estándar

CONEXIONES DEL ADAPTADOR DE LA CONSOLA Y EL MÓDEM

La tabla siguiente muestra la ficha técnica del conector RJ-45. Para utilizar un puerto UART estándar, los puertos de la consola y del módem utilizan esta configuración.

RJ-45	Señal	Abreviatura	DCE
1	Request To Send	RTS	Entrada
2	Data Terminal Ready	DTR	Entrada
3	Transmitted Data	TD	Entrada
4, 5	Signal Ground	SGND	N/D
6	Received Data	RD	Salida
7	Not Connected		
8	Clear To Send	CTS	Salida

La siguiente tabla muestra la ficha técnica de la conexión del adaptador de RJ-45 a DB-9. Para utilizar un puerto UART estándar, los puertos de la consola y del módem utilizan esta configuración.

DB9	Señal	Abreviatura	DTE	DCE	RJ45
1	Data Carrier Detect	DCD	Entrada	Salida	NC
2	Received Data	RD	Entrada	Salida	3
3	Transmitted Data	TD	Salida	Entrada	6
4	Data Terminal Ready	DTR	Salida	Entrada	7
5	Signal Ground	SGND	N/D	N/D	4
6	Data Set Ready	DSR	Entrada	Salida	2
7	Request To Send	RTS	Salida	Entrada	8
8	Clear To Send	CTS	Entrada	Salida	1
9	Ring Indicator	RI	Entrada	Salida	NC

Nota: Si utiliza el cable de la consola suministrado con el dispositivo NetScreen para conectarlo a un módem, tendrá que adquirir e instalar un adaptador de módem nulo en el conector del módem.

Índice

A

- ADSL
 - conexión al puerto 129
 - conexión del cable 129
 - configuración de la interfaz 142
- Agregar circuitos virtuales 143
- Ajuste de la fecha 138
- Ajuste de la hora 138
- Ajuste del reloj del dispositivo 138
- ajustes predeterminados 141
 - restaurar 151
- Anexo A 129
- Anexo B 129
 - configuración para Deutsch Telecom 145
- antenas 131

C

- cambiar el modo de puerto 148
- Cambio del modo de puerto 148
- Capa de adaptación ATM 5 142
- Comprobación de conectividad 151
- Conector DB-9 160
- Conector RJ-45 160
- Conectores
 - alimentación 155
 - puerto 155
- Conectores de alimentación 155
- Conectores de puertos 155
- Conexión de la alimentación 132
- configuración
 - ajustes predeterminados 141
 - opcionales 146
 - red inalámbrica 139
 - requerida 137, 141
 - SSID 140
- Configuración de directivas adicionales 147
- contraseña, cambiar 138
- convenciones 136
 - CLI 126
 - WebUI 126

D

- Deutsch Telecom, configuración del Anexo B 145
- Diodos LED
 - estado de los puertos 157
- Diodos LED de estado de los puertos 157
- Dirección de la interfaz de la zona Trust 151
- Dirección IP estática 142
 - configuración 145

G

- Gestión del dispositivo desde un anfitrión (“host”) específico 147

I

- Identificador de trayecto virtual/Identificador de canal virtual
 - Consulte* VPI/VCI
- Identificador del conjunto de servicios
 - Consulte* SSID
- inalámbrica
 - antenas 131
 - configuración 139
 - utilización de la interfaz predeterminada 131
- Inalámbrico
 - Zona Trust 139
 - Zona Wzone1 140
- Inclusión de circuitos virtuales 143
- Interfaz de respaldo en la zona Untrust 150
- Interfaz gráfica, convenciones 126
- interfaz wireless1 140
- interfaz wireless2
 - acceso 135
 - cambio de la dirección de interfaz 151
 - definición de SSID para 140
 - enlace de zonas 139
 - Zona Trust 139

L

- LED
 - estado 156
- LED de estado 156

M

Microfiltro 130
Modificar el nombre de usuario y la contraseña 138
modo de ruta 147
modo transparente 147
Montaje del bastidor con el dispositivo 132
Montaje del dispositivo en el bastidor 132
Multiplexado AAL5 142
multiplexado, configuración 143

N

Nombre de usuario, cambiar 138

O

Organización del manual 125

P

PPPoA 142
 configuración 144
PPPoE 142
 configuración 144
Protocolo punto a punto sobre ATM
 Consulte PPPoA
Protocolo punto a punto sobre Ethernet
 Consulte PPPoE
Publicaciones de NetScreen 127
puerto sin confianza 131
Puertos Ethernet de confianza 131

R

Registro del dispositivo 135
Restablecimiento de los ajustes
 predeterminados 151
Restricción de administración desde un anfitrión
 ("host") específico 147

S

Separador de señal 130
SSID, Identificador del conjunto de servicios 140

U

Utilización de la consola 137
Utilización del orificio de restablecimiento 152

V

VPI/VCI 142
 configuración 143

W

WebUI
 acceso 136
Wireless
 conexión 129, 131

Z

Zona Untrust, configuración de la interfaz de
 respaldo 150

目次

はじめに	165
本書の構成	165
WebUI の規則	166
CLI の規則	166
NetScreen ドキュメント	167
第 1 章 デバイスの接続	169
NetScreen デバイスのネットワークへの接続	169
デバイスのアントラステッドネットワークへの接続.....	169
ADSL ポートの接続	169
アントラステッドポートへの接続	171
内部ネットワークまたはワークステーションへのデバイスの接続.....	171
トラステッドイーサネットポートの接続	171
ワイヤレスインターフェースの使用	171
電源の接続	172
ラックの取り付け (オプション):	172
第 2 章 デバイスの構成	175
デバイスのアクセス	175
WebUI の使用.....	175
Telnet の使用	176
コンソール接続の使用	177
必要な構成	177
管理者ログイン名およびパスワードを変更する.....	178
日付および時間の設定	178
ワイヤレスの構成	179
ワイヤレスネットワークの構成	180
ADSL の構成	181
ADSL インターフェースの構成	182
ADSL インターフェースに仮想回路を追加する.....	183
VPI/VCI および複合方式.....	183
PPPoE または PPPoA.....	184
Annex B モード.....	185
静的 IP アドレスおよびネットマスク	185
オプションの構成	186
管理の制限.....	187
他のポリシーの構成.....	187
動作モード.....	187
ポートモードを変更する.....	188
バックアップ Untrust ゾーンインターフェースの構成.....	190

Trust または Wireless2 インターフェースアドレスの変更	191
外部との接続性の確認	191
デバイスを工場出荷時のデフォルト設定にリセットする	191
リセットスイッチの使用.....	192
第 3 章 ハードウェアの説明	193
ポートと電源のコネクタ	193
ステータス LED	194
デバイスの主要ステータス LED.....	195
ポートステータス LED.....	195
仕様.....	197
索引	199

はじめに

Juniper Networks NetScreen-5GT ワイヤレスデバイスは、**IPSec** 仮想プライベートネットワーク (**VPN**) およびファイアウォールサービスを、統合ワイヤレス **802.11 b/g** インターフェースを使用する営業所や小売店向けに提供しています。**NetScreen-5GT** ワイヤレスデバイスは、**NetScreen** の中央側ハイエンド製品に装備されているファイアウォール、**VPN**、およびトラフィック管理と同じテクノロジーを駆使しています。

Juniper Networks は、**3** 種類の **NetScreen-5GT** ワイヤレスデバイスのモデルを提供しています。

- **NetScreen-5GT** ワイヤレス : ワイヤレスのみのモデル。
- **NetScreen-5GT** ワイヤレス **ADSL A : Annex A** モデルを装備したワイヤレスは、標準の電話回線を使用する **ADSL** をサポートします (**POTS**)。
- **NetScreen-5GT** ワイヤレス **ADSL B : Annex B** モデルを装備したワイヤレスは、**ISDN** (総合デジタル通信網) を使用する **ADSL** をサポートします。

モデルはすべて、最大 **4** つのワイヤレス セキュリティゾーンまでサポートします。いずれの **ADSL** モデルも **ANSI T1.413 Issue 2**、**ITU G.992.1. (G.dmt)**、および **ITU 992.2 (G.lite)** 規格をサポートします。

モデルはそれぞれ次の **3** つのソフトウェアバージョンをサポートします。

- **10** ユーザバージョンは、最大 **10** 人のユーザをサポートします。
- **Plus** バージョンは、無制限のユーザをサポートします。
- **Extended** バージョンは **Plus** バージョンと同じ性能を装備している上に、高可用性 (**NSRP Lite**)、**DMZ** セキュリティゾーン、追加セッションとトンネル機能などの追加機能もあります。

本書の構成

本書には **3** つの章と付録があります。

第 1 章、「**デバイスの接続**」この章では、デバイスのネットワークへの接続方法、電源やアンテナの接続方法、**NetScreen-5GT** ワイヤレスデバイスのラックへの取り付け方法を説明します。

第 2 章、「**デバイスの構成**」では、**NetScreen-5GT** ワイヤレス (**ADSL**) のデフォルト設定と操作およびデバイスの仕様に必要な構成を説明します。

第 3 章、「**ハードウェアの説明**」では、**NetScreen-5GT** ワイヤレスポート、**LED**、電源要件を説明します。

付録 A、「**仕様**」には、**NetScreen-5GT** ワイヤレスデバイスの物理的仕様のリストがあります。

WEBUI の規則

本書を通して、シェブロン (>) はメニューオプションやリンクをクリックする WebUI のナビゲーションを示しています。

例： **Objects > Addresses > List > New**

新規アドレス構成のダイアログボックスにアクセスするには次の手順に従います。

1. メニュー列の **Objects** をクリックします。
Objects メニューの選択項目が表示されます。
2. (**Applet** メニュー¹) マウスカーソルを **Addresses** に合わせます。
(**DHTML** メニュー) **Addresses** をクリックします。
Addresses メニューの選択項目が表示されます。
3. **List** をクリックします。
アドレスのリストが表示されます。
4. 右上隅の **New** リンクをクリックします。
新規アドレス構成のダイアログボックスが表示されます。

CLI の規則

次の規則は、コマンドラインインターフェース (CLI) コマンドの構文を記述する際に適用されます。

- 角括弧 [] 内にあるものはすべてオプションです。
- 中括弧 { } 内にあるものはすべて必須です。
- 選択肢が複数ある場合、各選択肢はパイプ (|) で区切られています。たとえば、

```
set interface { ethernet1 | ethernet2 | ethernet3 }  
manage
```

は、「**ethernet 1**、**ethernet 2**、または **ethernet 3** インターフェースの管理オプションを設定する」という意味です。
- 変数は斜体で表示されます。例えば、次のように表示されます。

```
set admin user name1 password xyz
```

-
1. メニュー列の下にある **Toggle Menu** をクリックして、**applet** か **DHTML** のどちらかのメニュータイプを選択できます。

CLI コマンドが文中に記載されている場合には、**太字**で表示されます (変数は例外で、必ず斜体です)。例えば、次のように表示されます。「**NetScreen** デバイスのシリアルナンバーを表示するには、**get system** コマンドを使用します」

注記： キーワードを入力する際には、そのキーワードを間違いなく識別できる文字数を入力するだけで十分です。たとえば、**set admin user joe j12fmt54** のコマンドを入力する場合、**set adm u joe j12fmt54** と入力するだけで十分です。コマンドを入力する際にはこのショートカットが使用できますが、本書に記載されるコマンドはすべて本来の形式で記載されています。

NETSCREEN ドキュメント

Juniper Networks NetScreen の技術関連文書を入手するには、www.juniper.net/techpubs/ にアクセスしてください。

テクニカルサポートについては、<http://www.juniper.net/support/> にある **Case Manager** のリンクを使って事例サポートを開くか、**1-888-314-JTAC** (米国内) か **1-408-745-9500** (米国外から) までお問い合わせください。

本書の内容に間違いや欠落などがあった場合には、以下の **E** メールアドレスまでご連絡ください。

techpubs-comments@juniper.net

デバイスの接続

本章では、**NetScreen-5GT** ワイヤレスデバイスのネットワークへの接続方法、電源への接続方法、アンテナへの接続方法を説明しています。オプションの **NetScreen-5GT** ワイヤレスラックマウントキットを使用する場合には、本章の終わりに記載されているラックの取り付け方法を参照してください。

注記： 安全上の注意と手順については、『**NetScreen Safety Guide (安全ガイド)**』を参照してください。このマニュアルの指示事項は、身体に危害を及ぼす恐れのある状況を警告するものです。設備機器についてはすべて、電気回路に関する危険を認識し、事故を防止する標準の手順を熟知した上で操作してください。

NETSCREEN デバイスのネットワークへの接続

NetScreen デバイスは、内部ネットワークとアントラステッドネットワークの間に配置すると、ネットワークにファイアウォールを配備し、一般的なセキュリティを確保します。このセクションでは、物理的な接続について説明します。

デバイスのアントラステッドネットワークへの接続

NetScreen-5GT ワイヤレスデバイスのどのモデルを使用するかによって、以下のいずれかの方法でアントラステッドネットワークに接続できます。

- **NetScreen** デバイスの **ADSL** ポートから **ADSL** 接続を使用する
- **NetScreen** デバイスのアントラステッドポートからイーサネット接続を使用する

ADSL ポートの接続

NetScreen-5GT ワイヤレス **ADSL** デバイスの **ADSL** ポートから提供された **ADSL** ケーブルを電話線に接続します。デバイスの **Annex A** バージョンの **ADSL** ポートは **RJ-11** コネクタを使用しますが、**Annex B** バージョンは **RJ-45** コネクタを使用します。**Annex B** モデルの場合、**ADSL** ポートから電話線への接続ケーブルは、**10 Base-T** イーサネットケーブル（ストレート）とまったく外見が同じです。

警告： **NetScreen** デバイスのコンソール、モデム、またはイーサネットポートから誤って電話線に接続しないように注意してください。

NetScreen-5GT ワイヤレス **ADSL** デバイスでは、**ADSL** 回線が外部ネットワークへの主要な接続になります。外部ネットワークへのバックアップデータリンクのために、**NetScreen-5GT** ワイヤレス **ADSL** デバイスのアントラステッドポートからイーサネットケーブルを外部ルーターまたは **DSL**、あるいはケーブルモデムに接続するか、デバイスのモデムポートからシリアルケーブルを外部モデムに接続できます。

警告： デバイスのアントラステッドポートとモデムポートの両方を、同時に外部のネットワークに接続することはできません。

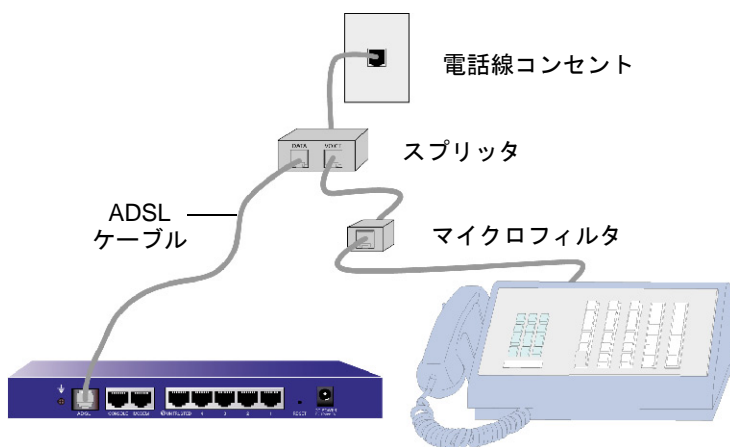
スプリッタとマイクロフィルタの接続

信号スプリッタは、電話信号を音声通信のための低周波数の音声信号とデータ通信のための高周波数データ信号に分割します。サービスプロバイダは通常、プロバイダのネットワークに電話線を接続する装置の一部としてスプリッタを設置します。

サービスプロバイダの装置によっては、自分で設置することができるスプリッタもあります。スプリッタを自分自身でインストールする場合は、**ADSL** ケーブルを **NetScreen** デバイスと電話線からスプリッタ上の該当するコネクタ（例、「データ」または「音声」）に接続し、スプリッタのもう一方の終端を電話線に接続します。

ADSL 回線に接続された各電話、ファックス、留守番電話、またはアナログモデムにマイクロフィルタを設置する必要があります。マイクロフィルタは電話線の高周波数のノイズを除去します。電話、ファックス、留守番電話、またはアナログモデムとスプリッタの音声コネクタの間の電話線上にマイクロフィルタを設置します。

以下は、マイクロフィルタやスプリッタのインストールの例を示します。（サービスプロバイダから適切なマイクロフィルタまたはスプリッタを入手してください。）



アントラステッドポートへの接続

インターネット接続を外部ルーター、DSL モデムまたはケーブルモデムに確立でき、ネットワークのファイアウォールと一般的なセキュリティを提供します。高速接続を確立するには、NetScreen-5GT ワイヤレスデバイスの **Untrusted** インターフェースから指定されたイーサネットケーブルを外部ルーターまたはモデムに接続します。NetScreen-5GT ワイヤレスデバイスは、正しい速度、全二重、および極性の設定を自動感知します。

NetScreen-5GT ワイヤレス ADSL デバイスを使用している場合は、ADSL 接続の方法について、[169 ページの「ADSL ポートの接続」](#)と [170 ページの「スプリッタとマイクロフィルタの接続」](#)を参照してください。

内部ネットワークまたはワークステーションへのデバイスの接続

ローカルエリアネットワーク (LAN) またはワークステーションを、以下のいずれかまたは両方の方法で接続できます。

- NetScreen デバイスの 1 つまたは複数のトラステッドイーサネットポートを通じて接続する
- NetScreen デバイスのワイヤレスインターフェースを使用する

トラステッドイーサネットポートの接続

NetScreen-5GT ワイヤレスデバイスにはトラステッドイーサネットポートが 4 つあります。スイッチまたはハブ経由で LAN に接続するときにこれらの 1 つまたは複数のポートを使用できます。ポートのうち 1 つかすべてをワークステーションに直接接続して、ハブやスイッチの必要性をなくすこともできます。クロスケーブルかストレートケーブルのいずれかを使用して、イーサネットポートを他のデバイスに接続できます。

ワイヤレスインターフェースの使用

ワイヤレスインターフェースを使用する場合、デバイスで指定されたアンテナに接続する必要があります。標準 2dB の無指向性アンテナを使用している場合、デバイスの背面の **A** と **B** というマークのポストにねじ止めし、[193 ページの「ポートと電源のコネクタ」](#)を参照してください。アンテナを肘でまげて、バルクヘッドコネクタに圧力をかけます。

電源の接続

NetScreen-5GT ワイヤレスデバイスを電源に接続するには次の手順に従って行います。

1. 電源ケーブルの **DC** コネクタ側をデバイスの背面にある **DC** 電源ポートに差し込みます。
2. 電源ケーブルの **AC** アダプタ側を **AC** 電源コンセントに差し込みます。

警告：弊社では電源接続用にサージ保安器を使用することをお勧めします。

ラックの取り付け (オプション):

NetScreen-5GT ワイヤレスラックマウントキットを使用すれば、標準の **19** インチ設備ラック内に **NetScreen-5GT** ワイヤレスデバイスを **2** つまで取り付けることができます。

NetScreen-5GT ワイヤレスラックマウントキットには取り付け方法とラック取り付けトレイが付属しています。このトレイの寸法は、次のとおりです。

幅：	48.26 cm	19 in.
高さ	4.013 cm	1-5/8 インチ (1 ラック単位)
奥行き：	33.655 cm	13-1/4 インチ

NetScreen-5GT ワイヤレスデバイス、ラックマウントキットと設備ラックの他に次の必要になります。

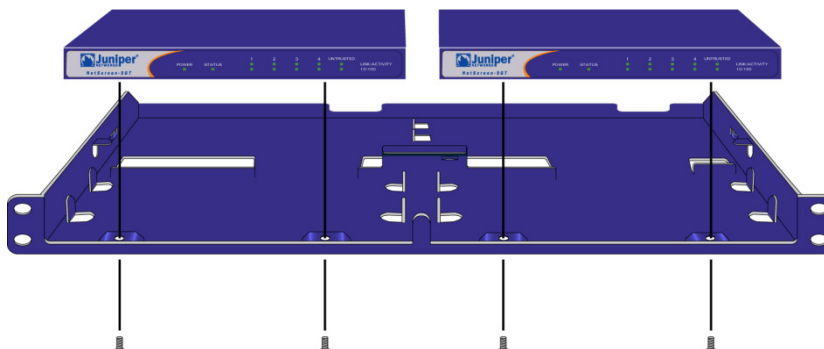
- プラスのネジ回し
- 設備ラックのネジサイズに合うネジ **4** 本

ラックにデバイスを取り付けるには以下の手順で行います。

1. 取り付けようとしている **NetScreen-5GT** ワイヤレスの各デバイスの底面からプラスのネジ回しを使ってネジを **2** 本取り外します。(ネジは次のステップで使用するのに取っておきます。) ネジはデバイスの底面で正面パネルの近くにあります。



2. デバイスをラックマウントトレイに入れて、ステップ 1 で取り外したネジを使ってトレイに固定します。



3. 左と右のトレイプレートを設置ラックにネジで固定します。



電源コードやイーサネットケーブルはトレイの底面にある開口部から通すようにするか、または後壁にあるくぼみ部分から出すようにします。デバイスの後部にあるスペースは電源装置を納めるのに使用することもできます。

デバイスの構成

本章では、**NetScreen-5GT** ワイヤレスデバイスをネットワークに接続してからの構成方法について説明します。**ScreenOS WebUI** グラフィカルインターフェースを使用して初めてデバイスにアクセスする場合、設定開始ウィザードを使用して基本構成を行うことができます。このウィザードの使用法については、**Juniper Networks NetScreen-5GT Wireless Getting Started Guide** を参照してください。

本章で説明されているトピックは以下のとおりです。

- デバイスのアクセス
- 必要な構成
- ワイヤレスの構成
- **ADSL** の構成
- オプションの構成
- 外部との接続性の確認
- デバイスを工場出荷時のデフォルト設定にリセットする

注記： **NetScreen** デバイスを設定し、インターネットへの接続を確認したら、お持ちの製品を www.juniper.net/support/ で登録し、内部のウィルス対策や **Deep Inspection Signature Service** など、デバイスへの構成の **ScreenOS** サービスを有効にしてください。製品を登録した後で、**WebUI** を使用してサービスの購読を行います。お持ちの製品の登録と特定のサービスの購読に関する詳細は、**ScreenOS 5.0.0** の『**NetScreen** 概念と用例 **ScreenOS** リファレンス ガイド』の「基本」の「システムパラメータ」の章を参照してください。

デバイスのアクセス

このセクションでは、**WebUI**、**Telnet**、または **Console** 接続を使用して **NetScreen** にアクセスする方法を説明します。

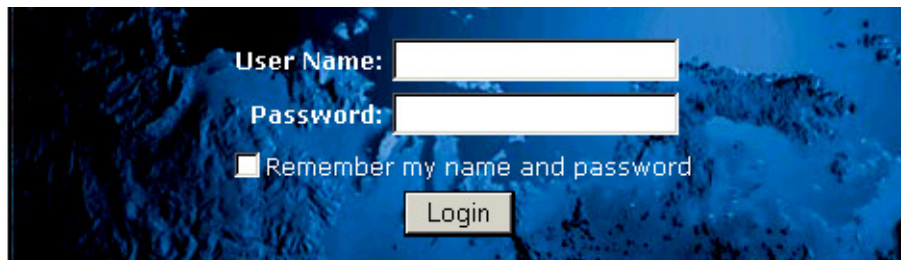
WebUI の使用

ScreenOS WebUI とは、**Web** ブラウザから使用できるグラフィカルインターフェースです。**WebUI** を使用するには、**Trust** または **wireless2** インターフェースと同じサブネットワーク上からアクセスする必要があります。**WebUI** 管理アプリケーションのある **NetScreen-5GT** ワイヤレスデバイスにアクセスするには、以下の手順に従って行います。

1. ブラウザを起動し、**URL** フィールドに **Trust** または **wireless2** インターフェースの **IP** アドレスを入力してから、**Enter** キーを押します。たとえば、**URL** フィールドに以下のように入力します。

192.168.1.1

NetScreen の WebUI ソフトウェアでは次のようなログインプロンプトが表示されます。



注記： 設定開始ウィザードを省略するように選択すると、**WebUI** のログインプロンプトが自動的に表示されます。

2. デフォルトのユーザー名とパスワードを変更していない場合は、**User Name** および **Password** フィールドの両方に **netscreen** と入力して、**Login** をクリックします (小文字のみを使用してください。ユーザー名フィールドでもパスワードフィールドでも、大文字小文字が区別されます)。

Telnet の使用

Telnet とは、**IP** (インターネットプロトコル) ネットワークからデバイスをアクセスできるようにするアプリケーションです。

注記： **SSH (Secure Shell)** アプリケーションを使用すれば、**NetScreen** デバイスにもアクセスできます。詳細については、**ScreenOS 5.0.0** の『**NetScreen** 概念と用例 **ScreenOS** リファレンス ガイド』の「管理」部の「管理」の章を参照してください。

Telnet を使用してデバイスの構成を行うには、ワークステーションから **Telnet** セッション中に **ScreenOS** の **CLI (Command Line Interface, コマンドラインインターフェース)** コマンドを入力します。

1. **Trust** インターフェースまたは **wireless2** の **IP** アドレスに対して **Telnet** クライアントアプリケーションを開始します。たとえば、以下のように入力します。

```
telnet 192.168.1.1
```
2. デフォルトのユーザー名とパスワードを変更していない場合は、**Login** および **Password** プロンプトの両方で **netscreen** と入力します (小文字のみを使用してください。ログインプロンプトでもパスワードプロンプトでも、大文字小文字が区別されます)。

コンソール接続の使用

NetScreen-5GT ワイヤレスデバイスのコンソールポートを使うと、ワークステーションまたは端末に接続されたシリアルケーブルからデバイスにアクセスできるようになります。コンソール接続を使用してデバイスの構成を行うには、ワークステーションのターミナルエミュレーションプログラムまたは端末で **ScreenOS** の **CLI** コマンドを入力します。

注記： コンソール接続の場合には、**RJ-45** オスコネクタと **DB-9** メスコネクタのそれぞれを両端に持つシリアルケーブルが必要になります。シリアルケーブルのコネクタピン配列については、[付録 A](#)、[仕様](#)を参照してください。

コンソール接続を確立するには、次の手順に従って行います。

1. シリアルケーブルの **DB-9** メス側をコンピュータのシリアルポートに差し込みます (**DB-9** コネクタがポートに正しくはめこまれているかを確認します)。
2. シリアルケーブルの **DB-9** コネクタの反対側を **RJ-45 DB-9** ポートに差し込みます (**DB-9** コネクタが **RJ-45 DB-9** ポートに正しくはめこまれているかを確認します)。
3. シリアルケーブルの **RJ-45** オス側を **NetScreen-5GT** ワイヤレスデバイスのコンソールポートに差し込みます (**RJ-45** コネクタがポートに正しくはめこまれているかを確認します)。
4. シリアルターミナルエミュレーションプログラムを起動します (通常使用されるターミナルプログラムは **Hilgreave HyperTerminal** です)。 **NetScreen-5GT** ワイヤレスデバイスでコンソールセッションを開始するのに必要な設定は次のとおりです。
 - ボーレート : **9600**
 - パリティ : なし
 - データビット : **8**
 - ストップビット : **1**
 - 制御フロー : なし
5. デフォルトのユーザー名とパスワードを変更していない場合は、**Login** および **Password** プロンプトの両方で **netscreen** と入力します (小文字のみを使用してください。ログインフィールドでもパスワードフィールドでも、大文字小文字が区別されます)。

必要な構成

このセクションでは、デバイスの使用に必要な構成について説明します。

注記： デバイスのデフォルト設定を復旧するには、[191](#) ページの「[デバイスを工場出荷時のデフォルト設定にリセットする](#)」を参照してください。

管理者ログイン名およびパスワードを変更する

NetScreen の全製品ではデフォルトで同じ管理者名とパスワード (**netscreen**) を使用するため、管理者名とパスワードをすぐに変更することが賢明です。管理者名とパスワードをそれぞれ **netscreen** と **netscreen** から **darwin1** と **1240jes** に変更するには、以下の手順に従って行います。

WebUI

Configuration > Admin > Administrators > Edit (NetScreen 管理者の名前):

次のように入力してから **OK** をクリックします。

Administrator Name: darwin1

Old Password: netscreen

注記: パスワードを入力しても、**WebUI** 上に表示されません。

New Password: 1240jes

Confirm New Password: 1240jes

CLI

```
set admin name darwin1
set admin password 1240jes
save
```

異なるレベルの管理者を作成する方法の詳細については、**ScreenOS 5.0.0** の『**NetScreen** 概念と用例 **ScreenOS** リファレンス ガイド』の「管理」部の「管理」の章を参照してください。

日付および時間の設定

NetScreen デバイスに設定された時刻は、VPN トンネルの設定やスケジュール時間などのイベントに影響します。NetScreen デバイスの日付や時間をもっとも簡単に設定する方法は、デバイス上のシステムクロックをお使いのコンピュータのクロックに同期させることです。WebUI からこれを行うには、以下の手順に従って実行します。

1. **Configuration > Date/Time: Sync Clock with Client** ボタンをクリックします。
コンピュータクロックで夏時間 (DTS) を使用可能にしているかどうかを指定するように求めるポップアップメッセージが表示されます。
2. **Yes** をクリックすると、システムクロックを同期化して夏時間に合わせて調整します。**No** をクリックすると、夏時間に合わせずにシステムクロックを同期化します。

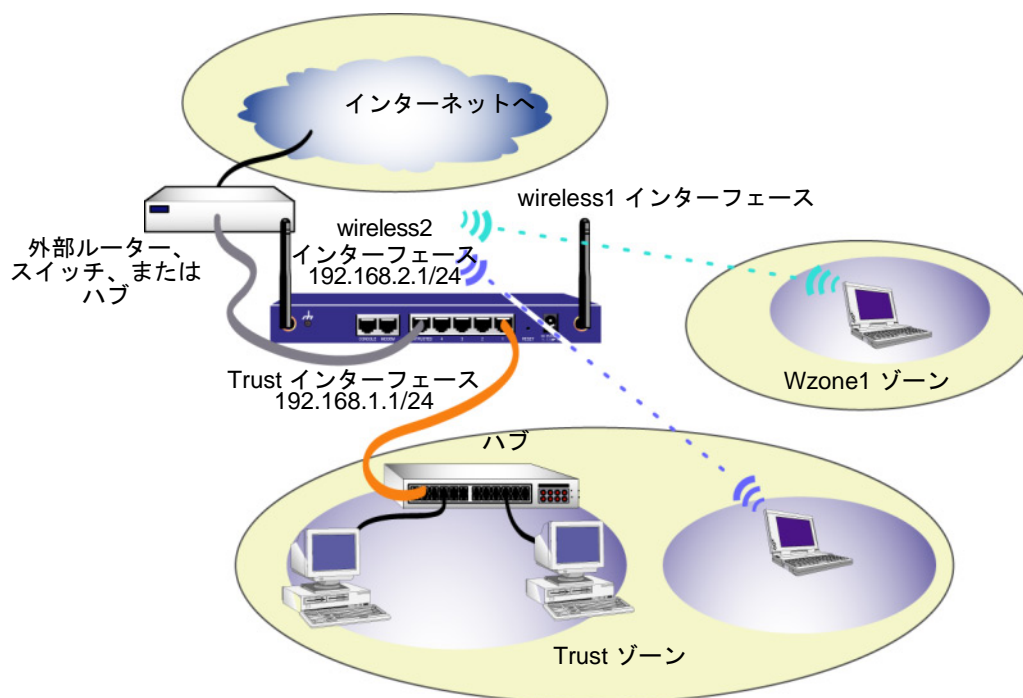
また、**Telnet** または コンソールセッションで **CLI** の **set clock** コマンドを使用して、手動で日付と時間を設定することもできます。

ワイヤレスの構成

このセクションでは、**NetScreen** デバイスでワイヤレスインターフェースを構成する方法について説明します。インストールしたライセンスの種類によって、**NetScreen-5GT** ワイヤレスデバイスには最大 **4** つのセキュリティゾーンを構成できます。ゾーンバインディングとのインターフェースはあらかじめ定義されており、構成するポートモードによって異なります。また、**Untrust** ゾーンにワイヤレスインターフェースを割り当てることはできません。**NetScreen** デバイスでは、最低 **1** つのワイヤレスインターフェースを構成して、**WLAN** (ワイヤレスローカルエリアネットワーク) を作成する必要があります。

注記： 米国または日本以外の国で **NetScreen-5GT** ワイヤレスデバイスを動作する場合は、**set wlan country-code** コマンドを使用してから **WLAN** 接続を確立してください。このコマンドを使用すると、選択可能なチャネル範囲を設定し、電力レベルを送信できます。

次の図は **NetScreen-5GT** ワイヤレスデバイスのデフォルト構成を示します。



デフォルトのワイヤレスインターフェースには、あらかじめ「**wireless2**」という名前が定義されています。**Trust** インターフェースおよび **wireless2** インターフェースは、**Trust** ゾーンにバインドされており、サブネットワークアドレスはそれぞれ、**192.168.1.1/24** と **192.168.2.1/24** に設定されています。つまり、**Trust** ゾーンで接続するデバイスはすべて、**Trust** インターフェースまたは **wireless2** インターフェースのどちらかと同じサブネットワークにある必要があります。また、**NetScreen** デバイスは **192.168.1.1/24** および **192.168.2.1/24** サブネットワークの **IP** アドレスをデバイスに割り当てるように構成されています。詳細情報は、**191** ページの「**Trust** または **Wireless2** インターフェースアドレスの変更」を参照してください。

デフォルトでは、**wireless1** インターフェースは **Wzone1** ゾーンにバインドされており、**IP** アドレスは割り当てられていません。**wireless1** インターフェースを使用する場合は、**IP** アドレスを設定する必要があります。詳細については、*NetScreen-5GT Wireless Reference Guide* を参照してください。

NetScreen デバイスは **Trust** ゾーンのデバイスから発信されたインターネットへのあらゆるタイプのトラフィックを許可しますが、インターネットから発信されたトラフィックがネットワークへと到達することを許可しません。この他の制限を構成することもできますが、詳細については [187 ページの「他のポリシーの構成」](#) を参照してください。

ワイヤレスネットワークの構成

ワイヤレスネットワークは、**SSIDs (Service Set Identifiers)** として参照される名前で構成されています。**SSID** を指定すると、同じ位置に複数のワイヤレスネットワークを持つことができます。各デバイスには最大 **8** つの **SSID** を設定できます。**SSID** の名前を設定してその属性を設定することができます。

SSID の名前に **netscreen open** と設定するには、ワイヤレスネットワーク接続を許可して、**wireless2** インターフェースをアクティブにします。

WebUI

Wireless > SSID > New: 次のように入力してから **OK** をクリックします。

SSID: “netscreen open”

Wireless Interface Binding: wireless2 (選択)

Activate Changes > Activate Changes ボタンをクリックします。

CLI

```
set ssid name "netscreen open"  
set ssid "netscreen open" authentication open encryption  
none  
set ssid "netscreen open" interface wireless2  
exec wlan reactivate
```

wireless2 インターフェースに **SSID** を設定すると、デバイスを構成するための手順 [175 ページの「デバイスのアクセス」](#) に従って、デフォルトの **wireless2** インターフェース **IP** アドレスを使用してアクセスすることができます。構成例、**SSID** 属性、ワイヤレスセキュリティ構成に関する **CLI** コマンドの詳細については、*NetScreen-5GT Wireless Reference Guide* を参照してください。

ADSL の構成

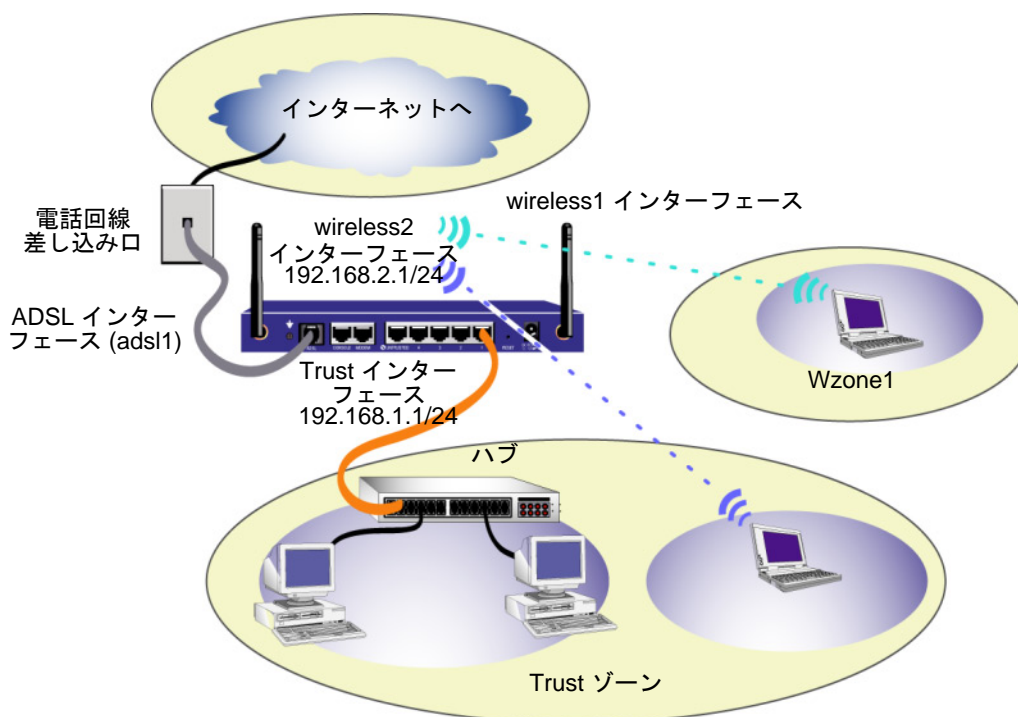
このセクションでは、NetScreen-5GT ワイヤレス ADSL Annex A および B の出荷時のデフォルトの設定と操作について説明します。ほとんどの場合、デフォルトで設定されているので構成する必要のある項目はわずかしかなりません。

このセクションでは、Untrust ゾーンインターフェースの以下の構成について説明します。

- **ADSL** インターフェースの構成
- **ADSL** インターフェースに仮想回路を追加する
- **VPI/VCI** および複合方式
- **PPPoE** または **PPPoA**
- **Annex B** モード
- 静的 **IP** アドレスおよびネットマスク

注記： デバイスのデフォルト設定を復旧するには、**191** ページの「デバイスを工場出荷時のデフォルト設定にリセットする」を参照してください。

次の図では NetScreen-5GT ワイヤレス ADSL デバイスのデフォルト構成を示します。



ADSL インターフェースには、あらかじめ「**adsl1**」という名前が定義されており、これはお使いのネットワークからインターネットへの主要接続となります。NetScreen デバイス (およびネットワーク上のデバイス) のインターネット接続を許可するには、ISP (Internet Service Provider, インターネットサービスプロバイダ) から得られる情報に従って **adsl1** インターフェースを構成する必要があります。182 ページの「ADSL インターフェースの構成」を参照してください。

NetScreen デバイスは **Trust** ゾーンのデバイスから発信されたインターネットへのあらゆるタイプのトラフィックを許可しますが、インターネットから発信されたトラフィックがネットワークへ到達することは許可しません。この他の制限も構成することもできますが、詳細については 187 ページの「他のポリシーの構成」を参照してください。

ADSL インターフェースの構成

お使いのネットワークでは、NetScreen デバイス上で ADSL インターフェース「**adsl1**」を使用して、ATM (非同期転送モード) 仮想回路経由でサービスプロバイダーのネットワークに接続しています。さらに仮想回路を構成するには、ADSL サブインターフェースを作成します (詳細については、183 ページの「ADSL インターフェースに仮想回路を追加する」を参照してください)。

WebUI から、**Network > Interfaces** ページにアクセスし、NetScreen デバイスの現在のインターフェース一覧を参照してください。Telnet またはコンソールセッションを使用している場合は、CLI コマンド **get interface** と入力します。**adsl1** インターフェースが **Untrust** ゾーンにバインドされていることが分かります。ICW を使用してデバイスを設定した場合は、IP アドレスとネットマスクがすでに **adsl1** インターフェースに割り当てられている可能性があります。

注記: ADSL インターフェースを使用しない場合は、**set interface adsl1 zone null** コマンドを使用して **Null** ゾーンにバインドします。ICW を使用してデバイスを設定している場合は、**Untrust** ゾーンへのデフォルトのインターフェースとして、ADSL インターフェース以外のインターフェースを選択できます。

NetScreen デバイスをサービスプロバイダーのネットワークに接続できるようにするには、**adsl1** インターフェースを構成する必要があります。そのためには、サービスプロバイダーから以下の情報を入手してください。

- VPI/VCI (仮想パス識別子および仮想チャネル識別子) の値
- 以下のいずれかの AAL5 (ATM Adaptation Layer 5) 複合方式
 - 仮想回路 (VC) ベースの複合方式 (各プロトコルは個別の ATM VC に引き継がれる)
 - 論理リンク制御 (LLC) カプセル化。複数のプロトコルを同一 ATM VC に引き継ぐことができる (デフォルトの複合方式)
- PPPoE (Point-to-Point Protocol over Ethernet) または PPPoA (Point-to-Point Protocol over ATM) を利用したサービスプロバイダーのネットワークへの接続用にサービスプロバイダーから割り当てられたユーザー名およびパスワード
- 認証方法 (PPPoE または PPPoA 接続のいずれかがある場合)
- オプションで、ご使用のネットワークの静的 IP アドレスおよびネットマスク値

ADSL インターフェースに仮想回路を追加する

仮想回路を追加するには、ADSL インターフェースにサブインターフェースを作成します。ADSL サブインターフェースは最大 **10** 個まで作成できます。たとえば、「Corp1」というユーザー定義ゾーンにバインドされている **adsl1.1** という名前の新しいサブインターフェースを作成するには、以下の手順に従って行います。

WebUI

Network > Interfaces > New ADSL Sub-IF: 次のように入力して、**Apply** をクリックします。

Interface Name: adsl1.1

VPI/VCI: 0/35

Zone Name: Corp1 (選択)

CLI

```
set interface adsl1.1 pvc 0 35 zone corp1
save
```

ADSL サブインターフェースは、**182** ページの「**ADSL インターフェースの構成**」に説明のあるように、**VPI/VCI** 値の設定を含むメインの ADSL インターフェースと同様に構成する必要があります。ADSL サブインターフェースは、メインの ADSL インターフェースとは個別に構成します。つまり、メインの ADSL インターフェースとは異なる複合方式、**VPI/VCI** および **PPP** クライアントをサブインターフェースに構成することができます。また、メインの ADSL インターフェースに静的 **IP** アドレスがなくても、サブインターフェースに静的 **IP** アドレスを構成することができます。片方のインターフェースが **PPPoA** に、もう片方が **PPPoE** に構成されており、どちらも **LLC** 複合方式を使用している場合は、サブインターフェースとメインの ADSL インターフェースは同じ **VPI/VCI** 値を使用できます。

VPI/VCI および複合方式

サービスプロバイダーでは、各 **VC** 接続に対し、**VPI/VCI** のペアを割り当てています。たとえば、**VPI/VCI** のペアとして **1/1** を受信したとすると、これは、**VPI** 値が **1**、**VCI** 値が **1** であることを意味しています。この値は、サービスプロバイダーが **DSLAM (Digital Subscriber Line Access Multiplexer)** の加入者側で構成する値と一致していなければなりません。

adsl1 インターフェースで **VPI/VCI** ペアを **1/1** に構成するには、以下の手順に従って実行します。

WebUI

Network > Interfaces > Edit (adsl1 インターフェース): **VPI/VCI** フィールドに **1/1** を入力し、**Apply** をクリックします。

CLI

```
set interface adsl1 pvc 1 1
save
```

デフォルトでは、**NetScreen-5GT** ワイヤレス ADSL デバイスは、各 **VC** に対し **LLC** ベースの複合方式を使用しています。**adsl1** インターフェース上で **VPI/VCI** を **1/1** に構成し、**VC** で **LLC** カプセル化を使用するには、以下の手順に従って実行します。

WebUI

Network > Interfaces > Edit (adsl1 インターフェース): 以下を入力して、**Apply** をクリックします。

VPI/VCI: 1 / 2

Multiplexing Method: LLC (選択)

CLI

```
set interface adsl1 pvc 1 1 mux llc
save
```

PPPoE または PPPoA

NetScreen デバイスには、**PPPoE** クライアントと **PPPoA** クライアントの両方があり、**ADSL** リンクを介してサービスプロバイダーのネットワークに接続します。**PPPoE** は **ADSL** カプセル化のもっとも一般的な形式であり、ネットワーク上の各ホストの終端に利用されます。**PPPoA** は、**PPP** セッションが **NetScreen** デバイスで終了するため、基本的にビジネスクラスのサービスに利用されます。**NetScreen** デバイスがサービスプロバイダーのネットワークに接続できるようにするには、サービスプロバイダーが割り当てたユーザー名とパスワードを構成する必要があります。**PPPoA** の構成は、**PPPoE** の構成に似ています。

注記: **NetScreen** デバイスは、各仮想回路で 1 つの **PPPoE** セッションのみに対応しています。

PPPoE にユーザー名「**roswell**」とパスワード「**area51**」を構成して、**PPPoE** の構成を **adsl1** インターフェースにバインドするには、以下の手順に従って実行します。

WebUI

Network > PPPoE > New: 次のように入力して **OK** をクリックします。

PPPoE Instance: poe1

Bound to Interface: adsl1 (選択)

Username: roswell

Password: area51

CLI

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1
save
```

NetScreen デバイスで構成可能な **PPPoE** や **PPPoA** のパラメータには他に、認証方法 (デフォルトでは、チャレンジハンドシェイク式認証プロトコルかパスワード認証プロトコルのいずれかをサポート)、アイドルタイムアウト (デフォルトでは **30 分**) などがあります。サービスプロバイダーのサーバーと適切な通信を行うために構成する必要のある他の **PPPoE** や **PPPoA** のパラメータについては、ご利用のサービスプロバイダーにお尋ねください。

Annex B モード

NetScreen-5GT ワイヤレス ADSL デバイスの Annex B モデルを Deutsch Telecom の ADSL 線に接続する場合は、この機器での操作用に、ADSL ポートに物理インターフェースを構成する必要があります。このためには、以下の手順に従って実行します。

WebUI

Network > Interfaces > Edit (adsl1 インターフェース): Annex B モードに DT を選択し、**Apply** をクリックします。

CLI

```
set interface adsl1 phy annex-b-mode dt
save
```

デバイスの Annex A モデルを使用しているか、または Deutsch Telecom 以外の機器に接続している場合は、この設定を行う必要はありません。

静的 IP アドレスおよびネットマスク

ISP からネットワーク用の特定の固定 IP アドレスおよびネットマスクを割り当てられている場合、ネットワークの IP アドレスとネットマスクおよび NetScreen デバイスに接続したルーターポートの IP アドレスを構成します。また、デバイスが静的 IP アドレスを使用するよう指定する必要があります (デフォルトでは、NetScreen デバイスは PPPoE または PPPoA クライアントとして動作し、PPPoE または PPPoA サーバーとのネゴシエーションを介して、ADSL インターフェースの IP アドレスを受信します)。

ネットワークに静的 IP アドレス 1.1.1.1/24 を設定するには、以下の手順に従って実行します。

WebUI

Network > Interfaces > Edit (adsl1 インターフェース): 以下を入力して、**Apply** をクリックします。

IP Address/Netmask: 1.1.1.1/24

Static IP: (選択)

注記: PPPoE または PPPoA インスタンスを構成して、前のセクションの説明にあるように、adsl1 インターフェースにバインドする必要があります。「Obtain IP using PPPoE」または「Obtain IP using PPPoA」と、PPPoE または PPPoA インスタンスの名前を必ず選択してください。

CLI

```
set interface adsl1 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

または

```
set interface adsl1 ip 1.1.1.1/24
set pppoa name poa1 static-ip
save
```

ドメイン名およびアドレス解決に **DNS** (ドメイン名システム) を使用するには、ネットワーク上のコンピュータが最低 **1** つの **DNS** サーバーの **IP** アドレスを持っている必要があります。**NetScreen** デバイスが **PPPoE** または **PPPoA** を介して **ADSL** インターフェースの **IP** アドレスを受信すると、自動的に **DNS** サーバーの **IP** アドレスも受信します。ネットワーク上のコンピュータが **NetScreen** デバイスの **DHCP** サーバーから **IP** アドレスを取得すると、**DNS** サーバーのアドレスも取得します。

ADSL インターフェースに静的 **IP** アドレスを割り当てると、サービスプロバイダーはユーザーに **DNS** サーバーの **IP** アドレスを割り当てます。ネットワーク上の各コンピュータに **DNS** サーバーアドレスを構成するか、または **Trust** ゾーンインターフェースに **DHCP** サーバーを構成して、各コンピュータに **DNS** アドレスを割り当てます。

Trust インターフェースに **DHCP** サーバーを構成して、ネットワーク上のコンピュータに **DNS** アドレス **1.1.1.152** を割り当てするには、以下の手順に従って実行します。

WebUI

Network > DHCP > Edit (Trust インターフェース) > DHCP Server: DNS1 に **1.1.1.152** を入力し、**Apply** をクリックします。

CLI

```
set interface trust dhcp server option dns1 1.1.1.152
save
```

オプションの構成

このセクションでは、**NetScreen-5GT** ワイヤレスデバイス上で構成する以下の機能について説明します。

- [管理の制限](#)
- [他のポリシーの構成](#)
- [動作モード](#)
- [ポートモードを変更する](#)
- [バックアップ Untrust ゾーンインターフェースの構成](#)
- [Trust または Wireless2 インターフェースアドレスの変更](#)

注記: 本書では、すべてのオプションの構成について詳しく説明しているわけではありません。詳細については、**ScreenOS 5.0.0** の『**NetScreen** 概念と用例 **ScreenOS** リファレンスガイド』の該当する章を参照してください。

管理の制限

デフォルトでは、ログインとパスワードを知っているネットワークの誰でも **NetScreen** デバイスを管理できます。**NetScreen** デバイスを構成してネットワーク上の 1 つ以上の特定のホストからのみ管理するようにできます (**NetScreen** デバイス上で使用可能にする **WebUI**、**Telnet**、**ping** などのサービスタイプを選択できます)。

詳細については、**ScreenOS 5.0.0** の『**NetScreen 概念と用例 ScreenOS リファレンス ガイド**』の「管理」部の「管理」の章を参照してください。

他のポリシーの構成

NetScreen-5GT ワイヤレスデバイスは、ネットワークの **Trust** ゾーン内のワークステーションには外部コンピュータのあらゆるサービスへのアクセスを許可する一方、外部コンピュータに対してはワークステーションへのアクセスまたはセッション開始を許可しないというデフォルトのポリシーを使用して構成されています。外部コンピュータによってお使いのコンピュータと特定のセッション開始を許可するように **NetScreen** デバイスに指示するポリシーを構成できます。ポリシーの作成や変更については、**ScreenOS 5.0.0** の『**NetScreen 概念と用例 ScreenOS リファレンス ガイド**』の「基本」部の「ポリシー」の章を参照してください。

動作モード

動作モードとは、**NetScreen** デバイスのインターフェースがゾーン間のトラフィックを処理する方法のことです。デフォルトでは、**NetScreen-5GT** ワイヤレスデバイスは **Trust** インターフェースで **NAT (Network Address Translation, ネットワークアドレス変換機能)** を使用可能にしたルートモードで動作します。つまり、**Trust** ゾーンのデバイスがトラフィックをインターネットに送信すると **NetScreen** デバイスはオリジナルのソース **IP** アドレスを **Untrust** インターフェースの **IP** アドレスで置き換えます。**NetScreen** デバイスは「秘密の」**IP** アドレスをネットワークにあるデバイスに割り当てる一方、これらのアドレスはネットワーク外部にあるコンピュータには隠れたままになります。

ネットワークにあるデバイスすべてに公開 **IP** アドレスがある場合には、**NAT** を使用不可にした状態で **NetScreen** デバイスをルートモードに構成できます。**NAT** を使用不可状態にしたルートモードでは、**NetScreen** デバイスは **IP** アドレスを確認した上でトラフィックを配信します。**NAT** を使用不可にした状態でルートモードに構成する方法についての詳細は、**ScreenOS 5.0.0** の『**NetScreen 概念と用例 ScreenOS リファレンス ガイド**』の「基本」部にある「インターフェースモード」の章を参照してください。

ポートモードを変更する

ポートモードとは、物理ポート、論理インターフェース、およびゾーンのバインディングのことです。

警告：ポートモードを変更すると **NetScreen** デバイスの既存の構成が削除されますので、ポートモードの変更はデバイスを構成する前に行ってください。

以下は、**NetScreen-5GT** ワイヤレスデバイスのポートモードで提供されているポート、インターフェース、ゾーンバインディングの概要です。

ポート名 ^a	Trust - Untrust ポートモード ^b		Home-Work ポート モード		Trust/Untrust/DMZ (拡張)モード		Dual Untrust ポート モード		Combined ポート モード	
	インター フェース	ゾーン	インター フェース	ゾーン	インター フェース	ゾーン	インター フェース	ゾーン	インター フェース	ゾーン
1	trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet1	Trust	ethernet1	Work
2	trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet1	Trust	ethernet2	Home
3	trust	Trust	ethernet2	Home	ethernet2	DMZ	ethernet1	Trust	ethernet2	Home
4	trust	Trust	ethernet2	Home	ethernet2	DMZ	ethernet2	Untrust	ethernet3	Untrust
Untrust	untrust	Untrust	ethernet3	Untrust	ethernet3	Untrust	ethernet3	Untrust	untrust	Untrust
モデム ^c	serial	Null	serial	Null	serial	Null	serial	Null	serial	Null
	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1
	wireless2	Trust	wireless2	Work	wireless2	Trust	wireless2	Trust	wireless2	Work
			wireless3	Home	wireless3	DMZ			wireless3	Home
					wireless4	Wzone2				

- NetScreen アプライエンス シャーシ上のラベル。
- デフォルトのポートモード。
- Untrust Ethernet ポートまたはモデムポートを使用して、バックアップインターフェースを Untrust ゾーンに構成することができます。190 ページの「バックアップ Untrust ゾーンインターフェースの構成」参照。

以下の表は、ワイヤレスのみのポートモードに適用されます。

ポート名 ^a	Trust-Untrust ポートモード ^b		Home-Work ポートモード		Trust/Untrust/DMZ (Extended) モード	
	インターフェイス	ゾーン	インターフェイス	ゾーン	インターフェイス	ゾーン
1	trust	Trust	ethernet1	Work	ethernet1	Trust
2	trust	Trust	ethernet1	Work	ethernet1	Trust
3	trust	Trust	ethernet2	Home	ethernet2	DMZ
4	trust	Trust	ethernet2	Home	ethernet2	DMZ
Untrust	untrust	Null ^c	ethernet3	Null ^c	ethernet3	Null ^c
モデム	シリアル	Null ^c	シリアル	Null ^c	シリアル	Null ^c
ADSL	adsl1	Untrust	adsl1	Untrust	adsl1	Untrust
	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1
	wireless2	Trust	wireless2	Work	wireless2	Trust
			wireless3	Home	wireless3	DMZ
				wireless4	Wzone2	

- a. NetScreen アプライアンス シャーシ上のラベル。
 b. デフォルトのポートモード。
 c. Untrust Ethernet ポートまたはモデムポートを使用して、バックアップインターフェイスを Untrust ゾーンに構成することができます。190 ページの「バックアップ Untrust ゾーンインターフェイスの構成」参照。

NetScreen デバイスを **Home-Work** ポートモードに変更するには、以下の手順に従って実行します。

WebUI

Configuration > Port Mode: ドロップダウンリストから **Home-Work** を選択して、**Apply** をクリックします。

次のプロンプトが表示されたら **OK** をクリックします。

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

CLI

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

次の指示メッセージで、(はいの場合は) **y** を入力してください。

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

バックアップ Untrust ゾーンインターフェースの構成

デフォルトでは、NetScreen-5GT ワイヤレス ADSL デバイス上において、**adsl1** インターフェースがネットワーク外部への主要接続となります。NetScreen-5GT ワイヤレス ADSL デバイス上で利用できる各ポートモードを選択することにより、ネットワーク外部へのバックアップ接続として、アントラステッド **Ethernet** ポートまたはモデムポートのどちらかに接続するかを決定することができます (188 ページの「ポートモードを変更する」を参照)。バックアップインターフェースを **Untrust** ゾーンにバインドし、インターフェースを正しく構成してください。

注記： アントラステッド **Ethernet** ポートまたはモデムポート接続のいずれかを使用して構成できるバックアップインターフェースは **1** つだけです。バックアップ接続にアントラステッドポートを使用する場合は、トラスト - アントラストポートモードで **Untrust** インターフェースを構成するか、または他のポートモードで **ethernet3** インターフェースを構成してください。バックアップ接続にモデムポートを使用する場合は、すべてのポートモードにシリアルインターフェースを構成してください。

たとえば、**Untrust** インターフェースを **Untrust** ゾーンにバインドするには、以下の手順に従って実行します。

WebUI

Network > Interfaces > Edit (untrust インターフェース): Zone Name ドロップダウンリストから **Untrust** を選択し、**OK** をクリックします。

CLI

```
set interface untrust zone untrust
save
```

また、**Untrust** インターフェースに静的 IP アドレスを設定するか、またはインターフェースの IP アドレスを **DHCP** か **PPPoE** 経由のどちらで取得するかを指定する必要があります。インターフェースのパラメータ設定の詳細については、ScreenOS 5.0.0 の『NetScreen 概念と用例 ScreenOS リファレンスガイド』の「基本」の部にある「インターフェース」の章を参照してください。

adsl1 インターフェースと、**Ethernet** インターフェース (ポートモードによって **untrust** または **ethernet3** と名前が異なる) がシリアルインターフェースのいずれかが、**Untrust** ゾーンにバインドされている場合は、インターフェースフェールオーバーが自動的に構成されます。つまり、**adsl1** インターフェースが使用できなくなると、NetScreen デバイスは自動的にトラフィックをバックアップインターフェースに送信します。デバイスは、**adsl1** インターフェースが再び使用可能になると、トラフィックを自動的に **adsl1** インターフェースに送信します。

注記： **adsl1** インターフェースのみが、フェールオーバーから影響を受けます。つまり、**ADSL** サブインターフェースも構成している場合でも、サブインターフェースはバックアップインターフェースにフェールオーバーしません。

また、**adsl1** インターフェース上で手動で強制的にフェールオーバーしたり、フェールバックすることもできます。詳細については、ScreenOS 5.0.0 の『NetScreen 概念と用例 ScreenOS リファレンスガイド』の「高可用性」の部の「インターフェースの冗長性」の章を参照してください。

Trust または Wireless2 インターフェースアドレスの変更

必要に応じて **Trust** インターフェースおよび ワイヤレスインターフェースの **IP** アドレスと ネットマスクを変更できます (**Trust** インターフェースまたは **wireless2** インターフェースが **NAT** モードになっている場合、お使いのネットワーク上にあるデバイスの **IP** アドレスは ネットワーク外のコンピュータから絶対に識別できないことを忘れないでください。外部のコンピュータが識別できるのは **Untrust** インターフェースの **IP** アドレスのみです)。例えば、ネットワークに既存する **IP** アドレスに合わせるように **Trust** インターフェースまたは **wireless2** インターフェースを変更する必要があるとします。**Trust** インターフェースまたは **wireless2** インターフェースの **IP** アドレスと ネットマスクを変更する場合には、**NetScreen** デバイスが **DHCP** を介してネットワーク上のデバイスに割り当てるアドレスの範囲を変更するか、**Trust** インターフェースまたは **wireless2** インターフェース上にある **DHCP** サーバーを使用不可にするかのどちらかを行う必要があります。

ネットワーク上のコンピュータが **NetScreen** デバイスの **DHCP** サーバーから **IP** アドレスを取得すると、デバイスからデフォルトゲートウェイも取得します。コンピュータに静的に割り当てられた **IP** アドレスがある場合は、**NetScreen** デフォルト上の **Trust** インターフェースまたは **wireless2** インターフェースの **IP** アドレスにデフォルトゲートウェイを手動で設定しなければなりません。

Trust インターフェースまたは **wireless2** インターフェースに異なる **IP** アドレスおよび ネットマスクを割り当てる方法の詳細については、『*NetScreen 概念と用例 ScreenOS リファレンス ガイド*』の「基本」の部にある「インターフェース」の章を参照してください。

NetScreen デバイスの **DHCP** 設定の変更方法の詳細については、『*NetScreen 概念と用例 ScreenOS リファレンス ガイド*』の「基本」の部にある「システムパラメータ」の章を参照してください。

外部との接続性の確認

ネットワークのワークステーションがインターネットにあるリソースにアクセスできているかを確認するには、ネットワークのワークステーションから **Web** ブラウザを起動し次にある **URL** を入力します。www.juniper.net。

デバイスを工場出荷時のデフォルト設定にリセットする

管理者パスワードを失った場合には、以下の手順に従って **NetScreen** デバイスをデフォルトの設定にリセットできます。この操作を行うと既存の構成を破棄しますが、デバイスへのアクセスを復旧します。

警告: デバイスをリセットすると、既存の構成設定すべてが削除され、既存のファイアウォールと **VPN** サービスが無効になります。

デバイスをデフォルトの設定に復旧するには、次のいずれかの方法で行います。

- コンソール接続を使う。詳細については、**ScreenOS 5.0.0** の『*NetScreen 概念と用例 ScreenOS リファレンス ガイド*』の「管理」の部にある「管理」の章を参照してください。

- 次のセクションに説明があるように、デバイスの背面パネルにあるリセットスイッチを使う。

リセットスイッチの使用

デバイスをリセットして工場出荷時のデフォルト設定に復旧するには、リセットスイッチをピンホールに押し込みます。この操作を行うには、正面パネルにあるデバイス状況 **LED** を見るか、[177 ページの「コンソール接続の使用」](#)に説明があるようにコンソールセッションを開始するかのいずれかが必要となります。

1. 背面パネルにあるリセットスイッチを見つけます。しっかりした細い針金状のもの（クリップなど）をスイッチの小さな穴に **4～6 秒間**を押し込んでから手を離します。



リセットスイッチ

状況 **LED** が黄色に点滅します。コンソールに構成の消去が開始した旨のメッセージが表示され、システムは **SNMP/SYSLOG** 警報を送信します。

2. **1～2 秒**の間待ちます。

第 **1** 回目のリセット後、状況 **LED** は緑に点滅し、デバイスはもう一度リセットする用意ができたことを示します。コンソールにデバイスが **2** 度目の確認を待機中である旨のメッセージが表示されます。

3. 再度リセットスイッチを **4～6 秒**押しします。

コンソールに、**2** 度目の確認を行っているメッセージが表示されます。状況 **LED** が半秒間黄色に点灯してから、緑に点滅する状態へと戻ります。

デバイスは工場出荷時の設定にリセットされます。デバイスのリセット時に、状況 **LED** は半秒間こはく色に点灯してから、緑に点灯する状態へと戻ります。コンソールにデバイスの起動メッセージが表示されます。システムは構成された **SYSLOG** または **SNMP** のトラップホストに **SNMP** と **SYSLOG** の警報を發します。

デバイスが再起動すると、コンソールにデバイスのログインプロンプトが表示されます。ここで、状況 **LED** は緑色に点滅します。

一連の操作を正しい順序で完全に行わない場合には、構成への変更は行われずリセットのプロセスはキャンセルされ、コンソールに構成の削除が中止された旨のメッセージが表示されます。状況 **LED** は緑に点滅する状態へと戻ります。デバイスがリセットされなかった場合には、**SNMP** 警報が送信されて障害を確認します。

ハードウェアの説明

本章では、NetScreen-5GT ワイヤレスのシャーシの詳細について説明しています。

ポートと電源のコネクタ

NetScreen-5GT ワイヤレス デバイスの背面パネルにはポートと電源のコネクタがあります。

アンテナ B

アンテナ A



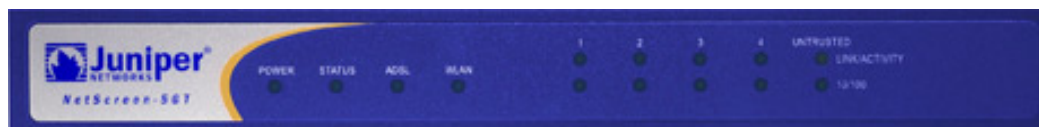
DC 電源コンセントは NetScreen-5GT ワイヤレスデバイスを電源に接続するものです。リセットスイッチを使えば、デバイスのリセットと工場出荷時のデフォルト設定への復旧を行うことができます。NetScreen-5GT ワイヤレスデバイスには次のようなポートがあります。

ポート	説明	コネクタ	速度 / プロトコル
ADSL	該当する場合は、ADSL データリンクを通じてインターネット接続を行います。	RJ-11 (Annex A) RJ-45 (Annex B)	ANSI T1.413 Issue 2 ITU G.992.1 (G.dmt) ITU 992.2 (G.lite)
コンソール	システムとのシリアル接続を行うことができます。コマンドラインインターフェース (CLI) のセッションを開始するために使います。	RJ-45	9600 bps/ RS-232
モデム	外部モデムを通じてダイヤルバックアップシリアルによるインターネット接続を有効にします。	RJ-45	9600 bps ~ 115 Kbps/ RS-232
アントラステッド	外部ルーター、DSL、またはケーブルモデムを通じてインターネットまたはアントラステッドネットワークへの1次接続またはバックアップ接続を有効にします。	RJ-45	10/100 Mbps/ イーサネット 全二重と極性を自動送信
1 ~ 4 のポート	ワークステーションへの直接接続またはスイッチかハブを使って LAN 接続を行うことができます。この接続では Telnet セッションまたは WebUI 管理アプリケーションを使ってデバイスの管理を行うことができます。	RJ-45	10/100 Mbps/ イーサネット 全二重と極性を自動送信
アンテナ A とアンテナ B	無線通信接続周辺のワークステーションに直接接続することを可能にします。この接続では Telnet セッションまたは WebUI 管理アプリケーションを使ってデバイスの管理を行うことができます。	RPSMA	802.11b 802.11g

警告: 電話回線か ISDN 回線を NetScreen-5GT ワイヤレスデバイスのモデムポートに直接接続しないでください。まず RS232 ポートを使ってデバイスをモデムに接続してから、回線に接続します。

ステータス LED

NetScreen-5GT ワイヤレスデバイスの正面パネルにはデバイス用の電源 LED とステータス LED およびインターフェース用のポートステータス LED があります。



デバイスの主要ステータス LED

デバイスステータス LED にはデバイスの正常動作の有無が示されます。次の表では、各 LED ステータスについて説明します。

LED	ステータス	意味
電源	緑	システムに電力が供給されていることを示します。
	オフ	システムに電力が供給されていないことを示します。
ステータス	点滅する緑	システムが機能していることを示します。
	緑	システムが起動していることを示します。
	赤	診断エラーまたはシステムの初期化エラーを示します。
	オフ	システムが機能していないことを示します。
ADSL (ワイヤレス ADSLのみ)	緑	ADSL ループが起動していることを示します。
	オフ	ADSL ループが起動していないことを示します。
WLAN	ゆっくり点滅している緑	ワイヤレス接続が確立されたが、リンクが使用されていないことを示します。
	高速で点滅する緑	ワイヤレス接続が確立されたことを示します。点滅速度はリンクの使用率に比例しています。
	オフ	ワイヤレス接続が確立していないことを示します。

ポートステータス LED

ポートステータス LED はデバイスのポートが正常動作しているかどうかを示します。次の表は考えられるポートステータスを説明しています。

LED	LED の色	LED の意味
リンク / 使用率	点滅する緑	デバイスがポートにイーサネットのトラフィックを検出したことを示します。
	オフ	ポートが他のデバイスとのリンクを確立していないことを示します。
	緑	ポートが他のデバイスとのリンクを確立したことを示します。
10/100	緑	ポートが 100 Base-T デバイスに接続していることを示します。
	オフ	ポートが 10 Base-T デバイスに接続していることを示します。

仕様

本付録には、NetScreen-5GT ワイヤレス デバイスの一般的なシステム仕様を記載しています。

サイズ		
高さ	2.93 cm	1.15 インチ
奥行き	18.45 cm	7.26 インチ
幅	20.8 cm	8.19 インチ
重量	0.9 kg	1.98 ポンド
電気要件		
スイッチングレギュレータ	AC アダプタ : 100V-240VAC +/- 10% 50/60 Hz, 15-18 Watts DC 入力 : 12 V, 1.25 - 1.5 Amp	
環境要件		
通常の高度	0 -40° C, 32-105° F	
相対湿度	10-90%	
結露なしの状態	10-90%	
最大通常高度は 2,000 メートル (6,526 フィート) です。		
認可		
安全性	UL、CUL、TUV、CE、CB	
電磁妨害 (EMI)	FCC Part 15 クラス B、VCCI、CE	
イーサネット接続		
規格	100Base-TX	
メディアタイプ	カテゴリ 5 以上 Unshielded Twisted Pair (UTP) (非シールドツイストペア) ケーブル	
最長距離	100 メートル (328.08 フィート)	
RJ-45 ツイストペアポートは、IEEE 802.3 タイプ 10/100 Base-T 規格に対応しています。		
ADSL コネクタ		
タイプ	6 ピン RJ-11 コネクタ、Annex A 用 RJ-45 コネクタ、Annex B 用	
メディアタイプ	標準電話線	

コンソールおよびモデムアダプターの接続

次の表は、**RJ-45** コネクタの定義を示します。標準的な **UART** ポートを使用するには、コンソールポートとモデムポートの両方が以下の構成になっている必要があります。

RJ-45	信号	略称	DCE
1	送信要求	RTS	In
2	データ送信準備完了	DTR	In
3	送信データ	TD	In
4, 5	接地信号	SGND	なし
6	受信データ	RD	Out
7	接続なし		
8	送信クリア	CTS	Out

以下のテーブルは、**RJ-45** から **DB-9** アダプタへの接続の定義を示します。標準的な **UART** ポートを使用するには、コンソールポートとモデムポートの両方が以下の構成になっている必要があります。

DB9	信号	略称	DTE	DCE	RJ45
1	データ搬送波検出	DCD	In	Out	NC
2	受信データ	RD	In	Out	3
3	送信データ	TD	Out	In	6
4	データ送信準備完了	DTR	Out	In	7
5	接地信号	SGND	なし	なし	4
6	データセット準備完了	DSR	In	Out	2
7	送信要求	RTS	Out	In	8
8	送信クリア	CTS	In	Out	1
9	リングインジケータ	RI	In	Out	NC

注記： *NetScreen* デバイスに装備されたコンソールケーブルを使用してモデムに接続する場合、モデムコネクタのヌルアダプターを取得し、インストールする必要があります。

索引

LED

ポートステータス 195

A

AAL5 複合 182

ADSL

インターフェースの構成 182

ケーブルの接続 169

ポートの接続 169

Annex A 169

Annex B 169

Deutsch Telecom の構成 185

ATM Adaptation Layer 5 182

D

DB-9 接続 198

Deutsch Telecom、Annex B の構成 185

L

LED

追跡 194

N

NetScreen ドキュメント 167

P

Point-to-Point Protocol over ATM

PPPoA を参照

Point-to-Point Protocol over Ethernet

PPPoE を参照

PPPoA 182

構成 184

PPPoE 182

構成 184

R

RJ-45 コネクタ 198

S

Service Set Identifier

SSID を参照

SSID、Service Set Identifier 180

T

Telnet、使用 176

Trust ゾーンインターフェースのアドレス 191

U

Untrust ゾーンへのバックアップインターフェース 190

Untrust ゾーン、バックアップインターフェースの構成 190

V

VPI/VCI 182

構成 183

W

WebUI

アクセス 175

WebUI、規則 166

Wireless1 インターフェース 180

Wireless2 インターフェース

SSID の設定 180

Trust ゾーン 179

アクセス 175

バインディングゾーン 179

wireless2 インターフェース

インターフェースアドレスの変更 191

あ

アンテナ 171

アントラステッドポート 171

か

ガイドの構成 165

仮想回路の追加 183

仮想回路、追加 183
仮想パス識別子 / 仮想チャンネル識別子
 VPI/VCI を参照
管理者名、変更 178

き

規則 175
 CLI 166
 WebUI 166

こ

構成
 SSID 180
 オプション 186
 デフォルトの設定 181
 必要 177, 181
 ワイヤレスネットワーク 179
構成の確認 191
コネクタ
 電源 193
 ポート 193
コンソール、使用 177

し

時間、設定 178
信号スプリッタ 170

す

ステータス **LED** 194

せ

静的 **IP** アドレス 182
 構成 185

つ

デバイスクロックの設定 178
デバイスの登録 175
デバイスのラックへの取り付け 172
デフォルト設定の復旧 191
デフォルトの設定 181
 復旧 191
電源コネクタ 193
電源の接続 172
電源、接続 172
透過モード 187
特定のホストからの管理の制限 187
特定のホストからのデバイスの管理 187
 トラストイーサネットポート 171
パスワード、変更 178
日付、設定 178
複合、構成 183
ポートコネクタ 193
ポートステータス **LED** 195
ポートモードの変更 188
ポートモード、変更 188
ポリシー、他の構成 187
マイクロフィルタ 170
ラックでのデバイスの取り付け 172
リセットスイッチ、使用 192
ルートモード 187
ログイン名とパスワードの変更 178
ワイヤレス
 Trust ゾーン 179
 Wzone1 ゾーン 180
 アンテナ 171
 構成 179
 接続中 169, 171
 デフォルトインターフェースの使用 171

目录

前言	203
组织	203
WebUI 惯例	204
CLI 惯例	204
NetScreen 出版物	205
第 1 章 连接设备	207
将 NetScreen 设备连接至网络	207
将设备连接至 Untrusted 网络	207
连接 ADSL 端口	207
连接 Untrusted 端口	208
将设备连接至内部网络或工作站	208
连接 Trusted 以太网端口	209
使用无线接口	209
连接电源	209
机架安装（可选）	209
第 2 章 配置设备	211
访问设备	211
使用 WebUI	211
使用 Telnet	212
使用控制台连接	213
所需的配置	213
更改管理员名称和密码	214
设置日期和时间	214
无线配置	215
配置无线网络	216
ADSL 配置	216
配置 ADSL 接口	217
为 ADSL 接口添加虚拟电路	219
VPI/VCI 和复用方法	219
PPPoE 或 PPPoA	220
Annex B 模式	220
静态 IP 地址和网络掩码	221
可选的配置	222
限制管理	223
配置附加策略	223
工作模式	223
更改端口模式	224
配置备份 Untrust 区域接口	226

更改 Trust 或 Wireless2 接口地址.....	227
验证外部连通性	227
重置设备使其恢复出厂缺省设置	227
使用 Reset 针孔.....	228
第 3 章 硬件说明.....	229
端口和电源连接器	229
状态 LED	230
设备的主要状态 LED	231
端口状态 LED.....	231
附录 A 规格	233
索引.....	237

前言

Juniper Networks 的 NetScreen-5GT Wireless 设备为使用集成无线 802.11b/g 接口的分支机构或零售渠道提供 IPSec 虚拟专用网 (VPN) 和防火墙服务。NetScreen-5GT Wireless 设备使用与 NetScreen 高端中央站点产品相同的防火墙、VPN、防病毒、深入检查、信息流管理技术。

Juniper Networks 提供三种型号的 NetScreen-5GT Wireless 设备：

- **NetScreen-5GT Wireless:** 仅无线应用型号。
- **NetScreen-5GT Wireless ADSL A:** Wireless + Annex A 型号通过标准电话线 (POTS) 支持 ADSL。
- **NetScreen-5GT Wireless ADSL B:** Wireless + Annex B 型通过综合业务数字网 (ISDN) 支持 ADSL。

所有型号均支持多达四个无线安全区。两种 ADSL 型号均支持 ANSI T1.413 Issue 2、ITU G.992.1 (G.dmt) 和 ITU 992.2 (G.lite) 标准。

每种型号均支持三个软件版本：

- 10 用户版本可以支持多达 10 个用户。
- Plus 版本支持任意数量的用户。
- Extended 版本提供与 Plus 版本同样的功能，另外有以下一些新功能：高可用性 (NSRP Lite)、DMZ 安全区以及附加的会话和通道功能。

组织

本手册有三章和一个附录。

[第 1 章](#)，“[连接设备](#)”介绍如何将设备连接至网络、如何连接电源和天线以及如何如何在机架中安装 NetScreen-5GT Wireless 设备。

[第 2 章](#)，“[配置设备](#)”介绍 NetScreen-5GT Wireless (ADSL) 的缺省设置和工作情况以及使用设备所需的配置。

[第 3 章](#)，“[硬件说明](#)”提供有关 NetScreen-5GT Wireless 端口、LED 和电源要求的概述。

[附录 A](#)，“[规格](#)”列出了有关 NetScreen-5GT Wireless 设备的物理规格。

WEBUI 惯例

在本书中，大于号 (>) 用于表示通过选择菜单选项和链接在 WebUI 中浏览。

范例：Objects > Addresses > List > New

要访问新地址配置对话框，请：

1. 在菜单栏中，单击 **Objects**。
Objects 菜单选项展开，显示 Objects 选项的子菜单。
2. (Applet 菜单¹) 将鼠标光标停留在 **Addresses** 上。
(DHTML 菜单) 单击 **Addresses**。
Addresses 选项展开，显示 Addresses 选项的子菜单。
3. 单击 **List**。
此时出现通讯簿表。
4. 单击右上角的 **New** 链接。
此时出现新地址配置对话框。

CLI 惯例

在表达命令行界面 (CLI) 命令的语法时，采用以下惯例：

- 中括号 [] 中的任何内容都是可选的。
- 在大括号 {} 中的任何内容都是必需的。
- 如果有多个选项，则使用竖线 (|) 分隔每个选项。范例：

```
set interface { ethernet1 | ethernet2 | ethernet3 }
manage
```

表示 “设置 ethernet1、ethernet2 或 ethernet3 接口的管理选项”。
- 变量采用斜体。范例：

```
set admin user name1 password xyz
```

CLI 命令在句子的上下文中出现时，采用**粗体**（除始终采用斜体的变量之外）。范例：“使用 **get system** 命令显示 NetScreen 设备的序列号。”

注意：输入关键字时，只需输入足够的字母就可以唯一识别单词。例如，要输入命令 **set admin user joe j12fmt54**，只要输入 **set adm u joe j12fmt54** 就足够了。尽管输入命令时可以使用此快捷方式，但是本文所述的所有命令均以完整的方式表达。

1. 可以单击菜单栏底部的 **Toggle Menu** 选项，选择 applet 或 DHTML 菜单类型。

NETSCREEN 出版物

要获取任何 Juniper Networks 的 NetScreen 产品技术文档，请访问 www.juniper.net/techpubs/。

如需技术支持，请单击 <http://www.juniper.net/support/> 上的 Case Manager 链接打开支持案例，或者致电 1-888-314-JTAC（美国国内）或 1-408-745-9500（美国以外）。

如果在以下内容中发现任何错误或遗漏，请用以下电子邮件地址与我们联系：

techpubs-comments@juniper.net

连接设备

本章介绍如何将 NetScreen-5GT Wireless 设备连接至网络以及如何连接电源和天线。如果是使用可选的 NetScreen-5GT Wireless 机架安装套件，请参阅本章结尾的机架安装说明。

注意： 有关安全警告和说明，请参阅《NetScreen Safety Guide》。此指南中的说明警告您哪些情况可能会造成人身伤害。在使用任何设备之前，要注意电路引发的危险，并熟悉标准操作，以免发生意外。

将 NETSCREEN 设备连接至网络

NetScreen 设备安装在内部网络和 Untrusted 网络之间时，可以起到防火墙的作用，并为网络提供一般性的安全保护。本节介绍物理连接。

将设备连接至 Untrusted 网络

根据所使用的 NetScreen-5GT Wireless 设备的型号，可以通过以下一种方式连接至 Untrusted 网络：

- 通过从 NetScreen 设备上的 ADSL 端口建立的 ADSL 连接
- 通过从 NetScreen 设备上的 Untrusted 端口建立的以太网连接

连接 ADSL 端口

使用附带的 ADSL 电缆从 NetScreen-5GT Wireless ADSL 设备上的 ADSL 端口连接至电话插孔。Annex A 型号的设备上的 ADSL 端口使用 RJ-11 连接器，而 Annex B 型号则使用 RJ-45 连接器。在使用 Annex B 型号的情况下，从 ADSL 端口连接至电话插孔的电缆在外观和布线方式上与直通 10 Base-T 以太网电缆完全相同。

警告： 请确保不要错将 NetScreen 设备上的 Console、Modem 或以太网端口连接至电话插孔。

在 NetScreen-5GT Wireless ADSL 设备上，ADSL 线路是与外部网络连接的主要连接线路。如需至外部网络的备份数据链路，可以使用以太网电缆从 NetScreen-5GT Wireless ADSL 设备上的 Untrusted 端口连接至外部路由器或 DSL 或电缆调制解调器，或者可以使用串行电缆从设备上的 Modem 端口连接至外部调制解调器。

警告： 不能将设备上的 Untrusted 端口和 Modem 端口同时连接至外部网络。

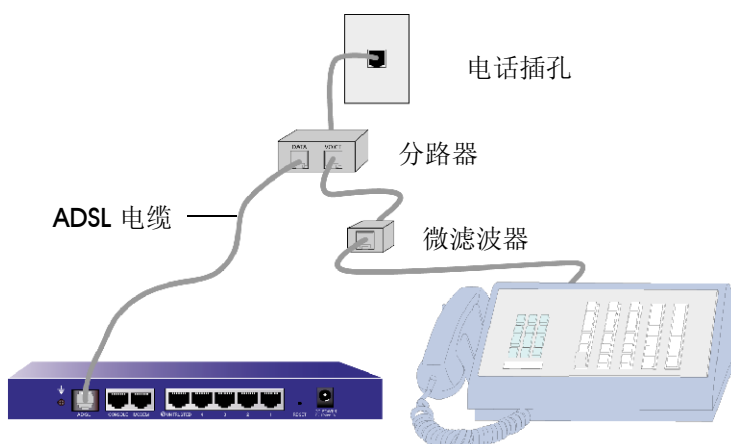
连接分路器和微滤波器

信号分路器将电话信号分成用于语音呼叫的低频语音信号和用于数据通讯的高频数据信号。服务提供商通常会随设备安装分路器，将用户现场的电话线路连接至提供商的网络。

根据服务提供商的设备不同，有些分路器可能也可以自己动手安装。如果自己安装此类分路器，请使用 ADSL 电缆从 NetScreen 设备和电话线路连接至分路器上的相应连接器（例如“data”或“voice”）。将分路器的另一端连接至电话插孔。

在每台连接至 ADSL 线路的电话、传真机、应答机或模拟调制解调器上，可能需要安装微滤波器。微滤波器会滤除电话线路中的高频噪声。微滤波器安装在电话、传真机、应答机或模拟调制解调器与分路器上语音连接器之间的电话线上。

下图所示为现场安装的微滤波器和分路器的一个范例。（必须从服务提供商处获得适当的微滤波器或分路器。）



连接 Untrusted 端口

可以与外部路由器、DSL 调制解调器或电缆调制解调器建立互联网连接，并为网络提供防火墙和一般性的安全保护。要建立高速连接，请使用附带的以太网电缆从 NetScreen-5GT Wireless 设备上的 Untrusted 接口连接至外部路由器或调制解调器。NetScreen-5GT Wireless 设备会自动检测到正确的速度、双工和极性设置。

如果是使用 NetScreen-5GT Wireless ADSL 设备，有关 ADSL 连接说明，请参阅第 207 页上的“连接 ADSL 端口”和第 208 页上的“连接分路器和微滤波器”。

将设备连接至内部网络或工作站

可以通过以下一种或两种方法连接局域网 (LAN) 或工作站：

- 通过 NetScreen 设备上的一个或多个 Trusted 以太网端口连接
- 使用 NetScreen 设备上的一个无线接口

连接 Trusted 以太网端口

NetScreen-5GT Wireless 设备有四个 Trust 以太网端口。可以使用这些端口上的一个或多个端口通过交换机或集线器连接至 LAN。也可以将一个或所有的端口直接连接至工作站，不使用集线器或交换机。可以使用交叉电缆或直通电缆将 NetScreen-5GT 端口连接至其它设备。

使用无线接口

如果使用无线接口，必须在设备上连接附带的天线。如果有标准的 2dB 全向天线，请将其拧到设备后面标有 A 和 B 的接柱上，请参阅第 229 页上的“端口和电源连接器”。要在天线的折弯处弯曲天线，切勿让闷头连接器受压。

连接电源

为 NetScreen-5GT Wireless 设备连接电源：

1. 将电源线的 DC 连接器端插入设备后面的 DC 电源插座。
2. 将电源线的 AC 适配器端插入 AC 电源。

警告： NetScreen 建议，在连接电源时接入电涌保护器。

机架安装（可选）

使用 NetScreen-5GT Wireless 机架安装套件，可以将一台或两台 NetScreen-5GT Wireless 设备安装到标准的 19 英寸设备机架内。NetScreen-5GT Wireless 机架安装套件包括安装说明和机架安装底盘。底盘的尺寸如下：

宽：	48.26 厘米	19 英寸
高：	4.013 厘米	1-5/8 英寸（1 个机架单位）
长：	33.655 厘米	13 -1/4 英寸

除 NetScreen-5GT Wireless 设备、机架安装套件和设备机架之外，还需要以下工具：

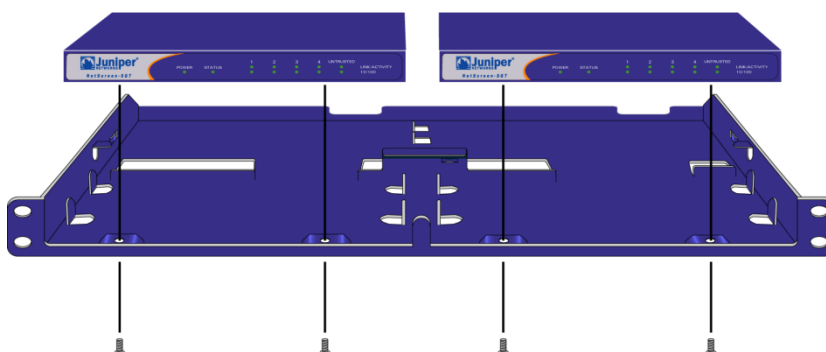
- 十字螺丝起子
- 四个与设备机架螺纹尺寸匹配的螺丝

在机架中安装设备：

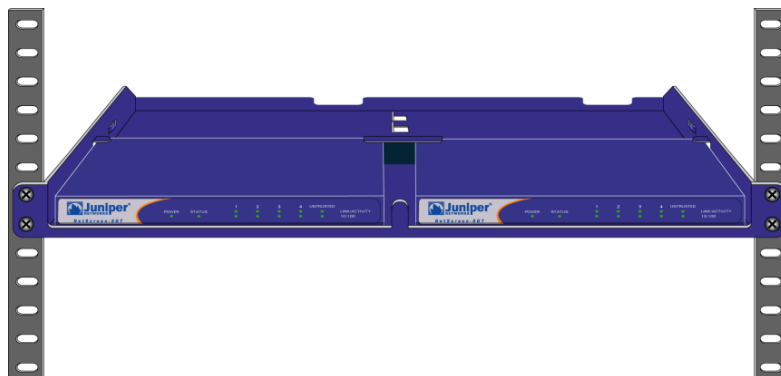
1. 使用十字螺丝起子从每台要安装的 NetScreen-5GT Wireless 设备下侧卸下两个螺丝。（保存好螺丝，以备下一步使用）螺丝位于设备下侧接近前面板的位置。



2. 将每台设备装入机架安装底盘，并使用在步骤 1 中卸下的螺丝将其固定到底盘上。



3. 用剩下的螺丝将左侧和右侧底盘金属板固定到设备机架上。



可以将电源线或以太网电缆穿过底盘平板上的开口或后壁上的凹陷。也可以使用设备后面的空间放置电源。

配置设备

本章介绍在将 NetScreen-5GT Wireless 设备连接至网络之后如何配置设备。如果是第一次使用 ScreenOS WebUI 图形接口访问设备，则可以使用初始配置向导 (ICW) 指导您完成基本配置。要使用此向导，请参阅《*Juniper Networks NetScreen-5GT Wireless Getting Started Guide*》和《*Juniper Networks NetScreen-5GT Wireless ADSL Getting Started Guide*》。

本章中介绍的主题包括：

- [访问设备](#)
- [所需的配置](#)
- [无线配置](#)
- [ADSL 配置](#)
- [可选的配置](#)
- [验证外部连通性](#)
- [重置设备使其恢复出厂缺省设置](#)

注意：在配置 NetScreen 设备和验证互联网连通性之后，必须在 www.juniper.net/support/ 上注册产品，这样才能在设备上激活某些 ScreenOS 服务（例如内部防病毒或深入检查签名服务）。在注册完产品之后，请使用 WebUI 预订服务。有关注册产品和获得预订特定服务的详细信息，请参阅 ScreenOS 5.0.0 的《NetScreen 概念与范例 ScreenOS 参考指南》“基本原理”卷中的“系统参数”一章。

访问设备

本节介绍如何使用 WebUI、Telnet 或 Console 连接访问 NetScreen 设备。

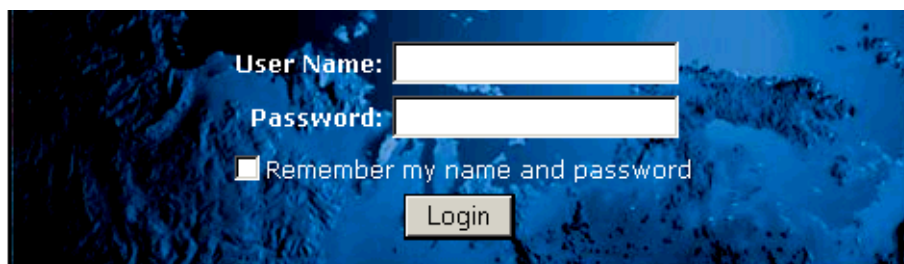
使用 WebUI

ScreenOS WebUI 是一个可以通过 Web 浏览器使用的图形接口。要使用 WebUI，必须与 Trust 或 wireless2 接口处于同一子网络内。要使用 WebUI 管理应用程序访问 NetScreen-5GT Wireless 设备，请：

1. 启动浏览器，为 URL 字段中的 Trust 或 wireless2 接口输入 IP 地址，然后按 Enter。例如，在 URL 字段中输入以下地址：

192.168.1.1

NetScreen WebUI 软件显示登录提示。



注意： 如果选择忽略 *Initial Configuration Wizard*（初始配置向导），WebUI 登录提示会自动出现。

2. 如果尚未更改缺省用户名和密码，请在 **User Name** 和 **Password** 字段中均输入 **netscreen**，然后单击 **Login**。（仅使用小写字母。User Name 和 Password 字段均区分大小写。）

使用 Telnet

Telnet 是一个应用程序，它使您可以通过互联网协议 (IP) 网络访问设备。

注意： 也可以使用安全 Shell (SSH) 应用程序访问 NetScreen 设备。有关详细信息，请参阅 ScreenOS 5.0.0 的《NetScreen 概念与范例 ScreenOS 参考指南》的“管理”卷中的“管理”一章。

要使用 Telnet 配置设备，请在工作站的 Telnet 会话中输入 ScreenOS 命令行界面 (CLI) 命令。

1. 使用 Trust 或 wireless2 接口的 IP 地址启动 Telnet 客户端应用程序。例如输入以下命令：

```
telnet 192.168.1.1
```
2. 如果尚未更改缺省用户名和密码，请在 **Login** 和 **Password** 提示字段中均输入 **netscreen**。（仅使用小写字母。Login 和 Password 提示字段均区分大小写。）

使用控制台连接

NetScreen-5GT Wireless 设备上的 Console 端口使您可以通过连接至工作站或终端的串行电缆访问设备。要使用控制台连接配置设备，请在终端或工作站上的终端仿真程序中输入 ScreenOS CLI 命令。

注意：要建立控制台连接，需要使用一条串行电缆，一端带有阳性 RJ-45 连接器，另一端带有阴性 DB-9 连接器。有关串行电缆的针脚排列，请参阅附录 A，“规格”。

建立控制台连接：

1. 将串行电缆的阴性 DB-9 一端插入计算机的串行端口。（确保 DB-9 连接器正确地插在端口上。）
2. 将 DB-9 连接器的另一端插入 RJ-45 DB-9 端口。（确保 DB-9 连接器正确地插在 RJ-45 DB-9 端口上。）
3. 将串行电缆的阳性 RJ-45 一端插入 NetScreen-5GT Wireless 设备的 Console（控制台）端口。（确保 RJ-45 连接器正确地插在端口上。）
4. 启动串行终端仿真程序。（通用的终端程序是 Hilgreave HyperTerminal。）要启动 NetScreen-5GT Wireless 设备的控制台会话，需要进行以下设置：
 - Baud Rate: 9600
 - Parity: 无
 - Data Bits: 8
 - Stop Bit: 1
 - Flow Control: 无
5. 如果尚未更改缺省用户名和密码，请在 **Login** 和 **Password** 提示字段中均输入 **netScreen**。（仅使用小写字母。Login 和 Password 字段均区分大小写。）

所需的配置

本节介绍要使用设备必须完成的配置。

注意：如果任何时候需要恢复设备的缺省设置，请参阅在 227 页“重置设备使其恢复出厂缺省设置”。

更改管理员名称和密码

因为所有的 NetScreen 产品均使用相同的缺省管理员名称和密码 (**netscreen**)，因此，最好立即更改管理员名称和密码。要将管理员名称和密码从 “netscreen” 和 “netscreen” 更改为 “darwin1” 和 “1240jes”，请：

WebUI

Configuration > Admin > Administrators > Edit (对于 NetScreen 管理员名称)：
输入以下内容，然后单击 **OK**：

Administrator Name: darwin1

Old Password: netscreen

注意： 输入密码时，WebUI 中并不显示密码。

New Password: 1240jes

Confirm New Password: 1240jes

CLI

```
set admin name darwin1
set admin password 1240jes
save
```

有关创建不同管理员级别的信息，请参阅 ScreenOS 5.0.0 的《NetScreen 概念与范例 ScreenOS 参考指南》的“管理”卷中的“管理”一章。

设置日期和时间

在 NetScreen 设备上设置的时间会影响诸如 VPN 通道设置和进度表的时间安排。在 NetScreen 设备上设置日期和时间的简便方法就是将 NetScreen 设备上的系统时钟与计算机上的时钟同步。要在 WebUI 中进行此操作：

1. Configuration > Date/Time: 单击 **Sync Clock with Client** 按钮。
此时会弹出一条消息，提示您指定是否已经在计算机时钟上启用夏令时 (DTS) 选项。
2. 单击 **Yes** 将同步系统时钟，并根据 DTS 调整系统时钟；或者单击 **No** 只同步系统时钟，不根据 DTS 对其进行调整。

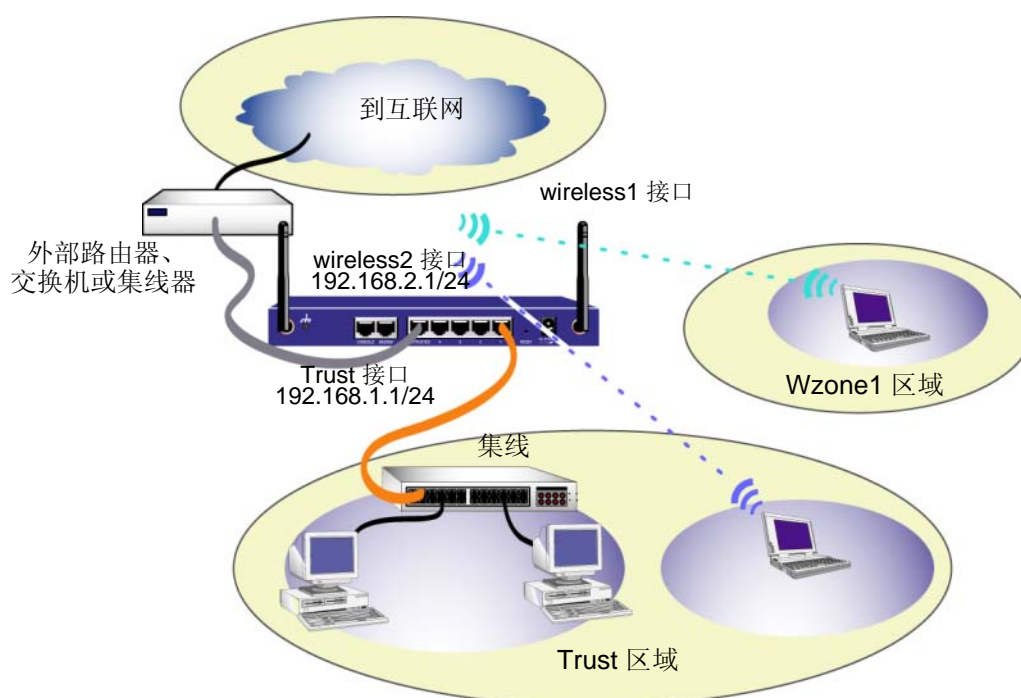
也可以在 Telnet 或控制台会话中使用 CLI **set clock** 命令，手动设置日期和时间。

无线配置

本节介绍有关在 NetScreen 设备上配置无线接口的信息。根据安装的许可类型，可以在 NetScreen-5GT Wireless 设备上配置多达四个无线安全区。接口与区域的绑定是预定义的，而且依赖配置的端口模式，不能指定至 Untrust 区域的无线接口。必须在 NetScreen 设备上配置至少一个无线接口，才能创建无线局域网 (WLAN)。

注意：如果是在美国或日本以外的某国家或地区使用 NetScreen-5GT Wireless 设备，则必须先运行 `set wlan country-code` 命令，然后才能建立 WLAN 连接。此命令用于设置可选信道范围和传输功率级别。

下图显示了 NetScreen-5GT Wireless 设备的缺省配置。



缺省无线接口的预定义名称为“wireless2”。Trust 和 wireless2 接口绑定到 Trust 区域，相应配置的子网络地址为 192.168.1.1/24 和 192.168.2.1/24。这意味着，在 Trust 区域内连接的所有设备均必须与 Trust 或 wireless2 接口处于同一子网络，而且其 IP 地址处于两个子网络的一个子网络内。同时配置 NetScreen 设备将 192.168.1.1/24 和 192.168.2.1/24 子网络的 IP 地址指定给设备。有关详细信息，请参阅在 227 页上的“更改 Trust 或 Wireless2 接口地址”。

在缺省情况下，wireless1 接口绑定到 Wzone1 区域，没有指定的 IP 地址。如果要使用 wireless1 接口，必须为其配置 IP 地址。有关详细信息，请参阅 *NetScreen-5GT Wireless Reference Guide*。

NetScreen 设备允许源自 Trust 区域内设备的任何类型的信息流进入互联网，但不允许任何源自互联网的信息流进入网络。可以配置额外的限制，有关详情，请参阅在 223 页上的“配置附加策略”。

配置无线网络

无线网络由称为“服务集标识符”(SSID)的名称组成。指定 SSID 使您可以在同一位置具有多个无线网络。在每台设备上最多可以配置 8 个 SSID。设置 SSID 名称之后,即可配置 SSID 属性。

要将 SSID 名称设置为 **netscreen open**, 允许无线网络连接, 并激活 wireless2 接口:

WebUI

Wireless > SSID > New: 输入以下内容, 然后单击 **OK**:

SSID: “netscreen open”

Wireless Interface Binding: wireless2 (精选)

Activate Changes > 单击 **Activate Changes** 按钮

CLI

```
set ssid name "netscreen open"
set ssid "netscreen open" authentication open encryption
none
set ssid "netscreen open" interface wireless2
exec wlan reactivate
```

将 SSID 设置为 wireless2 接口之后, 可以按照在 211 页上的“访问设备”介绍的步骤使用缺省 wireless2 接口 IP 地址访问设备, 以配置设备。有关配置范例、SSID 属性和与无线安全配置有关的命令, 请参阅《*NetScreen-5GT Wireless Reference Guide*》。

ADSL 配置

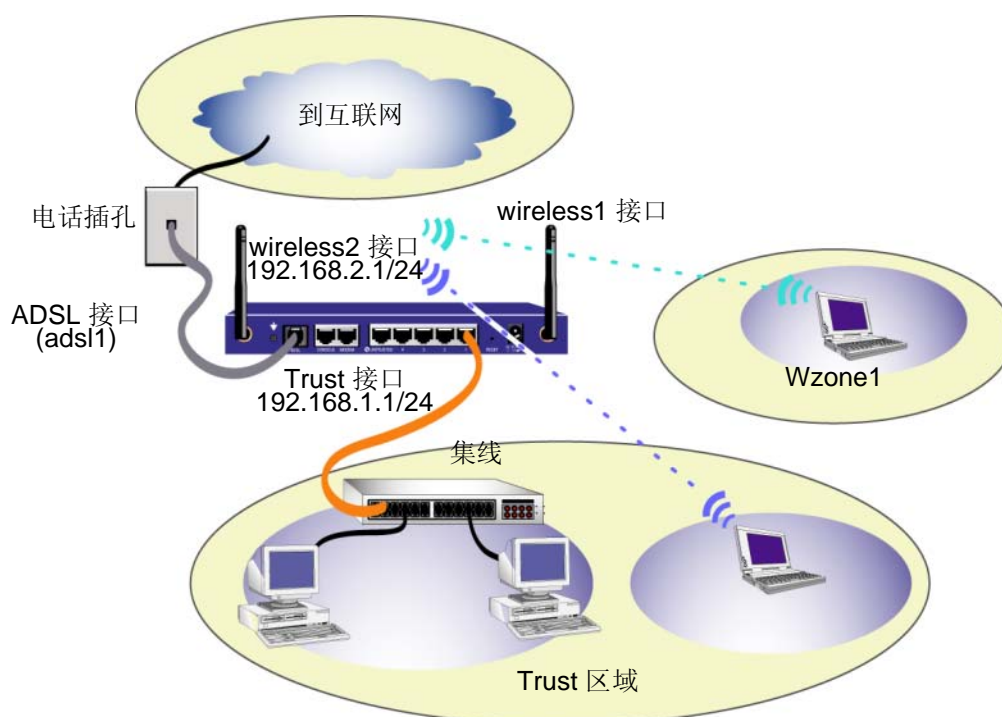
本节介绍出厂时 NetScreen-5GT Wireless ADSL Annex A 和 B 设备的缺省设置和工作情况。在大多数情况下, 这些缺省设置中只有几项是必须配置的。

本节介绍 Untrust 区域接口的以下配置:

- [配置 ADSL 接口](#)
- [为 ADSL 接口添加虚拟电路](#)
- [VPI/VCI 和复用方法](#)
- [PPPoE 或 PPPoA](#)
- [Annex B 模式](#)
- [静态 IP 地址和网络掩码](#)

注意: 如果任何时候需要恢复设备的缺省设置, 请参阅在 227 页上的“重置设备使其恢复出厂缺省设置”。

下图显示了 NetScreen-5GT Wireless ADSL 设备的缺省配置。



ADSL 接口的预定义名称为 “adsl1”，是网络与互联网之间的主要连接接口。要允许 NetScreen 设备（和网络上的设备）连接至互联网，必须根据服务提供商提供的信息配置 adsl1 接口。请参阅在 217 页上的“配置 ADSL 接口”。

NetScreen 设备允许源自 Trust 区域内设备的任何类型的信息流进入互联网，但不允许任何源自互联网的信息流进入网络。可以配置额外的限制，有关详情，请参阅在 223 页上的“配置附加策略”。

配置 ADSL 接口

网络使用 NetScreen 设备上的 ADSL 接口 “adsl1” 通过异步传输模式 (ATM) 虚拟电路连接至服务提供商的网络。可以通过创建 ADSL 子接口，配置额外的虚拟电路（有关详细信息，请参阅在 219 页上的“为 ADSL 接口添加虚拟电路”）。

在 WebUI 中，找到 Network > Interfaces 页面，查看 NetScreen 设备上的当前接口列表。如果是使用 Telnet 或控制台会话，请输入 CLI 命令 **get interface**。应该看到 adsl1 接口绑定到 Untrust 区域。如果曾经使用 ICW 配置设备，则可能已经为 adsl1 接口指定 IP 地址和网络掩码。

注意： 如果不希望使用 ADSL 接口，可以使用 **set interface adsl1 zone null** 命令将其绑定到 Null 区域。如果使用 ICW 配置设备，则可以选择除 ADSL 接口之外的其它接口作为缺省 Untrust 区域接口。

必须配置 adsl1 接口，才能使 NetScreen 设备连接至服务提供商的网络。要进行此操作，必须从服务提供商处获得以下信息：

- 虚拟路径标识符和虚拟信道标识符 (VPI/VCI) 值
- ATM 适配层 5 (AAL5) 复用方法，可以是以下方法之一：
 - 基于虚拟电路 (VC) 的复用，其中每种协议是通过单独的 ATM VC 传输的
 - 逻辑链路控制 (LLC) 封装协议，它允许在同一 ATM VC 上传输多种协议（缺省复用方法）
- 服务提供商分配的用户名和密码，用于使用以太网点对点协议 (PPPoE) 或 ATM 点对点协议 (PPPoA) 连接至服务提供商的网络
- 认证方法（如果有），针对 PPPoE 或 PPPoA 连接
- 网络的静态 IP 地址和网络掩码值（可选）

为 ADSL 接口添加虚拟电路

要添加虚拟电路，需要为 ADSL 接口创建子接口。可以创建多达 10 个 ADSL 子接口。例如，创建一个名为 “adsl1.1” 的新接口，该接口绑定到名为 “Corp1” 的用户定义区域：

WebUI

Network > Interfaces > New ADSL Sub-IF: 输入以下内容，然后单击 **Apply**：

Interface Name: adsl1.1

VPI/VCI: 0/35

Zone Name: Corp1 (精选)

CLI

```
set interface adsl1.1 pvc 0 35 zone corp1
save
```

必须按照与配置 ADSL 主接口相同的方式配置 ADSL 子接口，包括设置 VPI/VCI 值，如在 217 页上的 “配置 ADSL 接口” 中所述。ADSL 子接口的配置是独立于 ADSL 主接口的；也就是说，可以在子接口上配置与 ADSL 主接口不同的复用方法、VPI/VCI 和 PPP 客户端。即使 ADSL 主接口没有静态 IP 地址，也可以在子接口上配置静态 IP 地址。注意，如果在一个子接口和 ADSL 主接口中，一个接口是针对 PPPoA 配置的，而另一个接口是针对 PPPoE 配置的，且两个接口均使用 LLC 复用方法，则两者均可以使用同一 VPI/VCI 值。

VPI/VCI 和复用方法

服务提供商会为每个 VC 连接指定一个 VPI/VCI 值对。例如，可能会接收到 VPI/VCI 值对 1/1，这个值对表示一个 VPI 值 1 和一个 VCI 值 1。这些值必须与服务提供商在用户侧的数字用户线接入复用器 (DSLAM) 上配置的值相匹配。

在 adsl1 接口上配置 VPI/VCI 值对：

WebUI

Network > Interfaces > Edit (对于 adsl1 接口)：在 VPI/VCI 字段中输入 1/1，然后单击 **Apply**。

CLI

```
set interface adsl1 pvc 1 1
save
```

在缺省情况下，NetScreen-5GT Wireless ADSL 设备对每个 VC 均使用基于 LLC 的复用方法。在 adsl1 接口上配置 VPI/VCI 1/1 接口并在 VC 上使用 LLC 封装协议：

WebUI

Network > Interfaces > Edit (对于 adsl1 接口)：输入以下内容，然后单击 **Apply**：

VPI/VCI: 1 / 2

Multiplexing Method: LLC (精选)

CLI

```
set interface adsl1 pvc 1 1 mux llc
save
```

PPPoE 或 PPPoA

NetScreen 设备既有 PPPoE 客户端，也有 PPPoA 客户端，它通过 ADSL 链路连接至服务提供商。PPPoE 是最常用的 ADSL 封装协议，用于在网络中的每台主机上终止会话。PPPoA 主要用于公司级服务，因为 PPP 会话可以在 NetScreen 设备上终止。要使 NetScreen 设备连接至服务提供商网络，必须配置服务提供商分配的用户名和密码。PPPoA 的配置与 PPPoE 的配置类似。

注意： NetScreen 设备在每个虚拟电路上仅支持一个 PPPoE 会话。

为 PPPoE 配置用户名 “roswell” 和密码 “area51”，将 PPPoE 配置绑定到 adsl1 接口：

WebUI

Network > PPPoE > New: 输入以下内容，然后单击 **OK**：

PPPoE Instance: poe1
Bound to Interface: adsl1 (精选)
Username: roswell
Password: area51

CLI

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1
save
```

在 NetScreen 设备上还可以配置一些其它的 PPPoE 或 PPPoA 参数，包括认证方法（在缺省情况下，NetScreen 设备支持质询握手认证协议或密码认证协议）、空闲超时（缺省值为 30 分钟）等等。询问服务提供商，要与服务提供商的服务器建立正常的通讯，是否有其它必须配置的 PPPoE 或 PPPoA 参数。

Annex B 模式

如果将 NetScreen-5GT Wireless ADSL 设备的 Annex B 型号连接至 Deutsch Telecom ADSL 线路，则必须在 ADSL 端口上配置物理接口，才能使用此设备进行工作。要进行此操作，请：

WebUI

Network > Interfaces > Edit (对于 adsl1 接口)：选择 Annex B 模式为 **DT**，然后单击 **Apply**。

CLI

```
set interface adsl1 phy annex-b-mode dt
save
```


如果是使用该设备的 Annex A 型号或正在将该设备连接至非 Deutsch Telecom 设备，则不需要配置此设置。

静态 IP 地址和网络掩码

如果 ISP 给定了具体固定的网络 IP 地址和网络掩码，请配置网络的 IP 地址和网络掩码以及连接 NetScreen 设备的路由器端口的 IP 地址。另外，需要指定该设备将使用静态 IP 地址。（在缺省情况下，NetScreen 设备充当 PPPoE 或 PPPoA 客户端，并通过与 PPPoE 或 PPPoA 服务器的协商为 ADSL 接口接收一个 IP 地址）。

为网络配置静态 IP 地址 1.1.1.1/24:

WebUI

Network > Interfaces > Edit（对于 adsl1 接口）：输入以下内容，然后单击 **Apply**：

IP Address/Netmask: 1.1.1.1/24

Static IP: (精选)

注意：必须配置 PPPoE 或 PPPoA 实例，并将其绑定到 adsl1 接口，如上一节所述。确保选择 “Obtain IP using PPPoE” 或 “Obtain IP using PPPoA” 以及 PPPoE 或 PPPoA 实例的名称。

CLI

```
set interface adsl1 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

或

```
set interface adsl1 ip 1.1.1.1/24
set pppoa name poa1 static-ip
save
```

要使用域名系统 (DNS) 进行域名和地址解析，网络中的计算机需要具有至少一台 DNS 服务器的 IP 地址。如果 NetScreen 设备通过 PPPoE 或 PPPoA 为 ADSL 接口接收一个 IP 地址，则也会自动为 DNS 服务器接收 IP 地址。如果网络中的计算机从 NetScreen 设备上的 DHCP 服务器接收自己的 IP 地址，则这些计算机也获得这些 DNS 服务器的地址。

如果为 ADSL 接口指定静态 IP 地址，则服务提供商必须提供 DNS 服务器的 IP 地址。也可以在网络中的每台计算机上配置 DNS 服务器地址或在 Trust 区域接口上配置 DHCP 服务器，以便它为每台计算机提供 DNS 服务器地址。

在 Trust 接口上配置 DHCP 服务器，使其为网络中的计算机提供 DNS 服务器地址 1.1.1.152:

WebUI

Network > DHCP > Edit（对于 Trust 接口）> DHCP Server: 在 DSN1 中输入 1.1.1.152，然后单击 **Apply**。

CLI

```
set interface trust dhcp server option dns1 1.1.1.152
save
```

可选的配置

本节介绍以下一些可能要配置的 NetScreen-5GT Wireless 设备功能：

- [限制管理](#)
- [配置附加策略](#)
- [工作模式](#)
- [更改端口模式](#)
- [配置备份 Untrust 区域接口](#)
- [更改 Trust 或 Wireless2 接口地址](#)

注意： 本手册并没有对可选配置逐一进行详细介绍。有关详细信息，请参阅 ScreenOS 5.0.0 的《NetScreen 概念与范例 ScreenOS 参考指南》中的相应章节。

限制管理

在缺省情况下，网络中的任何用户，如果知道登录名和密码，均可以管理 NetScreen 设备。可以配置 NetScreen 设备，使其仅接受从网络中的一个或多个特定主机进行管理。（可以选择要在 NetScreen 设备上启用哪种服务，例如 WebUI、Telnet 和 Ping。）

有关详细信息，请参阅 ScreenOS 5.0.0 的《*NetScreen 概念与范例 ScreenOS 参考指南*》的“管理”卷中的“管理”一章。

配置附加策略

尽管为 NetScreen-5GT Wireless 配置的缺省策略允许网络 Trust 区域中的工作站访问外部计算机运行的任何类型的服务，但是外部计算机无权访问或启动工作站运行的会话。可以通过配置策略，要求 NetScreen 设备允许外部计算机启动您的计算机特定类型的会话。要创建或修改策略，请参阅 ScreenOS 5.0.0 的《*NetScreen 概念与范例 ScreenOS 参考指南*》的“管理”卷中的“管理”一章。

工作模式

*工作模式*是 NetScreen 设备上接口处理区域之间信息流的方式。在缺省情况下，NetScreen-5GT Wireless 设备在路由模式下工作，同时在 Trust 接口上启用网络地址转换 (NAT)。这意味着，当 Trust 区域中的设备发送信息流到互联网时，NetScreen 设备使用 Untrust 接口的 IP 地址替换初始的源 IP 地址。尽管 NetScreen 设备会为网络中的设备分配私有 IP 地址，但是网络外部的计算机始终看不到这些地址。

如果网络中所有的设备都有公共 IP 地址，则可以配置 NetScreen 设备使用不启用 NAT 的“路由”模式。在不启用 NAT 的“路由”模式下，NetScreen 设备通过检查 IP 地址转发信息流。有关配置设备使用不启用 NAT 的“路由”模式的详细信息，请参阅 ScreenOS 5.0.0 的《*NetScreen 概念与范例 ScreenOS 参考指南*》“基本原理”卷中的“接口模式”一章。

更改端口模式

端口模式是物理端口、逻辑接口和区域的绑定。

警告：更改端口模式会删除 NetScreen 设备上所有现有的配置。因此，在配置设备之前，应该更改端口模式。

下表简要列出了 NetScreen-5GT Wireless 设备上的端口模式所需的端口、接口和区域绑定：

端口名称 ^a	Trust-Untrust 端口模式 ^b		Home-Work 端口模式		Trust/Untrust/DMZ (Extended) 模式		Dual Untrust 端口模式		Combined 端口模式	
	接口	区域	接口	区域	接口	区域	接口	区域	接口	区域
1	trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet1	Trust	ethernet1	Work
2	trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet1	Trust	ethernet2	Home
3	trust	Trust	ethernet2	Home	ethernet2	DMZ	ethernet1	Trust	ethernet2	Home
4	trust	Trust	ethernet2	Home	ethernet2	DMZ	ethernet2	Untrust	ethernet3	Untrust
Untrusted	untrust	Untrust	ethernet3	Untrust	ethernet3	Untrust	ethernet3	Untrust	untrust	Untrust
Modem ^c	串行	Null	串行	Null	串行	Null	串行	Null	串行	Null
	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1
	wireless2	Trust	wireless2	Work	wireless2	Trust	wireless2	Trust	wireless2	Work
			wireless3	Home	wireless3	DMZ			wireless3	Home
					wireless4	Wzone2				

a. NetScreen 设备机箱上标示的名称。

b. 缺省端口模式。

c. 可以使用 Modem 端口，配置一个备份 Untrust 区域接口。请参阅在 226 页上的“配置备份 Untrust 区域接口”。

下表简要列出了 NetScreen-5GT Wireless ADSL 设备上的端口模式所需的端口、接口和区域绑定：

端口名称 ^a	Trust-Untrust 端口模式 ^b		Home-Work 端口模式		Trust/Untrust/DMZ (Extended) 模式	
	接口	区域	接口	区域	接口	区域
1	trust	Trust	ethernet1	Work	ethernet1	Trust
2	trust	Trust	ethernet1	Work	ethernet1	Trust
3	trust	Trust	ethernet2	Home	ethernet2	DMZ
4	trust	Trust	ethernet2	Home	ethernet2	DMZ
Untrusted	untrust	Null ^c	ethernet3	Null ^c	ethernet3	Null ^c
Modem	串行	Null ^c	串行	Null ^c	串行	Null ^c

端口名称 ^a	Trust-Untrust 端口模式 ^b		Home-Work 端口模式		Trust/Untrust/DMZ (Extended) 模式	
	接口	区域	接口	区域	接口	区域
ADSL	adsl1	Untrust	adsl1	Untrust	adsl1	Untrust
	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1
	wireless2	Trust	wireless2	Work	wireless2	Trust
			wireless3	Home	wireless3	DMZ
				wireless4	Wzone2	

- a. NetScreen 设备机箱上标示的名称。
- b. 缺省端口模式。
- c. 可以使用 Untrusted 以太网端口或 Modem 端口，配置一个备份 Untrust 区域接口。请参阅在 226 页上的“配置备份 Untrust 区域接口”。

将 NetScreen 设备更改为 Home-Work 端口模式：

WebUI

Configuration > Port Mode: 从下拉列表中选择 Home-Work，然后单击 **Apply**。

在出现下列提示时，单击 **OK**：

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

CLI

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

在出现下列提示时，输入 **y**（代表是）：

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

配置备份 Untrust 区域接口

在缺省情况下，在 NetScreen-5GT Wireless ADSL 设备上，adsl1 接口是与外部网络的主要连接接口。NetScreen-5GT Wireless ADSL 设备上提供的每种端口模式使您可以选择是连接 Untrusted 以太网端口还是 Modem 端口作为与外部网络的备份连接接口（请参阅在 224 页上的“更改端口模式”）。必须将备份接口绑定到 Untrust 区域并相应地配置接口。

注意： 可以使用 Untrusted 以太网端口或 Modem 端口连接，仅配置一个备份接口。如果使用 Untrusted 端口建立备份连接，请在 Trust-Untrust 端口模式下配置 Untrust 接口，或者为其它端口模式配置 ethernet3 接口。如果使用 Modem 端口建立备份连接，请为所有端口模式配置串行接口。

例如，将 Untrust 接口绑定到 Untrust 区域：

WebUI

Network > Interfaces > Edit（对于 untrust 接口）：从 Zone Name 下拉列表中选择 Untrust，然后单击 **OK**。

CLI

```
set interface untrust zone untrust
save
```

同时需要为 Untrust 接口设置静态 IP 地址，或者指定是否通过 DHCP 或 PPPoE 获取该接口的 IP 地址。有关配置接口参数的详细信息，请参阅 ScreenOS 5.0.0 的《NetScreen 概念与范例 ScreenOS 参考指南》的“基本原理”卷中的“接口”一章。

adsl1 接口和以太网接口（名为“untrust”或“ethernet3”，根据端口模式而定）或串行接口绑定到 Untrust 区域时，设备会自动配置接口故障切换。也就是说，如果 adsl1 接口不可用，NetScreen 设备会自动将信息流发送到备份接口。当 adsl1 接口可用时，设备会自动将信息流发送到 adsl1 接口。

注意： 只有 adsl1 接口受故障切换影响。也就是说，如果已同时配置 ADSL 子接口，子接口在故障切换时不会切换到备份接口。

也可以手动强制在 adsl1 接口上实现故障切换和故障恢复。有关详细信息，请参阅 ScreenOS 5.0.0 的《NetScreen 概念与范例 ScreenOS 参考指南》的“高可用性”卷中的“接口冗余”一章。

更改 Trust 或 Wireless2 接口地址

必要时，可以更改 Trust 接口和无线接口的 IP 地址和网络掩码。（切记，Trust 或 wireless2 接口处于 NAT 模式时，网络外部的计算机始终看不到网络中设备的 IP 地址，外部计算机看到的仅仅是 Untrust 接口的 IP 地址。）例如，可能需要更改 Trust 或 wireless2 接口，以匹配网络中现有的 IP 地址。如果更改 Trust 或 wireless2 接口的 IP 地址和网络掩码，则同时需要更改 NetScreen 设备通过 DHCP 分配给网络设备的地址范围，或者禁用 Trust 或 wireless2 接口上的 DHCP 服务器。

如果网络中的计算机从 NetScreen 设备上的 DHCP 服务器接收自己的 IP 地址，则这些计算机也从 NetScreen 设备获取其缺省网关。如果某计算机已经有静态分配的 IP 地址，则必须在 NetScreen 设备上手动将其缺省网关设置为 Trust 或 wireless2 接口的 IP 地址。

要为 Trust 或 wireless2 接口分配一个不同的 IP 地址和网络掩码，请参阅 ScreenOS 5.0.0 的《*NetScreen 概念与范例 ScreenOS 参考指南*》“基本原理”卷中的“接口”一章。

要更改 NetScreen 设备的 DHCP 设置，请参阅 ScreenOS 5.0.0 的《*NetScreen 概念与范例 ScreenOS 参考指南*》“基本原理”卷中的“系统参数”一章。

验证外部连通性

要验证网络中的工作站是否能够访问互联网中的资源，请从网络中的任何工作站启动 Web 浏览器并输入以下的 URL: www.juniper.net。

重置设备使其恢复出厂缺省设置

如果丢失了管理员密码，可以重置 NetScreen 设备使其恢复缺省设置。这样会破坏所有现有的配置，但是可恢复对设备的访问。

警告： 重置设备会删除所有现有的配置，并且会使现有的防火墙和 VPN 服务不可用。

可以使用以下方式中的一种将设备恢复到缺省设置：

- 使用控制台连接。有关详细信息，请参阅 ScreenOS 5.0.0 的《*NetScreen 概念与范例 ScreenOS 参考指南*》的“管理”卷中的“管理”一章。
- 使用设备后面板上的 Reset 针孔，如下一节所述。

使用 Reset 针孔

按 Reset 针孔可以重置设备并恢复出厂缺省设置。要执行此操作，需要查看前面板上的设备状态 LED 或启动控制台会话（如在 213 页上的“使用控制台连接”中所述）。

1. 找到后面板上的 Reset 针孔。使用又细又硬的金属丝（例如回形针），推压针孔四至六秒，然后松开。



Reset 针孔

Status LED 闪烁琥珀黄色。控制台上的消息提示，已经开始删除配置，并且系统发出一个 SNMP/SYSLOG 警示。

2. 等待一至二秒。

在第一次重置之后，Status LED 闪烁绿色；现在设备正在等待第二次重置。控制台消息现在提示，设备正在等待第二次确认。

3. 再次推压 Reset 针孔四至六秒。

控制台消息会验证第二次确认。Status LED 呈琥珀黄色亮起半秒，然后返回到闪烁绿色状态。

此时，设备即重置到其原始的出厂设置。设备重置时，Status LED 变为琥珀黄色半秒，然后返回到闪烁绿色状态。控制台显示设备启动消息。系统向已配置的 SYSLOG 或 SNMP 陷阱主机发出 SNMP 和 SYSLOG 警示。

在设备重新启动之后，控制台显示设备登录提示。状态 LED 现在闪烁绿色。

如果不严格按照顺序进行操作，重置过程会取消，且不更改任何配置，同时控制台消息提示已中止配置删除操作。状态 LED 返回到闪烁绿色状态。如果设备没有重置，则系统会发送 SNMP 警示确认失败。

硬件说明

本章提供 NetScreen-5GT Wireless 机箱的详细说明。

端口和电源连接器

NetScreen-5GT Wireless 设备的后面板上有端口和电源连接器。

天线 B

天线 A



DC POWER 插座用于连接电源至 NetScreen-5GT Wireless 设备。Reset 针孔用于重置设备使其恢复为出厂缺省设置。NetScreen-5GT Wireless 设备提供以下端口：

端口	说明	连接器	速度 / 协议
ADSL	在情况适合时，通过 ADSL 数据链路启用 Internet 连接。	RJ-11 (Annex A) RJ-45 (Annex B)	ANSI T1.413 Issue 2 ITU G.992.1 (G.dmt) ITU 992.2 (G.lite)
Console	启用与系统之间的串行连接。用于启动命令行界面 (CLI) 会话。	RJ-45	9600 bps/ RS-232
Modem	通过外部调制解调器启用拨号备份串行互联网连接。	RJ-45	9600 bps-115 Kbps/ RS-232
Untrusted	通过外部路由器或 DSL 或电缆调制解调器启用主要或备份互联网或不受信任网络连接。	RJ-45	10/100 Mbps/ 以太网 自动检测双工和极性
端口 1-4	通过交换机或集线器启用至工作站的直接连接或 LAN 连接。此连接同时使您可以通过 Telnet 会话或 WebUI 管理应用程序管理设备。	RJ-45	10/100 Mbps/ 以太网 自动检测双工和极性
天线 A 和 B	在无线电连接附近启用与工作站的直接连接。此连接使您可以通过 Telnet 会话或 WebUI 管理应用程序管理设备。	RPSMA	802.11b 802.11g

警告：切勿将电话线或 ISDN 线直接连接至 NetScreen-5GT Wireless 设备上的调制解调器端口。必须先使用 RS-232 端口将设备连接至调制解调器，然后将调制解调器连接至线路。

状态 LED

NetScreen-5GT Wireless 设备的前面板上有设备的电源和状态 LED，以及接口的端口状态 LED。



设备的主要状态 LED

设备状态 LED 表明设备工作是否正常。下表说明每个 LED 的状态。

LED	状态	含义
POWER	绿色	表明系统已通电。
	熄灭	表明系统没有通电。
STATUS	闪烁绿色	表明系统正在工作。
	绿色	表明系统正在启动。
	红色	表明诊断或系统初始化错误。
	熄灭	表明系统不可用。
ADSL (仅在 Wireless ADSL 上)	绿色	表明 ADSL 回路已打开。
	熄灭	表明 ADSL 回路已关闭。
WLAN	慢闪绿色	表明无线连接已经建立，但是没有链路活动。
	快闪绿色	表明无线连接已经建立。闪烁速度与链路活动成正比。
	熄灭	表明没有建立任何无线连接。

端口状态 LED

端口状态 LED 表明设备上的端口工作是否正常。下表说明端口的可能状态。

LED	LED 颜色	LED 的含义
Link/Activity	闪烁绿色	表明设备检测端口的以太网信息流。
	熄灭	表明端口尚未与其它设备建立链路。
	绿色	表明端口已经与其它设备建立链路。
10/100	绿色	表明端口已经连接至 100 Base-T 设备。
	熄灭	表明端口已经连接至 10 Base-T 设备。



规格

本附录提供 NetScreen-5GT Wireless 设备的一般系统规格。

属性		
高	2.93 厘米	1.15 英寸
长	18.45 厘米	7.26 英寸
宽	20.8 厘米	8.19 英寸
重量	0.9 千克	1.98 磅
电器设备		
开关调节器	AC 适配器：100 V-240 VAC +/- 10% 50/60 Hz, 15-18 瓦特 DC 输入：12 伏, 1.25 - 1.5 安培	
环境要求		
正常海拔高度	0-40°C, 32 -105°F	
相对湿度	10-90%	
不冷凝	10-90%	
最大正常海拔高度为 2,000 米（6,562 英尺）		
证书		
安全	UL、CUL、TUV、CE 和 CB	
EMI	FCC 第 15 部分 B 类 VCCI、CE	
以太网连接器		
标准	100 Base-TX	
介质类型	5 类以上 非屏蔽双绞线 (UTP) 电缆	
最长距离	100 米（328.08 英尺）	
RJ-45 双绞线端口符合 IEEE 802.3 Type 10/100 Base-T 标准		
ADSL 连接器		
类型	6 针 Annex A RJ-11 连接器 Annex B RJ-45 连接器	
介质类型	标准电话线	

控制台和调制解调器适配器连接

下表列出了 RJ-45 连接器的定义。要采用标准 UART 端口，控制台和调制解调器端口均使用这种配置。

RJ-45	信号	缩写	DCE
1	Request To Send (要求传送)	RTS	In
2	Data Terminal Ready (资料终端就绪)	DTR	In
3	Transmitted Data (传输资料)	TD	In
4, 5	Signal Ground (信号地)	SGND	不适用
6	Received Data (接收资料)	RD	Out
7	Not Connected (未连接)		
8	Clear To Send (可以传送)	CTS	Out

下表列出了 RJ-45 至 DB-9 适配器连接的定义。要采用标准 UART 端口，控制台和调制解调器端口必须均使用这种配置。

DB9	信号	缩写	DTE	DCE	RJ45
1	Data Carrier Detect (资料载波侦测)	DCD	In	Out	NC
2	Received Data (接收资料)	RD	In	Out	3
3	Transmitted Data (传输资料)	TD	Out	In	6
4	Data Terminal Ready (资料终端就绪)	DTR	Out	In	7
5	Signal Ground (信号地)	SGND	不适用	不适用	4
6	Data Set Ready (资料集就绪)	DSR	In	Out	2
7	Request To Send (要求传送)	RTS	Out	In	8
8	Clear To Send (可以传送)	CTS	In	Out	1
9	Ring Indicator (振口指示器)	RI	In	Out	NC

注意： 如果使用 NetScreen 设备附带的控制台电缆连接至调制解调器，则必须配备 null 调制解调器适配器并在调制解调器连接器上安装。

申请 DGT 使用手册必须包含以下信息：

本产品为经过型号认证的合格低功率射频电机，未经许可，任何公司、商店或用户均不得擅自更改频率、加大功率或原设计的特性及功能。

低功率射频电机的使用不得影响航空安全和干扰合法通信；如果发现有干扰现象，应立即停止使用并加以改善，直到不发生干扰，才能继续使用。

上述所谓的合法通信是指符合电信法规定的无线电通信活动。

低功率射频电机受合法通信或工业、科学及医疗用电波辐射性电机设备干扰属于正常现象。

索引

A

AAL5 复用 218

ADSL

连接电缆 207

连接端口 207

配置接口 217

Annex A 207

Annex B 207

为 Deutch Telecom 配置 220

ATM 适配层 5 218

ATM 点对点协议

请参阅 PPPoA

C

策略, 配置附加 223

从特定主机管理设备 223

D

DB-9 连接器 234

Deutch Telecom, 配置 Annex B 220

到 Untrust 区域的备份接口 226

电源, 连接 209

电源连接器 229

端口连接器 229

端口状态 LED 231

端口模式, 更改 224

F

服务集标识符

请参阅 SSID

复用, 配置 219

G

管理员名称, 更改 214

惯例 211

CLI 204

WebUI 204

更改登录名和密码 214

更改端口模式 224

H

恢复 227

恢复缺省设置 227

J

静态 IP 地址 218

L

LED

端口状态 231

状态 230

连接电源 209

连接器

电源 229

端口 229

路由模式 223

M

密码, 更改 214

N

NetScreen 出版物 205

O

微滤波器 208

限制从特定主机管理 223

无线

连接 207, 208

配置 215

使用缺省接口 209

天线 209

Trust 区域 215

Wzone1 区域 215

无线接口

绑定区域 215

控制台, 使用 213

P

- PPPoA 218
 - 配置 220
- PPPoE 218
 - 配置 220
- 配置
 - 缺省设置 216
 - 所需的 213, 216
 - 可选的 222
 - 无线网络 215
 - SSID 216
- 配置 221

Q

- 缺省设置 216

R

- Reset 针孔, 使用 228
- RJ-45 连接器 234
- 日期, 设置 214

S

- SSID, 服务集标识符 216
- 设置设备时钟 214
- 时间, 设置 214

T

- Trust 区域接口的地址 227
- Trust 以太网端口 209
- 添加虚拟电路 219
- 天线 209
- 透明模式 223

U

- Untrust 区域, 配置备份接口 226

- Untrusted 端口 208

V

- VPI/VCI 218
 - 配置 219

W

- WebUI
 - 访问 211
- WebUI, 惯例 204
- wireless1 接口 215
- wireless2 接口
 - 访问 211
 - 更改接口地址 227
 - 设置 SSID 216
 - Trust 区域 215

Y

- 以太网点对点协议 (PPPoE)
 - 请参阅 PPPoE
- 验证连通性 227

X

- 信号分路器 208
- 虚拟电路, 添加 219
- 虚拟路径标识符 / 虚拟信道标识符
 - 请参阅 VPI/VCI

Z

- 在机架中安装设备 209
- 指南的组织方法 203
- 注册设备 211
- 状态 LED 230

目錄

前言.....	241
組織	241
WebUI 慣例	242
CLI 慣例	242
NetScreen 刊物	243
第 1 章 連接裝置	245
將 NetScreen 裝置連接至網路	245
將裝置連接至 Untrusted 網路	245
連接 ADSL 連接埠	245
連接 Untrusted 連接埠	246
將裝置連接至內部網路或工作站	246
連接 Trusted 乙太網路連接埠	247
使用無線介面	247
連接電源	247
機架安裝（可選）	247
第 2 章 設定裝置	249
存取裝置	249
使用 WebUI	249
使用 Telnet	250
使用主控台連接	251
所需的設定	251
變更管理員名稱和密碼	252
設定日期和時間	252
無線設定	253
設定無線網路	254
ADSL 設定	254
設定 ADSL 介面	255
為 ADSL 介面新增虛擬電路	257
VPI/VCI 和多工方法	257
PPPoE 或 PPPoA	258
Annex B 模式	258
靜態 IP 位址和網路遮罩	259
可選的設定	260
限制管理	261
設定附加政策	261
工作模式	261
變更連接埠模式	262
設定備份 Untrust 區域介面	264

變更 Trust 或 Wireless2 介面位址.....	265
驗證外部連接性	265
重設裝置使其復原出廠預設設定	265
使用 Reset 針孔.....	266
第 3 章 硬體說明.....	267
連接埠和電源連接器	267
狀態 LED	268
裝置的主要狀態 LED	269
連接埠狀態 LED	269
附錄 A 規格	271
索引.....	275

前言

Juniper Networks 的 NetScreen-5GT Wireless 裝置為使用整合無線 802.11b/g 介面的分支機構或零售渠道提供 IPSec 虛擬私人網路 (VPN) 和防火牆服務。NetScreen-5GT Wireless 裝置使用與 NetScreen 高階中央站台產品相同的防火牆、VPN、防病毒、深入檢查、通訊流量管理技術。

Juniper Networks 提供三種型號的 NetScreen-5GT Wireless 裝置：

- **NetScreen-5GT Wireless**：僅無線應用型號。
- **NetScreen-5GT Wireless ADSL A**：Wireless + Annex A 型號透過標準電話線 (POTS) 支援 ADSL。
- **NetScreen-5GT Wireless ADSL B**：Wireless + Annex B 型透過整合業務數位網路 (ISDN) 支援 ADSL。

所有型號均支援多達四個無線安全區。兩種 ADSL 型號均支援 ANSI T1.413 Issue 2、ITU G.992.1 (G.dmt) 和 ITU 992.2 (G.lite) 標準。

每種型號均支援三個軟體版本：

- 10 使用者版本可以支援多達 10 個使用者。
- Plus 版本支援任意數量的使用者。
- Extended 版本提供與 Plus 版本同樣的功能，另外有以下一些新功能：高可用性 (NSRP Lite)、DMZ 安全區以及附加的會話和通道功能。

組織

本手冊有三章和一個附錄。

[第 1 章](#)，“[連接裝置](#)”介紹如何將裝置連接至網路、如何連接電源和天線以及如何在機架中安裝 NetScreen-5GT Wireless 裝置。

[第 2 章](#)，“[設定裝置](#)”介紹 NetScreen-5GT Wireless (ADSL) 的預設設定和工作情況以及使用裝置所需的設定。

[第 3 章](#)，“[硬體說明](#)”提供有關 NetScreen-5GT Wireless 連接埠、LED 和電源要求的概述。

[附錄 A](#)，“[規格](#)”列出了有關 NetScreen-5GT Wireless 裝置的規格。

WebUI 慣例

在本書的各章節中，大於號 (>) 用於表示透過選擇功能表選項和連結在 WebUI 中導覽。

範例：Objects > Addresses > List > New

要存取新位址設定對話方塊，請：

1. 在功能表欄中，按一下 **Objects**。
Objects 功能表選項展開，顯示 Objects 選項的子功能表。
2. (Applet 功能表¹) 將滑鼠游標暫留在 **Addresses** 上。
(DHTML 功能表) 按一下 **Addresses**。
Addresses 選項展開，顯示 Addresses 選項的子功能表。
3. 按一下 **List**。
此時出現通訊錄表格。
4. 按一下右上角的 **New** 連結。
此時會出現新位址設定對話方塊。

CLI 慣例

在表達命令行介面 (CLI) 指令的語法時，採用以下慣例：

- 中括弧 [] 中的任何內容都是可選的。
- 大括弧 { } 中的任何內容都是必需的。
- 如果有多個選項，則使用導線 (|) 分隔每個選項。例如，

```
set interface { ethernet1 | ethernet2 | ethernet3 }  
manage
```

表示「設定 ethernet1、ethernet2 或 ethernet3 介面的管理選項」。
- 變數採用斜體。範例：

```
set admin user name1 password xyz
```

CLI 指令在句子的上下文中出現時，採用**粗體**（除始終採用斜體的變量之外）。範例：「使用 **get system** 指令顯示 NetScreen 裝置的序號。」

注意：輸入關鍵字時，只需輸入足夠的字母就可以唯一識別單詞。例如，要輸入指令 **set admin user joe j12fmt54**，只要輸入 **set adm u joe j12fmt54** 就足夠了。儘管輸入指令時可以使用此快捷方式，但是本文所述的所有指令均以完整的方式表達。

1. 可以按一下功能表欄底部的 **Toggle Menu** 選項，選擇 applet 或 DHTML 功能表類型。

NETSCREEN 刊物

要獲取任何 Juniper Networks 的 NetScreen 產品技術文件，請造訪

www.juniper.net/techpubs/。

如需技術支援，請按一下 <http://www.juniper.net/support/> 上的 Case Manager 連結開啓支援案例，或者致電 1-888-314-JTAC（美國國內）或 1-408-745-9500（美國以外）。

如果在以下內容中發現任何錯誤或遺漏，請用以下電子郵件地址與我們聯絡：

techpubs-comments@juniper.net

連接裝置

本章介紹如何將 NetScreen-5GT Wireless 裝置連接至網路以及如何連接電源和天線。如果使用 NetScreen-5GT Wireless 機架安裝選購件，請參閱本章結尾的機架安裝說明。

注意：有關安全警告和說明，請參閱《NetScreen Safety Guide》。此指南中的說明警告您哪些情況可能會造成人身傷害。在使用任何設備之前，要注意電路引發的危險，並熟悉標準操作，以免發生意外。

將 NETSCREEN 裝置連接至網路

NetScreen 裝置安裝在內部網路和 Untrusted 網路之間時，可以起到防火牆的作用，並為網路提供一般性的安全保護。本節介紹實體連接。

將裝置連接至 Untrusted 網路

根據所使用的 NetScreen-5GT Wireless 裝置的型號，可以透過以下一種方式連接至 Untrusted 網路：

- 透過從 NetScreen 裝置上的 ADSL 連接埠建立的 ADSL 連接
- 透過從 NetScreen 裝置上的 Untrusted 連接埠建立的乙太網路連接

連接 ADSL 連接埠

使用附帶的 ADSL 纜線從 NetScreen-5GT Wireless ADSL 裝置上的 ADSL 連接埠連接至電話插孔。Annex A 型號的裝置上的 ADSL 連接埠使用 RJ-11 連接器，而 Annex B 型號則使用 RJ-45 連接器。在使用 Annex B 型號的情況下，從 ADSL 連接埠連接至電話插孔的纜線在外觀和佈線方式上與直通 10 Base-T 乙太網路纜線完全相同。

警告：請確定不要錯將 NetScreen 裝置上的 Console、Modem 或乙太網路連接埠連接至電話插孔。

在 NetScreen-5GT Wireless ADSL 裝置上，ADSL 線路是與外部網路連接的主要連接線路。如需至外部網路的備份資料連結，可以使用乙太網路纜線從 NetScreen-5GT Wireless ADSL 裝置上的 Untrusted 連接埠連接至外部路由器或 DSL 或纜線數據機，或者可以使用序列纜線從裝置上的 Modem 連接埠連接至外部數據機。

警告：不能將裝置上的 Untrusted 連接埠和 Modem 連接埠同時連接至外部網路。

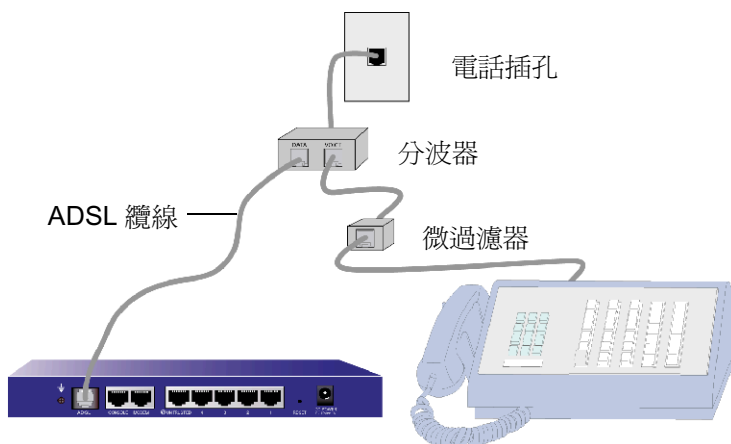
連接分波器和微過濾器

信號分波器將電話信號分成用於語音呼叫的低頻語音信號和用於和用於資料通訊流量的高頻資料信號。服務提供商通常會隨裝置安裝分波器，將使用者現場的電話線路連接至提供商的網路。

根據服務供應商的裝置的不同，有些分波器可能也可以自己動手安裝。如果自己安裝此類分波器，請使用 ADSL 纜線從 NetScreen 裝置和電話線路連接至分波器上的相應連接器（例如「data」或「voice」）。將分波器的另一端連接至電話插孔。

在每台連接至 ADSL 線路的電話、傳真機、答錄機或類比數據機上，可能需要安裝微過濾器。微過濾器會濾除電話線路中的高頻噪聲。微過濾器安裝在電話、傳真機、答錄機或類比數據機與分波器上語音連接器之間的電話線上。

下圖所示為現場安裝的微過濾器和分波器的一個範例。（必須從服務提供商處獲得適當的微過濾器或分波器。）



連接 Untrusted 連接埠

可以與外部路由器、DSL 數據機或纜線數據機建立互聯網連接，並為網路提供防火牆和一般性的安全保護。要建立高速連接，請使用附帶的乙太網路纜線從 NetScreen-5GT Wireless 裝置上的 Untrusted 介面連接至外部路由器或數據機。NetScreen-5GT Wireless 裝置會自動偵測到正確的速度、雙工和極性設置。

如果使用 NetScreen-5GT Wireless ADSL 裝置，有關 ADSL 連接說明，請參閱第 245 頁上的「[連接 ADSL 連接埠](#)」和第 246 頁上的「[連接分波器和微過濾器](#)」。

將裝置連接至內部網路或工作站

可以透過以下一種或兩種方法連接區域網路 (LAN) 或工作站：

- 透過 NetScreen 裝置上的一個或多個 Trusted 乙太網路連接埠連接
- 使用 NetScreen 裝置上的一個無線介面

連接 Trusted 乙太網路連接埠

NetScreen-5GT Wireless 裝置有四個 Trust 乙太網路連接埠。可以使用這些連接埠上的一個或多個連接埠透過交換機或集線器連接至 LAN。也可以將一個或所有的連接埠直接連接至工作站，不使用集線器或交換機。可以使用交叉纜線或直通纜線將 NetScreen-5GT 連接埠連接至其他裝置。

使用無線介面

如果使用無線介面，必須在裝置上連接附帶的天線。如果有標準的 2dB 全向天線，請將其旋轉到裝置後面標有 A 和 B 的接柱上，請參閱第 267 頁上的「[連接埠和電源連接器](#)」。要在天線的折彎處彎曲天線，切勿讓閃頭連接器受壓。

連接電源

為 NetScreen-5GT Wireless 裝置連接電源：

1. 將電源線的 DC 連接器端插入設備後面的 DC 電源插座。
2. 將電源線的 AC 轉接器端插入 AC 電源。

警告：NetScreen 建議，在連接電源時接入電涌保護器。

機架安裝（可選）

使用 NetScreen-5GT Wireless 機架安裝套件，可以將一個或兩個 NetScreen-5GT Wireless 裝置安裝到標準的 19 英寸設備機架內。NetScreen-5GT Wireless 機架安裝套件包括安裝說明和機架安裝底盤。底盤的尺寸如下：

寬：	48.26 厘米	19 英寸
高：	4.013 厘米	1-5/8 英寸（1 個機架單位）
長：	33.655 厘米	13 -1/4 英寸

除 NetScreen-5GT Wireless 裝置、機架安裝套件和裝置機架之外，還需要以下工具：

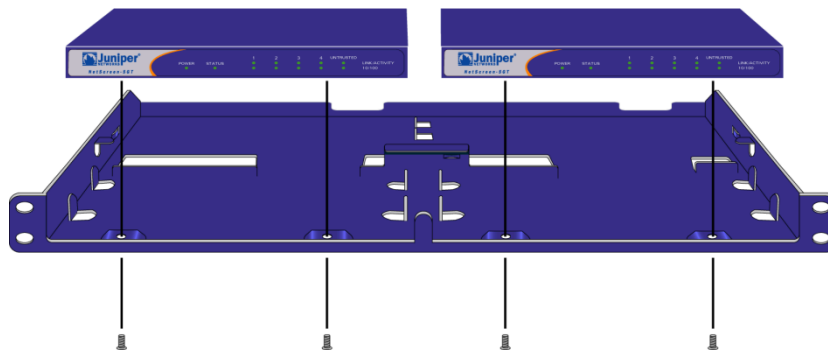
- 十字螺絲起子
- 四個與設備機架螺紋尺寸相符的螺絲

在機架內安裝裝置：

1. 使用十字螺絲起子從每台要安裝的 NetScreen-5GT Wireless 裝置下側卸下兩個螺絲。（保存好螺絲，以備下一步使用）螺絲位於裝置下側接近前面板的位置。



2. 將每台裝置裝入機架安裝底盤，並使用在步驟 1 中卸下的螺絲將其固定到底盤上。



3. 用剩下的螺絲將左側和右側底盤金屬板固定到設備機架上。



可以將電源線或乙太網路電纜穿過底盤平板的開口或後壁上的凹陷。也可以使用裝置後面的空間放置電源。

設定裝置

本章介紹在將 NetScreen-5GT Wireless 裝置連接至網路之後如何設定裝置。如果是第一次使用 ScreenOS WebUI 圖形介面存取裝置，則可以使用初始設定精靈 (ICW) 指導您完成基本設定。要使用此精靈，請參閱《Juniper Networks NetScreen-5GT Wireless Getting Started Guide》和《Juniper Networks NetScreen-5GT Wireless ADSL Getting Started Guide》。

本章中介紹的主題包括：

- 存取裝置
- 所需的設定
- 無線設定
- ADSL 設定
- 可選的設定
- 驗證外部連接性
- 重設裝置使其復原出廠預設設定

*注意：*在設定 NetScreen 裝置和驗證網際網路連接性之後，必須在 www.juniper.net/support/ 上註冊產品，這樣才能在裝置上啟動某些 ScreenOS 服務（例如內部防病毒或深入檢查簽名服務）。在註冊完產品之後，請使用 WebUI 預訂服務。有關註冊產品和獲得預訂特定服務的詳細資訊，請參閱 ScreenOS 5.0.0 的《NetScreen 概念與範例 ScreenOS 參考指南》「基本原理」卷中的「系統參數」一章。

存取裝置

本節介紹如何使用 WebUI、Telnet 或 Console 連接存取 NetScreen 裝置。

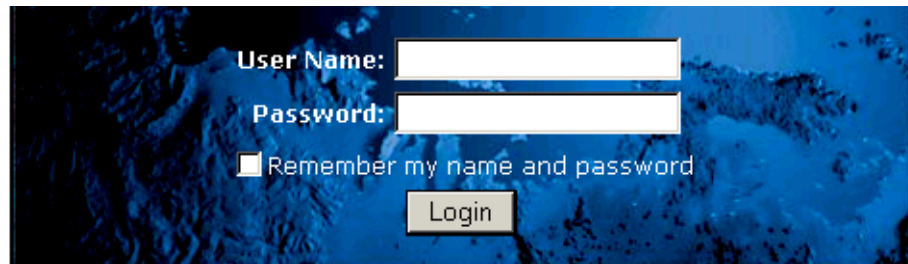
使用 WebUI

ScreenOS WebUI 是一個可以透過 web 瀏覽器使用的圖形介面。要使用 WebUI，必須與 Trust 或 wireless2 介面處於同一子網路。要使用 WebUI 管理應用程度存取 NetScreen-5GT Wireless 裝置，請：

1. 啟動瀏覽器，在 URL 欄位中輸入 Trust 或 wireless2 介面的 IP 位址，請按 Enter。
例如，在 URL 欄位中輸入以下地址：

192.168.1.1

NetScreen WebUI 軟體顯示登入提示。



注意：如果選擇略過 *Initial Configuration Wizard*（初始設定精靈），WebUI 登入提示會自動出現。

2. 如果尚未變更預設使用者名稱和密碼，請在 **User Name** 和 **Password** 欄位中均輸入 **netscreen**，然後按一下 **Login**。（僅使用小寫字母。User Name 和 Password 欄位均區分大小寫。）

使用 Telnet

Telnet 是一個應用程式，它使您可以透過網際網路通訊協定 (IP) 網路存取裝置。

注意：也可以使用安全 Shell (SSH) 應用程式存取 NetScreen 裝置。有關詳細資訊，請參閱 ScreenOS 5.0.0 的《NetScreen 概念與範例 ScreenOS 參考指南》的「管理」卷中的「管理」一章。

要使用 Telnet 設定裝置，請在工作站的 Telnet 會話中輸入 ScreenOS 指令行介面 (CLI) 指令。

1. 使用 Trust 或 wireless2 介面的 IP 位址啟動 Telnet 用戶端應用程式。例如，輸入以下指令：
telnet 192.168.1.1
2. 如果尚未變更預設使用者名稱和密碼，請在 **Login** 和 **Password** 提示欄位中均輸入 **netscreen**。（僅使用小寫字母。Login 和 Password 提示欄位均區分大小寫。）

使用主控台連接

NetScreen-5GT Wireless 裝置上的 Console 連接埠使您可以透過連接至工作站或終端的序列纜線存取裝置。要使用主控台連接設定裝置，請在終端或工作站上的終端模擬程式中輸入 ScreenOS CLI 指令。

注意：要建立主控台連接，需要使用一條序列纜線，一端帶有凸 RJ-45 連接器另一端帶有凹 DB-9 連接器。有關序列纜線的針腳排列，請參閱附錄 A，「規格」。

建立主控台連接：

1. 將序列電纜的凹 DB-9 一端插入電腦的序列連接埠。（確定 DB-9 連接器正確地插在連接埠上。）
2. 將 DB-9 連接器的另一端插入 RJ-45 DB-9 連接埠。（確定 DB-9 連接器正確地插在 RJ-45 DB-9 連接埠上。）
3. 將序列纜線的凸 RJ-45 一端插入 NetScreen-5GT Wireless 裝置的 Console 連接埠。（確定 RJ-45 連接器正確地插在連接埠上。）
4. 啟動序列終端模擬程式。（通用的終端程式是 Hilgreave HyperTerminal。）要啟動 NetScreen-5GT Wireless 裝置的主控台會話，需要進行以下設定：
 - Baud Rate: 9600
 - Parity: 無
 - Data Bits: 8
 - Stop Bit: 1
 - Flow Control: 無
5. 如果尚未變更預設使用者名稱和密碼，請在 **Login** 和 **Password** 提示欄位中均輸入 **netScreen**。（僅使用小寫字母。Login 和 Password 欄位均區分大小寫。）

所需的設定

本節介紹要使用裝置必須完全的設定。

注意：如果任何時候需要復原裝置的預設設定，請參閱“[重設裝置使其復原出廠預設設定](#)”在 265 頁。

變更管理員名稱和密碼

因為所有的 NetScreen 產品均使用相同的預設管理員名稱和密碼 (**netscreen**)，因此，最好立即變更管理員名稱和密碼。要將管理員名稱和密碼從「netscreen」和「netscreen」變更爲「darwin1」和「1240jes」，請：

WebUI

Configuration > Admin > Administrators > Edit (對於 NetScreen 管理員名稱)：
輸入以下內容，然後按一下 **OK**：

Administrator Name: darwin1

Old Password: netscreen

注意：輸入密碼時，WebUI 中並不顯示密碼。

New Password: 1240jes

Confirm New Password: 1240jes

CLI

```
set admin name darwin1
set admin password 1240jes
save
```

有關建立不同管理員級別的資訊，請參閱 ScreenOS 5.0.0 的《NetScreen 概念與範例 ScreenOS 參考指南》的「管理」卷中的「管理」一章。

設定日期和時間

在 NetScreen 裝置上設定的時間會影響諸如 VPN 通道設定和排程的時間安排。在 NetScreen 裝置上設定日期和時間的簡便方法就是將 NetScreen 裝置上的系統時鐘與電腦上的時鐘同步。要在 WebUI 中進行此操作：

1. Configuration > Date/Time：按一下 **Sync Clock with Client** 按鈕。
此時會彈出一條訊息，提供您指定是否已經在電腦時鐘上啟用夏令時間 (DTS) 選項。
2. 按一下 **Yes** 將同步系統時鐘，並根據 DTS 調整系統時鐘；或者按一下 **No** 只同步系統時鐘，不根據 DTS 對其進行調整。

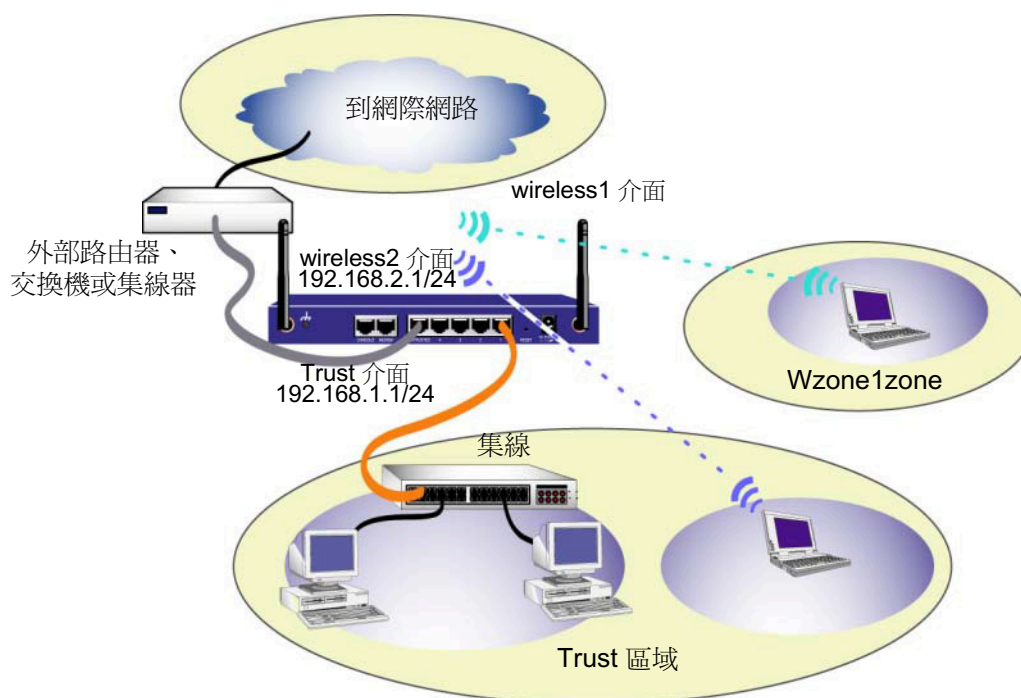
也可以在 Telnet 或主控台會話中使用 CLI **set clock** 指令，手動設定日期和時間。

無線設定

本節介紹有關在 NetScreen 裝置上設定無線介面的資訊。根據安裝的許可類型，可以在 NetScreen-5GT Wireless 裝置上設定多達四個無線安全區。介面與區域的繫結是預先定義的，而且依賴設定的連接埠模式，不能將無線介面指定給 Untrust 區域。必須在 NetScreen 裝置上設定至少一個無線介面，才能建立無線區域網路 (WLAN)。

注意：如果是在美國或日期以外的某國家或地區使用 NetScreen-5GT Wireless 裝置，則必須先運行 `set wlan country-code` 指令，然後才能建立 WLAN 連接。此指令用於設定可選通道範圍和傳輸功率級別。

下圖顯示了 NetScreen-5GT Wireless 裝置的預設設定。



預設無線介面的預先定義名稱爲「wireless2」。Trust 和 wireless2 介面繫結到 Trust 區域，相應設定的子網路位址爲 192.168.1.1/24 和 192.168.2.1/24。這意味著，在 Trust 區域內連接的所有裝置均必須與 Trust 或 wireless2 介面處於同一子網路，而且其 IP 位址處於兩個子網路的一個子網路內。同時組態 NetScreen 裝置將 192.168.1.1/24 和 192.168.2.1/24 子網路的 IP 位址指定給裝置。有關詳細資訊，請參閱“[變更 Trust 或 Wireless2 介面位址](#)”在 265 頁。

在預設情況下，wireless1 介面繫結到 Wzone1 區域，沒有指定的 IP 位址。如果要使用 wireless1 介面，必須爲其組態 IP 位址。有關詳細資訊，請參閱 *NetScreen-5GT Wireless Reference Guide*。

NetScreen 裝置允許源自 Trust 區域內裝置的任何類型的通訊流量進入網際網路，但不允許任何源自網際網路的通訊流量進入網路。可以組態額外的限制，有關詳情，請參閱“[設定附加政策](#)”在 261 頁。

設定無線網路

無線網路由稱為「服務集識別字」(SSID)的名稱組成。指定 SSID 使您可以在同一位置具有多個無線網路。在每台裝置上最多可以設定 8 個 SSID。設定 SSID 名稱之後，即可設定 SSID 屬性。

要將 SSID 名稱設定為 **netscreen open**，允許無線網路連接，並啟動 wireless2 介面：

WebUI

Wireless > SSID > New：輸入以下內容，然後按一下 **OK**：

SSID: "netscreen open"

Wireless Interface Binding: wireless2 (精選)

Activate Changes > 按一下 **Activate Changes** 按鈕

CLI

```
set ssid name "netscreen open"  
set ssid "netscreen open" authentication open encryption  
none  
set ssid "netscreen open" interface wireless2  
exec wlan reactivate
```

將 SSID 設定為 wireless2 介面之後，可以按照 [“存取裝置”](#) 在 249 頁介紹的步驟使用預設 wireless2 介面 IP 位址存取裝置，以設定裝置。有關設定範例、SSID 屬性和與無線安全設定有關的指令，請參閱 *《NetScreen-5GT Wireless Reference Guide》*。

ADSL 設定

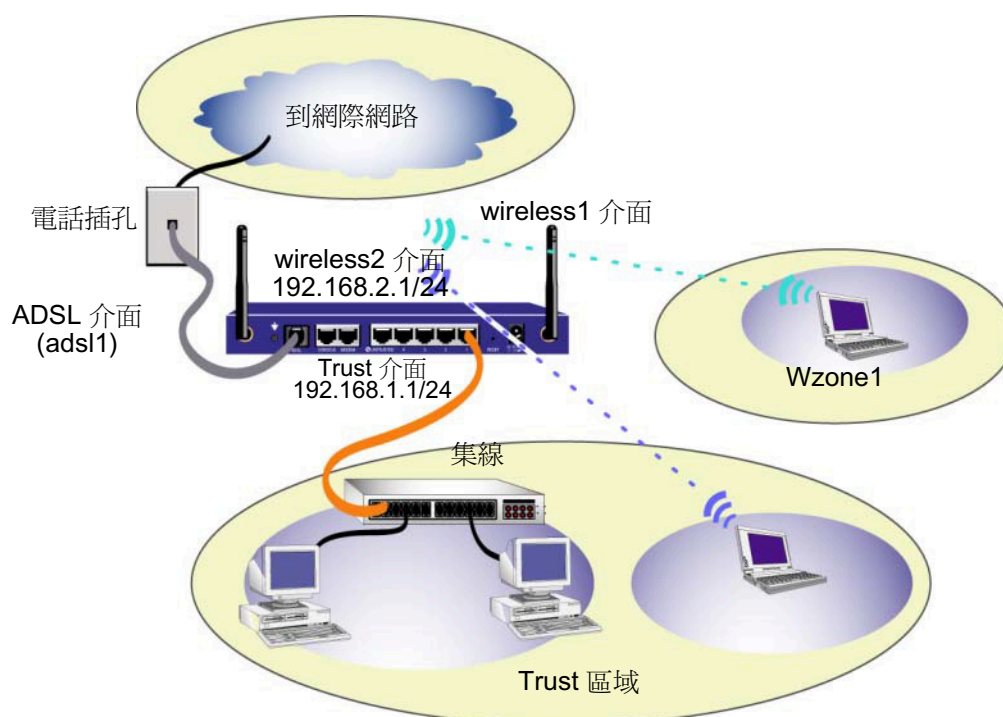
本節介紹出廠時 NetScreen-5GT Wireless ADSL Annex A 和 B 裝置的預設設定的工作情況。在大多數情況下，這些預設設定中只有幾項是必須設定的。

本節介紹 Untrust 區域介面的以下設定：

- [設定 ADSL 介面](#)
- [為 ADSL 介面新增虛擬電路](#)
- [VPI/VCI 和多工方法](#)
- [PPPoE 或 PPPoA](#)
- [Annex B 模式](#)
- [靜態 IP 位址和網路遮罩](#)

注意：如果任何時候需要復原裝置的預設設定，請參閱 [“重設裝置使其復原出廠預設設定”](#) 在 265 頁。

下圖顯示了 NetScreen-5GT Wireless ADSL 裝置的預設設定。



ADSL 介面的預先定義名稱爲「adsl1」，是網路與網際網路之間的主要連接介面。要允許 NetScreen 裝置（和網路上的裝置）連接至網際網路，必須根據服務供應商提供的資訊設定 adsl1 介面。請參閱 [“設定 ADSL 介面”](#) 在 255 頁。

NetScreen 裝置允許源自 Trust 區域內裝置的任何類型的通訊流量進入網際網路，但不允許任何源自網際網路的通訊協定進入網路。可以設定額外的限制，有關詳情，請參閱 [“設定附加政策”](#) 在 261 頁。

設定 ADSL 介面

網路使用 NetScreen 裝置上的 ADSL 介面「adsl1」透過非同步傳輸模式 (ATM) 虛擬電路連接至服務供應商的網路。可以透過建立 ADSL 子介面，設定額外的虛擬電路（有關詳細資訊，請參閱 [“爲 ADSL 介面新增虛擬電路”](#) 在 257 頁）。

在 WebUI 中，找到 Network > Interfaces 頁面，查看 NetScreen 裝置上的當前介面清單。如果使用 Telnet 或主控台會話，請輸入 CLI 指令 **get interface**。應該看到 adsl1 介面繫結到 Untrust 區域。如果曾經使用 ICW 設定裝置，則可能已經爲 adsl1 介面指定 IP 位址和網路遮罩。

注意：如果不希望使用 ADSL 介面，可以使用 **set interface adsl1 zone null** 指令將其繫結到 Null 區域。如果使用 ICW 設定裝置，則可以選擇除 ADSL 介面之外的其它介面作爲至 Untrust 區域的預設介面。

必須設定 `adsl1` 介面，才能使 NetScreen 裝置連接至服務供應商的網路。要進行此操作，必須從服務供應商處獲得以下資訊：

- 虛擬路徑識別字和虛擬通道識別字 (VPI/VCI) 值
- ATM 配接層 5 (AAL5) 多工方法，可以是以下方法之一：
 - 基於虛擬電路 (VC) 的多工，其中每種通訊協定是透過單獨的 ATM VC 傳輸的
 - 邏輯連結控制 (LLC) 封裝通訊協定，它允許在同一 ATM VC 上傳輸多種通訊協定（預設多工方法）
- 服務供應商指定的使用者名稱和密碼，用於使用乙太網路點對點通訊協定 (PPPoE) 或 ATM 點對點通訊協定 (PPPoA) 連接至服務供應商的網路
- 驗證方法（如果有），針對 PPPoE 或 PPPoA 連接
- 網路的靜態 IP 位址和網路遮罩值（可選）

為 ADSL 介面新增虛擬電路

要新增虛擬電路，需要為 ADSL 介面建立子介面。可以建立多達 10 個 ADSL 子介面。例如，建立一個名為「adsl1.1」的新介面，該介面繫結到名為「Corp1」的使用者定義區域：

WebUI

Network > Interfaces > New ADSL Sub-IF：輸入以下內容，然後按一下 **Apply**：

Interface Name: adsl1.1

VPI/VCI: 0/35

Zone Name: Corp1 (精選)

CLI

```
set interface adsl1.1 pvc 0 35 zone corp1
save
```

必須按照與設定 ADSL 主介面相同的方式設定 ADSL 子介面，包括設定 VPI/VCI 值，如“設定 ADSL 介面”在 255 頁中所述。ADSL 子介面的設定是獨立於 ADSL 主介面的；也就是說，可以在子介面上設定與 ADSL 主介面不同的多工方法、VPI/VCI 和 PPP 用戶端。即使 ADSL 主介面沒有靜態 IP 位址，也可以在子介面上設定靜態 IP 位址。注意，如果在一個子介面和 ADSL 主介面中，一個介面是針對 PPPoA 設定的，而另一個介面是針對 PPPoE 設定的，且兩個介面均使用 LLC 多工方法，則兩者均可以使用同一 VPI/VCI 值。

VPI/VCI 和多工方法

服務供應商會為每個 VC 連接指定一個 VPI/VCI 值對。例如，可能會接收到 VPI/VCI 值對 1/1，這個值對表示一個 VPI 值 1 和一個 VCI 值 1。這些值必須與服務供應商在使用者的數位用戶線接取多工器 (DSLAM) 上設定的值相符。

在 adsl1 介面上組態 VPI/VCI 值對：

WebUI

Network > Interfaces > Edit (對於 adsl1 介面)：在 VPI/VCI 欄位中輸入 1/1，然後按一下 **Apply**。

CLI

```
set interface adsl1 pvc 1 1
save
```

在預設情況下，NetScreen-5GT Wireless ADSL 裝置對每個 VC 均使用基於 LLC 的多工方法。在 adsl1 介面上設定 VPI/VCI 1/1 介面並在 VC 上使用 LLC 封裝通訊協定：

WebUI

Network > Interfaces > Edit (對於 adsl1 介面)：輸入以下內容，然後按一下 **Apply**：

VPI/VCI: 1 / 2

Multiplexing Method: LLC (精選)

CLI

```
set interface adsl1 pvc 1 1 mux llc
save
```

PPPoE 或 PPPoA

NetScreen 裝置既有 PPPoE 用戶端，也有 PPPoA 用戶端，它透過 ADSL 連結連接至服務供應商。PPPoE 是最常用的 ADSL 封裝通訊協定，用於在網路中的每台主機上終止會話。PPPoA 主要用於公司級服務，因為 PPP 會話可以在 NetScreen 裝置上終止。要使 NetScreen 裝置連接至服務供應商網路，必須設定服務供應商指定的使用者名稱和密碼。PPPoA 的設定與 PPPoE 的設定類似。

注意：NetScreen 裝置在每個虛擬電路上僅支援一個 PPPoE 會話。

為 PPPoE 設定使用者名稱「roswell」和密碼「area51」，將 PPPoE 設定繫結到 adsl1 介面：

WebUI

Network > PPPoE > New：輸入以下內容，然後按一下 **OK**：

PPPoE Instance: poe1
Bound to Interface: adsl1 (精選)
Username: roswell
Password: area51

CLI

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1
save
```

在 NetScreen 裝置上還可以設定一些其它的 PPPoE 或 PPPoA 參數，包括驗證方法（在預設情況下，NetScreen 裝置支援詢問交握式驗證通訊協定或密碼驗證通訊協定）、閒置逾時（預設值為 30 分鐘）等等。詢問服務供應商，要與服務供應商的服務器建立正常的通訊，是否有其它必須設定的 PPPoE 或 PPPoA 參數。

Annex B 模式

如果將 NetScreen-5GT Wireless ADSL 裝置的 Annex B 型號連接至 Deutsch Telecom ADSL 線路，則必須在 ADSL 連接埠上設定介面，才能使用此設備進行工作。要進行此操作，請：

WebUI

Network > Interfaces > Edit（對於 adsl1 介面）：選擇 Annex B 模式為 **DT**，然後按一下 **Apply**。

CLI

```
set interface adsl1 phy annex-b-mode dt
save
```

如果使用該裝置的 Annex A 型號或正在將該裝置連接至非 Deutsch Telecom 設備，則不需要設定此設定。

靜態 IP 位址和網路遮罩

如果 ISP 給定了具體固定的網路 IP 位址和網路遮罩，請設定網路的 IP 位址和網路遮罩以及連接 NetScreen 裝置的路由器連接埠的 IP 位址。另外，需要指定該裝置將使用靜態 IP 位址。（在預設情況下，NetScreen 裝置充當 PPPoE 或 PPPoA 用戶端，並透過與 PPPoE 或 PPPoA 服務器的協商為 ADSL 介面接收一個 IP 位址）。

為網路設定靜態 IP 位址 1.1.1.1/24：

WebUI

Network > Interfaces > Edit（對於 adsl1 介面）：輸入以下內容，然後按一下 **Apply**：

IP Address/Netmask: 1.1.1.1/24

Static IP: (精選)

注意：必須設定 PPPoE 或 PPPoA 實例，並將其繫結到 adsl1 介面，如上一節所述。確定選擇「Obtain IP using PPPoE」或「Obtain IP using PPPoA」以及 PPPoE 或 PPPoA 實例的名稱。

CLI

```
set interface adsl1 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

或

```
set interface adsl1 ip 1.1.1.1/24
set pppoa name poa1 static-ip
save
```

要使用網域名稱系統 (DNS) 進行網域名稱和位址解析，網路中的電腦需要具有至少一臺 DNS 服務器的 IP 位址。如果 NetScreen 裝置透過 PPPoE 或 PPPoA 為 ADSL 介面接收一個 IP 位址，則也會自動接收 DNS 服務器的 IP 位址。如果網路中的電腦從 NetScreen 裝置上的 DHCP 服務器接收自己的 IP 位址，則這些電腦也會獲得這些 DNS 服務器的位址。

如果為 ADSL 介面指定靜態 IP 位址，則服務供應商必須提供 DNS 服務器的 IP 位址。也可以在網路中的每臺電腦上設定 DNS 服務器位址或在 Trust 區域介面上組態 DHCP 服務器，以便它為每臺電腦提供 DNS 服務器位址。

在 Trust 介面上設定 DHCP 服務器，使其為網路中的電腦提供 DNS 服務器位址 1.1.1.152：

WebUI

Network > DHCP > Edit (對於 Trust 介面) > DHCP Server : 在 DSN1 中輸入 1.1.1.152，然後按一下 **Apply**。

CLI

```
set interface trust dhcp server option dns1 1.1.1.152
save
```

可選的設定

本節介紹以下一些可能要設定的 NetScreen-5GT Wireless 裝置功能：

- [限制管理](#)
- [設定附加政策](#)
- [工作模式](#)
- [變更連接埠模式](#)
- [設定備份 Untrust 區域介面](#)
- [變更 Trust 或 Wireless2 介面位址](#)

注意：本手冊並沒有對可選設定逐一進行詳細介紹。有關詳細資訊，請參閱 ScreenOS 5.0.0 的《NetScreen 概念與範例 ScreenOS 參考指南》中的相應章節。

限制管理

在預設情況下，網路中的任何使用者，如果知道登入名稱和密碼，均可以管理 NetScreen 裝置。可以設定 NetScreen 裝置，使其僅接受從網路中的一個或多個特定主機進行管理。（可以選擇要在 NetScreen 裝置上啓用哪種服務，例如 WebUI、Telnet 和 Ping。）

有關詳細資訊，請參閱 ScreenOS 5.0.0 的《*NetScreen 概念與範例 ScreenOS 參考指南*》的「管理」卷中的「管理」一章。

設定附加政策

儘管為 NetScreen-5GT Wireless 設定的預設政策允許網路 Trust 區域中的工作站存取外部電腦執行的任何類型的服務，但是外部電腦無權存取或啓動工作站執行的會話。可以透過設定政策，要求 NetScreen 裝置允許外部電腦啓動您的電腦執行的特定類型的會話。要建立或修改政策，請參閱 ScreenOS 5.0.0 的《*NetScreen 概念與範例 ScreenOS 參考指南*》的「管理」卷中的「管理」一章。

工作模式

*工作模式*是 NetScreen 裝置上介面處理區域之間通訊流量的方式。在預設情況下，NetScreen-5GT Wireless 裝置在路由模式下工作，同時在 Trust 介面上啓用網路位址轉換 (NAT)。這意味著，當 Trust 區域中的裝置傳送通訊流量到網際網路時，NetScreen 裝置使用 Untrust 介面的 IP 位址替換初始來源 IP 位址。儘管 NetScreen 裝置會為網路中的裝置指定私有 IP 位址，但是網路外部電腦始終看不到這些位址。

如果網路中所有的裝置都有公開 IP 位址，則可以設定 NetScreen 裝置使用不啓用 NAT 的「路由」模式。在不啓用 NAT 的「路由」模式下，NetScreen 裝置透過檢查 IP 位址轉發通訊流量。有關設定裝置使用不啓用 NAT 的「路由」模式的詳細資訊，請參閱 ScreenOS 5.0.0 的《*NetScreen 概念與範例 ScreenOS 參考指南*》「基本原理」卷中的「介面模式」一章。

變更連接埠模式

連接埠模式是物理連接埠、邏輯介面和區域的繫結。

警告：變更連接埠模式會刪除 NetScreen 裝置上所有現有的設定。因此，在設定裝置之前，應該變更連接埠模式。

下表簡發列出了 NetScreen-5GT Wireless 裝置上的連接埠模式的連接埠、介面和區域繫結：

連接埠名稱 ^a	Trust-Untrust 連接埠模式 ^b		Home-Work 連接埠模式		Trust/Untrust/DMZ (Extended) 模式		Dual Untrust 模式		Combined 連接埠模式	
	介面	區域	介面	區域	介面	區域	介面	區域	介面	區域
1	trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet1	Trust	ethernet1	Work
2	trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet1	Trust	ethernet2	Home
3	trust	Trust	ethernet2	Home	ethernet2	DMZ	ethernet1	Trust	ethernet2	Home
4	trust	Trust	ethernet2	Home	ethernet2	DMZ	ethernet2	Untrust	ethernet3	Untrust
Untrusted	untrust	Untrust	ethernet3	Untrust	ethernet3	Untrust	ethernet3	Untrust	untrust	Untrust
Modem ^c	序列	Null	序列	Null	序列	Null	序列	Null	序列	Null
	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1
	wireless2	Trust	wireless2	Work	wireless2	Trust	wireless2	Trust	wireless2	Work
			wireless3	Home	wireless3	DMZ			wireless3	Home
					wireless4	Wzone2				

a. NetScreen 設備機箱上標示的名稱。

b. 預設連接埠模式

c. 可以使用 Untrust 乙太網路連接埠或 Modem 連接埠，設定一個至 Untrust 區域的備份介面，請參閱 “設定備份 Untrust 區域介面” 在 264 頁。

下表簡發列出了 NetScreen-5GT Wireless ADSL 裝置上的連接埠模式的連接埠、介面和區域繫結：

連接埠名稱 ^a	Trust-Untrust 連接埠模式 ^b		Home-Work 連接埠模式		Trust/Untrust/DMZ (Extended) 模式	
	介面	區域	介面	區域	介面	區域
1	trust	Trust	ethernet1	Work	ethernet1	Trust
2	trust	Trust	ethernet1	Work	ethernet1	Trust
3	trust	Trust	ethernet2	Home	ethernet2	DMZ
4	trust	Trust	ethernet2	Home	ethernet2	DMZ
Untrusted	untrust	Null ^c	ethernet3	Null ^c	ethernet3	Null ^c
Modem	序列	Null ^c	序列	Null ^c	序列	Null ^c
ADSL	adsl1	Untrust	adsl1	Untrust	adsl1	Untrust
	wireless1	Wzone1	wireless1	Wzone1	wireless1	Wzone1
	wireless2	Trust	wireless2	Work	wireless2	Trust
			wireless3	Home	wireless3	DMZ
				wireless4	Wzone2	

a. NetScreen 設備機箱上標示的名稱。

b. 預設連接埠模式

c. 可以使用 Untrust 乙太網路連接埠或 Modem 連接埠，設定一個至 Untrust 區域的備份介面，請參閱“設定備份 Untrust 區域介面”在 264 頁。

將 NetScreen 裝置變更為 Home-Work 連接埠模式：

WebUI

Configuration > Port Mode: 從下拉清單中選擇 Home-Work，然後按一下 **Apply**。

在出現下列提示時，按一下 **OK**：

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

CLI

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

在出現下列提示時，輸入 **y**（代表是）：

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

設定備份 Untrust 區域介面

在預設情況下，在 NetScreen-5GT Wireless ADSL 裝置上，adsl1 介面是與外部網路的主要連接介面。NetScreen-5GT Wireless ADSL 裝置上提供的每種連接埠模式使您可以選擇是連接 Untrusted 乙太網路連接埠還是 Modem 連接埠作為至外部網路的備份連接介面（請參閱“變更連接埠模式”在 262 頁）。必須將備份介面繫結到 Untrust 區域並相應地設定介面。

注意：可以使用 Untrusted 乙太網路連接埠或 Modem 連接埠連接，僅設定一個備份介面。如果使用 Untrusted 連接埠建立備份連接，請在 Trust-Untrust 連接埠模式下設定 Untrust 介面，或者為其它連接埠模式設定 ethernet3 介面。如果使用 Modem 連接埠建立為所有連接埠模式設定串行介面。

例如，將 Untrust 介面繫結到 Untrust 區域：

WebUI

Network > Interfaces > Edit（對於 untrust 介面）：從 Zone Name 下拉清單中選擇 Untrust，然後按一下 **OK**。

CLI

```
set interface untrust zone untrust
save
```

同時需要為 Untrust 介面設定靜態 IP 位址，或者指定是否透過 DHCP 或 PPPoE 獲取該介面的 IP 位址。有關設定介面參數的詳細資訊，請參閱 ScreenOS 5.0.0 的《NetScreen 概念與範例 ScreenOS 參考指南》的「基本原理」卷中的「介面」一章。

adsl1 介面和乙太網路介面（名為「untrust」或「ethernet3」，根據連接埠模式而定）或序列介面繫結到 Untrust 區域時，裝置會自動設定介面故障後轉移。也就是說，如果 adsl1 介面不可用，NetScreen 裝置會自動將通訊流量傳送到備份介面。adsl1 介面可用時，裝置會自動將通訊流量傳送到 adsl1 介面。

注意：只有 adsl1 介面受故障後轉移影響。也就是說，如果已同時設定 ADSL 子介面，子介面在故障後轉移時不會轉移到備份介面。

也可以手動強制在 adsl1 介面上實現故障後轉移和容錯回復。有關詳細資訊，請參閱 ScreenOS 5.0.0 的《NetScreen 概念與範例 ScreenOS 參考指南》的「高可用性」卷中的「介面冗餘」一章。

變更 Trust 或 Wireless2 介面位址

必要時，可以變更 Trust 介面和無線介面的 IP 位址和網路遮罩。（切記，Trust 或 wireless2 介面處於 NAT 模式時，網路外部的電腦始終看不到網路中裝置的 IP 位址，外部電腦看到的僅僅是 Untrust 介面的 IP 位址。）例如，可能需要變更 Trust 或 wireless2 介面，以符合網路中現有的 IP 位址。如果變更 Trust 或 wireless2 介面的 IP 位址和網路遮罩，則同時需要變更 NetScreen 裝置透過 DHCP 指定給網路裝置的位址範圍，或者停用 Trust 或 wireless2 介面上的 DHCP 服務器。

如果網路中的電腦從 NetScreen 裝置上的 DHCP 服務器接收自己的 IP 位址，則這些電腦也從 NetScreen 裝置獲得其預設閘道。如果某電腦已經有靜態指定的 IP 位址，則必須在 NetScreen 裝置上手動將其預設閘道設定為 Trust 或 wireless2 介面的 IP 位址。

要為 Trust 或 wireless2 介面指定一個不同的 IP 位址和網路遮罩，請參閱 ScreenOS 5.0.0 的《NetScreen 概念與範例 ScreenOS 參考指南》「基本原理」卷中的「介面」一章。

要變更 NetScreen 裝置的 DHCP 設定，請參閱 ScreenOS 5.0.0 的《NetScreen 概念與範例 ScreenOS 參考指南》「基本原理」卷中的「系統參數」一章。

驗證外部連接性

要驗證網路中的工作站是否能夠存取網際網路中的資源，請從網路中的任何工作站啟動 Web 瀏覽器並輸入以下的 URL: www.juniper.net。

重設裝置使其復原出廠預設設定

如果遺失了管理員密碼，可以重設 NetScreen 裝置使其復原預設設定。這樣會破壞所有現有的設定，但是可復原對裝置的存取。

警告：重設裝置會刪除所有現有的設定，並且會使現有的防火牆和 VPN 服務不可用。

可以使用以下方式中的一種將裝置復原到其預設設定：

- 使用主控台連接。有關詳細資訊，請參閱 ScreenOS 5.0.0 的《NetScreen 概念與範例 ScreenOS 參考指南》的「管理」卷中的「管理」一章。
- 使用裝置後面板上的 Reset 針孔，如下一節所述。

使用 Reset 針孔

按 Reset 針孔可以重設裝置並復原出廠預設設定。要執行此操作，需要檢視前面板上的裝置狀態 LED 或啟動主控台會話（如“使用主控台連接”在 251 頁中所述）。

1. 找到後面板上的 Reset 針孔。使用又細又硬的金屬絲（例如迴紋針），推壓針孔四至六秒然後鬆開。



Reset 針孔

Status LED 閃爍琥珀黃色。主控台上的訊息提示，已經開始刪除設定，並且系統發出一個 SNMP/SYSLOG 警示。

2. 等待一至二秒。

在第一次重設之後，Status LED 閃爍綠色；現在裝置正在等待第二次重設。主控台訊息現在提示，裝置正在等待第二次確認。

3. 再次推壓 Reset 針孔四至六秒。

主控台訊息會驗證第二次確認。Status LED 呈琥珀黃色亮起半秒，然後返回到閃爍綠色狀態。

此時，裝置即重設到其原始的出廠設定。裝置重設時，Status LED 變為琥珀黃色半秒，然後返回到閃爍綠色狀態。主控台顯示裝置啟動訊息。系統向已設定的 SYSLOG 或 SNMP 回報主機發出 SNMP 和 SYSLOG 警示。

在裝置重新啟動之後，主控台顯示裝置登入提示。狀態 LED 現在閃爍綠色。

如果不嚴格按照順序進行操作，重設過程會取消，且不變更任何設定，同時主控台訊息提示已中止設定刪除操作。Status LED 返回到閃爍綠色狀態。如果裝置沒有重設，則系統會傳送 SNMP 警示確認失敗。

硬體說明

本章提供 NetScreen-5GT Wireless 機架的詳細說明。

連接埠和電源連接器

NetScreen-5GT Wireless 裝置的後面板上有連接埠和電源連接器。



DC POWER 插座用於連接電源至 NetScreen-5GT Wireless 裝置。Reset 針孔用於重設裝置使其復原為出廠預設設定。NetScreen-5GT Wireless 裝置提供以下連接埠：

連接埠	說明	連接器	速度 / 通訊協定
ADSL	在情況適合時，透過 ADSL 資料連結啟用 Internet 連線。	RJ-11 (Annex A) RJ-45 (Annex B)	ANSI T1.413 Issue 2 ITU G.992.1 (G.dmt) ITU 992.2 (G.lite)
Console	啟用與系統之間的序列連接。用於啟動指令行介面 (CLI) 會話。	RJ-45	9600 bps/ RS-232
Modem	透過外部數據機啟用撥號備份序列互聯網連線。	RJ-45	9600 bps-115 Kbps/ RS-232
Untrusted	透過外部路由器或 DSL 或纜線數據機啟用主要或備份互聯網或不受信任的網路連接。	RJ-45	10/100 Mbps/ 乙太網路 自動偵測雙工和極性
連接埠 1-4	透過交換機或集線器啟用至工作站的直接連接或 LAN 連接。此連接同時使您可以透過 Telnet 會話或 WebUI 管理應用程度管理裝置。	RJ-45	10/100 Mbps/ 乙太網路 自動偵測雙工和極性
天線 A 和 B	在無線電連接附近啟用與工作站的直接連接。此連接使您可以透過 Telnet 會話或 WebUI 管理應用程式管理裝置。	RPSMA	802.11b 802.11g

警告：不要將電話線或 ISDN 線路直接連接至 NetScreen-5GT Wireless 裝置上的數據機連接埠。必須先使用 RS-232 連接埠將裝置連接至數據機，然後將數據機連接至線路。

狀態 LED

NetScreen-5GT Wireless 裝置的前面板上有裝置的電源和狀態 LED，以及介面的連接埠狀態 LED。



裝置的主要狀態 LED

裝置狀態 LED 表明裝置工作是否正常。下表說明每個 LED 的狀態。連接埠狀態 LED

LED	狀態	含義
POWER	綠色	表明系統已通電。
	熄滅	表明系統沒有通電。
STATUS	閃爍綠色	表明系統正在工作。
	綠色	表明系統正在啓動。
	紅色	表明診斷或系統初始化錯誤。
	熄滅	表明系統不可用。
ADSL (僅在 Wireless ADSL 上)	綠色	表明 ADSL 迴路已打開。
	熄滅	表明 ADSL 迴路已關閉。
WLAN	慢閃綠色	表明無線連接已經建立，但是沒有連結活動。
	快閃綠色	表明無線連接已經建立。閃爍速度與連結活動成正比。
	熄滅	表明沒有建立任何無線連接。

連接埠狀態 LED

連接埠狀態 LED 表明裝置上的連接埠工作是否正常。下表說明連接埠的可能狀態。

LED	LED 顏色	LED 的含義
Link/Activity	閃爍綠色	表明裝置檢測連接埠的乙太網路通訊流量。
	熄滅	表明連接埠尚未與其它裝置建立連結。
	綠色	表明連接埠已經與其它裝置建立連結。
10/100	綠色	表明連接埠已經連接至 100 Base-T 裝置。
	熄滅	表明連接埠已經連接至 10 Base-T 裝置。



規格

本附錄提供 NetScreen-5GT Wireless 裝置的一般系統規格。

屬性		
高	2.93 厘米	1.15 英吋
長	18.45 厘米	7.26 英吋
寬	20.8 厘米	8.19 英吋
重量	0.9 千克	1.98 磅
電器設備		
開關穩壓器	AC 配電器：100V-240VAC +/- 10% 50/60 Hz 15-18 瓦特 DC 輸入：12 伏特 1.25-1.5 安培	
環境要求		
正常海拔高度	0-40 攝氏度，32-105 華氏度	
相對濕度	10-90%	
不冷凝	10-90%	
最高海拔高度為	2,000 米（6,562 英尺）	
認證		
安規	UL、CUL、TUV、CE 和 CB	
EMI	FCC 第 15 部份 B 類 VCCI、CE	
乙太網路連接器		
標準	100 Base-TX	
媒體類型	5 類以上 無屏蔽雙絞線 (UTP) 纜線	
最長距離	100 米（328.08 英尺）	
RJ-45 雙絞線連接埠符合	IEEE 802.3 類型 10/100 Base-T 標準	
ADSL 連接器		
類型	6 針 Annex A RJ-11 連接器 Annex B RJ-45 連接器	
媒體類型	標準電話線	

主控台和數據機轉接器連接

下表列出了 RJ-45 連接器的定義。要採用標準 UART 連接埠，主控台和數據機連接埠均使用這種設定。

RJ-45	信號	縮寫	DCE
1	Request To Send (要求傳送)	RTS	In
2	Data Terminal Ready (資料終端就緒)	DTR	In
3	Transmitted Data (傳輸資料)	TD	In
4, 5	Signal Ground (信號地)	SGND	不適用
6	Received Data (接收資料)	RD	Out
7	Not Connected (未連接)		
8	Clear To Send (可以傳送)	CTS	Out

下表列出了 RJ-45 至 DB-9 轉接器連接的定義。要採用標準 UART 連接埠，主控台和數據機連接埠必須均使用這種設定。

DB9	信號	縮寫	DTE	DCE	RJ45
1	Data Carrier Detect (資料載波偵測)	DCD	In	Out	NC
2	Received Data (接收資料)	RD	In	Out	3
3	Transmitted Data (傳輸資料)	TD	Out	In	6
4	Data Terminal Ready (資料終端就緒)	DTR	Out	In	7
5	Signal Ground (信號地)	SGND	不適用	不適用	4
6	Data Set Ready (資料集就緒)	DSR	In	Out	2
7	Request To Send (要求傳送)	RTS	Out	In	8
8	Clear To Send (可以傳送)	CTS	In	Out	1
9	Ring Indicator (振口指示器)	RI	In	Out	NC

注意： 如果使用 NetScreen 裝置附帶的主控台纜線連接至數據機，則必須配備 null 數據機轉接器並在數據機連接器上安裝。

申請DGT使用手冊必須包含之資訊:

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電通信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

索引

A

ATM 點對點通訊協定

請參 PPPoA

AAL5 多工 256

ADSL

組態介面 255

連接埠 245

連接纜線 245

時間，設定 252

Annex A 245

Annex B 245

為 Deutsch Telecom 組態 258

ATM 配接層 5 256

B

變更連接埠模式 262

變更登入名稱和密碼 252

C

從特定主機管理裝置 261

D

DB-9 連接器 272

Deutsch Telecom，組態 Annex B 258

電源，連接 247

電源連接器 267

多工，組態 257

F

復原預設設定 265

復原 265

服務集識別字

請參 SSID

G

管理員名稱，變更 252

慣例

CLI 242

WebUI 242

J

靜態 IP 位址 256

L

LED

狀態 268

連接埠狀態 269

路由模式 261

連接埠狀態 LED 269

連接埠連接器 267

連接埠模式，變更 262

連接電源 247

連接器

連接埠 267

電源 267

M

密碼，變更 252

N

NetScreen ↓ 物 243

P

PPPoA 256

組態 258

PPPoE 256

組態 258

R

Reset 針孔，使用 266

RJ-45 連接器 272

日期，設定 252

S

SSID，服務集識別字 254

設定裝置時鐘 252

T

Trust 乙太網路連接埠 247

Trust 區域介面的位址 265

天線 247

透明模式 261

U

Untrust 區域，組態備份介面 264

Untrusted 連接埠 246

V

VPI/VCI 256

組態 257

W

WebUI

存取 249

WebUI, 慣例 242

wireless1 介面 253

wireless2 介面

存取 249

設定 SSID 254

繫結區域 253

變更介面位址 265

Trust 區域 253

微過濾器 246

無線

天線 247

使用預設介面 247

連接 245, 246

Trust 區域 253

Wzone1 區域 253

X

新增虛擬電路 257

信號分波器 246

限制從特定主機管理 261

虛擬路徑識別字 / 虛擬通道識別字

請參 VPI/VCI

虛擬電路，新增 257

Y

驗證連接性 265

預設設定 254

乙太網路點對點通訊協定 (PPPoE)

請參 PPPoE

Z

組態 259

狀態 LED 268

註冊裝置 249

在機 247

主控台，使用 251

指南的組織方法 241

組態

可選的 260

所需的 251, 254

無線網路 253

預設設定 254

SSID 254