

SSG20 Hardware and Installation Guide

Important:

We are providing the following guide as a courtesy, but no longer support the documented product. The SSG20 firewall reached end of service in January 2020.

For information about a currently supported firewall that might better suit your needs, we recommend the [SRX300 Services Gateway](#).



Security Products

SSG 20 Hardware Installation and Configuration Guide

English
Français
Deutsch
Español
日本語
简体中文
繁體中文

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-015646-01, Revision 02

Copyright Notice

Copyright © 2006 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

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 Juniper Networks' 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.

Table of Contents

	About This Guide	5
	Organization	6
	WebUI Conventions	6
	CLI Conventions	7
	Obtaining Documentation and Technical Support	8
Chapter 1	Hardware Overview	9
	Port and Power Connectors	10
	Front Panel	11
	System Status LEDs	11
	Port Descriptions	13
	Ethernet Ports	13
	Console Port	13
	AUX Port	14
	Mini Physical Interface Module Port Descriptions	14
	Back Panel	16
	Power Adapter	16
	Radio Transceivers	16
	Grounding Lug	16
	Antennae Types	17
	USB Port	17
Chapter 2	Installing and Connecting the Device	19
	Before You Begin	20
	Installing Equipment	20
	Connecting Interface Cables to a Device	22
	Connecting the Power	22
	Connecting a Device to a Network	23
	Connecting a Device to an Untrusted Network	23
	Ethernet Ports	24
	Serial (AUX/Console) Ports	24
	Connecting Mini PIMs to an Untrusted Network	24
	ADSL2/2+ Mini PIM	24
	ISDN, T1, E1, and V.92 Mini PIMs	25
	Connecting a Device to an Internal Network or a Workstation	25
	Ethernet Ports	25
	Wireless Antennae	26

Chapter 3	Configuring the Device	27
	Accessing a Device.....	28
	Using a Console Connection	28
	Using the WebUI	29
	Using Telnet	30
	Default Device Settings	31
	Basic Device Configuration	33
	Root Admin Name and Password	33
	Date and Time.....	34
	Bridge Group Interfaces	34
	Administrative Access	35
	Management Services.....	35
	Hostname and Domain Name	36
	Default Route.....	36
	Management Interface Address	36
	Backup Untrust Interface Configuration	37
	Basic Wireless Configuration.....	37
	Mini PIM Configuration	41
	ADSL2/2 + Interface	41
	Virtual Circuits	42
	VPI/VCI and Multiplexing Method.....	42
	PPPoE or PPPoA	43
	Static IP Address and Netmask.....	44
	ISDN Interface.....	45
	T1 Interface	45
	E1 Interface	46
	V.92 Modem Interface	47
	Basic Firewall Protections	48
	Verifying External Connectivity.....	48
	Resetting a Device to Factory Defaults	49
Chapter 4	Servicing the Device	51
	Required Tools and Parts	51
	Replacing a Mini-Physical Interface Module	51
	Removing a Blank Faceplate.....	52
	Removing a Mini PIM	52
	Installing a Mini PIM	53
	Upgrading Memory	54
Appendix A	Specifications	57
	Physical.....	58
	Electrical	58
	Environmental Tolerance	58
	Certifications.....	59
	Safety	59
	EMC Emissions.....	59
	EMC Immunity	59
	ETSI.....	59
	T1 Interface	60
	Connectors.....	60

Appendix B	Initial Configuration Wizard	63
	Index.....	85

About This Guide

The Juniper Networks Secure Services Gateway (SSG) 20 device is an integrated router and firewall platform that provides Internet Protocol Security (IPSec) virtual private network (VPN) and firewall services for a branch office or a retail outlet.

Juniper Networks offers two models of the SSG 20 device:

- SSG 20, which supports auxiliary (AUX) connectivity
- SSG 20-WLAN, which supports integrated 802.11a/b/g wireless standards

Both SSG 20 devices support universal serial bus (USB) storage and two mini physical interface module (PIM) slots that can hold any of the mini PIMs. The devices also provide protocol conversions between local area networks (LANs) and wide area networks (WANs).

NOTE: The configuration instructions and examples in this document are based on the functionality of a device running ScreenOS 5.4. Your device might function differently depending on the ScreenOS version you are running. For the latest device documentation, refer to the Juniper Networks Technical Publications website at <http://www.juniper.net/techpubs/hardware>. To see which ScreenOS versions are currently available for your device, refer to the Juniper Networks Support website at <http://www.juniper.net/customers/support/>.

Organization

This guide contains the following sections:

- Chapter 1, “Hardware Overview,” describes the chassis and components of an SSG 20 device.
- Chapter 2, “Installing and Connecting the Device,” describes how to mount an SSG 20 device and how to connect cables and power to the device.
- Chapter 3, “Configuring the Device,” describes how to configure and manage an SSG 20 device and how to perform some basic configuration tasks.
- Chapter 4, “Servicing the Device,” describes service and maintenance procedures for the SSG 20 device.
- Appendix A, “Specifications,” provides general system specifications for the SSG 20 device.
- Appendix B, “Initial Configuration Wizard,” provides detailed information about using the Initial configuration Wizard (ICW) for an SSG 20 device.

WebUI Conventions

To perform a task with the WebUI, you first navigate to the appropriate dialog box, where you then define objects and set parameters. A chevron (>) shows the navigational sequence through the WebUI, which you follow by clicking menu options and links. The set of instructions for each task is divided into navigational path and configuration settings.

The following figure lists the path to the address configuration dialog box with the following sample configuration settings:

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

Address Name: addr_1
IP Address/Domain Name:
 IP/Netmask: (select), 10.2.2.5/32
Zone: Untrust

Figure 1: Navigational Path and Configuration Settings

The screenshot shows the Juniper NSRP configuration interface. The breadcrumb path is 'Objects > Addresses > Configuration'. The version is 'n200_5.0.0:NSRP(M)'. The left sidebar shows a navigation menu with options: Home, Configuration, Network, Screening, Policies, VPNs, Objects, Reports, Wizards, Help, and Logout. The main content area is titled 'Configuration' and contains the following fields:

- Address Name:** addr_1
- Comment:** (empty)
- IP Address/Domain Name:**
 - ☒ IP/Netmask: 10.2.2.5 / 32
 - ☐ Domain Name: (empty)
- Zone:** Untrust (dropdown menu)
- Buttons:** OK, Cancel

CLI Conventions

The following conventions are used to present the syntax of CLI commands in examples and in text.

In examples:

- 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, the ethernet2, or the ethernet3 interface.”

- Variables are in *italic* type:

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

In text:

- Commands are in **boldface** type.
- Variables are in *italic* type.

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

Obtaining Documentation and Technical Support

To obtain technical documentation for any Juniper Networks 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 this document, please contact us at the following email address:

techpubs-comments@juniper.net

Chapter 1

Hardware Overview

This chapter provides detailed descriptions of the SSG 20 chassis and its components. It contains the following sections:

- “Port and Power Connectors” on page 10
- “Front Panel” on page 11
- “Back Panel” on page 16

Port and Power Connectors

This section describes and displays the location of the built-in ports and power connectors. Refer to the following figure for built-in port locations and Table 1 for the power connector descriptions.

Figure 2: Built-in Port and Mini-PIM Location

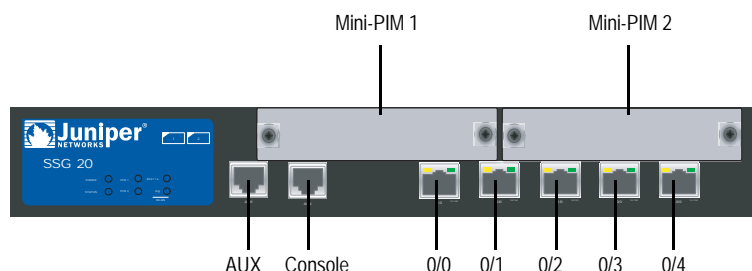


Table 1: SSG 20 Ports and Power Connectors

Port	Description	Connector	Speed/Protocol
0/0-0/4	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.	RJ-45	10/100 Mbps Ethernet Autosensing duplex and auto MDI/MDIX
USB	Enables a 1.1 USB connection with the system.	N/A	12M (full speed) or 1.5M (low speed)
Console	Enables a serial connection with the system. Used for terminal-emulation connectivity to launch CLI sessions.	RJ-45	9600 bps/RS-232C serial
AUX	Enables a backup RS-232 async serial Internet connection through an external modem.	RJ-45	9600 bps — 115 Kbps/RS-232C serial
Mini PIM			
ADSL 2/2 +	Enables an Internet connection through an ADSL data link.	RJ-11 (Annex A) RJ-45 (Annex B)	ANSI T1.413 Issue 2 (Annex A only) ITU G.992.1 (G.dmt) ITU G.992.3 (ADSL2) ITU G.992.5 (ADSL2 +)
V.92 Modem	Enables a primary or backup Internet or untrusted network connection to a service provider.	RJ-11	9600 bps — 115 Kbps/RS-232 serial autosensing duplex and polarity
T1	Enables a connection to the T1 line to the untrusted network.	RJ-45	1.544 Mbps (full-time slots)
E1	Enables a connection to the E1 line to the untrusted network.	RJ-45	2.048 Mbps (full-time slots)
ISDN	Enables the ISDN line to be used as the untrust or backup interface. (S/T)	RJ-45	B-channels at 64 Kbps Leased line at 128 Kbps
Antenna A & B (SSG 20-WLAN)	Enables a direct connection to workstations in the vicinity of a wireless radio connection.	RPSMA	802.11 a (54 Mbps on 5GHz radio band) 802.11 b (11 Mbps on 2.4 GHz radio band) 802.11 g (54 Mbps on 2.4 GHz radio band) 802.11 superG (108 Mbps on 2.4 GHz and 5GHz radio bands)

Front Panel

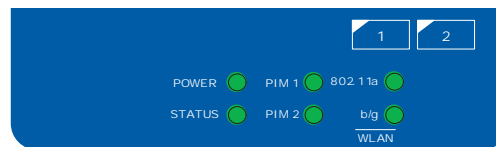
This section describes the following elements on the front panel of an SSG 20 device:

- System Status LEDs
- Port Descriptions
- Mini Physical Interface Module Port Descriptions

System Status LEDs

The system status LEDs display information about critical device functions. Figure 3 illustrates the position of each status LED on the front of the SSG 20-WLAN device. The WLAN LEDs are only present on the SSG 20-WLAN device.

Figure 3: Status LEDs



When the system powers up, the POWER LED changes from off to blinking green, and the STATUS LED changes in the following sequence: red, green, blinking green. Startup takes approximately two minutes to complete. If you want to turn the system off and on again, we recommend you wait a few seconds between shutting it down and powering it back up. Table 2 provides the name, color, status, and description of each system status LED.

Table 2: Status LED Descriptions

Name	Color	Status	Description
POWER	Green	On steadily	Indicates that the system is receiving power.
		Off	Indicates that the system is not receiving power.
	Red	On steadily	Indicates that the device is not operating normally.
		Off	Indicates that the device is operating normally.
STATUS	Green	On steadily	Indicates that the system is starting or performing diagnostics.
		Blinking	Indicates that the device is operating normally.
	Red	Blinking	Indicates that there is an error detected.
PIM 1	Green	On steadily	Indicates that the mini PIM is functioning.
		Blinking	Indicates that the mini PIM is passing traffic.
		Off	Indicates that the mini PIM is not operational.

Name	Color	Status	Description
PIM 2	Green	On steadily	Indicates that the mini PIM is functioning.
		Blinking	Indicates that the mini PIM is passing traffic.
		Off	Indicates that the mini PIM is not operational.
WLAN (On WLAN device only)			
802.11a	Green	On steadily	Indicates that a wireless connection is established but there is no link activity.
		Blinking slowly	Indicates that a wireless connection is established. The baud rate is proportional to the link activity.
		Off	Indicates that there is no wireless connection established.
b/g	Green	On steadily	Indicates that a wireless connection is established but there is no link activity.
		Blinking slowly	Indicates that a wireless connection is established. The baud rate is proportional to the link activity.
		Off	Indicates that there is no wireless connection established.

Port Descriptions

This section explains the purpose and function of the following:

- Ethernet Ports
- Console Port
- AUX Port

Ethernet Ports

Five 10/100 Ethernet ports provide LAN connections to hubs, switches, local servers, and workstations. You can also designate an Ethernet port for management traffic. The ports are labeled **0/0** through **0/4**. For the default zone bindings for each Ethernet port, see “Default Device Settings” on page 31.

When configuring one of the ports, reference the interface name that corresponds to the location of the port. From left to right on the front panel, the interface names for the ports are **ethernet0/0** through **ethernet0/4**.

Figure 4 displays the location of the LEDs on each Ethernet port.

Figure 4: Activity Link LEDs Location

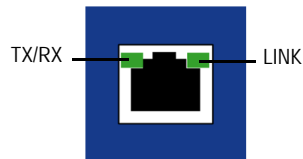


Table 3 describes the Ethernet port LEDs.

Table 3: LAN Port LEDs

Name	Color	Status	Description
LINK	Green	On steadily	Port is online.
		Off	Port is offline.
TX/RX	Green	Blinking	Traffic is passing through. The baud rate is proportional to the link activity.
		Off	Port might be on but is not receiving data.

Console Port

The Console port is an RJ-45 serial port wired as data circuit-terminating equipment (DCE) that can be used for local administration. Use a straight-through cable when using a terminal connection and a crossover cable when connecting to another DCE device. An RJ-45 to DB-9 adapter is supplied.

See “Connectors” on page 60 for the RJ-45 connector pinouts.

AUX Port

The auxiliary (AUX) port is an RJ-45 serial port wired as data terminal equipment (DTE) that can be connected to a modem to allow remote administration. We do not recommend using this port for regular remote administration. The AUX port is typically assigned to be the backup serial interface. The baud rate is adjustable from 9600 bps to 115200 bps and requires hardware flow control. Use a straight-through cable when connecting to a modem and a crossover cable when connecting to another DTE device.

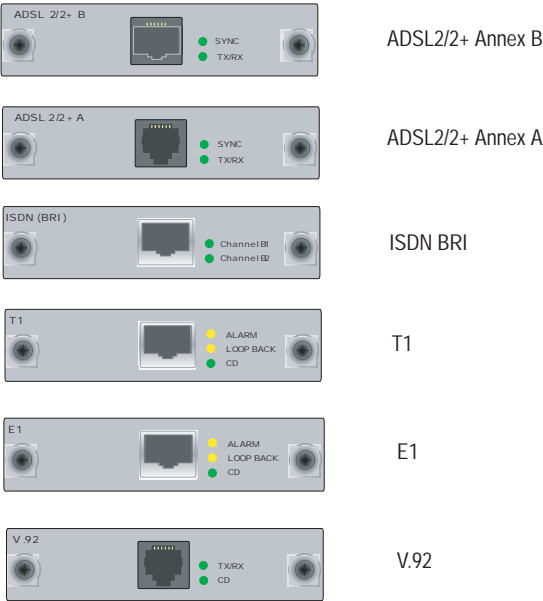
See “Connectors” on page 60 for the RJ-45 connector pinouts.

Mini Physical Interface Module Port Descriptions

Each mini physical interface module (PIM) supported on a device has the following components:

- One cable connector port—Accepts a network media connector. Figure 5 shows the available mini PIMs. You can install up to two mini PIMs in a device.

Figure 5: Mini PIMs for the SSG 20



- Two to three status LEDs—Indicate port status. Table 4 describes the meaning of the LED states.

Table 4: Mini PIM LED States on the SSG 20

Type	Name	Color	State	Description
ADSL 2/2 + (Annex A and B)	SYNC	Green	On steadily	Indicates that the ADSL interface is trained
			Blinking	Indicates training is in progress
			Off	Indicates that the interface is idle
	TX/RX	Green	Blinking	Indicates that traffic is passing through
			Off	Indicates that no traffic is passing through
ISDN (BRI)	CH B1	Green	On steadily	Indicates that B-Channel 1 is active
			Off	Indicates that B-Channel 1 is not active
	CH B2	Green	On steadily	Indicates that B-Channel 2 is active
			Off	Indicates that B-Channel 2 is not active
T1/E1	ALARM	Yellow	On steadily	Indicates that there is a local or remote alarm; device has detected a failure
			Off	Indicates that there are no alarms or failures
	LOOP BACK	Yellow	On steadily	Indicates that a loopback or line state is detected
			Off	Indicates that the loopback is not active
	CD	Green	On steadily	Indicates a carrier was detected and the internal DSU/CSU in the mini PIM is communicating with another DSU/CSU
			Off	Indicates that carrier detect is not active
V.92	CD	Green	On steadily	Indicates that the link is active
			Off	Indicates that the serial interface is not in service
	TX/RX	Green	Blinking	Indicates that traffic is passing through
			Off	Indicates that no traffic is passing through



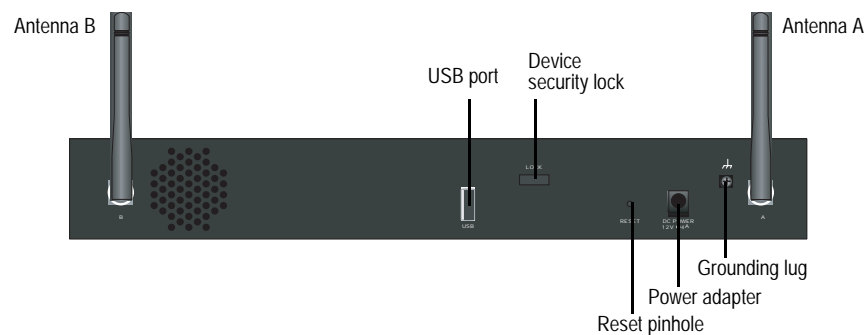
CAUTION: Mini PIMs are not hot-swappable. You must install them in the front panel slots before powering on the device.

Back Panel

This section describes the following elements on the back panel of an SSG 20 device:

- Power Adapter
- Radio Transceivers
- Grounding Lug
- Antennae Types
- USB Port

Figure 6: Back Panel of an SSG 20-WLAN Device



Power Adapter

The POWER LED on the front panel of a device either glows green or is off. Green indicates correct function, and off indicates power-adapter failure or that the device is off.

Radio Transceivers

The SSG 20-WLAN contains two wireless connectivity radio transceivers, which support 802.11a/b/g standards. The first transceiver (WLAN 0) uses the 2.4 GHz radio band, which supports the 802.11b standard at 11 Mbps, the 802.11g standard at 54 Mbps, and 802.11 SuperG standard at 108 Mbps. The second radio transceiver (WLAN 1) uses the 5GHz radio band, which supports the 802.11a standard at 54 Mbps. For information on configuring the wireless radio band, see “Basic Wireless Configuration” on page 37.

Grounding Lug

A one-hole grounding lug is provided on the rear of the chassis to connect the device to earth ground (see Figure 6).

To ground the device before connecting power, connect a grounding cable to earth ground and then attach the cable to the lug on the rear of the chassis.

Antennae Types

The SSG 20-WLAN device supports three types of custom-built radio antennae:

- **Diversity antennae** — The diversity antennae provide 2dBi directional coverage and a fairly uniform level of signal strength within the area of coverage and are suitable for most installations. This type of antennae is shipped with the device.
- **External omnidirectional antenna** — The external antenna provides 2dBi omnidirectional coverage. Unlike diversity antennae, which function as a pair, an external antenna operates to eliminate an echo effect that can sometimes occur from slightly delayed characteristics in signal reception when two are in use.
- **External directional antenna** — The external directional antenna provides 2dBi unidirectional coverage and is appropriate for locations like hallways and outer walls (with the antenna facing inward).

USB Port

The USB port on the back panel of an SSG 20 device accepts a universal serial bus (USB) storage device or USB storage device adapter with a compact-flash disk installed, as defined in the *CompactFlash Specification* published by the CompactFlash Association. When the USB storage device is installed and configured, it automatically acts as a secondary boot device if the primary compact-flash disk fails on startup.

The USB port allows file transfers such as device configurations, user certifications, and update version images between an external USB storage device and the internal flash storage located in the security device. The USB port supports USB 1.1 specification at either low speed (1.5M) or full speed (12M) file transfer.

To transfer files between the USB storage device and an SSG 20, perform the following steps:

1. Insert the USB storage device into the USB port on the security device.
2. Save the files from the USB storage device to the internal flash storage on the device with the **save {software | config | image-key} from usb filename to flash** CLI command.
3. Before removing the USB storage device, stop the USB port with the **exec usb-device stop** CLI command.
4. It is now safe to remove the USB storage device.

If you want to delete a file from the USB storage device, use the **delete file usb:/filename** CLI command.

If you want to view the saved file information on the USB storage device or internal flash storage, use the **get file** CLI command.

Chapter 2

Installing and Connecting the Device

This chapter describes how to mount an SSG 20 device and connect cables and power to the device. This chapter contains the following sections:

- “Before You Begin” on page 20
- “Installing Equipment” on page 20
- “Connecting Interface Cables to a Device” on page 22
- “Connecting the Power” on page 22
- “Connecting a Device to a Network” on page 23

NOTE: For safety warnings and instructions, refer to the *Juniper Networks Security Products Safety Guide*. Before working on any equipment, you should be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

Before You Begin

The location of the chassis, the layout of the mounting equipment, and the security of your wiring room are crucial for proper system operation.



WARNING: To prevent abuse and intrusion by unauthorized personnel, install the SSG 20 device in a secure environment.

Observing the following precautions can prevent shutdowns, equipment failures, and injuries:

- Before installation, always check that the power supply is disconnected from any power source.
- Ensure that the room in which you operate the device has adequate air circulation and that the room temperature does not exceed 104°F (40°C).
- Do not place the device in an equipment-rack frame that blocks an intake or exhaust port. Ensure that enclosed racks have fans and louvered sides.
- Correct these hazardous conditions before any installation: moist or wet floors, leaks, ungrounded or frayed power cables, or missing safety grounds.

Installing Equipment

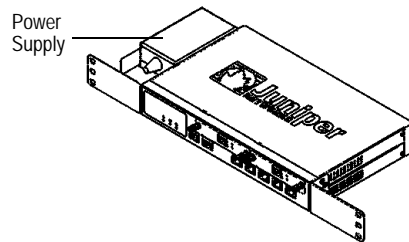
You can front-mount, wall-mount, or desk-mount an SSG 20 device. The mounting kits may be purchased separately.

To mount an SSG 20 device, you need a number-2 phillips screwdriver (not provided) and screws that are compatible with the equipment rack (included in the kit).

NOTE: When mounting a device, make sure that it is within reach of the power outlet.

To front-mount an SSG 20 device onto a standard 19-inch equipment rack, perform the following steps:

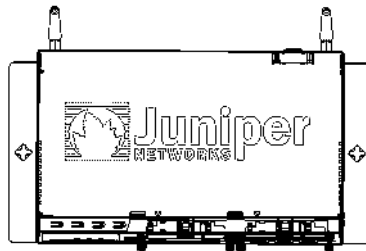
Figure 7: SSG 20 Front-mount



1. Align the power supply rack-mount ear to the left-front edge of the device.
2. Place the screws in the holes and use a phillips screwdriver to secure them.
3. Align the other rack-mount ear to the right-front edge of the device.
4. Place the screws in the holes and use a phillips screwdriver to secure them.
5. Mount the device on the rack with the provided screws.
6. Plug the power supply into the power outlet.

To wall-mount an SSG 20 device, perform the following steps:

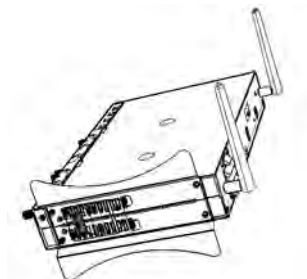
Figure 8: SSG 20 Wall-mount



1. Align the wall-mount ears to the device.
2. Place the screws in the holes and use a phillips screwdriver to secure them.
3. Ensure that the wall to be used is smooth, flat, dry, and sturdy.
4. Mount the device on the wall using the provided screws.
5. Plug the power supply into the power outlet.

To desk-mount an SSG 20 device, perform the following steps:

Figure 9: SSG 20 Desk-mount



1. Attach the desktop stand to the side of the device. We recommend using the side closest to the power adapter.
2. Place the mounted device on the desktop.
3. Plug in the power adapter and connect the power supply to the power outlet.

Connecting Interface Cables to a Device

To connect the interface cable to a device, perform the following steps:

1. Have ready a length of the type of cable used by the interface.
2. Insert the cable connector into the cable-connector port on the interface faceplate.
3. Arrange the cable as follows to prevent it from dislodging or developing stress points:
 - a. Secure the cable so that it is not supporting its own weight as it hangs to the floor.
 - b. Place any excess cable out of the way in a neatly coiled loop.
 - c. Use fasteners to maintain the shape of the cable loops.

Connecting the Power

To connect the power to a device, perform the following steps:

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.

Connecting a Device to a Network

An SSG 20 device provides firewall and general security for networks when it is placed between internal networks and the untrusted network. This section describes the following:

- Connecting a Device to an Untrusted Network
- Connecting a Device to an Internal Network or a Workstation

Connecting a Device to an Untrusted Network

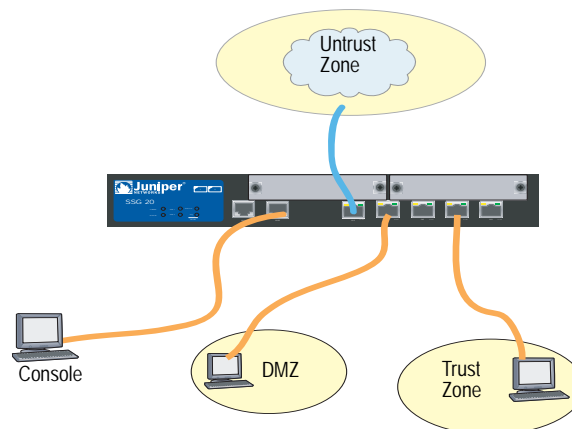
You can connect your SSG 20 device to an untrusted network in one of the following ways:

- Ethernet Ports
- Serial (AUX/Console) Ports
- Connecting Mini PIMs to an Untrusted Network

Figure 10 shows the SSG 20 with basic network cabling connections with two blank mini-PIMs and the 10/100 Ethernet ports cabled as follows:

- The port labeled 0/0 (ethernet0/0 interface) is connected to the untrust network.
- The port labeled 0/1 (ethernet0/1 interface) is connected to a workstation in the DMZ security zone.
- The port labeled 0/3 (bgroup0 interface) is connected to a workstation in the Trust security zone.
- The Console port is connected to a serial terminal for management access.

Figure 10: Basic Networking Example



Ethernet Ports

To establish a high-speed connection, connect the provided Ethernet cable from the Ethernet port marked 0/0 on an SSG 20 device to the external router. The device autosenses the correct speed, duplex, and MDI/MDIX settings.

Serial (AUX/Console) Ports

You can connect to the untrusted network with an RJ-45 straight-through serial cable and an external modem.



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

Connecting Mini PIMs to an Untrusted Network

This section explains how to connect the device mini PIMs to an untrusted network.

ADSL2/2+ Mini PIM

Connect the provided ADSL cable from the ADSL2/2+ mini PIM 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.

Connecting Splitters and Microfilters

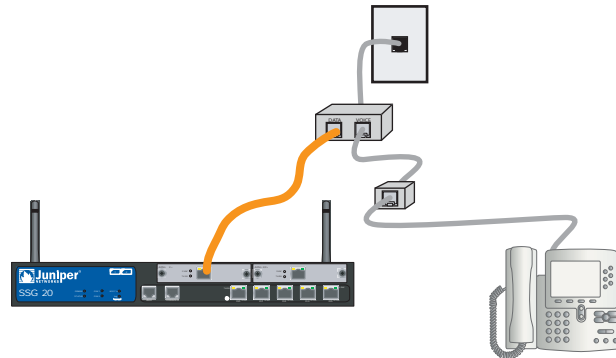
A *signal splitter* divides the telephone signal into low-frequency voice signals for voice calls and high-frequency data signals for data traffic. Your service provider usually installs the splitter as part of the equipment that connects your site telephone lines to the provider network.

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 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.

Figure 11 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.)

Figure 11: Microfilter and Splitter on Your Network Connection



ISDN, T1, E1, and V.92 Mini PIMs

To connect the mini PIMs to a device, perform the following steps:

1. Have ready a length of the type of cable used by the interface.
2. Insert the cable connector into the cable-connector port on the interface faceplate.
3. Arrange the cable as follows to prevent it from dislodging or developing stress points:
 - a. Secure the cable so that it is not supporting its own weight as it hangs to the floor.
 - b. Place any excess cable out of the way in a neatly coiled loop.
 - c. Use fasteners to maintain the shape of the cable loops.

To configure the ISDN, E1, T1, or V.92 mini PIM, see “Mini PIM Configuration” on page 41.

Connecting a Device to an Internal Network or a Workstation

You can connect your local area network (LAN) or workstation with the Ethernet and/or wireless interfaces.

Ethernet Ports

An SSG 20 device contains five Ethernet ports. You can use one or more of these ports to connect to LANs through 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 crossover or straight-through cables to connect the Ethernet ports to other devices. See “Default Device Settings” on page 31 for the default zone-to-interface bindings.

Wireless Antennae

If you are using the wireless interface, you need to connect the provided antennae on the device. If you have the standard 2dB diversity antennae, use screws to attach them onto the posts marked A and B at the back of the device. Bend each antenna at its elbows, making sure not to put pressure on the bulkhead connectors.

Figure 12: SSG 20-WLAN Antennae Location



If you are using the optional external antenna, follow the connection instructions that came with that antenna.

Chapter 3

Configuring the Device

ScreenOS software is preinstalled on an SSG 20 device. When the device is powered on, it is ready to be configured. While the device has a default factory configuration that allows you to initially connect to the device, you need to perform further configuration for your specific network requirements.

This chapter contains the following sections:

- “Accessing a Device” on page 28
- “Default Device Settings” on page 31
- “Basic Device Configuration” on page 33
- “Basic Wireless Configuration” on page 37
- “Mini PIM Configuration” on page 41
- “Basic Firewall Protections” on page 48
- “Verifying External Connectivity” on page 48
- “Resetting a Device to Factory Defaults” on page 49

NOTE: After you configure a device and verify connectivity through the remote network, you must register your product at www.juniper.net/support/ so certain ScreenOS services, such as Deep Inspection Signature Service and Antivirus (purchased separately), 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, refer to the *Fundamentals* volume of the *Concepts & Examples ScreenOS Reference Guide* for the ScreenOS version running on the device.

Accessing a Device

You can configure and manage a device in several ways:

- **Console:** The Console port on the device allows you to access the device through a serial cable connected to your workstation or terminal. To configure the device, you enter ScreenOS command line interface (CLI) commands on your terminal or in a terminal-emulation program on your workstation.
- **WebUI:** The ScreenOS Web User Interface (WebUI) is a graphical interface available through a browser. To initially use the WebUI, the workstation on which you run the browser must be on the same subnetwork as the device. You can also access the WebUI through a secure server using Secure Sockets Layer (SSL) with secure HTTP (S-HTTP).
- **Telnet/SSH:** Telnet and SSH are applications that allows you to access devices through an IP network. To configure the device, you enter ScreenOS CLI commands in a Telnet session from your workstation. For more information, refer to the *Administration* volume of the *Concepts & Examples ScreenOS Reference Guide*.
- **NetScreen-Security Manager:** NetScreen-Security Manager is a Juniper Networks enterprise-level management application that enables you to control and manage Juniper Networks firewall/IPSec VPN devices. For instructions on how to manage your device with NetScreen-Security Manager, refer to the *NetScreen-Security Manager Administrator's Guide*.

Using a Console Connection

NOTE: Use a straight-through RJ-45 CAT5 serial cable with a male RJ-45 connector to plug into the Console port on the device.

To establish a console connection, perform the following steps:

1. Plug the female end of the supplied DB-9 adapter into the serial port of your workstation. (Be sure that the DB-9 is inserted properly and secured.) Figure 13 shows the type of DB-9 connector that is needed.

Figure 13: DB-9 Adapter



2. Plug the male end of the RJ-45 CAT5 serial cable into the Console port on the SSG 20. (Be sure that the other end of the CAT5 cable is inserted properly and secured in the DB-9 adapter.)

3. Launch a serial terminal-emulation program on your workstation. The required settings to launch a console session are as follows:

- Baud rate: 9600
- Parity: None
- Data bits: 8
- Stop bit: 1
- Flow Control: None

4. If you have not yet changed the default login for the admin name and password, enter **netscreen** at both the login and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive.)

For information on how to configure the device with the CLI commands, refer to the *Concepts & Examples ScreenOS Reference Guide*.

5. (Optional) By default, the console times out and terminates automatically after 10 minutes of idle time. To remove the timeout, enter **set console timeout 0**.

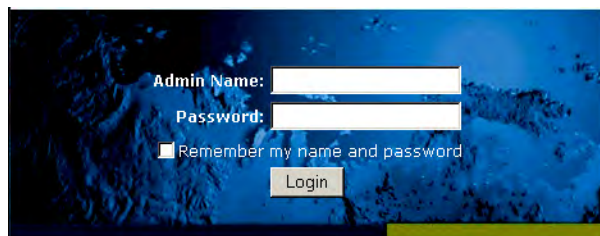
Using the WebUI

To use the WebUI, the workstation from which you are managing the device must initially be on the same subnetwork as the device. To access the device with the WebUI, perform the following steps:

1. Connect your workstation to the 0/2 — 0/4 port (bgroup0 interface in the Trust zone) on the device.
2. Ensure that your workstation is configured for Dynamic Host Configuration Protocol (DHCP) or is statically configured with an IP address in the 192.168.1.0/24 subnet.
3. Launch your browser, enter the IP address for the bgroup0 interface (the default IP address is 192.168.1.1/24), then press **Enter**.

NOTE: When the device is accessed through the WebUI the first time, the Initial Configuration Wizard (ICW) appears. If you decide to use the ICW to configure your device, see “Initial Configuration Wizard” on page 63.

The WebUI application displays the login prompt as shown in Figure 14.

Figure 14: WebUI Login Prompt

4. If you have not yet changed the default login for the admin name and password, enter **netscreen** at both the admin name and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive.)

Using Telnet

To establish a Telnet connection, perform the following steps:

1. Connect your workstation to the 0/2 — 0/4 port (bgroup0 interface in the Trust zone) on the device.
2. Ensure that your workstation is configured for DHCP or is statically configured with an IP address in the 192.168.1.0/24 subnet.
3. Start a Telnet client application to the IP address for the bgroup0 interface (the default IP address is 192.168.1.1). For example, enter **telnet 192.168.1.1**.

The Telnet application displays the login prompt.

4. If you have not yet changed the default login for the login and password, enter **netscreen** at both the login and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive.)
5. (Optional) By default, the console times out and terminates automatically after 10 minutes of idle time. To remove the timeout, enter **set console timeout 0**.

Default Device Settings

This section describes the default settings and operation of an SSG 20 device.

Table 5 shows the default zone bindings for ports on the devices.

Table 5: Default Physical Interface to Zone Bindings

Port Label	Interface	Zone
10/100 Ethernet ports:		
0/0	ethernet0/0	Untrust
0/1	ethernet0/1	DMZ
0/2	bgroup0 (ethernet0/2)	Trust
0/3	bgroup0 (ethernet0/3)	Trust
0/4	bgroup0 (ethernet0/4)	Trust
AUX	serial0/0	Null
WAN mini PIM ports (x = mini PIM slot 1 or 2):		
ADSL2/2 + (Annex A)	adsl(x/0)	Untrust
ADSL2/2 + (Annex B)	adsl(x/0)	Untrust
T1	serial(x/0)	Untrust
E1	serial(x/0)	Untrust
ISDN	bri(x/0)	Untrust
V.92	serial(x/0)	Null

A bridge group (bgroup) is designed to allow network users to switch between wired and wireless traffic without having to reconfigure or reboot the device. By default, the ethernet0/2 — ethernet0/4 interfaces, labeled as ports 0/2 — 0/4 on the device, are grouped together as the bgroup0 interface, have the IP address 192.168.1.1/24, and are bound to the Trust security zone. You can configure up to four bgroups.

If you want to set an Ethernet or a wireless interface into a bgroup, you must first make sure that the Ethernet or wireless interface is in the Null security zone. Unsetting the Ethernet or wireless interface that is in a bgroup places the interface in the Null security zone. Once assigned to the Null security zone, the Ethernet interface can be bound to a security zone and assigned a different IP address.

To unset ethernet0/3 from bgroup0 and assign it to the Trust zone with a static IP address of 192.168.3.1/24, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port: deselect **ethernet0/3**, then click **Apply**.

List > Edit (ethernet0/3): Enter the following, then click **Apply**:

Zone Name: Trust (select)
IP Address/Netmask: 192.168.3.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
set interface ethernet0/3 zone trust
set interface ethernet0/3 ip 192.168.3.1/24
save
```

Table 6: Wireless and Logical Interface Bindings

SSG 20-WLAN	Interface	Zone
Wireless Interface Specifies a wireless interface, which is configurable to operate on 2.4G and/or 5G radio	wireless0/0 (default IP address is 192.168.2.1/24).	Trust
	wireless0/1-0/3.	Null
Logical Interfaces		
Layer-2 interface	vlan1 specifies the logical interfaces used for management and VPN traffic termination while the device is in Transparent mode.	N/A
Tunnel interfaces	tunnel.n specifies a logical tunnel interface. This interface is for VPN traffic.	N/A

You can change the default IP address on the bgroup0 interface to match the addresses on your LAN and WLAN. For configuring a wireless interface to a bgroup, see “Basic Wireless Configuration” on page 37.

NOTE: The bgroup interface does not work in Transparent mode when it contains a wireless interface.

For additional bgroup information and examples, refer to the *Concepts & Examples ScreenOS Reference Guide*.

There are no other default IP addresses configured on other Ethernet or wireless interfaces on a device; you need to assign IP addresses to the other interfaces, including the WAN interfaces.

Basic Device Configuration

This section describes the following basic configuration settings:

- Root Admin Name and Password
- Date and Time
- Bridge Group Interfaces
- Administrative Access
- Management Services
- Hostname and Domain Name
- Default Route
- Management Interface Address
- Backup Untrust Interface Configuration

Root Admin Name and Password

The root admin user has complete privileges for configuring an SSG 20 device. We recommend that you change the default root admin name and password (both **netscreen**) immediately.

To change the root admin name and password, use the WebUI or CLI as follows:

WebUI

Configuration > Admin > Administrators > Edit (for the netscreen administrator name value): Enter the following, then click **OK**:

Administrator Name:
Old Password: netscreen
New Password:
Confirm New Password:

NOTE: Passwords are not displayed in the WebUI.

CLI

```
set admin name name
set admin password pswd_str
save
```

Date and Time

The time set on an SSG 20 device affects events such as the setup of VPN tunnels. The easiest way to set the date and time on the device is to use the WebUI to synchronize the device system clock with the workstation clock.

To configure the date and time on a device, use the WebUI or CLI as follows:

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 option on your workstation clock.

2. Click **Yes** to synchronize the system clock and adjust it according to daylight saving time, or click **No** to synchronize the system clock without adjusting for daylight saving time.

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

Bridge Group Interfaces

By default, the SSG 20 device has Ethernet interfaces ethernet0/2 — ethernet0/4 grouped together in the Trust security zone. Grouping interfaces sets interfaces in one subnet. You can unset an interface from a group and assign it to a different security zone. Interfaces must be in the Null security zone before they can be assigned to a group. To place a grouped interface in the Null security zone, use the **unset interface interface port interface** CLI command.

The SSG 20-WLAN devices allow Ethernet and wireless interfaces to be grouped under one subnet.

NOTE: Only wireless and Ethernet interfaces can be set in a bgroup.

To configure a group with Ethernet and wireless interfaces, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port: deselect **ethernet0/3** and **ethernet0/4**, then click **Apply**.

Edit (bgroup1) > Bind Port: select **ethernet0/3**, **ethernet0/4**, and **wireless0/2**, then click **Apply**.

> Basic: Enter the following, then click **Apply**:

Zone Name: DMZ (select)
IP Address/Netmask: 10.0.0.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
unset interface bgroup0 port ethernet0/4
set interface bgroup1 port ethernet0/3
set interface bgroup1 port ethernet0/4
set interface bgroup1 port wireless0/2
set interface bgroup1 zone DMZ
set interface bgroup1 ip 10.0.0.1/24
save
```

Administrative Access

By default, anyone in your network can manage a device if they know the login and password.

To configure the device to be managed only from a specific host on your network, use the WebUI or CLI as follows:

WebUI

Configuration > Admin > Permitted IPs: Enter the following, then click **Add**:

IP Address/Netmask: *ip_addr/mask*

CLI

```
set admin manager-ip ip_addr/mask
save
```

Management Services

ScreenOS provides services for configuring and managing the device, such as SNMP, SSL, and SSH, which you can enable on a per-interface basis.

To configure the management services on the device, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > List > Edit (for ethernet0/0): Under **Management Services**, select or clear the management services you want to use on the interface, then click **Apply**.

CLI

```
set interface ethernet0/0 manage web
unset interface ethernet0/0 manage snmp
save
```

Hostname and Domain Name

The domain name defines the network or subnetwork that the device belongs to, while the hostname refers to a specific device. The hostname and domain name together uniquely identify the device in the network.

To configure the hostname and domain name on a device, use the WebUI or CLI as follows:

WebUI

Network > DNS > Host: Enter the following, then click **Apply**:

Host Name: *name*
Domain Name: *name*

CLI

```
set hostname name
set domain name
save
```

Default Route

The default route is a static route used to direct packets addressed to networks that are not explicitly listed in the routing table. If a packet arrives at the device with an address for which the device does not have routing information, the device sends the packet to the destination specified by the default route.

To configure the default route on the device, use the WebUI or CLI as follows:

WebUI

Network > Routing > Destination > New (trust-vr): Enter the following, then click **OK**:

IP Address/Netmask: 0.0.0.0/0.0.0.0
Next Hop
Gateway: (select)
Interface: ethernet0/2 (select)
Gateway IP Address: *ip_addr*

CLI

```
set route 0.0.0.0/0 interface ethernet0/2 gateway ip_addr
save
```

Management Interface Address

The Trust interface has the default IP address 192.168.1.1/24 and is configured for management services. If you connect the 0/2 — 0/4 ports on the device to a workstation, you can configure the device from a workstation in the 192.168.1.1/24 subnetwork using a management service such as Telnet.

You can change the default IP address on the Trust interface. For example, you might want to change the interface to match IP addresses that already exist on your LAN.

Backup Untrust Interface Configuration

The SSG 20 device allows you to configure a backup interface for untrust failover. To set a backup interface for untrust failover, perform the following steps:

1. Set the backup interface in the Null security zone with the **unset interface interface [port interface]** CLI command.
2. Bind the backup interface to the same security zone as the primary interface with the **set interface interface zone zone_name** CLI command.

NOTE: The primary and backup interfaces must be in the same security zone. One primary interface has only one backup interface, and one backup interface has only one primary interface.

To set the ethernet0/4 interface as the backup interface to the ethernet0/0 interface, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > Backup > Enter the following, then click **Apply**.

Primary: ethernet0/0
Backup: ethernet0/4
Type: track-ip (select)

CLI

```
unset interface bgroup0 port ethernet0/4
set interface ethernet0/4 zone untrust
set interface ethernet0/0 backup interface ethernet0/4 type track-ip
save
```

Basic Wireless Configuration

This section provides information for configuring the wireless interface on the SSG 20-WLAN device. Wireless networks consist of names referred to as Service Set Identifiers (SSIDs). Specifying SSIDs allows you to have multiple wireless networks reside in the same location without interfering with each other. An SSID name can have a maximum of 32 characters. If a space is part of the SSID name string, then the string must be enclosed with quotation marks. Once the SSID name is set, more SSID attributes can be configured. To use the wireless local area network (WLAN) capabilities on the device, you must configure at least one SSID and bind it to a wireless interface.

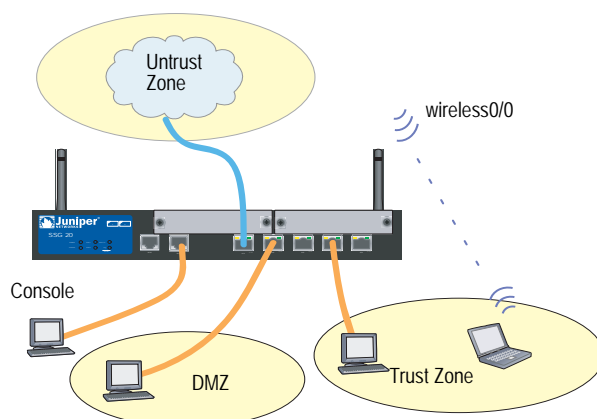
The SSG 20-WLAN device allows you to create up to 16 SSIDs, but only 4 of them can be used simultaneously. You can configure the device to use the 4 SSIDs on either one of the transceivers or split the use on both (for example, 3 SSIDs assigned to WLAN 0 and 1 SSID assigned to WLAN 1.) Use the **set interface wireless_interface wlan {0 | 1 | both}** CLI command to set the radio transceivers on the SSG 20-WLAN device.

Once you have set an SSID to the wireless0/0 interface, you can access the device using the default wireless0/0 interface IP address in the steps described in “Accessing a Device” on page 28. Figure 15 shows the default configuration for the SSG 20-WLAN device.

NOTE: If you are operating the SSG 20-WLAN device in a country other than the United States, Japan, Canada, China, Taiwan, Korea, Israel, or Singapore, then you must use the **set wlan country-code** CLI command or set it on the Wireless > General Settings WebUI page before a WLAN connection can be established. This command sets the selectable channel range and the transmit power level.

If your regional code is ETSI, you must set the correct country code that meets your local radio spectrum regulations.

Figure 15: Default SSG 20-WLAN Configuration



By default, the wireless0/0 interface is configured with the IP address 192.168.2.1/24. All wireless clients that need to connect to the Trust zone must have an IP address in the wireless subnetwork. You can also configure the device to use DHCP to automatically assign IP addresses in the 192.168.2.1/24 subnetwork to your devices.

By default, the wireless0/1 – wireless0/3 interfaces are defined as Null and do not have IP addresses assigned to them. If you want to use any of the other wireless interfaces, you must configure an IP address for it, assign an SSID to it, and bind it to a security zone. Table 7 displays the wireless authentication and encryption methods.

Table 7: Wireless Authentication and Encryption Options

Authentication	Encryption
Open	Allows any wireless client to access the device
Shared-key	WEP shared-key
WPA-PSK	AES/TKIP with pre-shared key
WPA	AES/TKIP with key from RADIUS server
WPA2-PSK	802.11i compliant with a pre-shared key
WPA2	802.11i compliant with a RADIUS server
WPA-Auto-PSK	Allows WPA and WPA2 type with pre-shared key
WPA-Auto	Allows WPA and WPA2 type with RADIUS server
802.1x	WEP with key from RADIUS server

Refer to the *Concepts & Examples ScreenOS Reference Guide* for configuration examples, SSID attributes, and CLI commands relating to wireless security configurations.

To configure a wireless interface for basic connectivity, use the WebUI or CLI as follows:

WebUI

1. Set the WLAN country code and IP address.

Wireless > General Settings > Select the following, then click **Apply**:

Country code: Select your code

IP Address/Netmask: *ip_add/netmask*

2. Set the SSID.

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

SSID:

Authentication:

Encryption:

Wireless Interface Binding:

3. (Optional) set the WEP key.

SSID > WEP Keys: Select the keyID, then click **Apply**.

4. Set the WLAN mode.

Network > Interfaces > List > Edit (wireless interface): Select **Both** for the WLAN mode, then click **Apply**.

5. Activate wireless changes.

Wireless > General Settings > Click **Activate Changes**.

CLI

1. Set the WLAN country code and IP address.

```
set wlan country-code {code_id}
set interface wireless_interface ip ip_addr/netmask
```

2. Set the SSID.

```
set ssid name name_str
set ssid name_str authentication auth_type encryption encryption_type
set ssid name_str interface interface
(optional) set ssid name_str key-id number
```

3. Set the WLAN mode.

```
set interface wireless_interface wlan both
```

4. Activate wireless changes.

```
save
exec wlan reactivate
```

You can set an SSID to operate in the same subnet as the wired subnet. This action allows clients to work in either interface without having to reconnect in another subnet.

To set an Ethernet and a wireless interface to the same bridge-group interface, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > List > Edit (*bgroup_name*) > Bind Port: Select the wireless and ethernet interfaces, then click **Apply**.

CLI

```
set interface bgroup_name port wireless_interface
set interface bgroup_name port ethernet_interface
```

NOTE: *Bgroup_name* can be bgroup0—bgroup3.

Ethernet_interface can be ethernet0/0—ethernet0/4.

Wireless_interface can be wireless0/0—wireless0/3.

If a wireless interface is configured, then you need to reactivate the WLAN with the **exec wlan reactivate** CLI command or click **Activate Changes** on the Wireless > General Settings WebUI page.

Mini PIM Configuration

This section explains how to configure the mini physical interface modules (PIMs):

- ADSL2/2 + Interface
- ISDN Interface
- T1 Interface
- E1 Interface
- V.92 Modem Interface

ADSL2/2+ Interface

Your network uses the ADSL2/2 + interface **adslx/0**, with x representing the mini PIM slot (1 or 2), on the 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 ADSL2/2 + subinterfaces. For more information, see "Virtual Circuits" on page 42.

In the WebUI, navigate to the Network > Interfaces > List page to see a list of the current interfaces on the device. If you are using a Telnet or Console session, enter the **get interface** CLI command. You should see that the adslx/0 interface is bound to the Untrust zone.

If you are using the ADSL2/2 + interface to connect to the service network of the provider, you must configure the adsl(x/0) interface. 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-based multiplexing, in which each protocol is carried over a separate ATM virtual circuit
 - Logical Link Control (LLC) encapsulation, which allows several protocols to be carried on the same ATM virtual circuit (the default multiplexing method)
- Username and password assigned by the service provider for connection to the service provider's network using either 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

Virtual Circuits

To add virtual circuits, you create subinterfaces to the ADSL2/2+ interface. You can create up to 10 ADSL2/2+ subinterfaces. For example, to create a new subinterface named **adsl1/0.1** bound to the predefined zone named **Untrust**, use the WebUI or CLI as follows:

WebUI

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

Interface Name: adsl1/0.1
VPI/VCI: 0/35
Zone Name: Untrust (select)

CLI

```
set interface adsl 1/0.1 pvc 0 35 zone Untrust
save
```

You need to configure an ADSL 2/2+ subinterface in the same way as the main ADSL2/2+ interface, including setting the VPI/VCI values, as described in “ADSL2/2+ Interface” on page 41. You configure an ADSL2/2+ subinterface independently of the main ADSL2/2+ interface; that is, you can configure a different multiplexing method, VPI/VCI, and PPP client on the subinterface than on the main ADSL2/2+ interface. You can also configure a static IP address on a subinterface, even if the main ADSL2/2+ interface does not have a static IP address.

VPI/VCI and Multiplexing Method

Your service provider assigns a VPI/VCI pair for each virtual-circuit connection. For example, you may receive the VPI/VCI pair 1/32, which means a VPI value of 1 and a VCI value of 32. 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 1/32 on the adsl1/0 interface, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > List > Edit (for the adsl1/0 interface): Enter **1/32** in the VPI/VCI field, then click **Apply**.

CLI

```
set interface adsl1/0 pvc 1 32
save
```

By default, the device uses Logical Link Control (LLC)-based multiplexing for each virtual circuit.

To configure the VPI/VCI 1/32 on the adslx/0 interface and use LLC encapsulation on the virtual circuit, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > List > Edit (for the adsl1/0 interface): Enter the following, then click **Apply**:

VPI/VCI: 1 / 32
Multiplexing Method: LLC (selected)

CLI

```
set interface adsl1/0 pvc 1 32 mux llc
save
```

PPPoE or PPPoA

An SSG 20 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 device. To allow the device to connect to the network of the service provider, you need to configure the username and password assigned by the service provider. The configuration for PPPoA is similar to the configuration for PPPoE.

NOTE: The device supports only one PPPoE session on each virtual circuit.

To configure the username **roswell** and password **area51** for PPPoE and bind the PPPoE configuration to the adsl1/0 interface, use the WebUI or CLI as follows:

WebUI

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

PPPoE Instance: poe1
Bound to Interface: adsl1/0 (select)
Username: roswell
Password: area51

CLI

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1/0
save
```

There are other PPPoE or PPPoA parameters that you can configure on the device, including method of authentication (by default, the 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.

Static IP Address and Netmask

If your service 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 device. You need to also specify that the device is to use the static IP address. (Typically, the 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.)

You need to configure a PPPoE or PPPoA instance and bind it to the adsl1/0 interface, as described in “PPPoE or PPPoA” on page 43. Make sure that you select **Obtain IP using PPPoE** or **Obtain IP using PPPoA** and the name of the PPPoE or PPPoA instance.

To configure the static IP address 1.1.1.1/24 for the network, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > List > Edit (for the adsl1/0 interface): Enter the following, then click **Apply**:

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

CLI

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

or

```
set interface adsl1/0 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 device receives an IP address for the ADSL2/2+ 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 address(es) from the DHCP server on the device, then the computers also obtain these DNS server addresses.

If you assign a static IP address to the ADSL2/2+ 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 you can 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 bgroup0 interface to provide the DNS server address 1.1.1.152 to computers in your network, use the WebUI or CLI as follows:

WebUI

Network > DHCP > Edit (for the bgroup0 interface) > DHCP Server: Enter 1.1.1.152 for DNS1, then click **Apply**.

CLI

```
set interface bgroup0 dhcp server option dns1 1.1.1.152
save
```

For more information about configuring the ADSL and ADSL2/2+ interfaces, refer to the *Concepts & Examples ScreenOS Reference Guide*.

ISDN Interface

Integrated Services Digital Network (ISDN) is a set of standards for digital transmission over different media created by the Consultative Committee for International Telegraphy and Telephone (CCITT) and International Telecommunications Union (ITU). As a dial-on-demand service, it has fast call setup and low latency as well as the ability to carry high-quality voice, data, and video transmissions. ISDN is also a circuit-switched service that can be used on both multipoint and point-to-point connections. ISDN provides a service router with a multilink Point-to-Point Protocol (PPP) connection for network interfaces. The ISDN interface is usually configured as the backup interface of the Ethernet interface to access external networks.

To configure the ISDN interface, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > List > Edit (bri1/0): Enter or select the following, then click **OK**:

```
BRI Mode: Dial Using BRI
Primary Number: 123456
WAN Encapsulation: PPP
PPP Profile: isdnprofile
```

CLI

```
set interface bri1/0 dialer-enable
set interface bri1/0 primary-number "123456"
set interface bri1/0 encaps ppp
set interface bri1/0 ppp profile isdnprofile
save
```

To configure the ISDN interface as the backup interface, see “Backup Untrust Interface Configuration” on page 37.

For more information on how to configure the ISDN interface, refer to the *Concepts & Examples ScreenOS Reference Guide*.

T1 Interface

The T1 interface is a basic Physical Layer protocol used by the Digital Signal level 1 (DS-1) multiplexing method in North America. A T1 interface operates at a bit-rate of 1.544 Mbps or speeds up to 24 DS0 channels.

The devices support the following T1 DS-1 standards:

- ANSI T1.107, T1.102
- GR 499-core, GR 253-core

- AT&T Pub 54014
- ITU G.751, G.703

To configure the T1 mini PIM, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > List > Edit (serial1/0): Enter or select the following, then click **OK**:

WAN Configure: main link
 WAN Encapsulation: cisco-hdlc
 Click **Apply**
 Fixed IP: (select)
 IP Address/Netmask 172.18.1.1/24

CLI

```
set interface serial1/0 encap cisco-hdlc
set interface serial1/0 ip 172.18.1.1/24
```

For information on how to configure the T1 interface, refer to the *Concepts & Examples ScreenOS Reference Guide*.

E1 Interface

The E1 interface is a standard wide area network (WAN) digital communications format designed to operate over copper facilities at a rate of 2.048 Mbps. Widely used outside North America, E1 is a basic time-division multiplexing scheme used to carry digital circuits.

The devices support the following E1 standards:

- ITU-T G.703
- ITU-T G.751
- ITU-T G.775

To configure the E1 mini PIM, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > List > Edit (serial1/0): Enter or select the following, then click **OK**:

WAN Configure: main link
 WAN Encapsulation: PPP
 Binding a PPP Profile: junipertest
 Click **Apply**
 Fixed IP: (select)
 IP Address/Netmask 172.18.1.1/24

CLI

```
set interface serial1/0 encapsulation ppp
set ppp profile "junipertest" static-ip
set ppp profile "junipertest" auth type chap
```

```

set ppp profile "junipertest" auth local-name "juniper"
set ppp profile "junipertest" auth secret "password"
set interface serial1/0 ppp profile "junipertest"
set interface serial1/0 ip 172.18.1.1/24
set user "server" type wan
set user "server" password "server"

```

For information on how to configure the E1 interface, refer to the *Concepts & Examples ScreenOS Reference Guide*.

V.92 Modem Interface

The V.92 interface provides an internal analog modem to establish a PPP connection to a service provider. You can configure the serial interface as a primary or backup interface, which is used in case of interface failover.

NOTE: The V.92 interface does not work in Transparent mode.

To configure the V.92 interface, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > List > Edit (for serial1/0): Enter the following, then click **OK**:

Zone Name: untrust (select)

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

ISP Name: isp_juniper
 Primary Number: 1234567
 Login Name: juniper
 Login Password: juniper

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

Modem Name: mod1
 Init String: AT&FS7=255S32=6
 Active Modem setting
 Inactivity Timeout: 20

CLI

```

set interface serial1/0 zone untrust
set interface serial1/0 modem isp isp_juniper account login juniper password
juniper
set interface serial1/0 modem isp isp_juniper primary-number 1234567
set interface serial1/0 modem idle-time 20
set interface serial1/0 modem settings mod1 init-strings AT&FS7=255S32=6
set interface serial1/0 modem settings mod1 active

```

For information on how to configure the V.92 modem interface, refer to the *Concepts & Examples ScreenOS Reference Guide*.

Basic Firewall Protections

The devices are configured with a default policy that permits workstations in the Trust zone of your network to access any resource in the Untrust security zone, while outside computers are not allowed to access or start sessions with your workstations. You can configure policies that direct the device to permit outside computers to start specific kinds of sessions with your computers. For information about creating or modifying policies, refer to the *Concepts & Examples ScreenOS Reference Guide*.

The SSG 20 device provides various detection methods and defense mechanisms to combat probes and attacks aimed at compromising or harming a network or network resource:

- ScreenOS SCREEN options secure a zone by inspecting, and then allowing or denying, all connection attempts that require crossing an interface to that zone. For example, you can apply port-scan protection on the Untrust zone to stop a source from a remote network from trying to identify services to target for further attacks.
- The device applies firewall policies, which can contain content-filtering and Intrusion Detection and Prevention (IDP) components, to the traffic that passes the SCREEN filters from one zone to another. By default, no traffic is permitted to pass through the device from one zone to another. To permit traffic to cross the device from one zone to another, you must create a policy that overrides the default behavior.

To set ScreenOS SCREEN options for a zone, use the WebUI or CLI as follows:

WebUI

Screening > Screen: Select the zone to which the options apply. Select the SCREEN options that you want, then click **Apply**:

CLI

```
set zone zone screen option
save
```

For more information about configuring the network-security options available in ScreenOS, refer to the *Concepts & Examples ScreenOS Reference Guide*.

Verifying External Connectivity

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

Resetting a Device to Factory Defaults

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



WARNING: Resetting the device deletes all existing configuration settings and disables all existing firewall and VPN services.

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

- Using a Console connection. For further information, refer to the *Concepts & Examples ScreenOS Reference Guide*.
- Using the reset pinhole on the back panel of the device, as described in the next section.

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 28.

To use the reset pinhole to reset and restore the default settings, perform the following steps:

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

The STATUS LED blinks red. 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 reset. The STATUS LED glows red 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 glows red 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 blinks green. The login and password are **netscreen**.

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.

Chapter 4

Servicing the Device

This chapter describes service and maintenance procedures for an SSG 20 device. It contains the following sections:

- “Required Tools and Parts” on this page
- “Replacing a Mini-Physical Interface Module” on this page
- “Upgrading Memory” on page 54

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

Required Tools and Parts

To replace a component on an SSG 20 device, you need the following tools and parts:

- Electrostatic bag or antistatic mat
- Electrostatic discharge (ESD) grounding wrist strap
- Phillips screwdriver, 1/8-inch

Replacing a Mini-Physical Interface Module

Both SSG 20 models have two slots in the front panel for wide area network mini physical interface modules (WAN mini PIMs). Mini PIMs in an SSG 20 device can be installed and replaced. The device must be powered off before you can remove or install a mini PIM.



CAUTION: Make sure the power is off to the device when removing a mini PIM. They are not hot-swappable.

Removing a Blank Faceplate

To maintain proper airflow through the SSG 20 device, blank faceplates should remain over slots that do not contain mini PIMs. Do not remove a blank faceplate unless you are installing a mini PIM in its empty slot.

To remove a blank faceplate, perform the following steps:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface on which you intend to place the mini PIM.
2. Attach an ESD grounding strap to your bare wrist and connect the strap to the ESD point on the chassis or to an outside ESD point if the SSG 20 device is disconnected from earth ground.
3. Unplug the power adapter from the device. Verify that the POWER LED is off.
4. Loosen and remove the screws on each side of the faceplate using a screwdriver.
5. Remove the faceplate, then place the faceplate in the electrostatic bag or on the antistatic mat.

Removing a Mini PIM

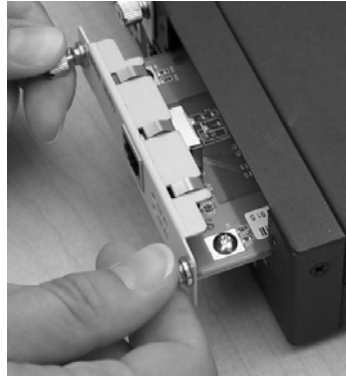
Mini PIMs are installed in the front panel of the SSG 20 device. A mini PIM weighs less than 0.2 lb (106g).

To remove a mini PIM, perform the following steps:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface on which you intend to place the mini PIM.
2. Attach an ESD grounding strap to your bare wrist and connect the strap to the ESD point on the chassis or to an outside ESD point if the SSG 20 device is disconnected from earth ground.
3. Unplug the power adapter from the device. Verify that the POWER LED is off.
4. Label the cables connected to the mini PIM so that you can later reconnect each cable to the correct mini PIM.
5. Disconnect the cables from the mini PIM.
6. If necessary, arrange the cables to prevent them from dislodging or developing stress points:
 - a. Secure the cables so that they are not supporting their own weight as they hang to the floor.
 - b. Place any excess cables out of the way in neatly coiled loops.
 - c. Use fasteners to maintain the shape of the cable loops.
7. Loosen and remove the screws on each side of the mini PIM faceplate using a screwdriver.

8. Grasp the screws on each side of the mini PIM faceplate and slide the mini PIM out of the device. Place the mini PIM in the electrostatic bag or on the antistatic mat.

Figure 16: Removing a Mini PIM



9. If you are not reinstalling a mini PIM into the empty slot, install a blank faceplate over the slot to maintain proper airflow.

Installing a Mini PIM

To install a mini PIM, perform the following steps:

1. Attach an ESD grounding strap to your bare wrist and connect the strap to the ESD point on the chassis or to an outside ESD point if the SSG 20 device is disconnected from earth ground.
2. Unplug the power adapter from the device. Verify that the POWER LED is off.
3. Grasp the screws on each side of the mini PIM faceplate and align the notches in the connector at the rear of the mini PIM with the notches in the mini PIM slot in the SSG 20 device. Then slide the mini PIM in until it lodges firmly in the device.

Figure 17: Installing a Mini PIM



CAUTION: Slide the mini PIM straight into the slot to avoid damaging the components on the mini PIM.

4. Tighten the screws on each side of the mini PIM faceplate using a 1/8-inch slotted screwdriver.
5. Insert the appropriate cables into the cable connectors on the mini PIM.

6. If necessary, arrange the cables to prevent them from dislodging or developing stress points:
 - a. Secure the cables so that they are not supporting their own weight as they hang to the floor.
 - b. Place any excess cables out of the way in neatly coiled loops.
 - c. Use fasteners to maintain the shape of the cable loops.
7. Unplug the power adapter from the device. Verify that the POWER LED glows steadily green after you press the power button.
8. Verify that the PIM status LED on the system dashboard glows steadily green to confirm that the mini PIM is online.

Upgrading Memory

You can upgrade an SSG 20 device from a single 128 MB dual in-line memory module (DIMM) dynamic random access memory (DRAM) to a 256 MB DIMM DRAM.

To upgrade the memory on an SSG 20 device, perform the following steps:

1. Attach an ESD grounding strap to your bare wrist and connect the strap to the ESD point on the chassis or to an outside ESD point if the device is disconnected from earth ground.
2. Unplug the AC cord from the power outlet.
3. Turn over the device so that its top is lying on a flat surface.
4. Use a phillips screwdriver to remove the screws from the memory-card cover. Keep the screws nearby for use when securing the cover later.
5. Remove the memory-card cover.

Figure 18: Bottom of Device



6. Release the 128 MB DIMM DRAM by pressing your thumbs outward on the locking tabs on each side of the module so that the tabs move away from the module.

Figure 19: Unlocking the Memory Module



7. Grip the long edge of the memory module and slide it out. Set it aside.

Figure 20: Removing Module Slots



8. Insert the 256 MB DIMM DRAM into the slot. Exerting even pressure with both thumbs upon the upper edge of the module, press the module downward until the locking tabs click into position.

Figure 21: Inserting the Memory Module



9. Place the memory-card cover over the slot.
10. Use the phillips screwdriver to tighten the screws, securing the cover to the device.

Appendix A

Specifications

This appendix provides general system specifications for an SSG 20 device. It contains the following sections:

- “Physical” on page 58
- “Electrical” on page 58
- “Environmental Tolerance” on page 58
- “Certifications” on page 59
- “Connectors” on page 60

Physical

Table 8: SSG 20 Physical Specifications

Description	Value
Chassis dimensions	294 mm x 194.8 mm x 44 mm (11.5 inches x 7.7 inches x 2 inches)
Device weight	1.53 kg (3.3 lbs) without PIMs installed
ISDN PIM	70g
ADSL Annex A PIM	106g
ADSL Annex B PIM	106g
T1 PIM	75g
E1 PIM	75g
V.92 PIM	79g

Electrical

Table 9: SSG 20 Electrical Specifications

Item	Specification
DC input voltage	12V
DC system current rating	3 - 4.16 Amps

Environmental Tolerance

Table 10: SSG 20 Environmental Tolerance

Description	Value
Altitude	No performance degradation to 6,600 ft (2,000 m)
Relative humidity	Normal operation ensured in relative humidity range of 10 to 90 percent, noncondensing
Temperature	Normal operation ensured in temperature range of 32°F (0°C) to 104°F (40°C) Nonoperating storage temperature in shipping carton: -4°F (-20°C) to 158°F (70°C)

Certifications

Safety

- CAN/CSA-C22.2 No. 60950-1-03/UL 60950-1 Safety of Information Technology Equipment
- EN 60950-1 (2000) Third Edition Safety of Information Technology Equipment
- IEC 60950-1 (1999) Third Edition Safety of Information Technology Equipment

EMC Emissions

- FCC Part 15 Class B (USA)
- EN 55022 Class B (Europe)
- AS 3548 Class B (Australia)
- VCCI Class B (Japan)

EMC Immunity

- EN 55024
- EN-61000-3-2 Power Line Harmonics
- EN-61000-3-3 Power Line Harmonics
- EN-61000-4-2 ESD
- EN-61000-4-3 Radiated Immunity
- EN-61000-4-4 EFT
- EN-61000-4-5 Surge
- EN-61000-4-6 Low Frequency Common Immunity
- EN-61000-4-11 Voltage Dips and Sags

ETSI

European Telecommunications Standards Institute (ETSI) EN-3000386-2: Telecommunication Network Equipment. Electromagnetic Compatibility Requirements; (equipment category–Other than telecommunication centers)

T1 Interface

- FCC Part 68 - TIA 968
- Industry Canada CS-03
- UL 60950-1 Applicable requirements for TNV circuit with outside plant lead connection

Connectors

Figure 22 shows the location of the pins on the RJ-45 connector.

Figure 22: RJ-45 Pinouts

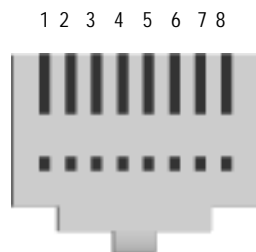


Table 11 lists the RJ-45 connector pinouts.

Table 11: RJ-45 Connector Pinouts

Pin	Name	I/O	Description
1	RTS Out	O	Request To Send
2	DTR Out	O	Data Terminal Ready
3	TxD	O	Transmit Data
4	GND	N/A	Chassis Ground
5	GND	N/A	Chassis Ground
6	RxD	I	Receive Data
7	DSR	I	Data Set Ready
8	CTS	I	Clear To Send

Figure 23 shows the location of the pins on the DB-9 female connector.

Figure 23: DB-9 Female Connector

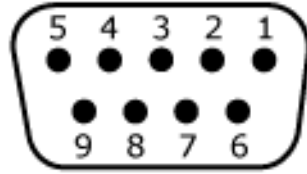


Table 12 provides the DB-9 connector pinouts.

Table 12: DB-9 Connector Pinouts

Pin	Name	I/O	Description
1	DCD	I	Carrier Detect
2	RxD	I	Receive Data
3	TxD	O	Transmit Data
4	DTR	O	Data Terminal Ready
5	GND	N/A	Signal Ground
6	DSR	I	Data Set Ready
7	RTS	O	Request To Send
8	CTS	I	Clear To Send
9	RING	I	Ring Indicator

Appendix B

Initial Configuration Wizard

This appendix provides detailed information about the Initial Configuration Wizard (ICW) for an SSG 20 device.

After you have physically connected your device to the network, you can use the ICW to configure the interfaces that are installed on your device.

This section describes the following ICW windows:

- Rapid Deployment Window on page 64
- Administrator Login Window on page 64
- WLAN Access Point Window on page 65
- Physical Interface Window on page 65
- ADSL2/2 + Interface Window on page 66
- T1 Interface Windows on page 68
- E1 Interface Windows on page 73
- ISDN Interface Windows on page 75
- V.92 Modem Interface Window on page 78
- Eth0/0 Interface (Untrust Zone) Window on page 78
- Eth0/1 Interface (DMZ Zone) Window on page 79
- Bgroup0 Interface (Trust Zone) Window on page 80
- Wireless0/0 Interface (Trust Zone) Window on page 81
- Interface Summary Window on page 82
- Physical Ethernet DHCP Interface Window on page 83
- Wireless DHCP Interface Window on page 83
- Confirmation Window on page 84

1. Rapid Deployment Window

Figure 24: Rapid Deployment Window



Rapid Deployment Wizard

Welcome to the Rapid Deployment Wizard.

Do you have a Rapid Deployment Configlet file?

☒ No, use the Initial Configuration Wizard instead.

☐ Yes, use the following Rapid Deployment Configlet file:

Load Configlet from:

☐ No, skip the Wizard and go straight to the WebUI management session instead.

If your network uses NetScreen-Security Manager (NSM), you can use a Rapid Deployment configlet to automatically configure the device. Obtain a configlet from your NSM administrator, select **Yes**, select **Load Configlet from:**, browse to the file location, then click **Next**. The configlet sets up the device for you, so you don't need to use the following steps to configure the device.

If you want to bypass the ICW and go directly to the WebUI, select the last option, then click **Next**.

If you are not using a configlet to configure the device and want to use the ICW, select the first option, then click **Next**. The ICW Welcome screen appears. Click **Next**. The Administrator Login window appears.

2. Administrator Login Window

Enter a new administrator login name and password, then click **Next**.

Figure 25: Administrator Login Window



Initial Configuration Wizard

Enter the administrator's login name and password:

Administrator Login Name:

Password:

Confirm Password:

Note: You cannot retrieve the login name and password if you lose it. Please make sure you have a copy of this information in a secure location.

HTTP Redirect: ☐

Note: HTTP Redirect will redirect all HTTP traffic to HTTPS, ie, HTTPS is only way to manage the device through Web browsers.

3. WLAN Access Point Window

If you are using the device in the WORLD or ETSI regulatory domain, you must choose a country code. Select the appropriate options, then click **Next**.

Figure 26: Wireless Access Point Country Code Window

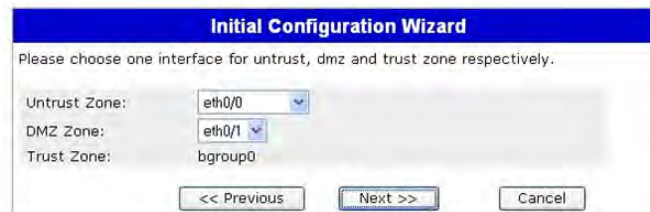


The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. The main area has a light gray background. At the top, it asks 'How do you want to configure the wireless access point?'. Below this, there are four dropdown menus: 'Regulatory Domain' set to 'WORLD', 'Country Code' set to 'NO_COUNTRY_SET', '2.4G Mode' set to '802.11b/g', and '5G Mode' set to '802.11a'. Below these is a checkbox labeled 'Configure wireless0/0 interface in trust zone.' which is checked. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

4. Physical Interface Window

On the interface-to-zone bindings screen, you set the interface to which you want to bind the Untrust security zone. Bgroup0 is prebound to the Trust security zone. Eth0/1 is bound to the DMZ security zone but is optional.

Figure 27: Physical Interface Window



The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. The main area has a light gray background. At the top, it asks 'Please choose one interface for untrust, dmz and trust zone respectively.'. Below this, there are three dropdown menus: 'Untrust Zone' set to 'eth0/0', 'DMZ Zone' set to 'eth0/1', and 'Trust Zone' set to 'bgroup0'. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

After binding an interface to a zone, you can configure the interface. The configuration windows that are displayed after this point depend on which mini-PIMs are installed in your security device. To continue configuring your device with the ICW, click **Next**.

5. ADSL2/2+ Interface Window

If you have the ADSL2/2 + mini P1M installed in your device, you can configure the adslx/0 interface using the following window.

NOTE: If you have two ADSL2/2 + mini-P1Ms installed on your device, you cannot configure the Multi-link feature with the ICW. To configure ML ADSL, refer to the *Concepts & Examples ScreenOS Reference Guide*.

Figure 28: ADSL Interface Configuration Window

Initial Configuration Wizard

Juniper
SSG 20

Please click the following links or the above figure to configure interfaces.
[adsl1/0\(Untrust Zone\)](#) [bggroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

How does the Juniper device connect to the outside via adsl1/0 interface?

VPI/VCI: 8 / 35

Multiplexing Method: LLC

RFC1483 Protocol Mode: ☒ Bridged ☐ Routed

Operating Mode: ☒ Auto ☐ ANSI DMT ☐ ITU DMT ☐ Adsl2 ☐ Adsl2+

☐ Dynamic IP via DHCP

☐ Dynamic IP via PPPoA

Username:

Password:

Confirm:

☐ Dynamic IP via PPPoE

Username:

Password:

Confirm:

☒ Static IP

Interface IP:

Netmask:

Gateway:

<< Previous Next >> Cancel

Table 13: Fields in ADSL Interface Configuration Window

Field	Description
Information from Service Provider:	
VPI/VCI	VPI/VCI values to identify the permanent virtual circuit.
Multiplexing Method	ATM multiplexing method (LLC is the default).
RFC1483 Protocol Mode	Protocol mode setting (Bridged is the default).
Operating Mode	Operating mode for the physical line (Auto is the default).
IP configuration settings	<ul style="list-style-type: none"> ■ Select Dynamic IP via DHCP to enable the device to receive an IP address for the ADSL interface from a service provider. ■ Select Dynamic IP via PPPoA to enable the device to act as a PPPoA client. Enter the username and password assigned by the service provider. ■ Select Dynamic IP via PPPoE to enable the device to act as a PPPoE client. Enter the username and password assigned by the service provider. ■ Select Static IP to assign a unique and fixed IP address to the ADSL interface. Enter the interface IP address, netmask, and gateway (the gateway address is the IP address of the router port connected to the device).

If you do not know these settings, refer to the *Common Settings for Service Providers* document that came with the service provider device.

6. T1 Interface Windows

If you have the T1 mini-PIM installed in your device and you selected the Frame Relay option, the following windows are displayed:

- T1 Physical Layer Tab Window
- T1 Frame Relay Tab Window

NOTE: If you have two T1 mini-PIMs installed on your device and you select the Multi-link option, you will see two Physical Layer tabs.

Figure 29: T1 Physical Layer Tab Window

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20 device. At the top, there's a navigation bar with icons for various configuration steps. Below the title bar, a message says: 'Please click the following links or the above figure to configure interfaces. [serial1/0\(Untrust_Zone\)](#) [hgroup0\(Trust_Zone\)](#) [eth0/1\(DMZ_Zone\)](#)'. Below this, a question asks: 'How does the Juniper device connect to the outside via serial1/0(T1) interface?'. There are three radio buttons for 'WAN Encapsulation': 'Frame Relay' (selected), 'PPP', and 'Cisco HDLC'. Below this, there are two tabs: 'Physical Layer' (selected) and 'Frame Relay'. The 'Physical Layer' tab contains several configuration options: 'Clocking:' with 'External' (selected) and 'Internal (Lab Use Only)'; 'Line Buildout:' with a dropdown set to '0~132' and 'Feet'; 'Line Encoding:' with 'AMI (Auto Mark Inversion)' and 'B8ZS (8-bits Zero Suppression)'; 'Byte Encoding:' with '7-bits per byte' and '8-bits per byte'; 'Frame Checksum:' with '16-bits' and '32-bits'; 'Framing Mode:' with 'Super Frame' and 'Extended Super Frame'; 'Idle Cycles Flag:' with '0x7E' and '0xFF(All Ones)'; 'Start/End Flags:' with 'Filler' and 'Share'; 'Invert data:' (checkbox, unchecked); 'Loopback Respond:' (checkbox, unchecked); and 'Time Slots:' with a dropdown set to '0' and a note '(0(all active), 1..24(e.g. 2,7-9))'. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Table 14: Fields in T1 Physical Layer Tab Window

Field	Description
Clocking	Sets the transmit clock on the interface.
Line Buildout	Sets the distance at which an interface drives a line. Default setting is 0 - 132 feet.
Line Encoding	Sets the line encoding format on the interface: <ul style="list-style-type: none"> ■ Auto Mark Inversion ■ 8-bits zero suppression
Byte Encoding	Sets the byte encoding on the T1 interface to use 7 bits per byte or 8 bits per byte. Default is 8 bits per byte.
Frame Checksum	Sets the size of checksum. Default is 16 .
Framing Mode	Sets the framing format. Default is Extended mode .
Idle Cycles Flag	Sets the value that the interface transmits during idle cycles. Default setting is 0x7E : <ul style="list-style-type: none"> ■ 0x7E (flags) ■ 0xFF (ones)
Start/End Flags	Sets the transmission of start and end flags to either filler or shared. The default is filler .
Invert Data checkbox	Enables inverted transmission of unused data bits.
Loopback Respond checkbox	Enables loopback on the T1 interface from the remote channel service unit (CSU).
Time Slots	Sets the use of time slots on a T1 interface. Default is 0 , all 24 time slots used.

Figure 30: T1 Frame Relay Tab Window

Initial Configuration Wizard

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.
[serial1/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

How does the Juniper device connect to the outside via serial1/0(T1) interface?
 WAN Encapsulation: ☒ Frame Relay ☐ PPP ☐ Cisco HDLC

Physical Layer **Frame Relay**

No-Keepalive: ☐
 Type: ☒ ANSI ☐ ITU

Please configure the sub interface.
 Interface Name: serial1/0. (1~32)
 Inverse ARP: ☐
 Frame Relay DLCI: (16~1022)
 Interface IP:
 Netmask:
 Gateway:

<< Previous Next >> Cancel

Table 15: Fields in T1 Frame Relay Tab Window

Field	Description
No-Keepalive checkbox	Enables no-keepalives.
Type	Sets the frame relay LMI type: <ul style="list-style-type: none"> ■ ANSI: American National Standards Institute supports data rates up to 8Mbps downstream and 1Mbps upstream. ■ ITU: International Telecommunications Union supports data rates of 6.144 Mbps downstream and 640 kbps upstream.
Interface Name	Sets the subinterface name.
Inverse ARP	Enables inverse Address Resolution Protocol for the subinterface.
Frame Relay DLCI	Assigns a data link connection identifier (DLCI) to the subinterface.
Interface IP	Sets the IP address for the subinterface.
Netmask	Sets the netmask for the subinterface.
Gateway	Sets the gateway address for the subinterface.

If you have the T1 mini-PIM installed in your device and you selected the PPP option, the following additional windows are displayed:

- PPP Option with PPP Tab Window
- PPP Option with Peer User Tab Window

Figure 31: PPP Option with PPP Tab Window

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20 device. The wizard is titled 'Initial Configuration Wizard' and features a Juniper SSG 20 logo. Below the logo, there is a message: 'Please click the following links or the above figure to configure interfaces.' followed by three links: [serial1/0\(Untrust Zone\)](#), [bgroup0\(Trust Zone\)](#), and [eth0/1\(DMZ Zone\)](#). The next question is 'How does the Juniper device connect to the outside via serial1/0(T1) interface?'. The 'WAN Encapsulation' options are: ☐ Frame Relay, ☒ PPP, and ☐ Cisco HDLC. Below this, there are three tabs: 'Physical Layer', 'PPP' (which is selected), and 'Peer User'. The 'PPP' tab contains two sections. The first section is 'Please create the PPP profile.' with fields for 'PPP Profile Name:', 'Authentication:' (with radio buttons for Any, CHAP, PAP, and None, where 'Any' is selected), 'Local User:', 'Password:', and a 'Static IP:' checkbox which is checked. The second section is 'Please configure the serial1/0 interface.' with fields for 'Interface IP:', 'Netmask:', and 'Gateway:'. At the bottom of the wizard, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Table 16: Fields in PPP Option with PPP Tab Window

Field	Description
PPP Profile Name	Sets the name of the PPP profile
Authentication	Sets the authentication type
Local User	Sets the name of the local user
Password	Sets the password for the local user
Static IP checkbox	Enables a static IP address
Interface IP	Sets the serialx/0 interface IP address
Netmask	Sets the serialx/0 netmask
Gateway	Sets the serialx/0 gateway address

Figure 32: PPP Option with Peer User Tab Window

Initial Configuration Wizard

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.
[serial1/0\(Untrust Zone\)](#) [hgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

How does the Juniper device connect to the outside via serial1/0(T1) interface?
 WAN Encapsulation: ☐ Frame Relay ☒ PPP ☐ Cisco HDLC

Physical Layer **PPP** Peer User

Peer User:
 Password:
 Status: ☒ Enable ☐ Disable

<< Previous Next >> Cancel

Table 17: Fields in PPP Option with Peer User Tab Window

Field	Description
Peer User	Sets the name of the peer user
Password	Sets the password for the peer user specified in the Peer User text field
Status	Enables or disables PPP

If you have the T1 mini-PIM installed in your device and you selected the Cisco HDLC option, the following window is displayed:

Figure 33: Cisco HDLC Option with Cisco HDLC Tab Window

Initial Configuration Wizard

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.
[serial1/0\(Untrust Zone\)](#) [hgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

How does the Juniper device connect to the outside via serial1/0(T1) interface?
 WAN Encapsulation: ☐ Frame Relay ☐ PPP ☒ Cisco HDLC

Physical Layer **Cisco HDLC**

Interface IP:
 Netmask:
 Gateway:

<< Previous Next >> Cancel

Table 18: Fields in Cisco HDLC Option with Cisco HDLC Tab Window

Field	Description
Interface IP	Sets the IP address for the T1 Cisco HDLC interface
Netmask	Sets the netmask for the T1 Cisco HDLC interface
Gateway	Sets the gateway address for the T1 Cisco HDLC interface

7. E1 Interface Windows

If you have the E1 mini-PIM installed in your device and you selected the Frame Relay option, the following windows are displayed:

- E1 Physical Layer Tab Window
- E1 Frame Relay Tab Window

NOTE: If you have two E1 mini PIMs installed on your device and you select the Multi-link option, you will see two Physical Layer tabs.

Figure 34: E1 Physical Layer Tab Window

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20. At the top, there's a Juniper logo and 'SSG 20'. Below it, a message says: 'Please click the following links or the above figure to configure interfaces.' with links for 'serial1/0(Untrust Zone)', 'eth0/1(DMZ Zone)', and 'bgroup0(Trust Zone)'. The main question is 'How does the Juniper device connect to the outside via serial1/0(E1) interface?'. Under 'WAN Encapsulation', 'Frame Relay' is selected with a radio button, while 'PPP' and 'Cisco HDLC' are unselected. Below this, there are two tabs: 'Physical Layer' (active) and 'Frame Relay'. The 'Physical Layer' tab contains several configuration options: 'Clocking' (External selected, Internal (Lab Use Only) unselected), 'Frame Checksum' (16-bits selected, 32-bits unselected), 'Framing Mode' (with CRC4 selected, without CRC4 and Unframed unselected), 'Idle Cycles Flag' (0x7E selected, 0xFF (All Ones) unselected), 'Start/End Flags' (Filler selected, Share unselected), 'Invert data' (checkbox is unchecked), and 'Time Slots' (0 selected, with a note '(0(all active), 2..32(e.g. 2,7-9))'). At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Table 19: Fields in E1 Physical Layer Tab Window

Field	Description
Clocking	Sets the transmit clock on the interface.
Frame Checksum	Sets the size of checksum. Default is 16 .
Framing Mode	Sets the framing format. Default is without CRC4 .
Idle Cycles Flag	Sets the value that the interface transmits during idle cycles. Default setting is 0x7E : <ul style="list-style-type: none"> ■ 0x7E (flags) ■ 0xFF (ones)
Start/End Flags	Sets the transmission of start and end flags to either filler or shared. The default is filler.
Invert Data checkbox	Enables inverted transmission of unused data bits.
Time Slots	Sets the use of time slots on a T1 interface. Default is 0 , all 32 time slots used.

Figure 35: E1 Frame Relay Tab Window**Table 20: Fields in E1 Frame Relay Tab Window**

Field	Description
No-Keepalive checkbox	Enables no-keepalives.
Type	Sets the frame relay LMI type: <ul style="list-style-type: none"> ■ ANSI: American National Standards Institute supports data rates up to 8Mbps downstream and 1Mbps upstream. ■ ITU: International Telecommunications Union supports data rates of 6.144 Mbps downstream and 640 kbps upstream.
Interface Name	Sets the subinterface name.
Inverse ARP checkbox	Enables inverse Address Resolution Protocol (ARP) for the subinterface.
Frame Relay DLCI	Assigns a DLCI to the subinterface.

Field	Description
Interface IP	Sets the IP address for the subinterface
Netmask	Sets the netmask for the subinterface
Gateway	Sets the gateway address for the subinterface

To configure the E1 interface with PPP options, see “PPP Option with PPP Tab Window” on page 71.

To configure the E1 interface with the Cisco HDLC, see “Cisco HDLC Option with Cisco HDLC Tab Window” on page 72.

8. ISDN Interface Windows

If you have the ISDN mini-PIM installed in your device, you can configure the brix/0 (Untrust) interface using the following window.

NOTE: If you have two ISDN mini PIMs installed in your device and you selected the Multi-link option, you will see two Physical Layer tabs.

Figure 36: ISDN Physical Layer Tab Window

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20 device. At the top, there's a navigation bar with icons for various configuration sections. Below this, a message says: 'Please click the following links or the above figure to configure interfaces.' with links to [bri1/0\(Untrust_Zone\)](#), [bgroup0\(Trust_Zone\)](#), and [eth0/1\(DMZ_Zone\)](#).

The main question is: 'How does the Juniper device connect to the outside via bri1/0 interface?'. There are two options: 'Leased Line Mode (128Kbps):' with an unchecked checkbox, and 'Dial Using BRI:' with an unchecked checkbox.

Below this, there are two tabs: 'Physical Layer' (selected) and 'Dialer Interface'. The 'Physical Layer' tab contains the following fields:

- Switch Type: A dropdown menu set to 'European Variants'.
- SPID1: A text input field with '(Optional)' to its right.
- SPID2: A text input field with '(Optional)' to its right.
- TEI Negotiation: Two radio buttons, 'First Call' (selected) and 'Power UP'.
- Calling Number: A text input field with '(Optional)' to its right.
- Sending Complete: An unchecked checkbox.

At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Table 21: Fields in ISDN Physical Layer Tab Window

Field	Description
Switch Type	Sets the service provider switch type: <ul style="list-style-type: none"> ■ att5e: At&T 5ESS ■ ntdms100: Nortel DMS 100 ■ ins-net: NTT INS-Net ■ etsi: European variants ■ ni1: National ISDN-1
SPID1	Service Provider ID, usually a seven-digit telephone number with some optional numbers. Only the DMS-100 and NI1 switch types require SPIDs. The DMS-100 switch type has two SPIDs assigned, one for each B-channel.
SPID2	Backup service provider ID.
TEI Negotiation	Specifies when to negotiate TEI, either at startup or on the first call. Typically this setting is used for ISDN service offerings in Europe and connections to DMS-100 switches that are designed to initiate TEI negotiation.
Calling Number	ISDN network billing number.
Sending Complete checkbox	Enables sending of complete information to outgoing setup message. Usually only used in Hong Kong and Taiwan.

You can select the bri1/0 interface to connect using dialer, multi-link dialer, leased line, or dial with BRI. Selecting neither, one, or both options displays a window similar to the following.

Figure 37: ISDN Connection Tab Window

Initial Configuration Wizard

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.

[bri1/0\(Untrust_Zone\)](#) [bgroup0\(Trust_Zone\)](#)

[eth0/1\(DMZ_Zone\)](#)

How does the Juniper device connect to the outside via bri1/0 interface?

Leased Line Mode (128kbps): ☐

Dial Using BRI: ☐

Physical Layer **Dialer Interface**

Please create the PPP profile.

PPP Profile Name:

Authentication: ☒ Any ☐ CHAP ☐ PAP ☐ None

Local User:

Password:

Static IP: ☒

Interface Name: dialer 1

Encapsulation Type: ☒ ppp ☐ Multi-Link PPP

Primary Number:

Alternative Number: (Optional)

Dialer Pool:

Interface IP:

Netmask:

Gateway:

<< Previous Next >> Cancel

Table 22: Fields in ISDN Connection Tab Window

Field	Description
PPP Profile Name	Sets a PPP profile name to the ISDN interface.
Authentication	Sets the PPP authentication type: <ul style="list-style-type: none"> ■ Any ■ CHAP: Challenge Handshake Authentication Protocol ■ PAP: Password Authentication Protocol ■ None
Local User	Sets the local user.
Password	Sets the password for the local user.
Static IP checkbox	Enables a static IP address for the interface.
Interface IP	Sets the interface IP address.
Interface Name (Dialer only)	Sets the dialer interface name. Default is dialer.1 .
Encapsulation Type	Sets the encapsulation type on the dialer and dialer using BRI interface. Default is PPP .
Primary Number	Sets the primary number for dialer and dialer using BRI interfaces.
Alternative Number	Sets the alternative (secondary) number to be used when the primary number cannot be used for connectivity.

Field	Description
Dialer Pool (Dialer only)	Sets the dialer pool name for the dialer interface.
Netmask	Sets the netmask.
Gateway	Sets the gateway address.

9. V.92 Modem Interface Window

If you have the V.92 mini-PIM installed in your device, you can configure the serialx/0 (Modem) interface using the following window:

Figure 38: Modem Interface Window

Table 23: Fields in Modem Interface Window

Field	Description
Modem Name	Sets the name for the modem interface
Init String	Sets the initialization string for the modem
ISP Name	Assigns a name to the service provider
Primary Number	Specifies the phone number to access the service provider
Alternative Number (optional)	Specifies an alternative phone number to access the service provider if the primary number does not connect
Login Name	Sets the login name for the service provider account
Password	Sets the password for the login name
Confirm	Confirms the password typed in the Password field

10. Eth0/0 Interface (Untrust Zone) Window

The eth0/0 interface can have a static or a dynamic IP address assigned via DHCP or PPPoE.

Figure 39: Eth0/0 Interface Window
Table 24: Fields in Eth0/0 Interface Window

Field	Description
Dynamic IP via DHCP	Enables the device to receive an IP address for the Untrust zone interface from a service provider.
Dynamic IP via PPPoE	Enables the device to act as a PPPoE client, receiving an IP address for the Untrust zone interface from a service provider. Enter the username and password assigned by the service provider.
Static IP	Assigns a unique and fixed IP address to the Untrust zone interface. Enter the Untrust zone interface IP address, netmask, and gateway address.

11. Eth0/1 Interface (DMZ Zone) Window

The eth0/1 interface can have a static or a dynamic IP address assigned via DHCP.

Figure 40: Eth0/1 Interface Window

Initial Configuration Wizard

Juniper
SSG 20

Please click the following links or the above figure to configure interfaces.
[eth0/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

Enter the IP address and netmask for the interface eth0/1(dmz zone).

☐ Dynamic IP via DHCP

☒ Static IP

Interface IP:

Netmask:

<< Previous Next >> Cancel

Table 25: Fields in Eth0/1 Interface Window

Field	Description
Dynamic IP via DHCP	Enables the device to receive an IP address for the DMZ interface from a service provider.
Static IP	Assigns a unique and fixed IP address to the DMZ interface. Enter the DMZ interface IP and netmask.

12. Bgroup0 Interface (Trust Zone) Window

The bgroup0 interface can have a static or a dynamic IP address assigned via DHCP.

The default interface IP address is **192.168.1.1** with a netmask of **255.255.255.0** or **24**.

Figure 41: Bgroup0 Interface Window

Initial Configuration Wizard

Juniper
SSG 20

Please click the following links or the above figure to configure interfaces.
[eth0/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

Enter the IP address and netmask for the interface bgroup0(trust zone).

☐ Dynamic IP via DHCP

☒ Static IP

Interface IP:

Netmask:

<< Previous Next >> Cancel

Table 26: Fields in Bgroup0 Interface Window

Field	Description
Dynamic IP via DHCP	Enables the device to receive an IP address for the Trust zone interface from a service provider.
Static IP	Assigns a unique and fixed IP address to the Trust zone interface. Enter the Trust zone interface IP address and netmask.

13. Wireless0/0 Interface (Trust Zone) Window

If you are configuring the SSG 20-WLAN device, you must set a Service Set Identifier (SSID) before the wireless0/0 interface can be activated. For detailed instructions about configuring your wireless interface(s), refer to the *Concepts & Examples ScreenOS Reference Guide*.

Figure 42: Wireless0/0 Interface Window

Initial Configuration Wizard

Please click this wlan radio to configure wireless.

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.

[eth0/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#) [wireless0/0\(Trust Zone\)](#)

How do you want to configure wireless0/0 interface(trust zone)?

Wlan Mode: 2.4G(802.11b/g)

SSID:

☒ Open ☐ No Encryption

☐ WPA-PSK ☒ Passphrase(8~63 ASCII):
 Confirm:
☐ PSK(64 hexadecimal):
 Confirm:
 Encryption Type: ☒ Auto ☐ TKIP ☐ AES

Interface IP: 192.168.2.1
 Netmask: 255.255.255.0

<< Previous Next >> Cancel

Table 27: Fields in Wireless0/0 Interface Window

Field	Description
Wlan Mode	Sets the WLAN radio mode: <ul style="list-style-type: none"> ■ 5G (802.11a). ■ 2.4G (802.11b/g). ■ Both (802.11a/b/g).
SSID	Sets the SSID name.
Authentication and Encryption	Sets the WLAN interface authentication and encryption: <ul style="list-style-type: none"> ■ Open authentication, the default, allows anyone to access the device. There is no encryption for this authentication option. ■ WPA Pre-Shared Key authentication sets the Pre-Shared Key (PSK) or passphrase that must be entered when accessing a wireless connection. You can choose to enter a HEX or an ASCII value for the PSK. A HEX PSK must be a 256-bit (64-text character) HEX value. An ASCII passphrase must be 8 to 63 text characters. You must select Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES) as the encryption type for this option, or select Auto to allow either option. ■ WPA2 Pre-Shared Key. ■ WPA Auto Pre-Shared Key.
Interface IP	Sets the WLAN interface IP address.
Netmask	Sets the WLAN interface netmask.

14. Interface Summary Window

After you have configured the WAN interfaces, you will see the Interface Summary window.

Figure 43: Interface Summary Window

The screenshot shows the 'Initial Configuration Wizard' window. At the top, it says 'Before proceeding further, review the following interface settings.' Below this is a section titled 'ISDN Configuration:' containing a table of settings:

Switch Type:	etsi	SPID2:	23488458235
SPID1:	32546564565	Calling Number:	01023456789
TEI Negotiation:	first call	Sending Complete:	enabled
T310 Value:	10	Dialer Enable:	disabled
Leased Line Mode:	disabled	Authentication:	any
PPP Profile:	myprofile	Password:	mypwd
Local User:	myuser	Interface IP:	122.122.122.122
PPP Static IP:	enabled		

Below the table is a text area showing the configuration commands:

```
set interface bri1/0 isdn switch-type etsi
set interface bri1/0 isdn spid1 "32546564565"
set interface bri1/0 isdn spid2 "23488458235"
set interface bri1/0 isdn tei-negotiation first-call
set interface bri1/0 isdn calling-number "01023456789"
set interface bri1/0 isdn t310-value "10"
```

At the bottom, it says 'Click Next to enter other configuration' and has three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Check your interface configuration, then click **Next** when ready to proceed. The Physical Ethernet DHCP Interface window appears.

15. Physical Ethernet DHCP Interface Window

Select **Yes** to enable your device to assign IP addresses to your wired network via DHCP. Enter the IP address range that you want your device to assign to clients using your network, then click **Next**.

Figure 44: Physical Ethernet DHCP Interface Window

The screenshot shows a window titled "Initial Configuration Wizard". The text inside asks: "Do you want the Juniper device to dynamically assign IP addresses to your local **wired** hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses." There are two radio buttons: "Yes" and "No". The "No" button is selected. Below the "Yes" button, there are four input fields: "IP Address Range Start" (192.168.1.33), "End" (192.168.1.126), "DNS Server 1 (optional)", and "DNS Server 2 (optional)". At the bottom, there are three buttons: "<< Previous", "Next >>", and "Cancel".

16. Wireless DHCP Interface Window

Select **Yes** to enable your device to assign IP addresses to your wireless network via DHCP. Enter the IP address range that you want your device to assign to clients using your network, then click **Next**.

Figure 45: Wireless DHCP Interface Window

The screenshot shows a window titled "Initial Configuration Wizard". The text inside asks: "Do you want the Juniper device to dynamically assign IP addresses to your local **wireless** hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses." There are two radio buttons: "Yes" and "No". The "No" button is selected. Below the "Yes" button, there are four input fields: "IP Address Range Start" (192.168.2.33), "End" (192.168.2.126), "DNS Server 1 (optional)", and "DNS Server 2 (optional)". At the bottom, there are three buttons: "<< Previous", "Next >>", and "Cancel".

17. Confirmation Window

Confirm your device configuration and change as needed. Click **Next** to save, reboot the device, and run the configuration.

Figure 46: Confirmation Window



Initial Configuration Wizard

Before proceeding further, review the following all device settings.

Admin Login:	netscreen		Password:	*****
Device is in NAT mode.				
ISDN Configuration:				
Switch Type:	etsi		SPID2:	23488458235
SPID1:	32546564565		TEI Negotiation:	first call
TEI Negotiation:	first call		Calling Number:	01023456789
T310 Value:	10		Sending Complete:	enabled
Leased Line Mode:	disabled		Dialer Enable:	disabled
PPP Profile:	myprofile		Authentication:	any

```

set admin password "netscreen"
set interface bri1/0 isdn switch-type etsi
set interface bri1/0 isdn spid1 "32546564565"
set interface bri1/0 isdn spid2 "23488458235"
set interface bri1/0 isdn tei-negotiation first-call
set interface bri1/0 isdn calling-number "01023456789"
  
```

Click Next to save CLI into device.

<< Previous Next >> Cancel

After the device reboots with the saved system configuration, the WebUI login prompt appears. For information on how to access the device using the WebUI, refer to “Using the WebUI” on page 29.

Index

A

AAL5 multiplexing.....	41
ADSL	
configuring interface	41
connecting the cable	24
connecting the port	24
Annex A	24
Annex B	24
antennae.....	26
ATM Adaptation Layer 5.....	41

B

backup interface to Untrust zone	37
--	----

C

cables	
ADSL.....	24
basic network connections.....	23
serial.....	24
certifications	
EMC (Emissions)	59
EMC Immunity.....	59
European Telecommunications Standards Institute (ETSI).....	59
safety.....	59
T1 Interface	60
configuration	
admin name and password.....	33
administrative access.....	35
ADSL 2/2 + mini-PIM	41
backup untrust interface.....	37
bridge groups (bgroup).....	34
date and time	34
default route	36
E1 mini-PIM.....	46
host and domain name.....	36
ISDN mini-PIM	45
management address.....	36
management services	35
T1 mini-PIM.....	46
USB.....	17
V.92 Modem mini-PIM.....	47
virtual circuits.....	42
VPI/VCI pair	42
wireless and Ethernet combined	40
wireless authentication and encryption.....	38
connection, basic network	23

D

default ip addresses.....	32
---------------------------	----

I

ISP IP address and netmask.....	44
---------------------------------	----

L

LEDs	
activity link on Ethernet ports	13
PIM 1	11
PIM 2	12
POWER	11
STATUS	11

M

management	
through a console	28
through a Telnet connection.....	30
through the WebUI	29
memory upgrade procedure	54
Mini-PIM	
blank faceplate	52
installation	53
removal	52
multiplexing, configuring.....	42

P

Point-to-Point Protocol over ATM	
<i>See</i> PPPoA	
Point-to-Point Protocol over Ethernet	
<i>See</i> PPPoE	
PPPoA	41
PPPoE.....	41

R

radio transceivers	
WLAN 0	16
WLAN 1	16
reset pinhole, using	49

S

static IP address.....	41
------------------------	----

U

Untrust zone, configuring backup interface	37
--	----

V

Virtual Path Identifier/Virtual Channel Identifier	
<i>See</i> VPI/VCI	

VPI/VCI	
configuring	42
values	41

W

wireless	
antennae	26
using the default interface	26
WLAN LEDs	
802.11a	12
b/g	12

Table des matières

	À propos du présent guide	5
	Organisation	6
	Conventions de l'interface utilisateur Web	6
	Conventions CLI	7
	Obtention de la documentation et d'une assistance technique	8
Chapitre 1	Présentation matérielle	9
	Ports et connecteurs d'alimentation	10
	Panneau avant	11
	DEL d'état système	11
	Descriptions des ports	13
	Ports Ethernet	13
	Port Console	13
	Port AUX	14
	Descriptions des ports des mini-modules d'interface physique	14
	Panneau arrière	16
	Adaptateur électrique	16
	Émetteurs-récepteurs radio	16
	Œillet du câble de mise à la terre	17
	Types d'antennes	17
	Port USB	17
Chapitre 2	Installation et connexion de l'appareil	19
	Avant-propos	20
	Installation de l'équipement	20
	Connexion des câbles d'interface à un appareil	22
	Connexion de l'alimentation	22
	Connexion de l'appareil à un réseau	23
	Connexion de l'appareil à un réseau non sécurisé	23
	Ports Ethernet	24
	Ports série (AUX/Console)	24
	Connexion des mini-modules d'interface physique à un réseau non sécurisé	24
	Mini-module d'interface physique ADSL2/2 +	24
	Mini-modules d'interface physique RNIS, T1, E1 et V.92	25
	Connexion de l'appareil à un réseau interne ou un poste de travail	26
	Ports Ethernet	26
	Antennes sans fil	26
Chapitre 3	Configuration de l'appareil	27
	Accès à l'appareil	28
	Utilisation d'une connexion de console	28
	Utilisation de l'interface utilisateur Web	29

Utilisation de Telnet.....	30
Paramètres par défaut de l'appareil	31
Configuration de base de l'appareil	33
Nom et mot de passe de l'administrateur racine	33
Date et heure.....	34
Interfaces du groupe pont.....	34
Accès administratif	35
Services de gestion	35
Nom d'hôte et nom de domaine.....	36
Route par défaut.....	36
Adresse de l'interface de gestion	36
Configuration de l'interface non sécurisée secondaire	37
Configuration sans fil de base	37
Configuration des mini-modules d'interface physique.....	41
Interface ADSL2/2 +	41
Circuits virtuels	42
VPI/VCI et méthode de multiplexage	42
PPPoE ou PPPoA.....	43
Adresse IP statique et masque de réseau	44
Interface RNIS	45
Interface T1	46
Interface E1	46
Interface à modem V.92.....	47
Protections pare-feu de base	48
Vérification de la connectivité externe	49
Restauration des paramètres par défaut de l'appareil	49
Chapitre 4 Entretien de l'appareil	51
Pièces et outils nécessaires	51
Remplacement d'un mini-module d'interface physique	51
Dépose d'une plaque avant de protection.....	52
Dépose d'un mini-module d'interface physique.....	52
Installation d'un mini-module d'interface physique	53
Mise à niveau de la mémoire	55
Annexe A Spécifications	59
Spécifications physiques	60
Spécifications électriques	60
Tolérance environnementale.....	60
Homologations.....	61
Sécurité	61
Émissions CEM.....	61
Immunité CEM	61
ETSI.....	61
Interface T1	62
Connecteurs.....	62
Annexe B Initial Configuration Wizard	65
Index.....	89

À propos du présent guide

L'appareil Secure Services Gateway (SSG) 20 de Juniper Networks est une plate-forme de routeur et de pare-feu intégrée qui offre des services de pare-feu et de réseau privé virtuel IPSec (Internet Protocol Security) à une succursale ou un point de vente.

Juniper Networks propose deux modèles de SSG 20 :

- SSG 20, qui prend en charge la connectivité auxiliaire (AUX),
- SSG 20-WLAN, qui prend en charge les normes sans fil 802.11 a/b/g intégrées.

Les deux appareils SSG 20 prennent en charge un emplacement de stockage USB (universal serial bus) et deux connecteurs de mini-modules d'interface physique qui acceptent tous les types de mini-modules d'interface physique. Les appareils proposent également des conversions de protocoles entre les réseaux locaux et les réseaux étendus.

REMARQUE : les exemples et instructions de configuration du présent document sont basés sur les fonctionnalités d'un appareil exécutant ScreenOS 5.4. Selon la version de ScreenOS exécutée, il est possible que votre appareil fonctionne différemment. Pour obtenir la dernière documentation de l'appareil, consultez le site Web de Juniper Networks Technical Publications à l'adresse <http://www.juniper.net/techpubs/hardware>. Pour connaître les versions de ScreenOS actuellement disponibles pour votre appareil, reportez-vous au site Web de l'assistance de Juniper Networks à l'adresse <http://www.juniper.net/customers/support/>.

Organisation

Le présent guide présente les sections suivantes :

- Le chapitre 1, « Présentation matérielle, » détaille le châssis et les composants d'un appareil SSG 20.
- Le chapitre 2, « Installation et connexion de l'appareil, » détaille la procédure de montage de l'appareil SSG 20 et de connexion des câbles et de l'alimentation à l'appareil.
- Le chapitre 3, « Configuration de l'appareil, » détaille la configuration et la gestion d'un appareil SSG 20, ainsi que les procédures d'exécution de tâches de configuration de base.
- Le chapitre 4, « Entretien de l'appareil, » détaille les procédures d'entretien et de maintenance des appareils SSG 20.
- L'annexe A, « Spécifications, » détaille les spécifications système générales des appareils SSG 20.
- L'annexe B, « Initial Configuration Wizard, » fournit des informations détaillées au sujet de l'utilisation de l'Initial Configuration Wizard (Assistant de configuration initiale) avec un appareil SSG 20.

Conventions de l'interface utilisateur Web

Pour procéder à une tâche à l'aide de l'interface utilisateur Web, vous devez d'abord accéder à la boîte de dialogue adaptée, dans laquelle vous pouvez ensuite définir les objets et les paramètres. Un chevron (>) indique la séquence de navigation dans l'interface utilisateur Web, séquence que vous suivez en cliquant sur les options de menu et les liens. L'ensemble d'instructions correspondant à chaque tâche est divisé de la manière suivante : un chemin de navigation et des paramètres de configuration.

La figure suivante indique le chemin vers la boîte de dialogue de configuration des adresses, avec les paramètres de configuration suivants :

Objects > Addresses > List > New : saisissez les informations suivantes, puis cliquez sur **OK** :

Address Name: addr_1
IP Address/Domain Name:
 IP/Netmask: (sélection), 10.2.2.5/32
Zone: Untrust

Figure 1 : chemin de navigation et paramètres de configuration

Conventions CLI

Les conventions suivantes sont utilisées pour présenter la syntaxe des commandes CLI dans les exemples et dans le texte.

Dans les exemples :

- 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 de l'interface ethernet1, ethernet2 ou ethernet3 ».

- Les variables sont en *italique* :

```
set admin user nom1 password xyz
```

Dans le texte :

- Les commandes sont en **gras**.
- Les variables sont en *italique*.

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 kathleen j12fmt54**, il vous suffit de saisir **set adm u kath j12fmt54**. Vous pouvez utiliser ce système de saisie rapide pour les commandes. Les commandes détaillées dans cette documentation sont cependant proposées dans leur version intégrale.

Obtention de la documentation et d'une assistance technique

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

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

Si vous trouvez des erreurs ou des omissions dans le présent document, veuillez nous contacter à l'adresse électronique suivante :

techpubs-comments@juniper.net

Chapitre 1

Présentation matérielle

Ce chapitre fournit des descriptions détaillées du châssis et des composants de l'appareil SSG 20. Il présente les sections suivantes :

- « Ports et connecteurs d'alimentation », page 10
- « Panneau avant », page 11
- « Panneau arrière », page 16

Ports et connecteurs d'alimentation

Cette section détaille et affiche l'emplacement des connecteurs d'alimentation et des ports intégrés. Reportez-vous à la figure suivante pour connaître l'emplacement des ports intégrés et au Tableau 1 pour consulter les descriptions des connecteurs d'alimentation.

Figure 2 : emplacement des mini-modules d'interface physique et des ports intégrés

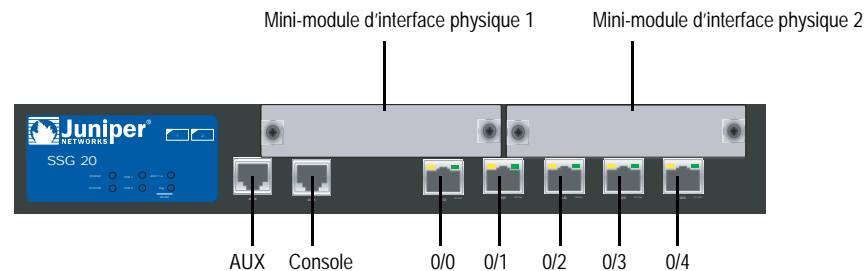


Tableau 1 : ports et connecteurs d'alimentation d'un appareil SSG 20

Port	Description	Connecteur	Vitesse/protocole
0/0-0/4	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 permet également de gérer l'appareil par l'intermédiaire d'une session Telnet ou de l'interface utilisateur Web.	RJ-45	Ethernet 10/100 Mbits/s Détection automatique du mode duplex et MDI/MDIX automatique
USB	Permet d'établir une connexion USB 1.1 avec le système.	S/O	12M (pleine vitesse) ou 1,5M (vitesse réduite)
Console	Permet d'établir une connexion série avec le système. Utilisé pour la connectivité d'émulation du terminal dans le cadre du lancement de sessions CLI.	RJ-45	9 600 bits/s/RS-232C série
AUX	Permet d'établir une connexion série asynchrone RS-232 secondaire à Internet par l'intermédiaire d'un modem externe.	RJ-45	9 600 bits/s – 115 Kbits/s/RS-232C série
Mini-module d'interface physique			
ADSL 2/2 +	Permet d'établir une connexion Internet au travers d'une liaison de données ADSL.	RJ-11 (annexe A) RJ-45 (annexe B)	ANSI T1.413 Issue 2 (annexe A uniquement) ITU G.992.1 (G.dmt) ITU G.992.3 (ADSL2) ITU G.992.5 (ADSL2 +)
Modem V.92	Permet d'établir une connexion principale ou secondaire à un fournisseur de services via Internet ou un réseau non sécurisé.	RJ-11	9 600 bits/s – 115 Kbits/s/RS-232 série, détection automatique du mode duplex et de la polarité
T1	Permet d'établir une connexion à la ligne T1 du réseau non sécurisé.	RJ-45	1 544 Mbits/s (connecteurs à plein temps)
E1	Permet d'établir une connexion à la ligne E1 du réseau non sécurisé.	RJ-45	2 048 Mbits/s (connecteurs à plein temps)

Port	Description	Connecteur	Vitesse/protocole
RNIS	Permet d'utiliser la ligne RNIS comme interface non sécurisée ou secondaire (S/T).	RJ-45	Canaux B à 64 Kbits/s Ligne louée à 128 Kbits/s
Antennes A et B (SSG 20-WLAN)	Permet d'établir une connexion directe avec des postes de travail se trouvant à proximité d'une connexion radio sans fil.	RPSMA	802.11 a (54 Mbits/s sur une bande de signaux radioélectriques de 5 GHz) 802.11 b (11 Mbits/s sur une bande de signaux radioélectriques de 2,4 GHz) 802.11 g (54 Mbits/s sur une bande de signaux radioélectriques de 2,4 GHz) 802.11 superG (108 Mbits/s sur des bandes de signaux radioélectriques de 2,4 et 5 GHz)

Panneau avant

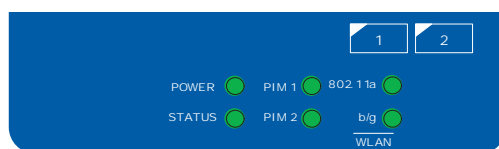
Cette section détaille les éléments suivants du panneau avant d'un appareil SSG 20 :

- DEL d'état système
- Descriptions des ports
- Descriptions des ports des mini-modules d'interface physique

DEL d'état système

Les DEL d'état système affichent des informations relatives aux fonctions essentielles de l'appareil. La Figure 3 illustre la position de chaque DEL d'état sur le panneau avant de l'appareil SSG 20-WLAN. Les DEL de réseau local sans fil sont uniquement présentes sur l'appareil SSG 20-WLAN.

Figure 3 : DEL d'état



Au démarrage du système, la DEL d'alimentation (POWER) se met à clignoter en vert et la DEL d'état (STATUS) change selon la séquence suivante : rouge, vert, clignotant en vert. Le démarrage nécessite environ deux minutes. Si vous souhaitez mettre le système hors tension, puis de nouveau sous tension, nous vous recommandons d'attendre quelques secondes entre l'arrêt et le redémarrage. Le Tableau 2 présente le nom, la couleur, l'état et la description de chaque DEL d'état système.

Tableau 2 : descriptions des DEL d'état

Nom	Couleur	État	Description
POWER	Vert	Allumée	Indique que le système est sous tension.
		Éteinte	Indique que le système n'est pas sous tension.
	Rouge	Allumée	Indique que l'appareil ne fonctionne pas normalement.
		Éteinte	Indique que l'appareil fonctionne normalement.
STATUS	Vert	Allumée	Indique que le système est en cours de démarrage ou procède à des diagnostics.
		Clignotante	Indique que l'appareil fonctionne normalement.
	Rouge	Clignotante	Indique qu'une erreur a été détectée.
PIM 1 (MODULE D'INTERFACE PHYSIQUE 1)	Vert	Allumée	Indique que le mini-module d'interface physique fonctionne.
		Clignotante	Indique que le trafic est en cours de transfert au niveau du mini-module d'interface physique.
		Éteinte	Indique que le mini-module d'interface physique ne fonctionne pas.
PIM 2 (MODULE D'INTERFACE PHYSIQUE 2)	Vert	Allumée	Indique que le mini-module d'interface physique fonctionne.
		Clignotante	Indique que le trafic est en cours de transfert au niveau du mini-module d'interface physique.
		Éteinte	Indique que le mini-module d'interface physique ne fonctionne pas.
WLAN (RÉSEAU LOCAL SANS FIL) (sur l'appareil de réseau local sans fil uniquement)			
802.11 a	Vert	Allumée	Indique qu'une connexion sans fil est établie mais qu'il n'y a pas d'activité de liaison.
		Clignotement lent	Indique qu'une connexion sans fil est établie. Le débit en bauds est proportionnel à l'activité de la liaison.
		Éteinte	Indique qu'aucune connexion sans fil n'a été établie.
b/g	Vert	Allumée	Indique qu'une connexion sans fil est établie mais qu'il n'y a pas d'activité de liaison.
		Clignotement lent	Indique qu'une connexion sans fil est établie. Le débit en bauds est proportionnel à l'activité de la liaison.
		Éteinte	Indique qu'aucune connexion sans fil n'a été établie.

Descriptions des ports

Cette section détaille l'objectif et le fonctionnement des éléments suivants :

- Ports Ethernet
- Port Console
- Port AUX

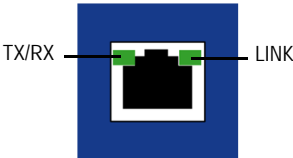
Ports Ethernet

Cinq ports Ethernet 10/100 permettent d'établir des connexions de réseau local à des hubs, commutateurs, serveurs locaux et postes de travail. Vous pouvez également utiliser un port Ethernet dans le cadre de la gestion du trafic. Les ports sont numérotés de **0/0** à **0/4**. Reportez-vous à la section « Paramètres par défaut de l'appareil », page 31 pour connaître les liaisons de zone par défaut de chaque port Ethernet.

Lors de la configuration d'un des ports, reportez-vous au nom d'interface correspondant à l'emplacement du port. Les noms d'interface des ports sont numérotés, de gauche à droite sur le panneau avant, de **ethernet0/0** à **ethernet0/4**.

La Figure 4 affiche l'emplacement des DEL de chaque port Ethernet.

Figure 4 : emplacement des DEL de liaison d'activité



Le Tableau 3 détaille les DEL des ports Ethernet.

Tableau 3 : DEL des ports de réseau local

Nom	Couleur	État	Description
LINK (LIAISON)	Vert	Allumée	Le port est en ligne.
		Éteinte	Le port est hors ligne.
TX/RX	Vert	Clignotante	Le trafic est en cours de transfert. Le débit en bauds est proportionnel à l'activité de la liaison.
		Éteinte	Il est possible que le port soit actif, il ne reçoit cependant pas de données.

Port Console

Le port Console est un port série RJ-45 câblé comme un équipement de terminaison de circuit de données et qui peut être utilisé dans le cadre de l'administration locale. Utilisez un câble direct lors de la connexion à un terminal et un câble de raccords croisés lors de la connexion à un autre équipement de terminaison de circuit de données. Un adaptateur RJ-45/DB-9 est fourni.

Reportez-vous à la section « Connecteurs », page 62 pour les schémas de brochage des connecteurs RJ-45.

Port AUX

Le port auxiliaire (AUX) est un port série RJ-45 câblé comme un équipement terminal de traitement de données et qui peut être connecté à un modem de manière à permettre l'administration à distance. Nous ne vous recommandons pas d'utiliser ce port dans le cadre de l'administration à distance normale. Le port AUX est généralement attribué à l'interface série secondaire. Le débit en bauds peut être compris entre 9 600 et 115 200 bits/s et nécessite un contrôle de flux matériel. Utilisez un câble direct lors de la connexion à un modem et un câble de raccords croisés lors de la connexion à un autre équipement terminal de traitement de données.

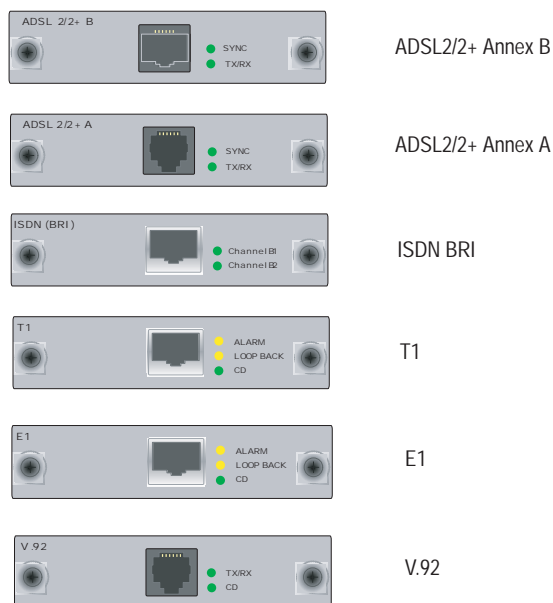
Reportez-vous à la section « Connecteurs », page 62 pour les schémas de brochage des connecteurs RJ-45.

Descriptions des ports des mini-modules d'interface physique

Chaque mini-module d'interface physique pris en charge dans un appareil dispose des composants suivants :

- Un port de connecteur de câble — accepte les connecteurs de supports réseau. La Figure 5 présente les mini-modules d'interface physique disponibles. Vous pouvez installer un maximum de deux mini-modules d'interface physique sur un appareil.

Figure 5 : mini-modules d'interface physique de l'appareil SSG 20



- Deux à trois DEL d'état — indiquent l'état des ports. Le Tableau 4 détaille la signification des différents états des DEL.

Tableau 4 : états des DEL des mini-modules d'interface physique de l'appareil SSG 20

Type	Nom	Couleur	État	Description
ADSL 2/2 + (annexes A et B)	SYNC	Vert	Allumée	Indique que l'interface ADSL est formée.
			Clignotante	Indique que la formation est en cours.
			Éteinte	Indique que l'interface est inactive.
	TX/RX	Vert	Clignotante	Indique que le trafic est en cours de transfert.
			Éteinte	Indique que le trafic n'est pas en cours de transfert.
ISDN (RNIS) (BRI)	CH B1 (CANAL B1)	Vert	Allumée	Indique que le canal B 1 est actif.
			Éteinte	Indique que le canal B 1 n'est pas actif.
	CH B2 (CANAL B2)	Vert	Allumée	Indique que le canal B 2 est actif.
			Éteinte	Indique que le canal B 2 n'est pas actif.
T1/E1	ALARM (ALARME)	Jaune	Allumée	Indique le déclenchement d'une alarme locale ou distante, l'appareil a détecté une anomalie.
			Éteinte	Indique l'absence d'alarme ou d'anomalie.
	LOOP BACK (BOUCLE AVEC RETOUR)	Jaune	Allumée	Indique qu'une boucle avec retour ou un état de ligne a été détecté.
			Éteinte	Indique que la boucle avec retour n'est pas active.
	CD	Vert	Allumée	Indique qu'une porteuse a été détectée et que la DSU/CSU interne du mini-module d'interface physique communique avec une autre DSU/CSU.
			Éteinte	Indique que la détection de porteuse n'est pas active.
V.92	CD	Vert	Allumée	Indique que la liaison est active.
			Éteinte	Indique que l'interface série n'est pas en fonctionnement.
	TX/RX	Vert	Clignotante	Indique que le trafic est en cours de transfert.
			Éteinte	Indique que le trafic n'est pas en cours de transfert.



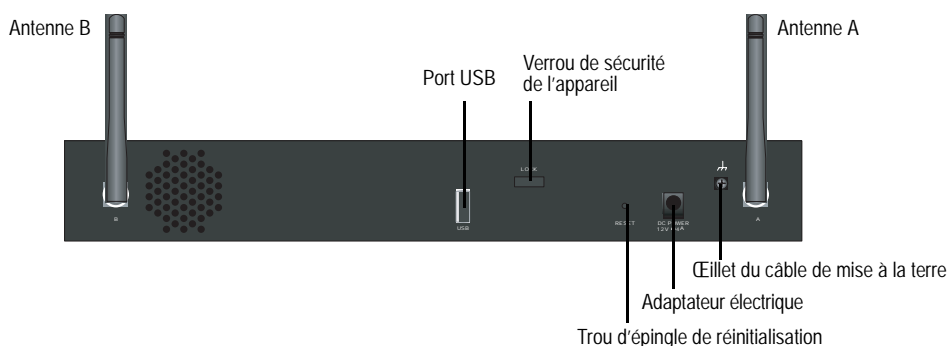
ATTENTION : les mini-modules d'interface physique ne sont pas remplaçables à chaud. Vous devez les installer dans les connecteurs du panneau avant avant de mettre l'appareil sous tension.

Panneau arrière

Cette section détaille les éléments suivants du panneau arrière d'un appareil SSG 20 :

- Adaptateur électrique
- Émetteurs-récepteurs radio
- Œillet du câble de mise à la terre
- Types d'antennes
- Port USB

Figure 6 : panneau arrière d'un appareil SSG 20-WLAN



Adaptateur électrique

La DEL POWER située sur le panneau avant de l'appareil est allumée en vert ou éteinte. L'allumage en vert indique un fonctionnement correct, l'extinction de la DEL indique une anomalie de l'adaptateur électrique ou que l'appareil est éteint.

Émetteurs-récepteurs radio

L'appareil SSG 20-WLAN dispose de deux émetteurs-récepteurs radio à connectivité sans fil, qui prennent en charge les normes 802.11a/b/g. Le premier émetteur-récepteur (WLAN 0) utilise la bande de signaux radioélectriques de 2,4 GHz, qui prend en charge la norme 802.11b à 11 Mbit/s, la norme 802.11g à 54 Mbit/s et la norme 802.11 SuperG à 108 Mbit/s. Le deuxième émetteur-récepteur (WLAN 1) utilise la bande de signaux radioélectriques de 5 GHz, qui prend en charge la norme 802.11a à 54 Mbit/s. Pour plus d'informations au sujet de la configuration de la bande de signaux radioélectriques sans fil, voir « Configuration sans fil de base », page 37.

Œillet du câble de mise à la terre

L'arrière du châssis est équipé d'un œillet de mise à la terre qui permet de relier l'appareil à la terre (reportez-vous à la Figure 6).

Pour mettre l'appareil à la terre avant de raccorder l'alimentation, connectez un câble de mise à la terre à la terre, puis fixez le câble à l'œillet situé à l'arrière du châssis.

Types d'antennes

L'appareil SSG 20-WLAN prend en charge trois types d'antennes radio spéciales :

- **Antennes de diversité** — les antennes de diversité présentent une couverture bidirectionnelle de 2 dBi et un niveau relativement uniforme d'intensité du signal au sein de la zone de couverture. Elles sont adaptées à la plupart des installations. Ce type d'antennes est livré avec l'appareil.
- **Antenne omnidirectionnelle externe** — l'antenne externe dispose d'une couverture omnidirectionnelle de 2 dBi. Contrairement aux antennes de diversité, qui fonctionnent par paire, l'antenne externe supprime l'effet d'écho qui est parfois généré par des caractéristiques de réception du signal légèrement retardées lors de l'utilisation de deux antennes.
- **Antenne directionnelle externe** — l'antenne directionnelle externe dispose d'une couverture unidirectionnelle de 2 dBi et est adaptée aux lieux tels que les couloirs et les murs extérieurs (avec l'antenne orientée vers l'intérieur).

Port USB

Le port USB situé sur le panneau arrière de l'appareil SSG 20 accepte les périphériques de stockage USB (universal serial bus) ou les adaptateurs de périphériques de stockage USB avec disque CompactFlash intégré, comme indiqué dans la *Spécification CompactFlash* publiée par la CompactFlash Association. Lorsque le périphérique de stockage USB est installé et configuré, il sert automatiquement d'appareil de démarrage secondaire en cas d'anomalie du disque CompactFlash principal lors du démarrage.

Le port USB permet de transférer des fichiers, tels que des configurations de l'appareil ou des certifications utilisateur, et de mettre les images des versions à jour entre un périphérique de stockage USB externe et l'emplacement de stockage Flash interne, situé dans l'appareil de sécurité. Le port USB prend en charge la spécification USB 1.1 lorsque le transfert de fichiers a lieu à faible vitesse (1,5M) ou à vitesse élevée (12M).

Procédez comme suit pour transférer des fichiers entre le périphérique de stockage USB et l'appareil SSG 20 :

1. Insérez le périphérique de stockage USB dans le port USB de l'appareil de sécurité.
2. Enregistrez les fichiers du périphérique de stockage USB dans l'emplacement de stockage Flash interne de l'appareil à l'aide de la commande CLI **save {software | config | image-key} from usb nomdefichier to flash**.
3. Avant de retirer le périphérique de stockage USB, arrêtez le port USB à l'aide de la commande CLI **exec usb-device stop**.
4. Vous pouvez désormais retirer le périphérique de stockage USB en toute sécurité.

Si vous souhaitez supprimer un fichier du périphérique de stockage USB, utilisez la commande CLI **delete file** *usb:/nomdefichier*.

Si vous souhaitez afficher les informations relatives aux fichiers enregistrés sur le périphérique de stockage USB ou dans l'emplacement de stockage Flash interne, utilisez la commande CLI **get file**.

Chapitre 2

Installation et connexion de l'appareil

Ce chapitre détaille la procédure de montage de l'appareil SSG 20 et de connexion des câbles et de l'alimentation à l'appareil. Ce chapitre présente les sections suivantes :

- « Avant-propos », page 20
- « Installation de l'équipement », page 20
- « Connexion des câbles d'interface à un appareil », page 22
- « Connexion de l'alimentation », page 22
- « Connexion de l'appareil à un réseau », page 23

REMARQUE : pour les instructions et consignes de sécurité, reportez-vous au manuel *Juniper Networks Security Products Safety Guide*. Avant de travailler sur les équipements, vous devez vous renseigner au sujet des risques présentés par les circuits électriques et vous familiariser avec les pratiques standard de prévention des accidents.

Avant-propos

L'emplacement du châssis, la disposition de l'équipement de montage et la sécurité de votre local électrique sont essentiels au bon fonctionnement du système.



AVERTISSEMENT : pour empêcher tout abus ou toute intrusion de personnes non autorisées, installez l'appareil SSG 20 dans un environnement sécurisé.

Afin de prévenir toute blessure corporelle et d'éviter toute défaillance ou panne du matériel, prenez les précautions suivantes :

- Avant installation, vérifiez toujours que le bloc d'alimentation n'est raccordé à aucune source d'alimentation.
- Assurez-vous que la pièce dans laquelle vous utilisez l'appareil présente une ventilation adaptée et que la température de la pièce ne dépasse pas 40 °C (104 °F).
- Ne placez pas l'appareil dans une baie d'installation de matériel qui obstrue les orifices d'entrée et d'échappement de l'air. Assurez-vous que les baies fermées disposent de ventilateurs et de fentes sur les côtés.
- Rectifiez les situations à risques suivantes avant toute installation : sols humides ou mouillés, fuites, câbles d'alimentation non mis à la terre ou dénudés ou absence de mise à la terre de sécurité.

Installation de l'équipement

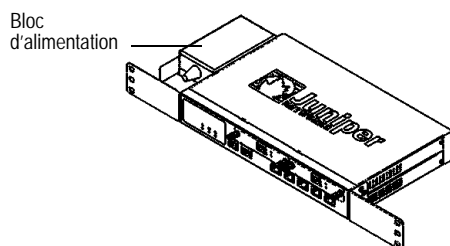
Vous pouvez installer les appareils SSG 20 de manière frontale, sur un mur ou sur un bureau. Les kits de montage sont disponibles séparément.

Dans le cadre de l'installation d'un appareil SSG 20, un tournevis cruciforme numéro 2 (non fourni) et des vis compatibles avec la baie de matériel (incluses dans le kit) sont nécessaires.

REMARQUE : lors de l'installation d'un appareil, assurez-vous qu'il se trouve à portée de la prise électrique.

Procédez comme suit pour installer un appareil SSG 20 de manière frontale dans une baie de matériel standard de 19 pouces :

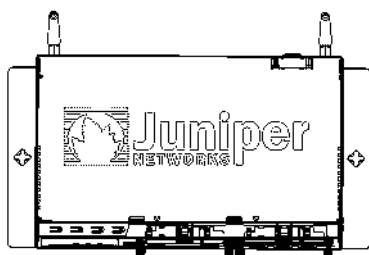
Figure 7 : installation frontale de l'appareil SSG 20



1. Alignez la patte de montage en baie du bloc d'alimentation sur le côté avant gauche de l'appareil.
2. Placez les vis dans les orifices et serrez-les à l'aide d'un tournevis cruciforme.
3. Alignez l'autre patte de montage en baie sur le côté avant droit de l'appareil.
4. Placez les vis dans les orifices et serrez-les à l'aide d'un tournevis cruciforme.
5. Installez l'appareil sur la baie à l'aide des vis fournies.
6. Branchez le bloc d'alimentation dans la prise électrique.

Procédez comme suit pour installer un appareil SSG 20 sur un mur :

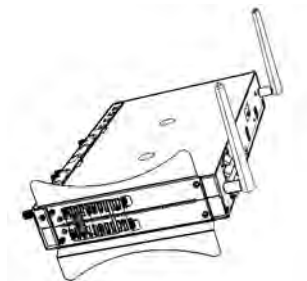
Figure 8 : installation murale de l'appareil SSG 20



1. Alignez les pattes de montage mural sur l'appareil.
2. Placez les vis dans les orifices et serrez-les à l'aide d'un tournevis cruciforme.
3. Assurez-vous que le mur à utiliser est lisse, plat, sec et solide.
4. Installez l'appareil sur le mur à l'aide des vis fournies.
5. Branchez le bloc d'alimentation dans la prise électrique.

Procédez comme suit pour installer un appareil SSG 20 sur un bureau :

Figure 9 : installation de l'appareil SSG 20 sur un bureau



1. Fixez le support du bureau sur le côté de l'appareil. Nous vous recommandons d'utiliser le côté situé le plus près de l'adaptateur électrique.
2. Placez l'appareil installé sur le bureau.
3. Branchez l'adaptateur électrique et raccordez le bloc d'alimentation à une prise électrique.

Connexion des câbles d'interface à un appareil

Procédez comme suit pour raccorder le câble d'interface à un appareil :

1. Préparez une certaine longueur du type de câble utilisé par l'interface.
2. Insérez le connecteur de câble dans le port de connecteur de câble de la plaque avant de l'interface.
3. Disposez le câble de la manière suivante afin d'éviter qu'il ne se détache ou qu'il ne développe des points de tension :
 - a. Fixez le câble de manière à ce qu'il ne soutienne pas son propre poids lorsqu'il est suspendu.
 - b. Placez le surplus de câble dans une boucle bien enroulée de manière à ce que le câble ne soit pas gênant.
 - c. Utilisez des éléments de fixation pour maintenir la forme des boucles de câble.

Connexion de l'alimentation

Procédez comme suit pour raccorder l'appareil à l'alimentation :

1. Insérez la fiche CC située 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 dans une source d'alimentation CA.



AVERTISSEMENT : nous vous recommandons d'installer un dispositif de protection contre les surtensions sur votre branchement électrique.

Connexion de l'appareil à un réseau

Lorsqu'il est placé entre les réseaux internes et le réseau non sécurisé, l'appareil SSG 20 assure des fonctions de pare-feu et de sécurité générale conçues pour les réseaux. Cette section détaille les éléments suivants :

- Connexion de l'appareil à un réseau non sécurisé
- Connexion de l'appareil à un réseau interne ou un poste de travail

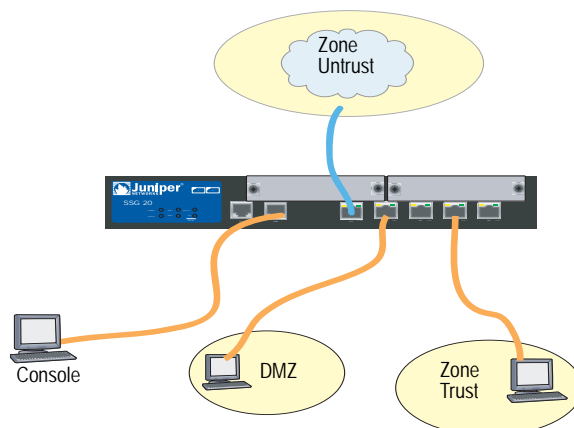
Connexion de l'appareil à un réseau non sécurisé

Vous pouvez connecter l'appareil SSG 20 à un réseau non sécurisé de l'une des manières suivantes :

- Ports Ethernet
- Ports série (AUX/Console)
- Connexion des mini-modules d'interface physique à un réseau non sécurisé

La Figure 10 présente l'appareil SSG 20 avec les connexions de câblage réseau de base lorsque l'appareil dispose de deux mini-modules d'interface physique vides et que les ports Ethernet 10/100 sont reliés de la manière suivante :

- Le port portant la mention 0/0 (interface ethernet0/0) est connecté au réseau non sécurisé.
- Le port portant la mention 0/1 (interface ethernet0/1) est connecté à un poste de travail de la zone de sécurité DMZ.
- Le port portant la mention 0/3 (interface bgroup0) est connecté à un poste de travail de la zone de sécurité Trust.
- Le port Console est connecté à un terminal série afin de permettre l'accès aux fonctions de gestion.

Figure 10 : exemple de mise en réseau de base

Ports Ethernet

Afin d'établir une connexion à haut débit, reliez le port Ethernet portant la mention 0/0 d'un appareil SSG 20 au routeur externe à l'aide du câble Ethernet fourni. L'appareil détecte automatiquement les paramètres de débit, du mode duplex et MDI/MDIX corrects.

Ports série (AUX/Console)

Vous pouvez vous connecter au réseau non sécurisé à l'aide d'un câble série RJ-45 direct et d'un modem externe.



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

Connexion des mini-modules d'interface physique à un réseau non sécurisé

Cette section indique comment connecter les mini-modules d'interface physique de l'appareil à un réseau non sécurisé.

Mini-module d'interface physique ADSL2/2+

Reliez le mini-module d'interface physique ADSL2/2+ à votre prise de téléphone à l'aide du câble ADSL fourni. 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, en apparence et en câblage, à un câble Ethernet 10 Base-T direct.

Connexion de séparateurs et de microfiltres

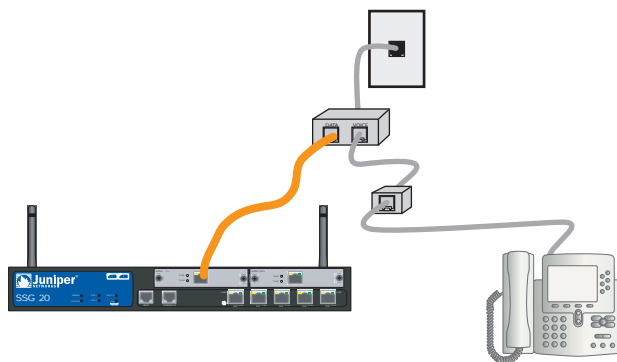
Un *séparateur de signaux* scinde le signal téléphonique en signaux vocaux à basse fréquence pour les communications vocales et en signaux de données à haute fréquence pour le trafic des données. Votre fournisseur de services installe généralement le séparateur en même temps que l'équipement permettant 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 les équipements utilisés par votre fournisseur de services. Si vous installez vous-même un séparateur de ce type, reliez l'appareil et la ligne de téléphone aux connecteurs adaptés (par exemple, « données » ou « voix ») du séparateur. Connectez l'autre fiche du séparateur à la prise de téléphone.

Vous devez 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.

La Figure 11 représente un exemple d'installation de microfiltre et de séparateur sur votre site (vous devez vous procurer les microfiltres ou séparateurs adaptés auprès de votre fournisseur de services).

Figure 11 : microfiltre et séparateur sur votre connexion réseau



Mini-modules d'interface physique RNIS, T1, E1 et V.92

Procédez comme suit pour connecter les mini-modules d'interface physique à un appareil :

1. Préparez une certaine longueur du type de câble utilisé par l'interface.
2. Insérez le connecteur de câble dans le port de connecteur de câble de la plaque avant de l'interface.
3. Disposez le câble de la manière suivante afin d'éviter qu'il ne se détache ou qu'il ne développe des points de tension :
 - a. Fixez le câble de manière à ce qu'il ne soutienne pas son propre poids lorsqu'il est suspendu.
 - b. Placez le surplus de câble dans une boucle bien enroulée de manière à ce que le câble ne soit pas gênant.
 - c. Utilisez des éléments de fixation pour maintenir la forme des boucles de câble.

Pour configurer le mini-module d'interface physique RNIS, E1, T1 ou V.92, reportez-vous à la section « Configuration des mini-modules d'interface physique », page 41.

Connexion de l'appareil à un réseau interne ou un poste de travail

Vous pouvez connecter votre réseau local ou votre poste de travail à l'aide des interfaces Ethernet et/ou sans fil.

Ports Ethernet

Les appareils SSG 20 disposent de cinq ports Ethernet. 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 tous les 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. Reportez-vous à la section « Paramètres par défaut de l'appareil », page 31 pour consulter les liaisons zone/interface par défaut.

Antennes sans fil

Si vous utilisez l'interface sans fil, vous devez connecter les antennes fournies à l'appareil. Si vous disposez des antennes de diversité 2 dB standard, fixez-les sur les montants A et B situés à l'arrière de l'appareil à l'aide de vis. Courbez les antennes au niveau des coudes, en veillant à ne pas appuyer sur les répartiteurs de câblage.

Figure 12 : emplacement des antennes de l'appareil SSG 20-WLAN



Si vous utilisez l'antenne externe en option, suivez les instructions de connexion fournies avec l'antenne.

Chapitre 3

Configuration de l'appareil

Le logiciel ScreenOS est installé de manière préalable dans des appareils SSG 20. Lors de la mise sous tension de l'appareil, ce dernier est prêt à être configuré. L'appareil dispose d'une configuration par défaut définie en usine qui permet de procéder à la connexion initiale de l'appareil. Une configuration supplémentaire adaptée à vos exigences réseau spécifiques est cependant nécessaire.

Ce chapitre présente les sections suivantes :

- « Accès à l'appareil », page 28
- « Paramètres par défaut de l'appareil », page 31
- « Configuration de base de l'appareil », page 33
- « Configuration sans fil de base », page 37
- « Configuration des mini-modules d'interface physique », page 41
- « Protections pare-feu de base », page 48
- « Vérification de la connectivité externe », page 49
- « Restauration des paramètres par défaut de l'appareil », page 49

REMARQUE : une fois l'appareil configuré et la connectivité vérifiée via le réseau distant, vous devez enregistrer le produit à l'adresse www.juniper.net/support/ de manière à ce que certains services ScreenOS, tels que le service de signatures Deep Inspection et l'antivirus (disponibles séparément), puissent être activés dans 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 au sujet de l'enregistrement de votre produit et de l'obtention d'abonnements pour des services spécifiques, reportez-vous au volume *Fundamentals* du manuel *Concepts & Examples ScreenOS Reference Guide* correspondant à la version de ScreenOS exécutée dans l'appareil.

Accès à l'appareil

Vous pouvez configurer et gérer un appareil de différentes manières :

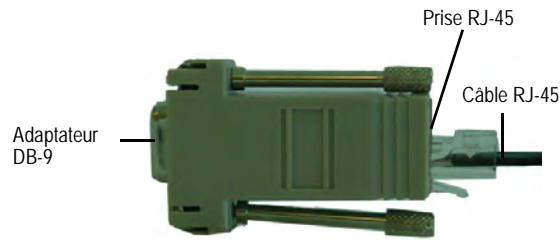
- **Console** : le port Console de l'appareil permet d'accéder à l'unité par l'intermédiaire d'un câble série connecté à votre poste de travail ou terminal. Pour configurer l'appareil, saisissez des commandes CLI (interface de ligne de commande) ScreenOS sur votre terminal ou dans un programme d'émulation de terminal exécuté sur votre poste de travail.
- **WebUI (Interface utilisateur Web)** : l'interface utilisateur Web de ScreenOS est une interface graphique disponible par l'intermédiaire d'un navigateur. Dans le cadre de l'utilisation initiale de WebUI (l'interface utilisateur Web), le poste de travail sur lequel vous exécutez le navigateur doit être situé dans le même sous-réseau que l'appareil. Vous pouvez également accéder à WebUI (l'interface utilisateur Web) par l'intermédiaire d'un serveur sécurisé utilisant le protocole (SSL) avec un protocole HTTP sécurisé (S-HTTP).
- **Telnet/SSH** : Telnet et SSH sont des applications permettant d'accéder à des appareils par l'intermédiaire d'un réseau IP. Pour configurer l'appareil, saisissez des commandes CLI (interface de ligne de commande) ScreenOS dans une session Telnet depuis votre poste de travail. Pour plus d'informations, reportez-vous au volume *Administration* du manuel *Concepts & Examples ScreenOS Reference Guide*.
- **NetScreen-Security Manager** : NetScreen-Security Manager est une application de gestion de Juniper Networks à l'échelle des entreprises qui permet de contrôler et de gérer les appareils de réseau privé virtuel IPSec/de pare-feu de Juniper Networks. Pour obtenir des instructions relatives à la procédure de gestion de l'appareil à l'aide de NetScreen-Security Manager, reportez-vous au manuel *NetScreen-Security Manager Administrator's Guide*.

Utilisation d'une connexion de console

REMARQUE : utilisez un câble série RJ-45 direct de catégorie 5 avec un connecteur RJ-45 mâle lors de la connexion au port Console de l'appareil.

Procédez comme suit pour établir une connexion de console :

1. Connectez la fiche femelle de l'adaptateur DB-9 fourni au port série de votre poste de travail (veillez à ce que le connecteur DB-9 soit inséré correctement et fermement). La Figure 13 illustre le type de connecteur DB-9 nécessaire.

Figure 13 : adaptateur DB-9

2. Connectez la fiche mâle du câble série RJ-45 de catégorie 20 au port Console de l'appareil SSG 5 (veillez à ce que l'autre fiche du câble de catégorie 5 soit insérée correctement et fermement dans l'adaptateur DB-9).
3. Lancez un programme d'émulation de terminal série sur votre poste de travail. Les paramètres nécessaires au lancement d'une session de console sont les suivants :
 - Débit (en bauds) : 9600
 - Parité : aucune
 - Bits de données : 8
 - Bit d'arrêt : 1
 - Contrôle de flux : aucun

4. Si vous n'avez pas encore modifié les nom d'utilisateur et mot de passe par défaut, saisissez **netscreen** aux invites de connexion et de mot de passe (n'utilisez que des lettres minuscules, les champs du nom de connexion et du mot de passe respectent tous deux la casse).

Pour obtenir des informations relatives à la configuration de l'appareil à l'aide des commandes CLI, reportez-vous au manuel *Concepts & Examples ScreenOS Reference Guide*.

5. (Facultatif) Par défaut, la session de la console arrive à expiration et s'arrête automatiquement après 10 minutes d'inactivité. Pour désactiver le délai d'expiration, saisissez **set console timeout 0**.

Utilisation de l'interface utilisateur Web

Dans le cadre de l'utilisation de l'interface utilisateur Web, le poste de travail à partir duquel vous gérez l'appareil doit initialement être situé dans le même sous-réseau que l'appareil. Procédez comme suit pour accéder à l'appareil à l'aide de l'interface utilisateur Web :

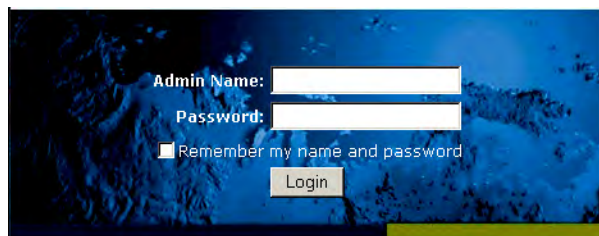
1. Connectez le poste de travail au port 0/2 — 0/4 (interface bgroup0 de la zone Trust) de l'appareil.
2. Assurez-vous que le poste de travail est configuré pour le protocole DHCP (Dynamic Host Configuration Protocol) ou est configuré de manière statique avec une adresse IP du sous-réseau 192.168.1.0/24.

3. Lancez le navigateur, saisissez l'adresse IP de l'interface bgroup0 (l'adresse IP par défaut est 192.168.1.1/24), puis appuyez sur **Enter**.

REMARQUE : si vous accédez pour la première fois à l'appareil par l'intermédiaire de l'interface utilisateur Web, l'Initial Configuration Wizard (Assistant de configuration initiale) apparaît. Si vous souhaitez configurer l'appareil à l'aide de l'Initial Configuration Wizard, reportez-vous à la section « Initial Configuration Wizard », page 65.

L'interface utilisateur Web affiche l'invite de connexion représentée dans la Figure 14.

Figure 14 : invite de connexion de l'interface utilisateur Web



4. Si vous n'avez pas encore modifié les nom d'administrateur et mot de passe par défaut, saisissez **netscreen** aux invites de connexion et de mot de passe (n'utilisez que des lettres minuscules, les champs du nom de connexion et du mot de passe respectent tous deux la casse).

Utilisation de Telnet

Procédez comme suit pour établir une connexion Telnet :

1. Connectez le poste de travail au port 0/2 — 0/4 (interface bgroup0 de la zone Trust) de l'appareil.
2. Assurez-vous que le poste de travail est configuré pour le protocole DHCP ou est configuré de manière statique avec une adresse IP du sous-réseau 192.168.1.0/24.
3. Démarrez une application cliente Telnet sur l'adresse IP de l'interface bgroup0 (l'adresse IP par défaut est 192.168.1.1). Saisissez, par exemple, **telnet 192.168.1.1**.

L'application Telnet affiche l'invite de connexion.

4. Si vous n'avez pas encore modifié les nom d'utilisateur et mot de passe par défaut, saisissez **netscreen** aux invites de connexion et de mot de passe (n'utilisez que des lettres minuscules, les champs du nom de connexion et du mot de passe respectent tous deux la casse).
5. (Facultatif) Par défaut, la session de la console arrive à expiration et s'arrête automatiquement après 10 minutes d'inactivité. Pour désactiver le délai d'expiration, saisissez **set console timeout 0**.

Paramètres par défaut de l'appareil

Cette section détaille les paramètres par défaut et le fonctionnement d'un appareil SSG 20.

Le Tableau 5 présente les liaisons de zones par défaut des ports des appareils.

Tableau 5 : interface physique par défaut des liaisons de zones

Mention attribuée au port	Interface	Zone
Ports Ethernet 10/100 :		
0/0	ethernet0/0	Untrust
0/1	ethernet0/1	DMZ
0/2	bgroup0 (ethernet0/2)	Trust
0/3	bgroup0 (ethernet0/3)	Trust
0/4	bgroup0 (ethernet0/4)	Trust
AUX	serial0/0	Null
Ports de mini-module d'interface physique de réseau étendu (x = connecteur de mini-module d'interface physique 1 ou 2) :		
ADSL2/2 + (annexe A)	adsl(x/0)	Untrust
ADSL2/2 + (annexe B)	adsl(x/0)	Untrust
T1	serial(x/0)	Untrust
E1	serial(x/0)	Untrust
RNIS	bri(x/0)	Untrust
V.92	serial(x/0)	Null

Le groupe pont (bgroup) permet aux utilisateurs réseau de commuter entre le trafic câblé et le trafic sans fil sans devoir reconfigurer ou redémarrer l'appareil. Par défaut, les interfaces ethernet0/2 — ethernet0/4, portant les mentions ports 0/2 — 0/4 sur l'appareil, sont regroupées en tant qu'interface bgroup0, disposent de l'adresse IP 192.168.1.1/24 et sont reliées à la zone de sécurité Trust. Vous pouvez configurer un maximum de quatre groupes bgroup.

Si vous souhaitez placer une interface Ethernet ou sans fil dans un groupe bgroup, vous devez d'abord vous assurer que l'interface Ethernet ou sans fil se trouve dans la zone de sécurité Null. Si vous retirez l'interface Ethernet ou sans fil du groupe bgroup, elle est placée dans la zone de sécurité Null. Une fois attribuée à la zone de sécurité Null, l'interface Ethernet peut être reliée à une zone de sécurité et une autre adresse ID peut lui être attribuée.

Pour retirer l'interface ethernet0/3 du groupe bgroup0 et la placer dans la zone Trust avec l'adresse IP statique 192.168.3.1/24, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port : désélectionnez **ethernet0/3**, puis cliquez sur **Apply**.

List > Edit (ethernet0/3) : saisissez les informations suivantes, puis cliquez sur **Apply** :

Zone Name: Trust (sélection)
IP Address/Netmask: 192.168.3.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
set interface ethernet0/3 zone trust
set interface ethernet0/3 ip 192.168.3.1/24
save
```

Tableau 6 : liaisons des interfaces sans fil et des interfaces logiques

SSG 20-WLAN	Interface	Zone
Interface sans fil	wireless0/0 (l'adresse IP par défaut est 192.168.2.1/24)	Trust
Définit une interface sans fil qui peut être configurée de manière à fonctionner sur des bandes de signaux radioélectriques de 2,4 G et/ou 5 G.	wireless0/1-0/3.	Null
Interfaces logiques		
Interface de couche 2	vlan1 fait référence aux interfaces logiques utilisées pour la gestion et l'arrêt de trafic du réseau privé virtuel lorsque l'appareil est en mode transparent.	S/O
Interfaces tunnel	tunnel.n fait référence à une interface tunnel logique. Cette interface est destinée au trafic de réseau privé virtuel.	S/O

Vous pouvez modifier l'adresse IP par défaut de l'interface bgroup0 conformément aux adresses de votre réseau local et de votre réseau local sans fil. Pour configurer l'interface sans fil d'un groupe bgroup, reportez-vous à la section « Configuration sans fil de base », page 37.

REMARQUE : l'interface bgroup ne fonctionne pas en mode transparent lorsqu'elle inclut une interface sans fil.

Pour obtenir des informations supplémentaires au sujet du groupe bgroup et des exemples, reportez-vous au manuel *Concepts & Examples ScreenOS Reference Guide*.

Aucune autre adresse IP par défaut n'est configurée sur les autres interfaces Ethernet ou sans fil de l'appareil. Vous devez définir les adresses IP des autres interfaces, interfaces de réseau étendu incluses.

Configuration de base de l'appareil

Cette section détaille les paramètres de configuration de base suivants :

- Nom et mot de passe de l'administrateur racine
- Date et heure
- Interfaces du groupe pont
- Accès administratif
- Services de gestion
- Nom d'hôte et nom de domaine
- Route par défaut
- Adresse de l'interface de gestion
- Configuration de l'interface non sécurisée secondaire

Nom et mot de passe de l'administrateur racine

L'administrateur racine dispose de tous les droits nécessaires à la configuration des appareils SSG 20. Nous vous recommandons de modifier immédiatement le nom et le mot de passe par défaut de l'administrateur racine (tous deux **netscreen**).

Pour modifier le nom et le mot de passe de l'administrateur racine, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

WebUI

Configuration > Admin > Administrators > Edit (pour la valeur du nom d'administrateur netscreen) : saisissez les informations suivantes, puis cliquez sur **OK** :

Administrator Name:
Old Password: netscreen
New Password:
Confirm New Password:

REMARQUE : les mots de passe ne sont pas affichés dans l'interface utilisateur Web.

CLI

```
set admin name nom  
set admin password motdepasse  
save
```


Date et heure

L'heure définie au niveau d'un appareil SSG 20 affecte des événements tels que la configuration des tunnels de réseau privé virtuel. Le moyen le plus simple pour régler la date et l'heure de l'appareil consiste à utiliser l'interface utilisateur Web pour synchroniser l'horloge système de l'appareil sur l'horloge du poste de travail.

Pour configurer la date et l'heure d'un appareil, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

1. Configuration > Date/Time : cliquez sur le bouton Sync Clock with Client.

Un message contextuel s'affiche, invitant à préciser si l'option de passage à l'heure d'été a été activée au niveau de l'horloge de votre poste de travail.

2. Cliquez sur **Yes** pour synchroniser l'horloge système et la régler en tenant compte de l'heure d'été ou sur **No** 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 de l'appareil.

Interfaces du groupe pont

Par défaut, l'appareil SSG 20 dispose des interfaces Ethernet ethernet0/2—ethernet0/4, regroupées dans la zone de sécurité Trust. Le fait de regrouper les interfaces les place dans un sous-réseau. Vous pouvez retirer une interface d'un groupe et l'affecter à une autre zone de sécurité. Avant d'être affectées à un groupe, les interfaces doivent se trouver dans la zone de sécurité Null. Pour placer une interface regroupée dans la zone de sécurité Null, utilisez la commande CLI **unset interface interface port interface**.

Les appareils SSG 20-WLAN permettent de regrouper des interfaces Ethernet et sans fil dans un même sous-réseau.

REMARQUE : seules les interfaces Ethernet et sans fil peuvent être placées dans un groupe bgroup.

Pour configurer un groupe disposant d'interfaces Ethernet et sans fil, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Network > Interfaces > List > Edit (bgroup0) > Bind Port : désélectionnez **ethernet0/3** et **ethernet0/4**, puis cliquez sur **Apply**.

Edit (bgroup1) > Bind Port : sélectionnez **ethernet0/3**, **ethernet0/4** et **wireless0/2**, puis cliquez sur **Apply**.

> Basic : saisissez les informations suivantes, puis cliquez sur **Apply** :

Zone Name: DMZ (sélection)
IP Address/Netmask: 10.0.0.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
unset interface bgroup0 port ethernet0/4
set interface bgroup1 port ethernet0/3
set interface bgroup1 port ethernet0/4
set interface bgroup1 port wireless0/2
set interface bgroup1 zone DMZ
set interface bgroup1 ip 10.0.0.1/24
save
```

Accès administratif

Par défaut, tous les utilisateurs connectés à votre réseau peuvent gérer l'appareil dès lors qu'ils en connaissent le nom de connexion et le mot de passe.

Pour configurer l'appareil de manière à ce qu'il ne puisse être géré qu'à partir d'un hôte spécifique du réseau, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Configuration > Admin > Permitted IPs : saisissez les informations suivantes, puis cliquez sur **Add** :

IP Address/Netmask: *adr_ip/masque*

CLI

```
set admin manager-ip adr_ip/masque
save
```

Services de gestion

ScreenOS propose des services de configuration et de gestion de l'appareil, tels que SNMP, SSL et SSH, que vous pouvez activer en fonction de l'interface.

Pour configurer les services de gestion de l'appareil, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Network > Interfaces > List > Edit (pour ethernet0/0) : sous **Management Services**, activez les services de gestion à utiliser dans l'interface, puis cliquez sur **Apply**.

CLI

```
set interface ethernet0/0 manage web
unset interface ethernet0/0 manage snmp
save
```

Nom d'hôte et nom de domaine

Le nom de domaine définit le réseau ou le sous-réseau auquel appartient l'appareil tandis que le nom d'hôte fait référence à un appareil spécifique. Le nom d'hôte et le nom de domaine permettent d'identifier ensemble de manière unique l'appareil au sein du réseau.

Pour configurer le nom d'hôte et le nom de domaine d'un appareil, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Network > DNS > Host : saisissez les informations suivantes, puis cliquez sur **Apply** :

Host Name: *nom*
Domain Name: *nom*

CLI

```
set hostname nom
set domain nom
save
```

Route par défaut

La route par défaut est une route statique utilisée pour diriger les paquets adressés à des réseaux qui ne figurent pas de manière explicite dans le tableau de routage. Si un paquet arrive dans l'appareil et dispose d'une adresse pour laquelle l'appareil ne dispose d'aucune information de routage, ce dernier envoie le paquet à la destination définie par la route par défaut.

Pour configurer la route par défaut de l'appareil, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Network > Routing > Destination > New (trust-vr) : saisissez les informations suivantes, puis cliquez sur **OK** :

IP Address/Netmask: 0.0.0.0/0.0.0.0
Next Hop
Gateway: (sélection)
Interface: ethernet0/2 (sélection)
Gateway IP Address: *adr_ip*

CLI

```
set route 0.0.0.0/0 interface ethernet0/2 gateway adr_ip
save
```

Adresse de l'interface de gestion

L'interface Trust dispose de l'adresse IP par défaut 192.168.1.1/24 et est configurée pour les services de gestion. Si vous connectez les ports 0/2—0/4 de l'appareil à un poste de travail, vous pouvez configurer l'appareil à partir d'un poste de travail du sous-réseau 192.168.1.1/24, à l'aide d'un service de gestion tel que Telnet.

Vous pouvez modifier l'adresse IP par défaut de l'interface Trust. Vous pouvez, par exemple, modifier l'interface conformément aux adresses IP qui existent déjà au niveau du réseau local.

Configuration de l'interface non sécurisée secondaire

L'appareil SSG 20 permet de configurer une interface secondaire en cas de défaillance de l'interface non sécurisée. Procédez comme suit pour définir une interface secondaire, utilisée en cas de défaillance de l'interface non sécurisée :

1. Placez l'interface secondaire dans la zone de sécurité Null à l'aide de la commande CLI **unset interface interface [port interface]**.
2. Reliez l'interface secondaire à la même zone de sécurité que l'interface principale à l'aide de la commande CLI **set interface interface zone nom_zone**.

REMARQUE : l'interface principale et l'interface secondaire doivent se trouver dans la même zone de sécurité. L'interface principale ne dispose que d'une seule interface secondaire et l'interface secondaire que d'une seule interface principale.

Pour définir l'interface ethernet0/4 comme interface secondaire de l'interface ethernet0/0, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Network > Interfaces > Backup > saisissez les informations suivantes, puis cliquez sur **Apply**.

Primary: ethernet0/0
Backup: ethernet0/4
Type: track-ip (sélection)

CLI

```
unset interface bgroup0 port ethernet0/4
set interface ethernet0/4 zone untrust
set interface ethernet0/0 backup interface ethernet0/4 type track-ip
save
```

Configuration sans fil de base

Cette section fournit des informations relatives à la configuration de l'interface sans fil de l'appareil SSG 20-WLAN. Les réseaux sans fil sont désignés par des noms SSID (Service Set Identifiers). La définition des SSID permet de disposer de plusieurs réseaux sans fil au même emplacement sans que ceux-ci n'interfèrent les uns avec les autres. Un nom SSID peut compter un maximum de 32 caractères. Si le nom SSID inclut un espace, la chaîne de caractères doit être placée entre guillemets. Une fois le nom SSID défini, vous pouvez configurer d'autres attributs SSID. Pour bénéficier des capacités de réseau local sans fil de l'appareil, vous devez configurer au moins un SSID et le relier à une interface sans fil.

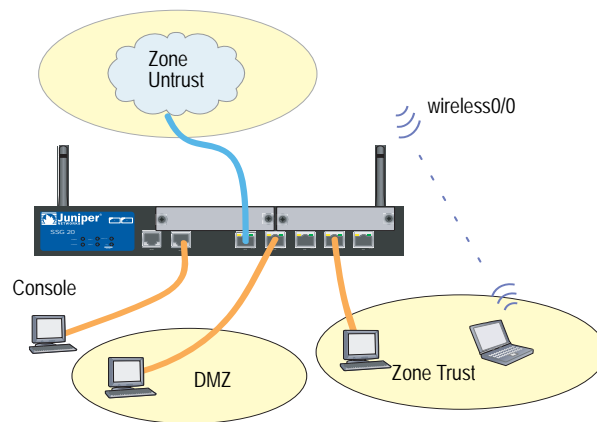
L'appareil SSG 20-WLAN permet de créer un maximum de 16 SSID. Cependant, seuls quatre peuvent être utilisés simultanément. Vous pouvez configurer l'appareil de manière à ce que les quatre SSID soient utilisés au niveau du même émetteur-récepteur ou répartir l'utilisation entre les deux émetteurs-récepteurs (trois SSID attribués au réseau local sans fil 0 et un SSID attribué au réseau local sans fil 1, par exemple). Utilisez la commande CLI **set interface interface_sansfil wlan {0 | 1 | both}** pour régler les émetteurs-récepteurs radio de l'appareil SSG 20-WLAN.

Une fois un SSID défini sur l'interface wireless0/0, vous pouvez accéder à l'appareil à l'aide de l'adresse IP par défaut de l'interface wireless0/0 (voir les étapes de la section « Accès à l'appareil », page 28). La Figure 15 présente la configuration par défaut de l'appareil SSG 20-WLAN.

REMARQUE: si vous utilisez l'appareil SSG 20-WLAN dans un pays autre que les États-Unis, le Japon, le Canada, la Chine, Taïwan, la Corée, Israël ou Singapour, vous devez utiliser la commande CLI **set wlan country-code** ou la définir dans la page Wireless > General Settings de l'interface utilisateur WebUI avant de pouvoir établir une connexion du type réseau local sans fil. Cette commande définit la plage de canaux disponibles et le niveau de puissance émise.

Si le code de votre région est ETSI, vous devez définir le code national adapté aux réglementations locales en matière de spectre des radiofréquences.

Figure 15 : configuration par défaut de l'appareil SSG 20-WLAN



L'interface wireless0/0 est configurée par défaut avec l'adresse IP 192.168.2.1/24. Tous les clients sans fil qui doivent se connecter à la zone Trust doivent disposer d'une adresse IP au sein du sous-réseau sans fil. Vous pouvez également configurer l'appareil de manière à ce qu'il utilise le protocole DHCP pour attribuer automatiquement à vos appareils des adresses IP au sein du sous-réseau 192.168.2.1/24.

Par défaut, les interfaces wireless0/1 – wireless0/3 sont définies comme Null et ne disposent d'aucune adresse IP. Si vous souhaitez utiliser une des autres interfaces sans fil, vous devez configurer une adresse IP pour l'interface, lui attribuer un SSID et la relier à une zone de sécurité. Le Tableau 7 présente les méthodes de chiffrement et d'authentification sans fil.

Tableau 7 : options de chiffrement et d'authentification sans fil

Authentification	Chiffrement
Ouverte	Permet à n'importe quel client sans fil d'accéder à l'appareil.
Clé partagée	Clé partagée WEP
WPA-PSK	AES/TKIP avec une clé partagée au préalable
WPA	AES/TKIP avec une clé du serveur RADIUS
WPA2-PSK	Compatible 802.11i avec une clé partagée au préalable
WPA2	Compatible 802.11i avec un serveur RADIUS
WPA-Auto-PSK	Type WPA ou WPA2 avec une clé partagée au préalable
WPA-Auto	Type WPA ou WPA2 avec un serveur RADIUS
802.1x	WEP avec une clé du serveur RADIUS

Pour obtenir des exemples de configuration, ainsi que des informations sur les attributs SSID et les commandes CLI relatives aux configurations de sécurité sans fil, reportez-vous au manuel *Concepts & Examples ScreenOS Reference Guide*.

Pour configurer une interface sans fil dans le cadre de la connectivité de base, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

1. Définissez le code national et l'adresse IP du réseau local sans fil.

Wireless > General Settings > sélectionnez les éléments suivants, puis cliquez sur **Apply** :

Country code: sélection de votre code
IP Address/Netmask: *adr_ip/masqueréseau*

2. Définissez le SSID.

Wireless > SSID > New : saisissez les informations suivantes, puis cliquez sur **OK** :

SSID:
Authentication:
Encryption:
Wireless Interface Binding:

3. (Facultatif) Définissez la clé WEP.

SSID > WEP Keys : sélectionnez l'identifiant de la clé, puis cliquez sur **Apply**.

4. Définissez le mode du réseau local sans fil.

Network > Interfaces > List > Edit (interface sans fil) : sélectionnez **Both** pour le mode du réseau local sans fil, puis cliquez sur **Apply**.

- Activez les modifications apportées à l'interface sans fil.

Wireless > General Settings > cliquez sur **Activate Changes**.

CLI

- Définissez le code national et l'adresse IP du réseau local sans fil.

```
set wlan country-code { code_id }
set interface interface_sansfil ip adr_ip/masqueréseau
```

- Définissez le SSID.

```
set ssid name name_str
set ssid nom authentication type_auth encryption type_chiffrement
set ssid nom interface interface
(Facultatif) set ssid nom key-id numéro
```

- Définissez le mode du réseau local sans fil.

```
set interface interface_sansfil wlan both
```

- Activez les modifications apportées à l'interface sans fil.

```
save
exec wlan reactivate
```

Vous pouvez configurer le SSID de manière à ce qu'il fonctionne au sein du même sous-réseau que le sous-réseau câblé. Cette action permet aux clients de travailler au niveau d'une interface ou de l'autre sans devoir se connecter à un autre sous-réseau.

Pour placer une interface Ethernet et une interface sans fil dans la même interface de groupe pont, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Network > Interfaces > List > Edit (*nom_bgroup*) > Bind Port : sélectionnez les interfaces sans fil et Ethernet, puis cliquez sur **Apply**.

CLI

```
set interface nom_bgroup port interface_ethernet
set interface nom_bgroup port interface_sansfil
```

REMARQUE: *nom_bgroup* peut être bgroup0—bgroup3.

interface_ethernet peut être ethernet0/0—ethernet0/4.

interface_sansfil peut être wireless0/0—wireless0/3.

Si une interface sans fil est configurée, vous devez réactiver le réseau local sans fil à l'aide de la commande CLI **exec wlan reactivate** ou cliquer sur **Activate Changes** dans la page Wireless > General Settings de l'interface utilisateur Web.

Configuration des mini-modules d'interface physique

Cette section indique comment configurer les mini-modules d'interface physique :

- Interface ADSL2/2 +
- Interface RNIS
- Interface T1
- Interface E1
- Interface à modem V.92

Interface ADSL2/2+

Votre réseau utilise l'interface ADSL2/2 + **adslx/0**, x représente le connecteur de mini-module d'interface physique (1 ou 2), de l'appareil pour se connecter au réseau du fournisseur de services par l'intermédiaire d'un circuit virtuel au mode de transfert asynchrone (ATM). Vous pouvez configurer d'autres circuits virtuels en créant des sous-interfaces ADSL2/2 + . Pour plus d'informations, reportez-vous à la section « Circuits virtuels », page 42.

Dans l'interface utilisateur Web, accédez à la page Network > Interfaces > List pour afficher la liste des interfaces de l'appareil. Si vous utilisez une session Telnet ou de console, saisissez la commande CLI **get interface**. Vous devriez constater que l'interface adslx/0 est reliée à la zone Untrust.

Si vous utilisez l'interface ADSL2/2 + pour vous connecter au réseau de services du fournisseur, vous devez configurer l'interface adsl(x/0). Pour cela, vous devez vous procurer les informations suivantes auprès de votre fournisseur de services :

- Valeurs Virtual Path Identifier (Identificateur de trajet virtuel) et Virtual Channel Identifier (Identificateur de canal virtuel) (VPI/VCI)
- Méthode de multiplexage Couche d'adaptation 5 (AAL5) au mode de transfert asynchrone (ATM), qui peut être l'une des méthodes suivantes :
 - Multiplexage utilisant un circuit virtuel, dans lequel chaque protocole est transporté sur un circuit virtuel ATM distinct
 - Encapsulation par commande de liaison logique (LLC), qui autorise le transport de plusieurs protocoles sur le même circuit virtuel ATM (il s'agit de la méthode de multiplexage par défaut)
- Nom d'utilisateur et mot de passe attribués par votre fournisseur de services pour vous connecter au réseau de votre fournisseur de services à l'aide du protocole PPPoE (Point-to-Point Protocol over Ethernet) ou PPPoA (Point-to-Point Protocol over ATM)
- Méthode d'authentification, le cas échéant, fournie pour la connexion PPPoE ou PPPoA
- En option, une adresse IP statique et une valeur de masque de réseau pour votre réseau

Circuits virtuels

Pour ajouter des circuits virtuels, vous devez créer des sous-interfaces dans l'interface ADSL2/2 + . Vous pouvez créer un maximum de dix sous-interfaces ADSL2/2 + . Pour créer une nouvelle sous-interface appelée **adsl1/0.1** reliée à la zone prédéfinie **Untrust**, par exemple, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Network > Interfaces > List > New ADSL Sub-IF : saisissez les informations suivantes, puis cliquez sur **Apply** :

Interface Name: adsl1/0.1
VPI/VCI: 0/35
Zone Name: Untrust (sélection)

CLI

```
set interface adsl 1/0.1 pvc 0 35 zone Untrust
save
```

Vous devez configurer la sous-interface ADSL 2/2 + de la même manière que l'interface ADSL 2/2 + principale, en définissant notamment les valeurs VPI/VCI comme indiqué à la section « Interface ADSL2/2 + », page 41. La configuration d'une sous-interface ADSL2/2 + s'effectue indépendamment de l'interface ADSL2/2 + 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 ADSL2/2 + principale. Vous pouvez également configurer une adresse IP statique sur une sous-interface, même si l'interface ADSL2/2 + principale ne comporte pas d'adresse IP statique.

VPI/VCI et méthode de multiplexage

Votre fournisseur de services attribue une paire VPI/VCI pour chaque connexion à un circuit virtuel. Vous pouvez, par exemple, recevoir la paire VPI/VCI 1/32, qui signifie une valeur de VPI de 1 et une valeur de VCI de 32. Ces valeurs doivent correspondre aux valeurs configurées par votre fournisseur de services du côté abonné du multiplexeur d'accès de lignes numériques d'abonnés (DSLAM).

Pour configurer la paire VPI/VCI 1/32 dans l'interface adsl1/0, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Network > Interfaces > List > Edit (pour l'interface adsl1/0) : saisissez **1/32** dans le champ VPI/VCI, puis cliquez sur **Apply**.

CLI

```
set interface adsl1/0 pvc 1 32
save
```

Par défaut, l'appareil utilise le multiplexage par commande de liaison logique (LLC) pour chaque circuit virtuel.

Pour configurer la paire VPI/VCI 1/32 dans l'interface adslx/0 et utiliser l'encapsulation LLC sur le circuit virtuel, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Network > Interfaces > List > Edit (pour l'interface adsl1/0) : saisissez les informations suivantes, puis cliquez sur **Apply** :

VPI/VCI: 1 / 32
Multiplexing Method: LLC (sélection)

CLI

```
set interface adsl1/0 pvc 1 32 mux llc
save
```

PPPoE ou PPPoA

Les appareils SSG 20 incluent à la fois des clients PPPoE et PPPoA pour se connecter au réseau du fournisseur de services par l'intermédiaire de la liaison ADSL. Le protocole PPPoE est la plus répandue des formes d'encapsulation ADSL et 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. Pour permettre à l'appareil de se connecter au réseau du fournisseur de services, vous devez configurer le nom d'utilisateur et le mot de passe qui vous ont été attribués par le fournisseur de services. La procédure de configuration du protocole PPPoA est semblable à la procédure de configuration du protocole PPPoE.

REMARQUE: l'appareil ne prend en charge qu'une seule session PPPoE sur chaque circuit virtuel.

Afin de configurer, par exemple, le nom d'utilisateur **roswell** et le mot de passe **area51** pour le protocole PPPoE et relier la configuration PPPoE à l'interface adsl1/0, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Network > PPP > PPPoE Profile > New : saisissez les informations suivantes, puis cliquez sur **OK** :

PPPoE Instance: poe1
Bound to Interface: adsl1/0 (sélection)
Username: roswell
Password: area51

CLI

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1/0
save
```

Il existe d'autres paramètres PPPoE ou PPPoA pouvant être configurés au niveau de l'appareil, tels que la méthode d'authentification (par défaut, l'appareil 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 de services si des paramètres PPPoE ou PPPoA supplémentaires doivent être configurés afin de permettre à l'appareil de communiquer correctement avec le serveur du fournisseur de services.

Adresse IP statique et masque de réseau

Si votre fournisseur de services 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. Vous devez également spécifier que l'appareil utilisera l'adresse IP statique (généralement, l'appareil 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).

Vous devez configurer une instance PPPoE ou PPPoA et la relier à l'interface `adsl1/0`, comme indiqué dans la section « PPPoE ou PPPoA », page 43. Veillez à sélectionner **Obtain IP using PPPoE** ou **Obtain IP using PPPoA** et le nom de l'instance PPPoE ou PPPoA.

Pour configurer l'adresse IP statique 1.1.1.1/24 pour le réseau, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Network > Interfaces > List > Edit (pour l'interface `adsl1/0`) : saisissez les informations suivantes, puis cliquez sur **Apply** :

IP Address/Netmask: 1.1.1.1/24
Static IP: (sélection)

CLI

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

ou

```
set interface adsl1/0 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 reçoit une adresse IP pour l'interface ADSL2/2+ 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 leur(s) adresse(s) IP auprès du serveur DHCP de l'appareil, les ordinateurs obtiennent également les adresses de serveurs DNS correspondantes.

Si vous attribuez une adresse IP statique à l'interface ADSL2/2+ , votre fournisseur de services doit vous fournir la ou les adresses IP du ou des serveurs 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 la zone Trust afin qu'il fournisse l'adresse du serveur DNS à chaque ordinateur.

Pour configurer le serveur DHCP dans l'interface `bgroup0` de manière à fournir l'adresse de serveur DNS 1.1.1.152 aux ordinateurs connectés à votre réseau, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Network > DHCP > Edit (pour l'interface bgroup0) > DHCP Server : saisissez **1.1.1.152** dans le champ DNS1, puis cliquez sur **Apply**.

CLI

```
set interface bgroup0 dhcp server option dns1 1.1.1.152
save
```

Pour plus d'informations au sujet de la configuration des interfaces ADSL et ADSL2/2+, reportez-vous au manuel *Concepts & Examples ScreenOS Reference Guide*.

Interface RNIS

Le réseau numérique à intégration de services (RNIS) est un ensemble de normes pour la transmission numérique via différents supports créées par le CCITT (Consultative Committee for International Telegraphy and Telephone) et l'ITU (International Telecommunications Union). En tant que service de connexion à la demande, il dispose d'un temps d'établissement des communications réduit et d'un faible délai de transit. Il est également en mesure de procéder à des transmissions de vidéos, de données et de la voix de haute qualité. Le RNIS est également un service de commutation de circuits qui peut être utilisé au niveau de connexions point à point et de connexions à points multiples. Le RNIS propose un routeur de services avec une connexion PPP (Point-to-Point Protocol) à liaisons multiples pour les interfaces réseau. L'interface RNIS est généralement configurée en tant qu'interface secondaire de l'interface Ethernet permettant d'accéder à des réseaux externes.

Pour configurer l'interface RNIS, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Network > Interfaces > List > Edit (bri1/0) : saisissez ou sélectionnez les éléments suivants, puis cliquez sur **OK** :

```
BRI Mode: Dial Using BRI
Primary Number: 123456
WAN Encapsulation: PPP
PPP Profile: isdnprofile
```

CLI

```
set interface bri1/0 dialer-enable
set interface bri1/0 primary-number "123456"
set interface bri1/0 encaps ppp
set interface bri1/0 ppp profile isdnprofile
save
```

Pour configurer l'interface RNIS en tant qu'interface secondaire, reportez-vous à la section « Configuration de l'interface non sécurisée secondaire », page 37.

Pour plus d'informations au sujet de la configuration de l'interface RNIS, reportez-vous au manuel *Concepts & Examples ScreenOS Reference Guide*.

Interface T1

L'interface T1 est un protocole de couche physique de base utilisé par la méthode de multiplexage de signal numérique de niveau 1 (DS-1) en Amérique du Nord. Les interfaces T1 fonctionnent à un débit binaire de 1 544 Mbits/s ou à des vitesses pouvant atteindre 24 canaux DS0.

Les appareils prennent en charge les normes DS-1 T1 suivantes :

- ANSI T1.107, T1.102
- GR 499-core, GR 253-core
- AT&T Pub 54014
- ITU G.751, G.703

Pour configurer le mini-module d'interface physique T1, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Network > Interfaces > List > Edit (serial1/0) : saisissez ou sélectionnez les éléments suivants, puis cliquez sur **OK** :

WAN Configure: main link
 WAN Encapsulation: cisco-hdlc
 Cliquez sur **Apply**.
 Fixed IP: (sélection)
 IP Address/Netmask: 172.18.1.1/24

CLI

```
set interface serial1/0 encap cisco-hdlc
set interface serial1/0 ip 172.18.1.1/24
```

Pour obtenir des informations relatives à la configuration de l'interface T1, reportez-vous au manuel *Concepts & Examples ScreenOS Reference Guide*.

Interface E1

L'interface E1 est un format de communications numériques de réseau étendu standard, conçu pour fonctionner via des équipements en cuivre, à un débit de 2 048 Mbits/s. Largement utilisée hors de l'Amérique du Nord, l'interface E1 est un schéma de multiplexage par répartition dans le temps de base, utilisé dans le cadre de la transmission des circuits numériques.

Les appareils prennent en charge les normes E1 suivantes :

- ITU-T G.703
- ITU-T G.751
- ITU-T G.775

Pour configurer le mini-module d'interface physique E1, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Network > Interfaces > List > Edit (serial1/0) : saisissez ou sélectionnez les éléments suivants, puis cliquez sur **OK** :

WAN Configure: main link
 WAN Encapsulation: PPP
 Binding a PPP Profile: junipertest
 Cliquez sur **Apply**.
 Fixed IP: (sélection)
 IP Address/Netmask: 172.18.1.1/24

CLI

```
set interface serial1/0 encapsulation ppp
set ppp profile "junipertest" static-ip
set ppp profile "junipertest" auth type chap
set ppp profile "junipertest" auth local-name "juniper"
set ppp profile "junipertest" auth secret "password"
set interface serial1/0 ppp profile "junipertest"
set interface serial1/0 ip 172.18.1.1/24
set user "server" type wan
set user "server" password "server"
```

Pour obtenir des informations relatives à la configuration de l'interface E1, reportez-vous au manuel *Concepts & Examples ScreenOS Reference Guide*.

Interface à modem V.92

L'interface V.92 dispose d'un modem analogique interne qui permet d'établir une connexion PPP à un fournisseur de services. Vous pouvez configurer l'interface série en tant qu'interface principale ou secondaire (utilisée en cas de défaillance de l'interface principale).

REMARQUE l'interface V.92 ne fonctionne pas en mode transparent.

Pour configurer l'interface V.92, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Network > Interfaces > List > Edit (pour serial1/0) : saisissez les informations suivantes, puis cliquez sur **OK** :

Zone Name: untrust (sélection)

ISP: saisissez les informations suivantes, puis cliquez sur **OK** :

ISP Name: isp_juniper
 Primary Number: 1234567
 Login Name: juniper
 Login Password: juniper

Modem: saisissez les informations suivantes, puis cliquez sur **OK** :

Modem Name: mod1
 Init String: AT&FS7=255S32=6
 Active Modem setting
 Inactivity Timeout: 20

CLI

```

set interface serial1/0 zone untrust
set interface serial1/0 modem isp isp_juniper account login juniper password
juniper
set interface serial1/0 modem isp isp_juniper primary-number 1234567
set interface serial1/0 modem idle-time 20
set interface serial1/0 modem settings mod1 init-strings AT&FS7=255S32=6
set interface serial1/0 modem settings mod1 active

```

Pour obtenir des informations relatives à la configuration de l'interface à modem V.92, reportez-vous au manuel *Concepts & Examples ScreenOS Reference Guide*.

Protections pare-feu de base

Les appareils sont configurés avec une règle par défaut qui permet aux postes de travail qui se trouvent dans la zone Trust de votre réseau d'accéder aux ressources de la zone de sécurité Untrust alors que les ordinateurs extérieurs à votre réseau ne sont pas autorisés à accéder ou à démarrer des sessions à l'aide de vos postes de travail. Vous pouvez configurer des règles de sécurité de façon à ce que l'appareil autorise les ordinateurs extérieurs à votre réseau à initier des sessions de type spécifique avec vos ordinateurs. Pour obtenir des informations au sujet de la création ou de la modification des règles, reportez-vous au manuel *Concepts & Examples ScreenOS Reference Guide*.

L'appareil SSG 20 dispose de différentes méthodes de détection et de différents mécanismes de défense pour lutter contre les vérifications et attaques dont l'objectif est de compromettre ou de nuire à un réseau ou à une ressource du réseau :

- Les options SCREEN de ScreenOS sécurisent une zone en vérifiant, puis en autorisant ou en refusant, l'ensemble des tentatives de connexion qui nécessitent le transit vers la zone en question par l'intermédiaire d'une interface. Vous pouvez, par exemple, activer une protection par interrogation des ports dans la zone Untrust de manière à empêcher la source d'un réseau distant d'identifier les services à cibler en vue de futures attaques.
- L'appareil applique des règles de pare-feu, qui peuvent inclure des composants de filtrage du contenu et de détection et de prévention des intrusions, au trafic qui passe d'une zone à l'autre via les filtres SCREEN. Par défaut, aucun trafic n'est autorisé à passer d'une zone à l'autre par l'intermédiaire de l'appareil. Pour autoriser le passage du trafic d'une zone à l'autre par l'intermédiaire de l'appareil, vous devez créer une règle qui annule le comportement par défaut.

Pour définir les options SCREEN de ScreenOS pour une zone, utilisez l'interface utilisateur Web ou les commandes CLI de la manière suivante :

Interface utilisateur Web

Screening > Screen : sélectionnez la zone à laquelle les options s'appliquent. Sélectionnez les options SCREEN souhaitées, puis cliquez sur **Apply**.

CLI

```

set zone zone screen option
save

```

Pour plus d'informations au sujet de la configuration des options de sécurité réseau disponibles sous ScreenOS, reportez-vous au manuel *Concepts & Examples ScreenOS Reference Guide*.

Vérification 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 sur n'importe quel poste de travail connecté à votre réseau et saisissez l'adresse URL suivante : www.juniper.net.

Restauration des paramètres par défaut de l'appareil

Si vous égarez votre mot de passe d'administrateur, vous pouvez restaurer les paramètres par défaut de l'appareil. Cette action écrase les configurations existantes mais restaure l'accès à l'appareil.



AVERTISSEMENT : la réinitialisation de l'appareil supprime tous les paramètres de configuration existants et désactive les services de pare-feu et de réseau privé virtuel existants.

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 manuel *Concepts & Examples ScreenOS Reference Guide*.
- Par l'intermédiaire du trou d'épingle de réinitialisation situé sur le panneau arrière de l'appareil, comme décrit dans la section suivante.

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 indiqué dans la section « Utilisation d'une connexion de console », page 28.

Procédez comme suit pour réinitialiser l'appareil et restaurer les paramètres par défaut à l'aide du trou d'épingle de réinitialisation :

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 déplié, par exemple), appuyez sur le bouton situé dans le trou d'épingle pendant quatre à six secondes, puis relâchez-le.

La DEL STATUS clignote en rouge. 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 STATUS clignote en vert, l'appareil attend maintenant la deuxième réinitialisation. Le message de la console indique maintenant que l'unité attend une deuxième confirmation.

3. Appuyez de 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 réinitialisation. La DEL STATUS s'allume en rouge pendant une demi-seconde, puis retourne à l'état clignotant vert.

L'appareil est maintenant réinitialisé et ses paramètres par défaut ont été restaurés. Lorsque l'appareil se réinitialise, la DEL STATUS s'allume en rouge pendant une demi-seconde, puis s'allume en vert. La console affiche les messages d'amorçage de l'appareil. Le système génère des alertes SNMP et SYSLOG aux hôtes de dérouterments SYSLOG ou SNMP configurés.

Une fois l'appareil redémarré, la console affiche l'invite de connexion à l'appareil. La DEL STATUS clignote en vert. Le nom de connexion et le mot de passe sont **netscreen**.

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 STATUS clignote de nouveau en vert. Si l'appareil n'a pas été réinitialisé, une alerte SNMP est transmise afin de confirmer l'échec de la procédure.

Chapitre 4

Entretien de l'appareil

Ce chapitre détaille les procédures d'entretien et de maintenance des appareils SSG 20. Il présente les sections suivantes :

- « Pièces et outils nécessaires », cette page
- « Remplacement d'un mini-module d'interface physique », cette page
- « Mise à niveau de la mémoire », page 55

REMARQUE pour connaître les instructions et consignes de sécurité, reportez-vous au manuel *Juniper Networks Security Products Safety Guide*. Les instructions du manuel vous mettent en garde vis-à-vis des situations susceptibles d'entraîner des blessures. Avant de travailler sur les équipements, vous devez vous renseigner au sujet des risques présentés par les circuits électriques et vous familiariser avec les pratiques standard de prévention des accidents.

Pièces et outils nécessaires

Pour remplacer un composant de l'appareil SSG 20, vous devez disposer des pièces et outils suivants :

- Sac électrostatique ou tapis antistatique
- Bracelet de mise à la terre contre les décharges électrostatiques
- Tournevis cruciforme, 1/8 po

Remplacement d'un mini-module d'interface physique

Le panneau avant des deux modèles SSG 20 est équipé de deux connecteurs pour les mini-modules d'interface physique de réseau étendu. Il est possible d'installer et de remplacer les mini-modules d'interface physique d'un appareil SSG 20. Avant de retirer ou d'installer un mini-module d'interface physique, vous devez mettre l'appareil hors tension.



ATTENTION : lorsque vous retirez un mini-module d'interface physique, assurez-vous que l'appareil n'est pas sous tension. Les mini-modules d'interface physique ne sont pas remplaçables à chaud.

Dépose d'une plaque avant de protection

Afin de préserver une circulation d'air convenable dans l'appareil SSG 20, vous devez laisser les plaques avant de protection sur les connecteurs qui ne contiennent aucun mini-module d'interface physique. Ne retirez la plaque avant de protection que lors de l'installation d'un mini-module d'interface physique dans un connecteur vide.

Procédez comme suit pour déposer une plaque avant de protection :

1. Placez un sac électrostatique ou un tapis antistatique sur la surface sur laquelle vous avez l'intention de poser le mini-module d'interface physique (la surface doit être plane et stable).
2. Fixez un bracelet de mise à la terre contre les décharges électrostatiques sur votre poignet nu et raccordez le bracelet au point de décharge électrostatique du châssis ou à un point de décharge électrostatique extérieur (si l'appareil SSG 20 n'est pas mis à la terre).
3. Débranchez l'adaptateur électrique de l'appareil. Assurez-vous que la DEL POWER est éteinte.
4. Desserrez et retirez les vis situées de chaque côté de la plaque avant à l'aide d'un tournevis.
5. Retirez la plaque avant, puis placez-la dans le sac électrostatique ou sur le tapis antistatique.

Dépose d'un mini-module d'interface physique

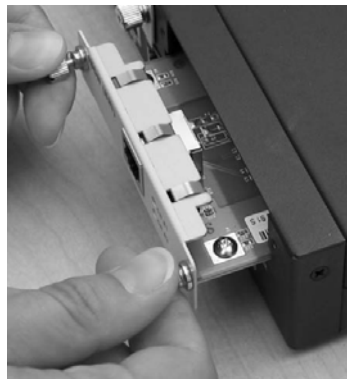
Les mini-modules d'interface physique sont insérés dans le panneau avant de l'appareil SSG 20. Le poids d'un mini-module d'interface physique est inférieur à 106 g (0,2 lb).

Procédez comme suit pour déposer un mini-module d'interface physique :

1. Placez un sac électrostatique ou un tapis antistatique sur la surface sur laquelle vous avez l'intention de poser le mini-module d'interface physique (la surface doit être plane et stable).
2. Fixez un bracelet de mise à la terre contre les décharges électrostatiques sur votre poignet nu et raccordez le bracelet au point de décharge électrostatique du châssis ou à un point de décharge électrostatique extérieur (si l'appareil SSG 20 n'est pas mis à la terre).
3. Débranchez l'adaptateur électrique de l'appareil. Assurez-vous que la DEL POWER est éteinte.

4. Étiquetez les câbles connectés au mini-module d'interface physique de manière à pouvoir reconnecter chaque câble au mini-module d'interface physique correspondant par la suite.
5. Déconnectez les câbles du mini-module d'interface physique.
6. Si nécessaire, disposez les câbles de manière à éviter qu'ils ne se détachent ou qu'ils ne développent des points de tension :
 - a. Fixez les câbles de manière à ce qu'ils ne soutiennent pas leur propre poids lorsqu'ils sont suspendus.
 - b. Placez le surplus de câble dans une boucle bien enroulée de manière à ce que le câble ne soit pas gênant.
 - c. Utilisez des éléments de fixation pour maintenir la forme des boucles de câble.
7. Desserrez et retirez les vis situées de chaque côté de la plaque avant du mini-module d'interface physique à l'aide d'un tournevis.
8. Saisissez les vis situées de chaque côté de la plaque avant du mini-module d'interface physique et faites glisser le mini-module d'interface physique hors de l'appareil. Placez le mini-module d'interface physique dans le sac électrostatique ou sur le tapis antistatique.

Figure 16 : dépose d'un mini-module d'interface physique



9. Si vous ne réinstallez pas un mini-module d'interface physique dans le connecteur vide, placez une plaque avant de protection sur le connecteur de manière à préserver une circulation d'air convenable.

Installation d'un mini-module d'interface physique

Procédez comme suit pour installer un mini-module d'interface physique :

1. Fixez un bracelet de mise à la terre contre les décharges électrostatiques sur votre poignet nu et raccordez le bracelet au point de décharge électrostatique du châssis ou à un point de décharge électrostatique extérieur (si l'appareil SSG 20 n'est pas mis à la terre).

2. Débranchez l'adaptateur électrique de l'appareil. Assurez-vous que la DEL POWER est éteinte.
3. Saisissez les vis situées de chaque côté de la plaque avant du mini-module d'interface physique et alignez les encoches du connecteur situé à l'arrière du mini-module d'interface physique sur les encoches du connecteur de l'appareil SSG 20. Faites ensuite glisser le mini-module d'interface physique jusqu'à ce qu'il soit fermement inséré dans l'appareil.

Figure 17 : installation d'un mini-module d'interface physique



ATTENTION : faites glisser le mini-module d'interface physique bien droit dans le connecteur de manière à ne pas endommager les composants du mini-module d'interface physique.

4. Serrez les vis situées de chaque côté de la plaque avant du mini-module d'interface physique à l'aide d'un tournevis pour écrous à fente de 1/8 po.
5. Insérez les câbles adaptés dans les connecteurs de câble du mini-module d'interface physique.
6. Si nécessaire, disposez les câbles de manière à éviter qu'ils ne se détachent ou qu'ils ne développent des points de tension :
 - a. Fixez les câbles de manière à ce qu'ils ne soutiennent pas leur propre poids lorsqu'ils sont suspendus.
 - b. Placez le surplus de câble dans une boucle bien enroulée de manière à ce que le câble ne soit pas gênant.
 - c. Utilisez des éléments de fixation pour maintenir la forme des boucles de câble.
7. Débranchez l'adaptateur électrique de l'appareil. Assurez-vous que la DEL POWER reste allumée en vert lorsque vous appuyez sur la touche d'alimentation.
8. Assurez-vous que la DEL d'état du mini-module d'interface physique située sur le panneau de commande du système reste allumée en vert pour confirmer que le mini-module d'interface physique est en ligne.

Mise à niveau de la mémoire

Vous pouvez procéder à la mise à niveau d'un appareil SSG 20 d'une mémoire vive dynamique à module de mémoire à double rangée de connexions de 128 Mo à 256 Mo.

Procédez comme suit pour mettre la mémoire d'un appareil SSG 20 à niveau :

1. Fixez un bracelet de mise à la terre contre les décharges électrostatiques sur votre poignet nu et raccordez le bracelet au point de décharge électrostatique du châssis ou à un point de décharge électrostatique extérieur (si l'appareil n'est pas mis à la terre).
2. Débranchez le cordon CA de la prise électrique.
3. Retournez l'appareil de manière à ce que sa partie supérieure repose sur une surface plane.
4. Retirez les vis du couvercle de la carte mémoire à l'aide d'un tournevis cruciforme. Conservez les vis à proximité de vous afin de pouvoir remettre le couvercle en place par la suite.
5. Retirez le couvercle de la carte mémoire.

Figure 18 : partie inférieure de l'appareil



6. Retirez la mémoire vive dynamique à module de mémoire à double rangée de connexions de 128 Mo en plaçant les pouces sur la partie extérieure des onglets de verrouillage situés de chaque côté du module de manière à les libérer du module.

Figure 19 : déverrouillage du module de mémoire



7. Saisissez par le côté long le module de mémoire et faites glisser le module vers l'extérieur. Mettez le module de côté.

Figure 20 : dépose du module



8. Insérez la mémoire vive dynamique à module de mémoire à double rangée de connexions de 256 Mo dans le connecteur. À l'aide des deux pouces, exercez une pression uniforme sur la partie supérieure du module, puis appuyez sur le module jusqu'à ce que les onglets de verrouillage s'enclenchent.

Figure 21 : insertion du module de mémoire



9. Remplacez le couvercle de la carte mémoire sur le connecteur.
10. Fixez le couvercle sur l'appareil en serrant les vis à l'aide du tournevis cruciforme.

Annexe A

Spécifications

Cette annexe détaille les spécifications système générales d'un appareil SSG 20. Elle présente les sections suivantes :

- « Spécifications physiques », page 60
- « Spécifications électriques », page 60
- « Tolérance environnementale », page 60
- « Homologations », page 61
- « Connecteurs », page 62

Spécifications physiques

Tableau 8 : spécifications physiques de l'appareil SSG 20

Description	Valeur
Dimensions du châssis	294 mm x 194,8 mm x 44 mm (11,5 po x 7,7 po x 2 po)
Poids de l'appareil	1,53 kg (3,3 lb), lorsque les mini-modules d'interface physique ne sont pas installés
Module d'interface physique RNIS	70 g
Module d'interface physique ADSL annexe A	106 g
Module d'interface physique ADSL annexe B	106 g
Module d'interface physique T1	75 g
Module d'interface physique E1	75 g
Module d'interface physique V.92	79 g

Spécifications électriques

Tableau 9 : spécifications électriques de l'appareil SSG 20

Élément	Spécification
Tension d'entrée CC	12 V
Courant nominal système CC	3 – 4,16 A

Tolérance environnementale

Tableau 10 : tolérance environnementale de l'appareil SSG 20

Description	Valeur
Altitude	Aucune baisse de performances jusqu'à 2 000 mètres (6 600 pi)
Humidité relative	Fonctionnement normal garanti avec une plage d'humidité relative comprise entre 10 et 90 %, sans condensation
Température	Fonctionnement normal garanti avec une plage de températures comprise entre 0 °C (32 °F) et 40 °C (104 °F) Température de stockage dans le carton d'expédition : -4 °C (-20 °F) à 70 °C (158 °F)

Homologations

Sécurité

- CAN/CSA-C22.2 n°60950-1-03/UL 60950-1, sécurité des équipements informatiques
- EN 60950-1 (2000) troisième édition, sécurité des équipements informatiques
- IEC 60950-1 (1999) troisième édition, sécurité des équipements informatiques

Émissions CEM

- FCC article 15 catégorie B (États-Unis)
- EN 55022 catégorie B (Europe)
- AS 3548 catégorie B (Australie)
- VCCI catégorie B (Japon)

Immunité CEM

- EN 55024
- EN-61000-3-2, harmonique des lignes électriques
- EN-61000-3-3, harmonique des lignes électriques
- EN-61000-4-2, immunité aux décharges électrostatiques
- EN-61000-4-3, immunité aux rayonnements électromagnétiques
- EN-61000-4-4, immunité aux transitoires rapides en salves
- EN-61000-4-5, immunité à l'onde de choc (foudre)
- EN-61000-4-6, immunité commune aux basses fréquences
- EN-61000-4-11, immunité aux creux et variations de tension

ETSI

EN-3000386-2 ETSI (European Telecommunications Standards Institute) : équipements des réseaux de télécommunication. Exigences en matière de compatibilité électromagnétique, (catégorie d'équipements - autre que les centres de télécommunication)

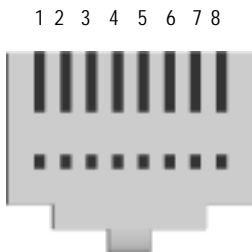
Interface T1

- FCC article 68 - TIA 968
- Industry Canada CS-03
- UL 60950-1, exigences applicables pour les circuits téléphoniques avec connexion de ligne extérieure à l'usine

Connecteurs

La Figure 22 indique l'emplacement des broches sur le connecteur RJ-45.

Figure 22 : schémas de brochage RJ-45



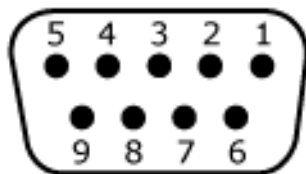
Le Tableau 11 répertorie les broches des connecteurs RJ-45.

Tableau 11 : broches des connecteurs RJ-45

Broche	Nom	E/S	Description
1	RTS Out	S	Demande d'émission
2	DTR Out	S	Terminal prêt
3	TxD	S	Transmission de données
4	GND	S/O	Mise à la terre du châssis
5	GND	S/O	Mise à la terre du châssis
6	RxD	E	Réception de données
7	DSR	E	Modem prêt
8	CTS	E	Prêt à émettre

La Figure 23 indique l'emplacement des broches sur le connecteur femelle DB-9.

Figure 23 : connecteur femelle DB-9



Le Tableau 12 répertorie les broches des connecteurs DB-9.

Tableau 12 : broches des connecteurs DB-9

Broche	Nom	E/S	Description
1	DCD	E	Détection de porteuse
2	RxD	E	Réception de données
3	TxD	S	Transmission de données
4	DTR	S	Terminal prêt
5	GND	S/O	Mise à la terre du signal
6	DSR	E	Modem prêt
7	RTS	S	Demande d'émission
8	CTS	E	Prêt à émettre
9	RING	E	Indicateur d'appel

Annexe B

Initial Configuration Wizard

Cette annexe fournit des informations détaillées au sujet de l'Initial Configuration Wizard (Assistant de configuration initiale) d'un appareil SSG 20.

Une fois l'appareil physiquement connecté au réseau, vous pouvez utiliser l'Initial Configuration Wizard pour configurer les interfaces installées sur l'appareil.

Cette section présente les fenêtres suivantes de l'Initial Configuration Wizard :

- Fenêtre de déploiement rapide page 66
- Fenêtre de connexion de l'administrateur page 66
- Fenêtre du point d'accès au réseau local sans fil page 67
- Fenêtre de l'interface physique page 67
- Fenêtre de l'interface ADSL2/2+ page 68
- Fenêtres de l'interface T1 page 70
- Fenêtres de l'interface E1 page 75
- Fenêtres de l'interface RNIS page 77
- Fenêtre de l'interface à modem V.92 page 80
- Fenêtre de l'interface eth0/0 (zone Untrust) page 81
- Fenêtre de l'interface eth0/1 (zone DMZ) page 82
- Fenêtre de l'interface bgroup0 (zone Trust) page 83
- Fenêtre de l'interface wireless0/0 (zone Trust) page 84
- Fenêtre du récapitulatif de l'interface page 85
- Fenêtre de l'interface DHCP Ethernet physique page 86
- Fenêtre de l'interface DHCP sans fil page 86
- Fenêtre de confirmation page 87

1. Fenêtre de déploiement rapide

Figure 24 : fenêtre de déploiement rapide

Si le réseau utilise NetScreen-Security Manager (NSM), vous pouvez configurer automatiquement l'appareil à l'aide d'un configlet de déploiement rapide. Demandez un configlet à votre administrateur NSM, sélectionnez **Yes**, sélectionnez **Load Configlet from:**, accédez à l'emplacement du fichier, puis cliquez sur **Next**. Le configlet procède à la configuration de l'appareil à votre place, il ne vous est donc pas nécessaire d'utiliser la procédure suivante pour configurer l'appareil.

Si vous souhaitez contourner l'Initial Configuration Wizard et accéder directement à l'interface utilisateur Web, sélectionnez la dernière option, puis cliquez sur **Next**.

Si vous ne configurez pas l'appareil à l'aide d'un configlet et souhaitez utiliser l'Initial Configuration Wizard, sélectionnez la première option, puis cliquez sur **Next**. L'écran de bienvenue de l'Initial Configuration Wizard s'affiche. Cliquez sur **Next**. La fenêtre de connexion de l'administrateur s'affiche.

2. Fenêtre de connexion de l'administrateur

Saisissez un nouveau nom et un nouveau mot de passe d'administrateur, puis cliquez sur **Next**.

Figure 25 : fenêtre de connexion de l'administrateur

3. Fenêtre du point d'accès au réseau local sans fil

Si vous utilisez l'appareil dans le domaine réglementaire WORLD ou ETSI, vous devez sélectionner un code national. Sélectionnez les options adaptées, puis cliquez sur **Next**.

Figure 26 : fenêtre du code national du point d'accès sans fil

The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. Below the title bar, the text 'How do you want to configure the wireless access point?' is displayed. The window contains several configuration options: 'Regulatory Domain' is set to 'WORLD'; 'Country Code' is set to 'NO_COUNTRY_SET'; '2.4G Mode' is set to '802.11b/g'; and '5G Mode' is set to '802.11a'. There is a checkbox labeled 'Configure wireless0/0 interface in trust zone.' which is checked. At the bottom of the window, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

4. Fenêtre de l'interface physique

Dans l'écran des liaisons interface/zone, sélectionnez l'interface à laquelle vous souhaitez relier la zone de sécurité Untrust. Le groupe bgroup0 est préalablement relié à la zone de sécurité Trust. L'interface eth0/1 est reliée à la zone de sécurité DMZ mais est facultative.

Figure 27 : fenêtre de l'interface physique

The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. Below the title bar, the text 'Please choose one interface for untrust, dmz and trust zone respectively.' is displayed. The window contains three configuration options: 'Untrust Zone' is set to 'eth0/0'; 'DMZ Zone' is set to 'eth0/1'; and 'Trust Zone' is set to 'bgroup0'. At the bottom of the window, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Une fois l'interface reliée à une zone, vous pouvez la configurer. Les fenêtres de configuration affichées à partir de là varient en fonction des mini-modules d'interface physique installés dans l'appareil de sécurité. Pour poursuivre la configuration de l'appareil à l'aide de l'Initial Configuration Wizard, cliquez sur **Next**.

5. Fenêtre de l'interface ADSL2/2+

Si le mini-module d'interface physique ADSL2/2 + est installé dans votre appareil, vous pouvez configurer l'interface adslx/0 à l'aide de la fenêtre suivante.

REMARQUE: si deux mini-modules d'interface physique ADSL2/2 + sont installés dans votre appareil, vous ne pouvez pas configurer la fonction de liaisons multiples à l'aide de l'Initial Configuration Wizard. Pour configurer la connexion ADSL à liaisons multiples, reportez-vous au manuel *Concepts & Examples ScreenOS Reference Guide*.

Figure 28 : fenêtre de configuration de l'interface ADSL

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20 device. At the top, there's a blue header with the Juniper logo and 'SSG 20'. Below it, a red text prompt says: 'Please click the following links or the above figure to configure interfaces.' followed by three links: [adsl1/0\(Untrust Zone\)](#), [bgroup0\(Trust Zone\)](#), and [eth0/1\(DMZ Zone\)](#).

The main configuration section is titled 'How does the Juniper device connect to the outside via adsl1/0 interface?'. It contains several fields and radio buttons:

- VPI/VCI:** Two input boxes with '8' and '35' respectively.
- Multiplexing Method:** A dropdown menu showing 'LLC'.
- RFC1483 Protocol Mode:** Two radio buttons: 'Bridged' (selected) and 'Routed'.
- Operating Mode:** Five radio buttons: 'Auto' (selected), 'ANSI DMT', 'ITU DMT', 'Adsl2', and 'Adsl2+'.
- Dynamic IP options:** Three radio buttons: 'Dynamic IP via DHCP', 'Dynamic IP via PPPoA', and 'Dynamic IP via PPPoE'. Each has associated fields for 'Username', 'Password', and 'Confirm'.
- Static IP:** A radio button that is selected. It has fields for 'Interface IP:', 'Netmask:', and 'Gateway:'.

At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Tableau 13 : champs de la fenêtre de configuration de l'interface ADSL

Champ	Description
Informations du fournisseurs de services :	
VPI/VCI	Valeurs VPI/VCI permettant d'identifier le circuit virtuel permanent
Multiplexing Method	Méthode de multiplexage ATM (LLC est la valeur par défaut)
RFC1483 Protocol Mode	Paramètre du mode de protocole (Bridged est la valeur par défaut)
Operating Mode	Mode de fonctionnement de la ligne physique (Auto est la valeur par défaut)
Paramètres de configuration IP	<ul style="list-style-type: none"> ■ Sélectionnez Dynamic IP via DHCP pour permettre à l'appareil de recevoir l'adresse IP de l'interface ADSL à partir d'un fournisseur de services. ■ Sélectionnez Dynamic IP via PPPoA pour permettre à l'appareil d'agir en tant que client PPPoA. Saisissez le nom d'utilisateur et le mot de passe attribués par le fournisseur de services. ■ Sélectionnez Dynamic IP via PPPoE pour permettre à l'appareil d'agir en tant que client PPPoE. Saisissez le nom d'utilisateur et le mot de passe attribués par le fournisseur de services. ■ Sélectionnez Static IP pour attribuer une adresse IP unique et fixe à l'interface ADSL. Saisissez l'adresse IP, le masque de réseau et la passerelle de l'interface (l'adresse de la passerelle correspond à l'adresse IP du port de routeur connecté à l'appareil).

Si vous ne connaissez pas ces paramètres, reportez-vous au document *Common Settings for Service Providers* inclus avec l'appareil du fournisseur de services.

6. Fenêtres de l'interface T1

Si le mini-module d'interface physique T1 est installé dans votre appareil et que l'option Frame Relay est sélectionnée, les fenêtres suivantes s'affichent :

- fenêtre T1 avec un onglet Physical Layer
- fenêtre T1 avec un onglet Frame Relay

REMARQUE : si deux mini-modules d'interface physique T1 sont installés dans votre appareil et si vous avez sélectionné l'option de liaisons multiples, deux onglets Physical Layer s'affichent.

Figure 29 : fenêtre T1 avec un onglet Physical Layer

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20 device. At the top, there's a navigation bar with icons for various configuration steps. Below it, a message says: 'Please click the following links or the above figure to configure interfaces.' followed by links for 'serial1/0(Untrust Zone)', 'bggroup0(Trust Zone)', and 'eth0/1(DMZ Zone)'. The main question is 'How does the Juniper device connect to the outside via serial1/0(T1) interface?'. Under 'WAN Encapsulation', 'Frame Relay' is selected. The 'Physical Layer' tab is active, showing various configuration options for the physical layer. At the bottom, there are buttons for '<< Previous', 'Next >>', and 'Cancel'.

Initial Configuration Wizard

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.
[serial1/0\(Untrust Zone\)](#) [bggroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

How does the Juniper device connect to the outside via serial1/0(T1) interface?

WAN Encapsulation: ☒ Frame Relay ☐ PPP ☐ Cisco HDLC

Physical Layer **Frame Relay**

Clocking: ☒ External ☐ Internal (Lab Use Only)

Line Buildout: 0~132 Feet

Line Encoding: ☐ AMI (Auto Mark Inversion) ☒ B8ZS (8-bits Zero Suppression)

Byte Encoding: ☐ 7-bits per byte ☒ 8-bits per byte

Frame Checksum: ☒ 16-bits ☐ 32-bits

Framing Mode: ☐ Super Frame ☒ Extended Super Frame

Idle Cycles Flag: ☒ 0x7E ☐ 0xFF(All Ones)

Start/End Flags: ☒ Filler ☐ Share

Invert data: ☐

Loopback Respond: ☐

Time Slots: 0 (0(all active), 1..24(e.g. 2,7-9))

<< Previous Next >> Cancel

Tableau 14 : champs de la fenêtre T1 avec un onglet Physical Layer

Champ	Description
Clocking	Permet de régler l'horloge de transmission de l'interface.
Line Buildout	Permet de définir la distance de transmission d'une ligne par l'interface. Le paramètre par défaut est compris entre 0 et 40 mètres (0 et 132 pieds).
Line Encoding	Permet de définir le format de codage de ligne dans l'interface : <ul style="list-style-type: none"> ■ Auto Mark Inversion ■ 8-bits zero suppression
Byte Encoding	Permet d'utiliser le codage par octet qui doit être utilisé dans l'interface T1 : 7 bits par octet ou 8 bits par octet. La valeur par défaut est 8 bits par octet.
Frame Checksum	Permet de définir la taille de la somme de contrôle. La valeur par défaut est 16 .
Framing Mode	Permet de définir le format de verrouillage de trame. La valeur par défaut est Extended mode .
Idle Cycles Flag	Permet de définir la valeur transmise par l'interface lors des cycles à vide. Le paramètre par défaut est 0x7E : <ul style="list-style-type: none"> ■ 0x7E (flags) ■ 0xFF (ones)
Start/End Flags	Permet de définir la transmission des drapeaux de début et de fin (filler ou shared). La valeur par défaut est filler .
Case à cocher Invert Data	Permet d'activer la transmission inversée des bits de données inutilisés.
Case à cocher Loopback Respond	Permet d'activer la boucle avec retour de l'interface T1 à partir d'une CSU (unité de services de canaux) distante.
Time Slots	Permet d'activer l'utilisation d'intervalle de temps au niveau d'une interface T1. La valeur par défaut est 0 , les 24 intervalles de temps disponibles sont utilisés.

Figure 30 : fenêtre T1 avec un onglet Frame Relay

Initial Configuration Wizard

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.
[serial1/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

How does the Juniper device connect to the outside via serial1/0(T1) interface?
 WAN Encapsulation: ☒ Frame Relay ☐ PPP ☐ Cisco HDLC

Physical Layer **Frame Relay**

No-Keepalive: ☐
 Type: ☒ ANSI ☐ ITU

Please configure the sub interface.
 Interface Name: serial1/0. (1~32)
 Inverse ARP: ☐
 Frame Relay DLCI: (16~1022)
 Interface IP:
 Netmask:
 Gateway:

<< Previous Next >> Cancel

Tableau 15 : champs de la fenêtre T1 avec un onglet Frame Relay

Champ	Description
Case à cocher No-Keepalive	Permet d'activer l'absence d'anomalies.
Type	Permet de définir le type LMI de relais de trames : <ul style="list-style-type: none"> ■ ANSI : l'American National Standards Institute prend en charge des débits maximaux de 8 Mbits/s dans le sens descendant et de 1 Mbits/s dans le sens ascendant. ■ ITU : l'International Telecommunications Union prend en charge des débits de 6 144 Mbits/s dans le sens descendant et de 640 bits/s dans le sens ascendant.
Interface Name	Permet de définir le nom de la sous-interface.
Inverse ARP	Permet d'activer le protocole de résolution d'adresses inverse de la sous-interface.
Frame Relay DLCI	Permet d'attribuer un identificateur de connexion de liaison de données (DLCI) à la sous-interface.
Interface IP	Permet de définir l'adresse IP de la sous-interface.
Netmask	Permet de définir le masque de réseau de la sous-interface.
Gateway	Permet de définir l'adresse de la passerelle de la sous-interface.

Si le mini-module d'interface physique T1 est installé dans votre appareil et que l'option PPP est sélectionnée, les fenêtres supplémentaires suivantes s'affichent :

- fenêtre de l'option PPP avec un onglet PPP
- fenêtre de l'option PPP avec un onglet Peer User

Figure 31 : fenêtre de l'option PPP avec un onglet PPP

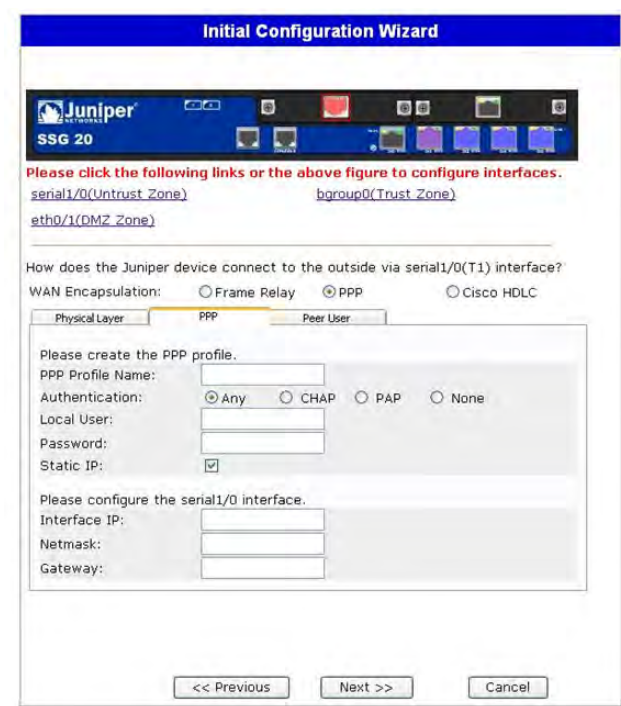


Tableau 16 : champs de la fenêtre de l'option PPP avec un onglet PPP

Champ	Description
PPP Profile Name	Permet de définir le nom du profil PPP.
Authentication	Permet de définir le type d'authentification.
Local User	Permet de définir le nom de l'utilisateur local.
Password	Permet de définir le mot de passe de l'utilisateur local.
Case à cocher Static IP	Permet d'activer une adresse IP statique.
Interface IP	Permet de définir l'adresse IP de l'interface serialx/0.
Netmask	Permet de définir le masque de réseau de l'interface serialx/0.
Gateway	Permet de définir l'adresse de la passerelle de l'interface serialx/0.

Figure 32 : fenêtre de l'option PPP avec un onglet Peer User

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20 device. At the top, there's a header with the Juniper logo and 'SSG 20'. Below it, a message says: 'Please click the following links or the above figure to configure interfaces.' followed by links: [serial1/0\(Untrust_Zone\)](#), [hgroup0\(Trust_Zone\)](#), and [eth0/1\(DMZ_Zone\)](#). The main question is 'How does the Juniper device connect to the outside via serial1/0(T1) interface?'. Under 'WAN Encapsulation:', there are three radio buttons: 'Frame Relay' (unselected), 'PPP' (selected), and 'Cisco HDLC' (unselected). Below this, there are three tabs: 'Physical Layer', 'PPP', and 'Peer User'. The 'Peer User' tab is selected and highlighted in yellow. It contains three input fields: 'Peer User:', 'Password:', and 'Status:'. The 'Status:' field has two radio buttons: 'Enable' (selected) and 'Disable' (unselected). At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Tableau 17 : champs de la fenêtre de l'option PPP avec un onglet Peer User

Champ	Description
Peer User	Permet de définir le nom de l'utilisateur du poste.
Password	Permet de définir le mot de passe de l'utilisateur de poste indiqué dans la zone de texte Peer User.
Status	Permet d'activer ou de désactiver le protocole PPP.

Si le mini-module d'interface physique T1 est installé dans votre appareil et que l'option de procédure de commande à haut niveau Cisco est sélectionnée, la fenêtre suivante s'affiche :

Figure 33 : fenêtre de l'option de procédure de commande à haut niveau Cisco avec un onglet Cisco HDLC

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20 device, similar to Figure 32. The 'WAN Encapsulation:' section has 'Cisco HDLC' selected. The 'Physical Layer' tab is selected and highlighted in yellow. It contains three input fields: 'Interface IP:', 'Netmask:', and 'Gateway:'. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Tableau 18 : champs de la fenêtre de l'option de procédure de commande à haut niveau Cisco avec un onglet Cisco HDLC

Champ	Description
Interface IP	Permet de définir l'adresse IP de l'interface de procédure de commande à haut niveau Cisco T1.
Netmask	Permet de définir le masque de réseau de l'interface de procédure de commande à haut niveau Cisco T1.
Gateway	Permet de définir l'adresse de la passerelle de l'interface de procédure de commande à haut niveau Cisco T1.

7. Fenêtres de l'interface E1

Si le mini-module d'interface physique E1 est installé dans votre appareil et que l'option Frame Relay est sélectionnée, les fenêtres suivantes s'affichent :

- fenêtre E1 avec un onglet Physical Layer
- fenêtre E1 avec un onglet Frame Relay

REMARQUE : si deux mini-modules d'interface physique E1 sont installés dans votre appareil et si vous avez sélectionné l'option de liaisons multiples, deux onglets Physical Layer s'affichent.

Figure 34 : fenêtre E1 avec un onglet Physical Layer



Tableau 19 : champs de la fenêtre E1 avec un onglet Physical Layer

Champ	Description
Clocking	Permet de régler l'horloge de transmission de l'interface.
Frame Checksum	Permet de définir la taille de la somme de contrôle. La valeur par défaut est 16 .
Framing Mode	Permet de définir le format de verrouillage de trame. La valeur par défaut est without CRC4 .
Idle Cycles Flag	Permet de définir la valeur transmise par l'interface lors des cycles à vide. Le paramètre par défaut est 0x7E : <div><input checked="" type="checkbox"/> 0x7E (flags) <input type="checkbox"/> 0xFF (ones)</div>
Start/End Flags	Permet de définir la transmission des drapeaux de début et de fin (filler ou shared). La valeur par défaut est filler.
Case à cocher Invert Data	Permet d'activer la transmission inversée des bits de données non utilisés.
Time Slots	Permet d'activer l'utilisation d'intervalle de temps au niveau d'une interface T1. La valeur par défaut est 0 , les 32 intervalles de temps disponibles sont utilisés.

Figure 35 : fenêtre E1 avec un onglet Frame Relay

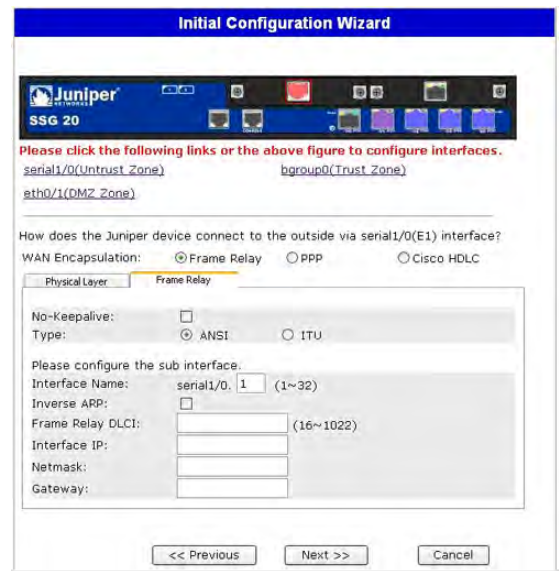


Tableau 20 : champs de la fenêtre E1 avec un onglet Frame Relay

Champ	Description
Case à cocher No-Keepalive	Permet d'activer l'absence d'anomalies.
Type	Permet de définir le type LMI de relais de trames : <div><input checked="" type="checkbox"/> ANSI : l'American National Standards Institute prend en charge des débits maximaux de 8 Mbits/s dans le sens descendant et de 1 Mbits/s dans le sens ascendant. <input type="checkbox"/> ITU : l'International Telecommunications Union prend en charge des débits de 6 144 Mbits/s dans le sens descendant et de 640 bits/s dans le sens ascendant.</div>

Champ	Description
Interface Name	Permet de définir le nom de la sous-interface.
Case à cocher Inverse ARP	Permet d'activer le protocole de résolution d'adresses (ARP) inverse de la sous-interface.
Frame Relay DLCI	Permet d'attribuer un DLCI à la sous-interface.
Interface IP	Permet de définir l'adresse IP de la sous-interface.
Netmask	Permet de définir le masque de réseau de la sous-interface.
Gateway	Permet de définir l'adresse de la passerelle de la sous-interface.

Pour configurer l'interface E1 à l'aide des options PPP, reportez-vous à la section « fenêtre de l'option PPP avec un onglet PPP », page 73.

Pour configurer l'interface E1 à l'aide de la procédure de commande à haut niveau Cisco, reportez-vous à la section « fenêtre de l'option de procédure de commande à haut niveau Cisco avec un onglet Cisco HDLC », page 74.

8. Fenêtres de l'interface RNIS

Si le mini-module d'interface physique RNIS est installé dans votre appareil, vous pouvez configurer l'interface bri1/0 (Untrust) à l'aide de la fenêtre suivante.

REMARQUE : si deux mini-modules d'interface physique RNIS sont installés dans votre appareil et si vous avez sélectionné l'option de liaisons multiples, deux onglets Physical Layer s'affichent.

Figure 36 : fenêtre RNIS avec un onglet Physical Layer



Tableau 21 : champs de la fenêtre RNIS avec un onglet Physical Layer

Champ	Description
Switch Type	Permet de définir le type de commutateur du fournisseur de services : <ul style="list-style-type: none"> ■ att5e : At&T 5ESS ■ ntdms100 : Nortel DMS 100 ■ ins-net : NTT INS-Net ■ etsi : European variants ■ ni1 : National ISDN-1
SPID1	Identifiant du fournisseur de services, généralement un numéro de téléphone à sept chiffres avec des numéros en option. Seuls les types de commutateur DMS-100 et NI1 nécessitent des SPID. Deux SPID sont attribués au type de commutateur DMS-100, un pour chaque canal B.
SPID2	Identifiant du fournisseur de services secondaire
TEI Negotiation	Permet d'indiquer à quel moment l'identificateur de point d'extrémité de terminal doit être négocié : au démarrage ou lors du premier appel. Ce paramètre est généralement utilisé dans le cadre des services RNIS proposés en Europe et des connexions à des commutateurs DMS-100 conçus pour initier la négociation de l'identificateur de point d'extrémité de terminal.
Calling Number	Numéro de facturation du réseau RNIS
Case à cocher Sending Complete	Permet d'activer l'envoi d'informations complètes au niveau du message de configuration sortant. Ce paramètre n'est généralement utilisé qu'à Hong Kong et Taiwan.

Vous pouvez configurer l'interface bri1/0 de manière à ce qu'elle se connecte à l'aide du composeur, du composeur à liaisons multiples, de la ligne louée ou de l'accès de base. Le fait de sélectionner une ou les deux options (ou aucune des options) affiche une fenêtre similaire à la suivante.

Figure 37 : fenêtre RNIS avec onglet Connection

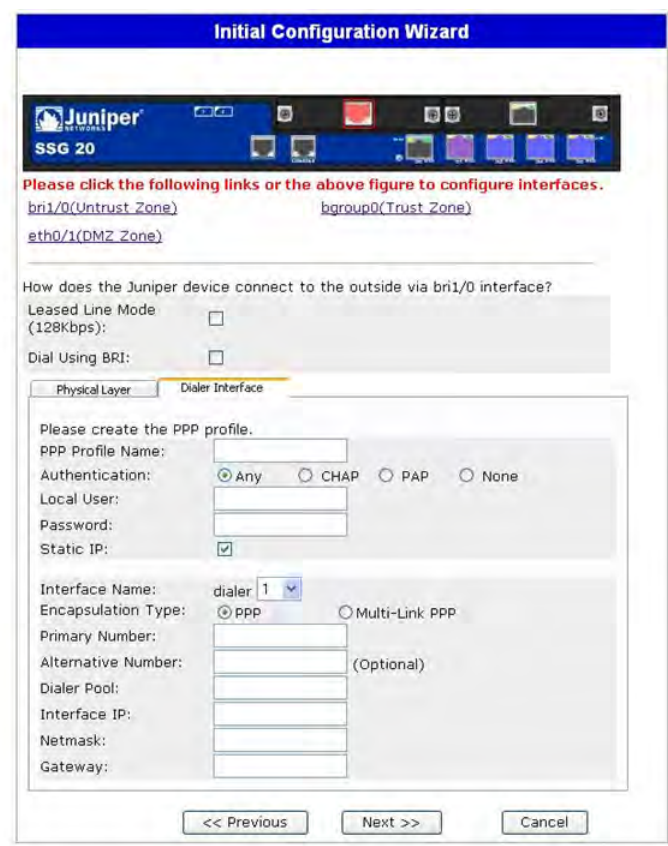


Tableau 22 : champs de la fenêtre RNIS avec onglet Connection

Champ	Description
PPP Profile Name	Permet de définir un nom de profil PPP au niveau de l'interface RNIS.
Authentication	Permet de définir le type d'authentification PPP : <ul style="list-style-type: none">■ Any■ CHAP : Challenge Handshake Authentication Protocol■ PAP : Password Authentication Protocol■ None
Local User	Permet de définir l'utilisateur local.
Password	Permet de définir le mot de passe de l'utilisateur local.
Case à cocher Static IP	Permet d'activer une adresse IP statique pour l'interface.
Interface IP	Permet de définir l'adresse IP de l'interface.
Interface Name (composeur uniquement)	Permet de définir le nom de l'interface du composeur. La valeur par défaut est dialer.1 .
Encapsulation Type	Permet de définir le type d'encapsulation du composeur et du composeur utilisant l'interface BRI (accès de base). La valeur par défaut est PPP .
Primary Number	Permet de définir le numéro principal du composeur et du composeur utilisant les interfaces BRI (accès de base).

Champ	Description
Alternative Number	Permet de définir le numéro alternatif (secondaire) qui doit être utilisé lorsque la connexion au numéro principal est impossible.
Dialer Pool (composeur uniquement)	Permet de définir le nom de la réserve de l'interface du composeur.
Netmask	Permet de définir le masque de réseau.
Gateway	Permet de définir l'adresse de la passerelle.

9. Fenêtre de l'interface à modem V.92

Si le mini-module d'interface physique V.92 est installé dans votre appareil, vous pouvez configurer l'interface serialx/0 (Modem) à l'aide de la fenêtre suivante :

Figure 38 : fenêtre de l'interface à modem

Tableau 23 : champs de la fenêtre de l'interface à modem

Champ	Description
Modem Name	Permet de définir le nom de l'interface à modem.
Init String	Permet de définir la chaîne de caractères d'initialisation du modem.
ISP Name	Permet d'attribuer un nom au fournisseur de services.
Primary Number	Permet de définir le numéro de téléphone permettant d'accéder au fournisseur de services.
Alternative Number (facultatif)	Permet de définir un autre numéro de téléphone permettant d'accéder au fournisseur de services en cas d'absence de connexion du numéro principal.
Login Name	Permet de définir le nom de connexion du compte du fournisseur de services.
Password	Permet de définir le mot de passe correspondant au nom de connexion.
Confirm	Permet de confirmer le mot de passe saisi dans le champ Password.

10. Fenêtre de l'interface eth0/0 (zone Untrust)

L'interface eth0/0 peut disposer d'une adresse IP statique ou dynamique, attribuée via le protocole DHCP ou PPPoE.

Figure 39 : fenêtre de l'interface eth0/0

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20. At the top, there's a header with the Juniper logo and 'SSG 20'. Below it, a message says: 'Please click the following links or the above figure to configure interfaces.' with three links: [eth0/0\(Untrust_Zone\)](#), [bgroup0\(Trust_Zone\)](#), and [eth0/1\(DMZ_Zone\)](#). The main section is titled 'Enter the IP address and netmask for the interface eth0/0(untrust zone)'. It has three radio button options: 'Dynamic IP via DHCP', 'Dynamic IP via PPPoE', and 'Static IP'. The 'Static IP' option is selected. Under 'Dynamic IP via PPPoE', there are fields for 'Username:', 'Password:', and 'Confirm:'. Under 'Static IP', there are fields for 'Interface IP:', 'Netmask:', and 'Gateway:'. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Tableau 24 : champs de la fenêtre de l'interface eth0/0

Champ	Description
Dynamic IP via DHCP	Permet à l'appareil de recevoir une adresse IP pour l'interface de la zone Untrust par l'intermédiaire d'un fournisseur de services.
Dynamic IP via PPPoE	Permet à l'appareil d'agir en tant que client PPPoE et de recevoir une adresse IP pour l'interface de la zone Untrust par l'intermédiaire d'un fournisseur de services. Saisissez le nom d'utilisateur et le mot de passe attribués par le fournisseur de services.
Static IP	Permet d'attribuer une adresse IP fixe et unique à l'interface de la zone Untrust. Définissez l'adresse IP, le masque de réseau et l'adresse de la passerelle de l'interface de la zone Untrust.

11. Fenêtre de l'interface eth0/1 (zone DMZ)

L'interface eth0/1 peut disposer d'une adresse IP statique ou dynamique, attribuée via le protocole DHCP.

Figure 40 : fenêtre de l'interface eth0/1



Tableau 25 : champs de la fenêtre de l'interface eth0/1

Champ	Description
Dynamic IP via DHCP	Permet à l'appareil de recevoir une adresse IP pour l'interface DMZ par l'intermédiaire d'un fournisseur de services.
Static IP	Permet d'attribuer une adresse IP fixe et unique à l'interface DMZ. Définissez l'adresse IP et le masque de réseau de l'interface DMZ.

12. Fenêtre de l'interface bgroup0 (zone Trust)

L'interface bgroup0 peut disposer d'une adresse IP statique ou dynamique, attribuée via le protocole DHCP.

L'adresse IP par défaut de l'interface est 192.168.1.1, avec le masque de réseau 255.255.255.0 ou 24.

Figure 41 : fenêtre de l'interface bgroup0



Tableau 26 : champs de la fenêtre de l'interface bgroup0

Champ	Description
Dynamic IP via DHCP	Permet à l'appareil de recevoir une adresse IP pour l'interface de la zone Trust par l'intermédiaire d'un fournisseur de services.
Static IP	Permet d'attribuer une adresse IP fixe et unique à l'interface de la zone Trust. Définissez l'adresse IP et le masque de réseau de l'interface de la zone Trust.

13. Fenêtre de l'interface wireless0/0 (zone Trust)

Si vous configurez l'appareil SSG 20-WLAN, vous devez définir un SSID (Service Set Identifier) avant d'activer l'interface wireless0/0. Pour obtenir des instructions détaillées relatives à la configuration de la ou des interfaces sans fil, reportez-vous au manuel *Concepts & Examples ScreenOS Reference Guide*.

Figure 42 : fenêtre de l'interface wireless0/0

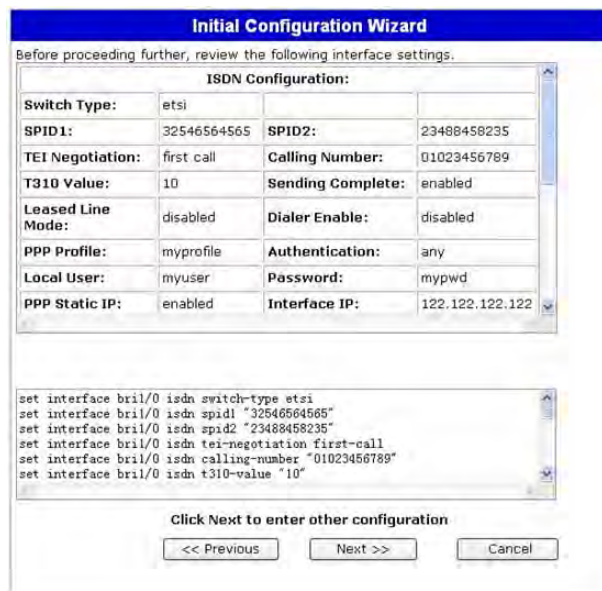
The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20 device. At the top, a blue banner reads 'Initial Configuration Wizard'. Below it, a red text prompt says 'Please click this wlan radio to configure wireless.' with a small icon of a radio. A toolbar with various icons is visible. Below the toolbar, a red text prompt says 'Please click the following links or the above figure to configure interfaces.' followed by four links: [eth0/0\(Untrust_Zone\)](#), [hgroup0\(Trust_Zone\)](#), [eth0/1\(DMZ_Zone\)](#), and [wireless0/0\(Trust_Zone\)](#). The main section is titled 'How do you want to configure wireless0/0 interface(trust zone)?'. It includes a 'Wlan Mode:' dropdown set to '2.4G(802.11b/g)'. Below this is an 'SSID:' text field. There are two main radio buttons: 'Open' (selected) and 'WPA-PSK'. Under 'Open', there is a 'No Encryption' option. Under 'WPA-PSK', there are three sub-options: 'Passphrase(8~63 ASCII):' (selected), 'PSK(64 hexadecimal):', and 'Encryption Type:' with radio buttons for 'Auto' (selected), 'TKIP', and 'AES'. Each of these sub-options has a 'Confirm:' label and a corresponding text field. At the bottom, there are fields for 'Interface IP:' (192.168.2.1) and 'Netmask:' (255.255.255.0). Navigation buttons at the bottom include '<< Previous', 'Next >>', and 'Cancel'.

Tableau 27 : champs de la fenêtre de l'interface wireless0/0

Champ	Description
Wlan Mode	Définissez le mode radio du réseau local sans fil : <ul style="list-style-type: none"> ■ 5 G (802.11 a) ■ 2,4 G (802.11 b/g) ■ Both (802.11 a/b/g)
SSID	Permet de définir le nom SSID.
Authentification et chiffrement	Permet de définir le mode d'authentification et de chiffrement de l'interface du réseau local sans fil : <ul style="list-style-type: none"> ■ L'authentification Open, valeur par défaut, permet à n'importe qui d'accéder à l'appareil. Il n'existe pas de chiffrement pour cette option d'authentification. ■ L'authentification WPA Pre-Shared Key définit la clé partagée au préalable ou la phrase de passe qui doit être saisie lors de l'établissement d'une connexion sans fil. Vous pouvez saisir une valeur hexadécimale ou ASCII pour la clé partagée au préalable. Une clé hexadécimale partagée au préalable doit correspondre à une valeur hexadécimale de 256 bits (64 caractères). Une phrase de passe ASCII doit comprendre entre 8 et 63 caractères. Vous devez sélectionner le protocole TKIP (Temporal Key Integrity Protocol) ou AES (Advanced Encryption Standard) comme type de chiffrement pour cette option ou sélectionner Auto pour activer une des options. ■ WPA2 Pre-Shared Key ■ WPA Auto Pre-Shared Key
Interface IP	Permet de définir l'adresse IP de l'interface du réseau local sans fil.
Netmask	Permet de définir le masque de réseau de l'interface du réseau local sans fil.

14. Fenêtre du récapitulatif de l'interface

Une fois les interfaces du réseau étendu configurées, la fenêtre du récapitulatif de l'interface s'affiche.

Figure 43 : fenêtre du récapitulatif de l'interface

Vérifiez la configuration de l'interface, puis cliquez sur **Next** lorsque vous êtes prêt à poursuivre. La fenêtre de l'interface DHCP Ethernet physique s'affiche.

15. Fenêtre de l'interface DHCP Ethernet physique

Sélectionnez **Yes** pour permettre à votre appareil d'attribuer des adresses IP à votre réseau câblé via le protocole DHCP. Saisissez la plage d'adresses IP que votre appareil doit attribuer aux clients à l'aide de votre réseau, puis cliquez sur **Next**.

Figure 44 : fenêtre de l'interface DHCP Ethernet physique

The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. The main area has a light blue background. The text reads: 'Do you want the Juniper device to dynamically assign IP addresses to your local **wired** hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses.' There are two radio buttons: 'Yes' and 'No'. The 'No' button is selected. Below the radio buttons, there are four input fields: 'IP Address Range Start' (192.168.1.33), 'End' (192.168.1.126), 'DNS Server 1 (optional)', and 'DNS Server 2 (optional)'. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

16. Fenêtre de l'interface DHCP sans fil

Sélectionnez **Yes** pour permettre à votre appareil d'attribuer des adresses IP à votre réseau sans fil via le protocole DHCP. Saisissez la plage d'adresses IP que votre appareil doit attribuer aux clients à l'aide de votre réseau, puis cliquez sur **Next**.

Figure 45 : fenêtre de l'interface DHCP sans fil

The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. The main area has a light blue background. The text reads: 'Do you want the Juniper device to dynamically assign IP addresses to your local **wireless** hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses.' There are two radio buttons: 'Yes' and 'No'. The 'No' button is selected. Below the radio buttons, there are four input fields: 'IP Address Range Start' (192.168.2.33), 'End' (192.168.2.126), 'DNS Server 1 (optional)', and 'DNS Server 2 (optional)'. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

17. Fenêtre de confirmation

Vérifiez la configuration de votre appareil et apportez aux modifications nécessaires. Cliquez sur **Next** pour procéder à l'enregistrement, au redémarrage de l'appareil et à l'exécution de la configuration.

Figure 46 : fenêtre de confirmation

Initial Configuration Wizard

Before proceeding further, review the following all device settings.

Admin Login:	netscreen		Password:	*****		
Device is in NAT mode.						
ISDN Configuration:						
Switch Type:	etsi		SPID1:	32546564565	SPID2:	23488458235
TEI Negotiation:	first call		Calling Number:	01023456789		
T310 Value:	10		Sending Complete:	enabled		
Leased Line Mode:	disabled		Dialer Enable:	disabled		
PPP Profile:	myprofile		Authentication:	any		

```

set admin password "netscreen"
set interface bril/0 isdn switch-type etsi
set interface bril/0 isdn spid1 "32546564565"
set interface bril/0 isdn spid2 "23488458235"
set interface bril/0 isdn tei-negotiation first-call
set interface bril/0 isdn calling-number "01023456789"
  
```

Click Next to save CLI into device.

<< Previous Next >> Cancel

Une fois l'appareil redémarré avec la configuration système enregistrée, l'invite de connexion de l'interface utilisateur Web apparaît. Pour obtenir des informations relatives à la procédure d'accès à l'appareil à l'aide de l'interface utilisateur Web, reportez-vous à la section « Utilisation de l'interface utilisateur Web », page 29.

Index

A

adresse IP et masque de réseau du fournisseur de services	44
adresse IP statique	41
adresses IP par défaut	32
ADSL	
configuration de l'interface	41
connexion du câble	24
connexion du port	24
Annexe A	24
Annexe B	24
antennes	26

C

câbles	
ADSL	24
connexions réseau de base	23
série	24
certifications	
immunité CEM	61
configuration	
accès administratif	35
adresse de gestion	36
association sans fil et Ethernet	40
chiffrement et authentification sans fil	38
circuits virtuels	42
date et heure	34
groupes ponts (bgroup)	34
hôte et nom de domaine	36
interface non sécurisée secondaire	37
mini-module d'interface physique à modem V.92	47
mini-module d'interface physique ADSL 2/2 +	41
mini-module d'interface physique E1	46
mini-module d'interface physique RNIS	45
mini-module d'interface physique T1	46
nom et mot de passe de l'administrateur	33
paire VPI/VCI	42
route par défaut	36
services de gestion	35
USB	17
connexion, réseau de base	23
Couche d'adaptation 5 au mode de transfert asynchrone (ATM)	41

D

DEL	
liaison d'activité sur les ports Ethernet	13
PIM 1	12
PIM 2	12
POWER	12
STATUS	12
DEL WLAN	
802.11a	12
b/g	12

E

émetteurs-récepteurs radio	
WLAN 0	16
WLAN 1	16

G

gestion	
par l'intermédiaire d'une connexion Telnet	30
par l'intermédiaire d'une console	28
par l'intermédiaire de l'interface utilisateur Web	29

H

homologations	
CEM (émissions)	61
European Telecommunications Standards Institute (ETSI)	61
interface T1	62
sécurité	61

I

interface secondaire vers zone Untrust	37
--	----

M

Mini-module d'interface physique	
dépose	52
installation	53
mini-module d'interface physique	
plaque avant de protection	52
multiplexage AAL5	41
multiplexage, configuration	42

P

Point-to-Point Protocol over ATM

Voir PPPoA

Point-to-Point Protocol over Ethernet

Voir PPPoE

PPPoA 41

PPPoE 41

procédure de mise à niveau de la mémoire 55

S

sans fil

antennes 26

utilisation de l'interface par défaut..... 26

T

trou d'épingle de réinitialisation, utilisation..... 49

V

Virtual Path Identifier (Identificateur de trajet

virtuel)/Virtual Channel Identifier (Identificateur de canal virtuel)

Voir VPI/VCI

VPI/VCI

configuration 42

valeurs..... 41

Z

zone Untrust, configuration d'une interface

secondaire 37

Inhaltsverzeichnis

Zu diesem Handbuch	5
Organisation	6
WebUI-Konventionen.....	6
Konventionen für die Befehlszeilenschnittstelle	7
Abrufen von Dokumentationen und technischem Support.....	8
Kapitel 1 Hardware – Überblick	9
Verbindungs- und Netzanschlüsse.....	10
Bedienfeld.....	11
Systemstatus-LEDs	11
Anschlüsse – Beschreibungen.....	13
Ethernet-Anschlüsse.....	13
Konsolenanschluss	13
AUX-Anschluss	14
Mini Physical Interface Module – Anschlussbeschreibungen.....	14
Rückseite	16
Stromadapter	16
Funktransceiver.....	16
Erdungsansatz	16
Antennentypen.....	17
USB-Anschluss.....	17
Kapitel 2 Installieren und Anschließen des Geräts	19
Einleitung.....	20
Installieren der Geräte.....	20
Anschließen von Schnittstellenkabeln an ein Gerät	22
Anschließen der Stromversorgung	22
Anschließen eines Geräts an ein Netzwerk.....	23
Anschließen des Geräts an ein nicht vertrauenswürdiges Netzwerk.....	23
Ethernet-Anschlüsse.....	24
Serielle (AUX-/Konsol-) Anschlüsse	24
Anschließen von Mini-PIMs an ein nicht vertrauenswürdiges Netzwerk... 24	
ADSL2/2 + Mini-PIM	24
ISDN, T1, E1 und V.92-Mini-PIMs.....	25
Anschließen des Geräts an ein internes Netzwerk oder	
eine Arbeitsstation	26
Ethernet-Anschlüsse.....	26
Wireless-Antennen.....	26
Kapitel 3 Konfigurieren des Geräts	27
Zugriff auf das Gerät	28
Verwenden einer Konsolenverbindung.....	28

Verwenden der WebUI	29
Verwenden von Telnet	30
Standardmäßige Geräteeinstellungen	31
Grundlegende Gerätekonfiguration	33
Administrator auf Stammebene – Name und Kennwort	33
Datum und Uhrzeit	34
Bridge-Gruppenschnittstellen	34
Administratorzugriff	35
Verwaltungsdienste	35
Host- und Domänenname	36
Standardroute	36
Adresse der Verwaltungsschnittstelle	36
Konfiguration der Untrust Sicherungsschnittstelle	37
Grundlegende Wireless-Konfiguration	37
Konfiguration des Mini-PIM	41
ADSL2/2 + -Schnittstelle	41
Virtuelle Verbindungen	42
VPI/VCI und Multiplexingmethode	42
PPPoE oder PPPoA	43
Statische IP-Adresse und Netzmaske	44
ISDN ISDN-Schnittstelle	45
T1-Schnittstelle	46
E1-Schnittstelle	46
V.92 Modemschnittstelle	47
Grundlegender Firewallschutz	48
Überprüfen der externen Verbindung	49
Zurücksetzen eines Geräts auf die werkseitigen Standardeinstellungen	49
Kapitel 4 Warten des Geräts	51
Erforderliche Werkzeuge und Teile	51
Ersetzen eines Mini-Physical Interface Module	51
Entfernen einer unbeschrifteten Frontscheibe	52
Entfernen eines Mini-PIM	52
Einbauen eines Mini-PIM	53
Erweitern des Arbeitsspeichers	54
Anhang A Technische Daten	57
Physisch	58
Elektrik	58
Umgebungstoleranz	58
Zertifizierungen	59
Sicherheit	59
EMC-Emissionen	59
EMC-Störfestigkeit	59
ETSI	59
T1-Schnittstelle	60
Stecker	60
Anhang B Assistent für die Anfangskonfiguration	63
Index	87

Zu diesem Handbuch

Das Secure Services Gateway (SSG) 20-Gerät von Juniper Networks ist eine integrierte Router- und Firewallplattform, die Zweigstellen oder Einzelhandelsgeschäften Internet Protocol Security (IPSec) Virtual Private Network (VPN)- und Firewalldienste bietet.

Juniper Networks bietet zwei Ausführungen des SSG 20-Geräts an:

- SSG 20, das Auxiliary (AUX)-Verbindung unterstützt.
- SSG 20-WLAN, das integrierte 802.11a/b/g-Wireless-Standards unterstützt.

Beide SSG 20-Geräte unterstützen Universal Serial Bus (USB)-Speichergeräte und verfügen über zwei Mini Physical Interface Module (PIM)-Steckplätze, die mit sämtlichen Mini-PIMs kompatibel sind. Die Geräte ermöglichen zudem Protokollkonvertierungen zwischen Local Area Networks (LANs) und Wide Area Networks (WANs).

HINWEIS: Die Konfigurationsanweisungen und Beispiele in diesem Dokument basieren auf den Funktionen eines Geräts, auf dem ScreenOS 5.4 ausgeführt wird. Die Funktionsweise Ihres Gerätes unterscheidet sich möglicherweise abhängig von der verwendeten ScreenOS-Version. Die aktuellsten Gerätedokumentationen erhalten Sie auf der Juniper Networks-Website für technische Informationen unter <http://www.juniper.net/techpubs/hardware>. Die derzeit für Ihr Gerät verfügbaren ScreenOS-Versionen werden auf der Juniper Networks-Supportwebsite unter <http://www.juniper.net/customers/support/> angezeigt.

Organisation

Dieses Handbuch ist in folgende Abschnitte gegliedert:

- In Kapitel 1, „Hardware – Überblick,“ werden das Gehäuse und die Komponenten eines SSG 20-Geräts beschrieben.
- In Kapitel 2, „Installieren und Anschließen des Geräts,“ werden die Montage eines SSG 20-Geräts sowie das Anschließen von Kabeln und der Stromversorgung an das Gerät beschrieben.
- In Kapitel 3, „Konfigurieren des Geräts,“ werden die Konfiguration und die Verwaltung eines SSG 20-Geräts sowie die Durchführung einiger grundlegender Konfigurationsaufgaben beschrieben.
- In Kapitel 4, „Warten des Geräts,“ werden die Wartungsmaßnahmen für SSG 20-Geräte erläutert.
- In Anhang A, „Technische Daten,“ finden Sie allgemeine technische Systemdaten für SSG 20-Geräte.
- In Anhang B bietet „Assistent für die Anfangskonfiguration,“ detaillierte Informationen zur Verwendung des Assistenten für die Anfangskonfiguration (Initial Configuration Wizard, ICW) für SSG 20-Geräte.

WebUI-Konventionen

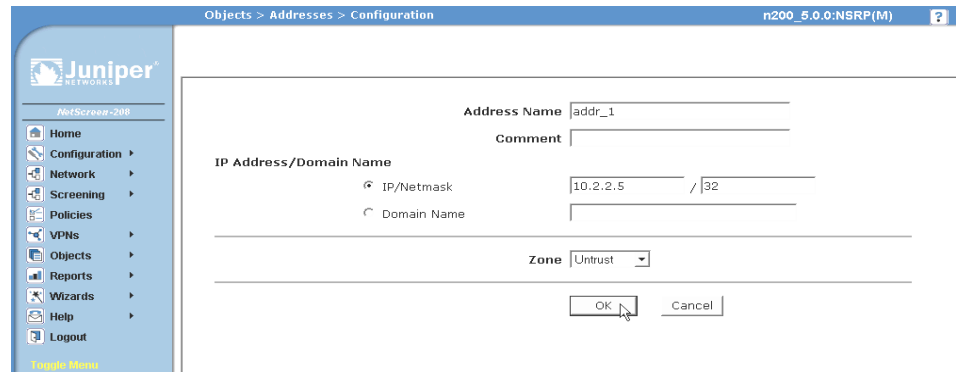
Navigieren Sie zum Ausführen einer Aufgabe mit der WebUI zuerst zum entsprechenden Dialogfeld, um dort Objekte zu definieren und Parameter festzulegen. Ein Rechtspfeil (>) zeigt die Schritte bei der Navigation durch die WebUI an, die durch Klicken auf Menüoptionen und Links ausgeführt werden. Die Anweisungen für jede Aufgabe werden in die Navigationspfad- und Konfigurationseinstellungen unterteilt.

Die folgende Abbildung zeigt den Pfad zum Adressenkonfigurations-Dialogfeld mit den folgenden Beispielkonfigurationseinstellungen:

Objects > Addresses > List > New: Geben Sie Folgendes ein, und klicken Sie dann auf **OK**:

Address Name: addr_1
 IP Address/Domain Name:
 IP/Netmask: (select), 10.2.2.5/32
 Zone: Untrust

Abbildung 1: Navigationspfad- und Konfigurationseinstellungen



Konventionen für die Befehlszeilenschnittstelle

Die folgenden Konventionen dienen zur Darstellung der Syntax der Befehlszeilenbefehle in Beispielen und Text.

In Beispielen:

- 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.

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

In Text:

- Befehle werden **fett** dargestellt.
- Variablen werden *kursiv* dargestellt.

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 kath j12fmt54** ist z. B. ausreichend für den Befehl **set admin user kathleen j12fmt54**. Obwohl solche Abkürzungen zum Eingeben von Befehlen verwendet werden können, sind alle in diesem Handbuch dokumentierten Befehle vollständig dargestellt.

Abrufen von Dokumentationen und technischem Support

Technische Dokumentationen für Juniper Networks-Produkte stehen 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.

Wenn Sie Fehler oder Auslassungen in diesem Dokument entdecken, schreiben Sie an folgende E-Mail-Adresse:

techpubs-comments@juniper.net

Kapitel 1

Hardware – Überblick

Dieses Kapitel beinhaltet detaillierte Beschreibungen des SSG 20-Chassis und seiner Komponenten. Der Anhang umfasst die folgenden Abschnitte:

- „Verbindungs- und Netzanschlüsse“ auf Seite 10
- „Bedienfeld“ auf Seite 11
- „Rückseite“ auf Seite 16

Verbindungs- und Netzanschlüsse

In diesem Abschnitt wird die Position der integrierten Anschlüsse und der Netzanschlüsse beschrieben und illustriert. Die folgende Abbildung enthält Darstellungen der Anschlusspositionen, und in Tabelle 1 sind die Netzanschlüsse beschrieben.

Abbildung 2: Position von integrierten Anschlüssen und Mini-PIM

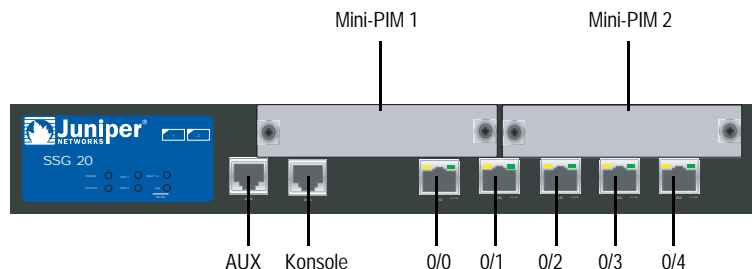


Tabelle 1: SSG 20-Anschlüsse und -Netzanschlüsse

Anschluss	Beschreibung	Stecker	Geschwindigkeit/Protokoll
0/0-0/4	Ermöglicht direkte Verbindungen mit Arbeitsstationen oder eine LAN-Verbindung über einen Switch oder Hub. Mithilfe dieser Verbindung kann das Gerät auch über eine Telnet-Sitzung oder die WebUI verwaltet werden.	RJ-45	Ethernet mit 10/100 MBit/s Automatische Erkennung von Duplex und automatischem MDI/MDIX
USB	Ermöglicht eine USB 1.1-Verbindung mit dem System.	Nicht zutreffend	12 MB (maximale Geschwindigkeit) oder 1,5 MB (minimale Geschwindigkeit)
Konsole	Ermöglicht eine serielle Verbindung mit dem System. Wird für Terminalemulationsverbindungen zum Starten von Befehlszeilenschnittstellen verwendet.	RJ-45	9.600 Bit/s/RS-232C seriell
AUX	Ermöglicht eine asynchrone serielle RS-232-Sicherungsverbindung zum Internet über ein externes Modem.	RJ-45	9.600 Bit/s-115 KBit/s/RS-232C seriell
Mini-PIM			
ADSL 2/2 +	Ermöglicht eine Internetverbindung über eine ADSL-Datenverbindung.	RJ-11 (Annex A) RJ-45 (Annex B)	ANSI T1.413 Ausgabe 2 (nur Annex A) ITU G.992.1 (G.dmt) ITU G.992.3 (ADSL2) ITU G.992.5 (ADSL2 +)
V.92-Modem	Ermöglicht eine Primär- oder Sicherungsverbindung zum Internet bzw. eine nicht vertrauenswürdige Netzwerkverbindung zu einem Dienstanbieter.	RJ-11	9.600 Bit/s-115 KBit/s/RS-232, serielle automatische Erkennung von Duplex und Polarität
T1	Ermöglicht eine Verbindung zur T1-Leitung des nicht vertrauenswürdigen Netzwerks.	RJ-45	1,544 MBit/s (Full-Time-Slots)
E1	Ermöglicht eine Verbindung zur E1-Leitung des nicht vertrauenswürdigen Netzwerks.	RJ-45	2,048 MBit/s (Full-Time-Slots)

Anschluss	Beschreibung	Stecker	Geschwindigkeit/Protokoll
ISDN	Ermöglicht die Verwendung der ISDN-Leitung als Untrust oder Sicherungsschnittstelle. (S/T)	RJ-45	B-Kanäle mit 64 KBit/s Geleaste Leitung mit 128 KBit/s
Antenne A und B (SSG 20-WLAN)	Ermöglicht eine direkte Verbindung mit Arbeitsstationen in der Nähe einer Wireless-Funkverbindung.	RPSMA	802.11 a (54 MBit/s bei Nutzung eines Frequenzbandes von 5 GHz) 802.11 b (11 MBit/s bei Nutzung eines Frequenzbandes von 4 GHz) 802.11 g (54 MBit/s bei Nutzung eines Frequenzbereichs von 2,4 GHz) 802.11 superG (108 MBit/s bei Nutzung eines Frequenzbandes von 2,4 GHz und 5 GHz)

Bedienfeld

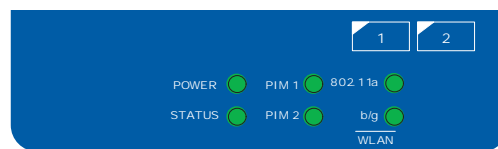
In diesem Abschnitt werden die folgenden Elemente auf dem Bedienfeld eines SSG 20-Geräts beschrieben:

- Systemstatus-LEDs
- Anschlüsse – Beschreibungen
- Mini Physical Interface Module – Anschlussbeschreibungen

Systemstatus-LEDs

Die Systemstatus-LEDs zeigen Informationen zu wichtigen Gerätefunktionen an. Abbildung 3 zeigt die Position jeder Status-LED auf der Vorderseite des SSG 20-WLAN-Geräts. Nur das SSG 20-WLAN-Gerät verfügt über WLAN-LEDs.

Abbildung 3: Status-LEDs



Beim Hochfahren des Systems blinkt die Strom-LED grün, und die Status-LED wechselt in dieser Abfolge: Rot, Grün, grün blinkend. Der Startvorgang nimmt etwa zwei Minuten in Anspruch. Möchten Sie das System aus- und anschließend wieder einschalten, wird empfohlen, nach dem Herunterfahren einige Sekunden zu warten, bevor das System wieder hochgefahren wird. Tabelle 2 beinhaltet den Namen, die Farbe, den Status und die Beschreibung jeder Systemstatus-LED.

Tabelle 2: Status-LED – Beschreibungen

Name	Farbe	Status	Beschreibung
POWER	Grün	Ständig leuchtend	Das System wird mit Strom versorgt.
		Aus	Das System wird nicht mit Strom versorgt.
	Rot	Ständig leuchtend	Das Gerät funktioniert nicht ordnungsgemäß.
		Aus	Das Gerät funktioniert ordnungsgemäß.
STATUS	Grün	Ständig leuchtend	Das System wird gestartet oder führt eine Diagnose durch.
		Blinkend	Das Gerät funktioniert ordnungsgemäß.
	Rot	Blinkend	Ein Fehler wurde festgestellt.
PIM 1	Grün	Ständig leuchtend	Das Mini-PIM funktioniert.
		Blinkend	Das Mini-PIM überträgt Datenverkehr.
		Aus	Das Mini-PIM ist außer Betrieb.
PIM 2	Grün	Ständig leuchtend	Das Mini-PIM funktioniert.
		Blinkend	Das Mini-PIM leitet Datenverkehr weiter.
		Aus	Das Mini-PIM ist außer Betrieb.
WLAN (nur WLAN-Gerät)			
802.11a	Grün	Ständig leuchtend	Die Wireless-Verbindung ist hergestellt, aber es liegt keine Verbindungsaktivität vor.
		Langsam blinkend	Eine Wireless-Verbindung ist hergestellt. Die Baudrate verhält sich proportional zur Verbindungsaktivität.
		Aus	Es ist keine Wireless-Verbindung hergestellt.
b/g	Grün	Ständig leuchtend	Die Wireless-Verbindung ist hergestellt, aber es liegt keine Verbindungsaktivität vor.
		Langsam blinkend	Eine Wireless-Verbindung ist hergestellt. Die Baudrate verhält sich proportional zur Verbindungsaktivität.
		Aus	Es ist keine Wireless-Verbindung hergestellt.

Anschlüsse – Beschreibungen

In diesem Abschnitt werden der Zweck und die Funktion folgender Elemente erläutert:

- Ethernet-Anschlüsse
- Konsolenanschluss
- AUX-Anschluss

Ethernet-Anschlüsse

Fünf 10/100-Ethernet-Anschlüsse ermöglichen LAN-Verbindungen zu Hubs, Switches, lokalen Servern und Arbeitsstationen. Zudem kann ein Ethernet-Anschluss für Verwaltungsdatenverkehr zugewiesen werden. Die Anschlüsse sind fortlaufend mit **0/0** bis **0/4** beschriftet. Unter „Standardmäßige Geräteeinstellungen“ auf Seite 31 erhalten Sie Informationen zu den standardmäßigen Zonenbindungen für jeden Ethernet-Anschluss.

Achten Sie bei der Konfiguration eines der Anschlüsse auf den Schnittstellennamen, der der Position des Anschlusses entspricht. Auf dem Bedienfeld werden die Schnittstellennamen für die Anschlüsse von links nach rechts fortlaufend mit **ethernet0/0** bis **ethernet0/4** bezeichnet.

Abbildung 4 zeigt die Position der LEDs auf jedem Ethernet-Anschluss an.

Abbildung 4: Position der Activity Link-LEDs

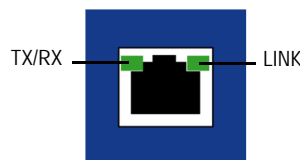


Tabelle 3 zeigt die Ethernet-Anschluss-LEDs an.

Tabelle 3: LAN-Anschluss-LEDs

Name	Farbe	Status	Beschreibung
LINK	Grün	Ständig leuchtend Aus	Anschluss ist online. Anschluss ist offline.
TX/RX	Grün	Blinkend Aus	Datenverkehr wird weitergeleitet. Die Baudrate verhält sich proportional zur Verbindungsaktivität. Der Anschluss ist möglicherweise aktiviert, empfängt jedoch keine Daten.

Konsolenanschluss

Beim Konsolenanschluss handelt es sich um einen seriellen RJ-45-Anschluss, der als zur lokalen Verwaltung verwendbares Data Circuit Terminating Equipment (DCE) verkabelt ist. Verwenden Sie bei einem Klemmanschluss ein Durchgangskabel und ein Crossoverkabel, wenn Sie eine Verbindung zu einem anderen DCE-Gerät herstellen. Ein Adapter für RJ-45 auf DB-9 wird mitgeliefert.

Informationen zu den Kontaktanordnungen der RJ-45-Stecker erhalten Sie unter „Stecker“ auf Seite 60.

AUX-Anschluss

Der Auxiliary (AUX)-Anschluss ist ein serieller RJ-45-Anschluss, der als Data Terminal Equipment (DTE) verkabelt ist. Durch Anschluss an ein Modem ist DTE für die Remoteverwaltung verwendbar. Dieser Anschluss sollte nicht regelmäßig für Remoteverwaltung verwendet werden. Der AUX-Anschluss wird normalerweise als serielle Sicherungsschnittstelle zugewiesen. Die Baudrate kann auf einen Wert zwischen 9.600 Bit/s und 115.200 Bit/s eingestellt werden und erfordert eine Hardwareflusssteuerung. Verwenden Sie beim Anschluss an ein Modem ein Durchgangskabel und beim Anschluss an ein anderes DTE-Gerät ein Crossoverkabel.

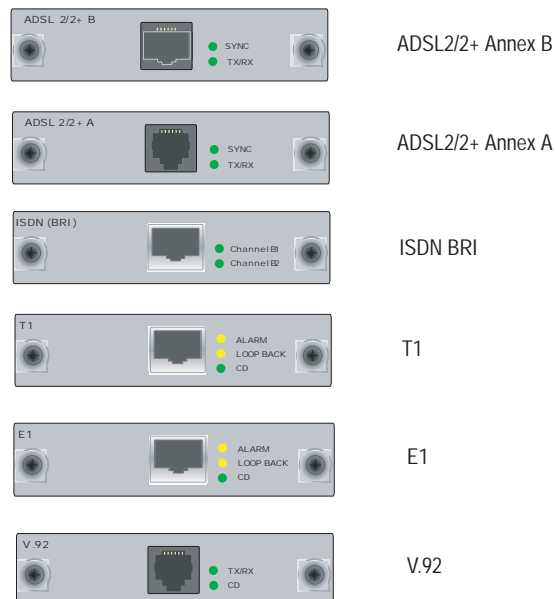
Informationen zu den Kontaktanordnungen der RJ-45-Stecker erhalten Sie unter „Stecker“ auf Seite 60.

Mini Physical Interface Module – Anschlussbeschreibungen

Jedes auf einem Gerät unterstützte Mini Physical Interface Module (PIM) verfügt über die folgenden Komponenten:

- Einen Kabelsteckeranschluss – Akzeptiert einen Netzwerkmedienstecker. Abbildung 5 enthält eine Darstellung der verfügbaren Mini-PIMs. In einem Gerät können maximal zwei Mini-PIMs installiert werden.

Abbildung 5: Mini-PIMs für das SSG 20



- Zwei bis drei Status-LEDs – Zeigt den Anschlussstatus an. In Tabelle 4 wird die Bedeutung der LED-Status erläutert.

Tabelle 4: LED-Status des Mini-PIM auf dem SSG 20

Typ	Name	Farbe	Status	Beschreibung
ADSL 2/2 + (Annex A und B)	SYNC	Grün	Ständig leuchtend	Eine Synchronisierung der ADSL-Schnittstelle wird durchgeführt.
			Blinkend	Die Synchronisierung ist in Bearbeitung.
			Aus	Die Schnittstelle ist nicht aktiv.
	TX/RX	Grün	Blinkend	Datenverkehr wird übertragen.
			Aus	Es wird kein Datenverkehr übertragen.
ISDN (BRI)	CH B1	Grün	Ständig leuchtend	B-Kanal 1 ist aktiv.
			Aus	B-Kanal 1 ist nicht aktiv.
	CH B2	Grün	Ständig leuchtend	B-Kanal 2 ist aktiv.
			Aus	B-Kanal 2 ist nicht aktiv.
T1/E1	ALARM	Gelb	Ständig leuchtend	Ein lokaler Alarm oder ein Remotealarm wurde ausgelöst; das Gerät hat einen Fehler festgestellt.
			Aus	Es ist kein Alarm oder Fehler ausgelöst worden bzw. aufgetreten.
	LOOP BACK	Gelb	Ständig leuchtend	Ein Loopback- oder Leitungsstatus wurde festgestellt.
			Aus	Das Loopback ist nicht aktiv.
	CD	Grün	Ständig leuchtend	Ein Trägersignal wurde festgestellt, und die interne DSU/CSU im Mini-PIM kommuniziert mit einer anderen DSU/CSU.
			Aus	Die Trägersignalerkennung ist nicht aktiv.
V.92	CD	Grün	Ständig leuchtend	Die Verbindung ist aktiv.
			Aus	Die serielle Schnittstelle ist außer Betrieb.
	TX/RX	Grün	Blinkend	Es wird kein Datenverkehr übertragen.
			Aus	Es wird kein Datenverkehr übertragen.



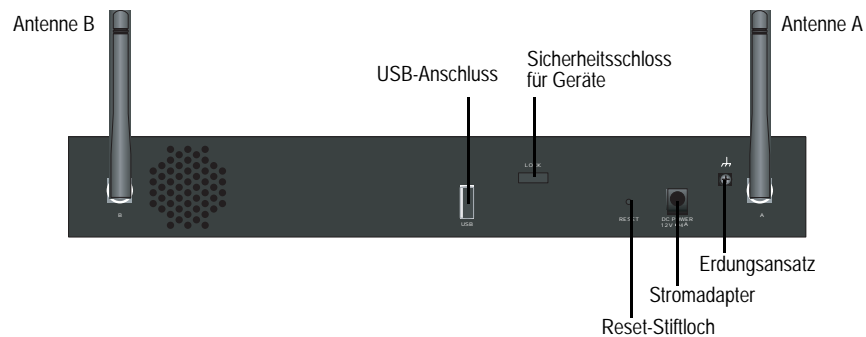
VORSICHT: Die Mini-PIMs sind nicht „hot-swappable“, d.h. der Austausch von Komponenten ist nicht möglich, während der Computer läuft. Die Mini-PIMs müssen vor Einschalten des Geräts in die Steckplätze auf dem Bedienfeld eingesetzt werden.

Rückseite

In diesem Abschnitt werden die folgenden Elemente auf der Rückseite eines SSG 20 Geräts beschrieben:

- Stromadapter
- Funktransceiver
- Erdungsansatz
- Antennentypen
- USB-Anschluss

Abbildung 6: Rückseite eines SSG 20-WLAN-Geräts



Stromadapter

Die Strom-LED auf dem Bedienfeld eines Geräts leuchtet entweder grün oder ist ausgeschaltet. Grün zeigt eine ordnungsgemäße Funktion an, wohingegen eine nicht leuchtende Strom-LED auf einen Stromadapterausfall oder auf den ausgeschalteten Zustand des Geräts hinweist.

Funktransceiver

Die SSG 20-WLAN-Gerät beinhaltet zwei Funktransceiver für Wireless-Verbindungen, die 802.11a/b/g-Standards unterstützen. Der erste Transceiver (WLAN 0) verwendet das 2,4 GHz-Frequenzband, das den 802.11b-Standard bei 11 MBit/s, den 802.11g-Standard bei 54 MBit/s sowie den 802.11 SuperG-Standard bei 108 MBit/s unterstützt. Der zweite Funktransceiver (WLAN 1) verwendet das 5 GHz-Frequenzband, das den 802.11a-Standard bei 54 MBit/s unterstützt. Informationen zur Konfiguration des Wireless-Frequenzbands erhalten Sie unter „Grundlegende Wireless-Konfiguration“ auf Seite 37.

Erdungsansatz

Auf der Rückseite des Chassis ist ein Ein-Loch-Erdungsansatz vorhanden, über den das Gerät geerdet wird (siehe Abbildung 6).

Stellen Sie mit einem Erdungskabel eine Erdung her, und bringen Sie anschließend das Kabel am Ansatz auf der Rückseite des Gehäuses an, um das Gerät vor Herstellung der Stromversorgung zu erden.

Antennentypen

Das SSG 20-WLAN-Gerät unterstützt drei Typen von speziell angefertigten Funkantennen:

- **Doppelantennen** – Die Doppelantennen ermöglichen eine Richtfunkübertragung mit 2 dBi und eine im Wesentlichen einheitliche Signalstärke im Bereich der Funkübertragung und sind für die meisten Installationen geeignet. Dieser Antennentyp wird zusammen mit dem Gerät geliefert.
- **Externe Rundstrahlantenne** – Die externe Antenne ermöglicht eine Rundstrahlübertragung mit 2 dBi. Im Gegensatz zu Doppelantennen, die paarweise eingesetzt werden, beseitigt eine externe Antenne Echoeffekte, die bei Verwendung von zwei Antennen gelegentlich aufgrund eines leicht verzögerten Signalempfangs auftreten.
- **Externe Richtantenne** – Die externe Richtantenne ermöglicht eine Funkübertragung mit 2 dBi in eine Richtung und ist für Orte wie Gänge und Außenmauern (dabei ist die Antenne nach innen gerichtet) geeignet.

USB-Anschluss

Der USB-Anschluss auf der Rückseite eines SSG 20-Geräts nimmt ein Universal Serial Bus (USB)-Speichergerät oder einen USB-Speichergeräteadapter auf, in dem ein Compact Flash-Datenträger installiert ist (siehe Definition in den von der CompactFlash Association veröffentlichten *technischen Angaben zu CompactFlash*. Ist das USB-Speichergerät installiert und konfiguriert, fungiert es automatisch als sekundäres Startgerät, falls beim Start ein Fehler beim primären Compact Flash-Datenträger auftritt.

Der USB-Anschluss ermöglicht Dateiübertragungen wie Gerätekonfigurationen, Benutzerzertifizierungen und die Aktualisierung von Versionsabbildern zwischen einem externen USB-Speichergerät und dem internen Flashspeicher im Sicherheitsgerät. Der USB-Anschluss unterstützt eine Dateiübertragung mit USB 1.1 entweder bei minimaler (1,5 MB) oder maximaler Geschwindigkeit (12 MB).

Führen Sie zur Übertragung von Dateien zwischen dem USB-Speichergerät und einem SSG 20 die folgenden Schritte aus:

1. Stecken Sie das USB-Speichergerät in den USB-Anschluss auf dem Sicherheitsgerät.
2. Speichern Sie die auf dem USB-Speichergerät enthaltenen Dateien mit dem Befehlszeilenbefehl **save {software config | image-key} from usb filename to flash** auf den internen Flashspeicher des Geräts.
3. Trennen Sie das USB-Speichergerät vor dem Entfernen mit dem Befehlszeilenbefehl **exec usb-device stop** vom USB-Anschluss.
4. Das USB-Speichergerät kann nun entfernt werden.

Möchten Sie vom USB-Speichergerät eine Datei löschen, verwenden Sie den Befehlszeilenbefehl **delete file** *usb:/filename* .

Möchten Sie Informationen zu den auf dem USB-Gerät oder dem internen Flashspeicher gespeicherten Dateien anzeigen, verwenden Sie den Befehlszeilenbefehl **get file**.

Kapitel 2

Installieren und Anschließen des Geräts

In diesem Kapitel wird die Montage eines SSG 20-Geräts sowie das Anschließen von Kabeln und der Stromversorgung an das Gerät beschrieben. Dieses Kapitel ist in folgende Abschnitte gegliedert:

- „Einleitung“ auf Seite 20
- „Installieren der Geräte“ auf Seite 20
- „Anschließen von Schnittstellenkabeln an ein Gerät“ auf Seite 22
- „Anschließen der Stromversorgung“ auf Seite 22
- „Anschließen eines Geräts an ein Netzwerk“ auf Seite 23

HINWEIS: Sicherheitshinweise und Anweisungen finden Sie im *Security Products Safety Guide* von Juniper Networks. 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.

Einleitung

Die Position des Chassis, die Reihenfolge bei der Verwendung der Montagegeräte und die Sicherheit des Kabelraums sind für eine ordnungsgemäße des Systems von entscheidender Bedeutung.



WARNHINWEIS: Installieren Sie das SSG 20-Gerät in einer sicheren Umgebung, um Missbrauch und dem Eindringen Unbefugter in den Raum vorzubeugen.

Durch Einhalten der folgenden Vorsichtsmaßnahmen können das Herunterfahren des Geräts sowie Gerätefehler und Verletzungen verhindert werden:

- Überprüfen Sie vor jeder Installation, ob das Netzteil von allen Stromquellen getrennt ist.
- Stellen Sie sicher, dass der Raum, in dem das Gerät betrieben werden soll, ausreichend belüftet ist und dass die Raumtemperatur 40°C (104°F) nicht übersteigt.
- Stellen Sie das Gerät nicht in einem Gerätegestellrahmen auf, durch den die Ein- und Auslassöffnungen blockiert werden. Ein geschlossenes Gestell muss über Lüfter und Lüftungsschlitze verfügen.
- Beseitigen Sie vor jeder Installation die folgenden gefährlichen Umgebungsbedingungen: Feuchte oder nasse Böden, Lecks, ungeerdete oder schadhafte Netzkabel sowie Steckdosen ohne ausreichende Erdung.

Installieren der Geräte

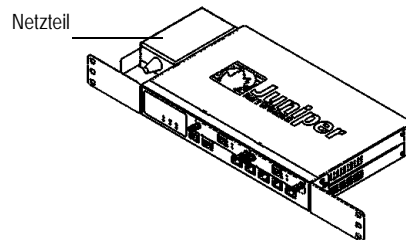
Für ein SSG 20-Gerät ist eine Front-, Wand- oder Schreibtischmontage möglich. Die Montagekits können einzeln gekauft werden.

Zum Montieren eines SSG 20-Geräts werden ein Kreuzschlitzschraubenzieher mittlerer Größe (nicht im Lieferumfang enthalten) und Schrauben benötigt, die mit dem Gerätegestell kompatibel sind (im Kit enthalten).

HINWEIS: Stellen Sie beim Montieren eines Geräts sicher, dass sich dieses nah genug an der Steckdose befindet.

Gehen Sie folgendermaßen vor, um die Frontmontage eines SSG 20-Geräts auf einem handelsüblichen 19 Zoll-Gerätegestell durchzuführen:

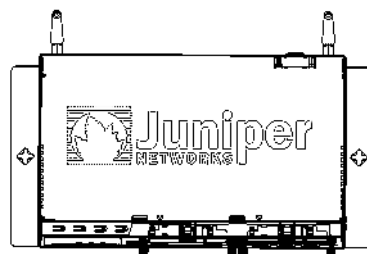
Abbildung 7: SSG 20-Frontmontage



1. Richten Sie die Öse des für eine Gestellmontage vorgesehenen Netzteils am linken vorderen Bereich des Geräts aus.
2. Fixieren Sie die Schrauben mit einem Kreuzschlitzschraubenzieher in den Öffnungen.
3. Richten Sie die andere Öse für die Gestellmontage am rechten vorderen Bereich des Geräts aus.
4. Fixieren Sie die Schrauben mit einem Kreuzschlitzschraubenzieher in den Öffnungen.
5. Montieren Sie das Gerät mit den mitgelieferten Schrauben auf dem Gestell.
6. Schließen Sie das Netzteil an die Steckdose an.

Führen Sie für die Wandmontage eines SSG 20-Geräts die folgenden Schritte aus:

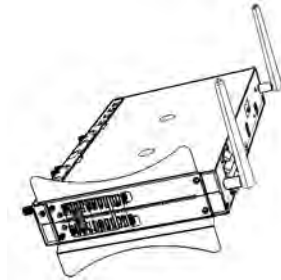
Abbildung 8: Wandmontage des SSG 20



1. Richten Sie die Ösen für die Wandmontage am Gerät aus.
2. Stecken Sie die Schrauben in die Öffnungen, und fixieren Sie diese mit einem Kreuzschlitzschraubenzieher.
3. Die für die Montage vorgesehene Wand muss glatt, eben, trocken und massiv sein.
4. Montieren Sie das Gerät mit den mitgelieferten Schrauben an der Wand.
5. Schließen Sie das Netzteil an die Steckdose an.

Führen Sie für die Schreibtischmontage eines SSG 20-Geräts die folgenden Schritte aus:

Abbildung 9: SSG 20-Schreibtischmontage



1. Befestigen Sie die Vorrichtung zum Aufstellen auf dem Schreibtisch am Gerät. Verwenden Sie am besten die Seite, die dem Stromadapter am nächsten liegt.
2. Stellen Sie das montierte Gerät auf den Schreibtisch.
3. Stecken Sie den Stromadapter ein, und schließen Sie das Netzteil an die Steckdose an.

Anschließen von Schnittstellenkabeln an ein Gerät

Führen Sie zum Anschließen des Schnittstellenkabels an ein Gerät die folgenden Schritte aus:

1. Sie benötigen die für die Schnittstelle erforderliche Kabelart in ausreichender Länge.
2. Stecken Sie den Kabelstecker in den entsprechenden Anschluss auf der Frontscheibe der Schnittstelle.
3. Ordnen Sie das Kabel folgendermaßen an, um ein Herausgleiten des Kabels oder das Entstehen von Belastungsstellen zu verhindern:
 - a. Bringen Sie das Kabel so an, dass es beim Herunterhängen nicht sein eigenes Gewicht stützen muss.
 - b. Ist noch überschüssige Kabellänge vorhanden, legen Sie das Kabel sorgfältig zu einer Schleife zusammen, und räumen Sie diese beiseite.
 - c. Fixieren Sie die Kabel mithilfe von Klemmen.

Anschließen der Stromversorgung

Führen Sie zum Herstellen einer Stromversorgung für das Gerät die folgenden Schritte aus:

1. Schließen Sie den Gleichstromstecker des Netzkabels an die Gleichstromnetzbuchse auf der Rückseite des Geräts an.

2. Schließen Sie den Wechselstromadapter des Netzkabels an eine Wechselstromquelle an.



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

Anschließen eines Geräts an ein Netzwerk

Ein SSG 20-Gerät bietet eine Firewall und allgemeine Sicherheitsfunktionen für Ihre Netzwerke, wenn es zwischen internen Netzwerken und dem nicht vertrauenswürdigen Netzwerk platziert wird. In diesem Abschnitt werden insbesondere die folgenden Themen behandelt:

- Anschließen des Geräts an ein nicht vertrauenswürdiges Netzwerk
- Anschließen des Geräts an ein internes Netzwerk oder eine Arbeitsstation

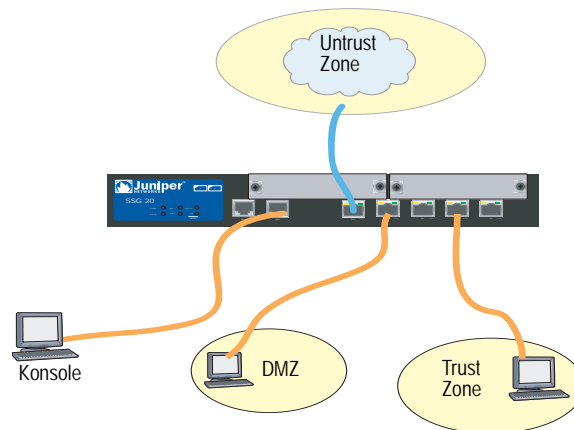
Anschließen des Geräts an ein nicht vertrauenswürdiges Netzwerk

Folgende Möglichkeiten stehen zum Anschluss des SSG 20-Geräts an ein nicht vertrauenswürdiges Netzwerk zur Verfügung:

- Ethernet-Anschlüsse
- Serielle (AUX-/Konsol-) Anschlüsse
- Anschließen von Mini-PIMs an ein nicht vertrauenswürdiges Netzwerk

Abbildung10 zeigt das SSG 20 mit den grundlegenden Netzkabelanschlüssen. Dabei sind zwei leere Mini-PIMs und die 10/100-Ethernet-Anschlüsse folgendermaßen verkabelt:

- Der mit „0/0“ gekennzeichnete Anschluss (Ethernet0/0-Schnittstelle) ist mit dem nicht vertrauenswürdigen Netzwerk verbunden.
- Der mit „0/1“ gekennzeichnete Anschluss (ethernet0/1-Schnittstelle) ist mit einer Arbeitsstation in der DMZ-Sicherheitszone verbunden.
- Der mit „0/3“ gekennzeichnete Anschluss (bgroup0-Schnittstelle) ist mit einer Arbeitsstation in der Trust Sicherheitszone verbunden.
- Der Konsolenanschluss ist zur Gewährleistung des Verwaltungszugriffs mit einem seriellen Terminal verbunden.

Abbildung 10: Grundlegender Netzwerkbetrieb – Beispiel

Ethernet-Anschlüsse

Schließen Sie zum Herstellen einer Hochgeschwindigkeitsverbindung das mitgelieferte Ethernet-Kabel für den Ethernet-Anschluss „0/0“ auf einem SSG 20-Gerät an den externen Router an. Das Gerät erkennt automatisch die erforderliche Geschwindigkeit, den Duplex und die MDI/MDIX-Einstellungen.

Serielle (AUX-/Konsol-) Anschlüsse

Eine Verbindung mit einem nicht vertrauenswürdigen Netzwerk kann mit einem seriellen RJ-45-Durchgangskabel und einem externen Modem hergestellt werden.



WARNHINWEIS: Schließen Sie nicht versehentlich die Konsolen-, AUX- oder Ethernet-Anschlüsse am Gerät an der Telefonanschlussdose an.

Anschließen von Mini-PIMs an ein nicht vertrauenswürdiges Netzwerk

In diesem Abschnitt wird das Verbinden des Mini-PIMs des Geräts mit einem nicht vertrauenswürdigen erläutert.

ADSL2/2+ Mini-PIM

Stellen Sie mit dem mitgelieferten ADSL-Kabel eine Verbindung zwischen der ADSL2/2+ -Mini-PIM und der Telefonbuchse her. 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.

Anschließen von Splitttern und Mikrofiltern

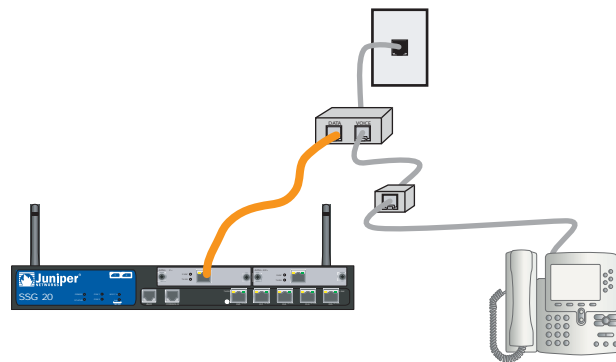
Ein *Signalsplitter* teilt das Telefonsignal in niederfrequente Sprachsignale für Telefonate und hochfrequente Datensignale für Datenverkehr auf. Der Dienstanbieter installiert den Splitter normalerweise zusammen mit dem Gerät, über das die Telefonleitungen an Ihrem Standort mit dem Netzwerk des Anbieters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

Abhängig von den vom Dienstanbieter bereitgestellten Geräten können Sie möglicherweise selbst Splitter installieren. In diesem Fall schließen Sie das ADSL-Kabel vom 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.

Abbildung 11 zeigt ein Beispiel für die Installation eines Mikrofilters und Splitters am Standort. (Die entsprechenden Mikrofilter oder Splitter erhalten Sie von Ihrem Dienstanbieter.)

Abbildung 11: Mikrofilter und Splitter in der Netzwerkverbindung



ISDN, T1, E1 und V.92-Mini-PIMs

Führen Sie zum Anschluss der Mini-PIMs an ein Gerät die folgenden Schritte aus:

1. Sie benötigen die für die Schnittstelle erforderliche Kabelart in ausreichender Länge.
2. Stecken Sie den Kabelstecker in den entsprechenden Anschluss auf der Frontscheibe der Schnittstelle.
3. Ordnen Sie das Kabel folgendermaßen an, um ein Herausgleiten des Kabels oder das Entstehen von Stresspunkten zu verhindern:
 - a. Bringen Sie das Kabel so an, dass es beim Herunterhängen nicht sein eigenes Gewicht stützen muss.
 - b. Ist noch überschüssige Kabellänge vorhanden, legen Sie das Kabel sorgfältig zu einer Schleife zusammen, und räumen Sie diese beiseite.
 - c. Fixieren Sie die Kabel mithilfe von Klemmen.

Informationen zur Konfiguration von ISDN, E1, T1 oder V.92-Mini-PIM erhalten Sie unter „Konfiguration des Mini-PIM“ auf Seite 41.

Anschließen des Geräts an ein internes Netzwerk oder eine Arbeitsstation

Ein Local Area Network (LAN) oder eine Arbeitsstation kann mit den Ethernet- und/oder den Wireless-Schnittstellen verbunden werden.

Ethernet-Anschlüsse

Ein SSG 20-Gerät verfügt über sieben Ethernet-Anschlüsse. Sie können mindestens einen dieser Anschlüsse für die Herstellung einer Verbindung zu 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 Durchgangskabel verwendet werden. Informationen zu den standardmäßigen Zone-zu-Schnittstelle-Bindungen erhalten Sie unter „Standardmäßige Geräteeinstellungen“ auf Seite 31.

Wireless-Antennen

Wenn Sie die Wireless-Schnittstelle verwenden, müssen Sie die mitgelieferten Antennen am Gerät anschließen. Wenn Sie über die standardmäßigen 2 dB-Doppelantennen verfügen, schrauben Sie diese an den mit A und B gekennzeichneten Anschlüssen auf der Geräterückseite fest. Biegen Sie jede Antenne jeweils am Gelenk, ohne dabei Druck auf die Stecker auszuüben.

Abbildung 12: SSG 20-WLAN – Position der Antennen



Führen Sie bei Verwendung der optionalen externen Antenne die beiliegenden Anweisungen für den Anschluss der Antenne aus.

Kapitel 3

Konfigurieren des Geräts

Die ScreenOS-Software ist auf einem SSG 20-Gerät vorinstalliert. Das Gerät wird in eingeschaltetem Zustand konfiguriert. Das Gerät verfügt über eine standardmäßige werkseitige Konfiguration, die den Erstanschluss an das Gerät ermöglicht. Für Ihre speziellen Netzwerkanforderungen müssen Sie jedoch eine Konfigurationen vornehmen.

Dieses Kapitel ist in folgende Abschnitte gegliedert:

- „Zugriff auf das Gerät“ auf Seite 28
- „Standardmäßige Geräteeinstellungen“ auf Seite 31
- „Grundlegende Gerätekonfiguration“ auf Seite 33
- „Grundlegende Wireless-Konfiguration“ auf Seite 37
- „Konfiguration des Mini-PIM“ auf Seite 41
- „Grundlegender Firewallschutz“ auf Seite 48
- „Überprüfen der externen Verbindung“ auf Seite 49
- „Zurücksetzen eines Geräts auf die werkseitigen Standardeinstellungen“ auf Seite 49

HINWEIS: Nach der Konfiguration eines Geräts und der Überprüfung der Verbindung über das Remotenetzwerk, muss das Produkt unter www.juniper.net/support/ registriert werden, damit bestimmte ScreenOS-Dienste, wie z.B. der Deep Inspection-Signaturdienst und der Virenschutz (einzeln erhältlich) auf dem Gerät aktiviert werden. Nach der Registrierung des Produkts abonnieren Sie den Dienst über die WebUI. Weitere Informationen zur Produktregistrierung und zum Abonnieren bestimmter Dienste erhalten Sie im Band *Grundlagen des Concepts & Examples ScreenOS Reference Guide* für die auf dem Gerät installierte ScreenOS-Version.

Zugriff auf das Gerät

Ein Gerät kann auf verschiedene Arten konfiguriert werden:

- **Konsole:** Der Konsolenanschluss am Gerät ermöglicht Ihnen den Zugriff auf das Gerät über ein serielles an die Arbeitsstation oder das Terminal angeschlossenes Kabel. Zum Konfigurieren des Geräts geben Sie am Terminal oder in einem Terminalemulationsprogramm auf Ihrer Arbeitsstation ScreenOS-Befehlszeilenbefehle ein.
- **WebUI:** Bei der ScreenOS-Webbenutzerschnittstelle (WebUI) handelt es sich um eine über einen Browser verfügbare grafische Schnittstelle. Zur Erstverwendung der WebUI muss sich die Arbeitsstation, auf der der Browser ausgeführt wird, im selben Subnetz wie das Gerät befinden. Der Zugriff auf die WebUI über einen sicheren Server kann auch unter Verwendung von Secure Sockets Layer (SSL) mit Secure HTTP (S-HTTP) erfolgen.
- **Telnet/SSH:** Telnet und SSH sind Anwendungen, die Ihnen den Zugriff auf Geräte über ein IP-Netzwerk ermöglichen. Zum Konfigurieren des Geräts geben Sie in einer Telnet-Sitzung an Ihrer Arbeitsstation ScreenOS-Befehlszeilenbefehle ein. Weitere Informationen erhalten Sie im Band *Verwaltung des Concepts & Examples ScreenOS Reference Guide*.
- **NetScreen-Security Manager:** NetScreen-Security Manager ist eine von Juniper Networks entwickelte Verwaltungsanwendung für Unternehmen, mit der Firewall-/IPSec VPN-Geräte von Juniper Networks gesteuert und verwaltet werden. Anweisungen zur Verwaltung des Geräts mithilfe von NetScreen-Security Manager erhalten Sie im *NetScreen-Security Administrator's Guide*.

Verwenden einer Konsolenverbindung

HINWEIS: Verwenden Sie ein serielles RJ-45 CAT5-Durchgangskabel mit einem RJ-45-Stecker, um eine Verbindung mit dem Konsolenanschluss am Gerät herzustellen.

Führen Sie zum Herstellen einer Konsolenverbindung die folgenden Schritte aus:

1. Schließen Sie den Buchsenstecker des mitgelieferten DB-9-Adapters an den seriellen Anschluss der Arbeitsstation an. (Der DB-9-Stecker muss ordnungsgemäß eingesteckt und gesichert sein.) Abbildung 13 zeigt den erforderlichen DB-9-Stecker.

Abbildung 13: DB-9-Adapter

2. Schließen Sie den Stecker des seriellen RJ-45 CAT5-Kabels am Konsolenanschluss am SSG 20 an. (Das andere Ende des CAT5-Kabels muss ordnungsgemäß an den DB-9-Adapter angeschlossen und gesichert sein.)
 3. Starten Sie auf der Arbeitsstation ein serielles Terminalemulationsprogramm. Folgende Einstellungen sind zum Starten einer Konsolensitzung erforderlich:
 - Baudrate: 9600
 - Parität: Keine
 - Datenbits: 8
 - Stoppbit: 1
 - Flusssteuerung: Keine
 4. Wenn Sie die Standardanmeldung für den Administratorknamen und das Kennwort noch nicht geändert haben, geben Sie bei den Eingabeaufforderungen „login“ und „password“ **netscreen** ein. (Verwenden Sie nur Kleinbuchstaben. Für die Felder „login“ und „password“ muss die Groß-/Kleinschreibung beachtet werden.)
- Informationen zur Konfiguration des Geräts mithilfe der Befehlszeilenbefehle erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.
5. Standardmäßig tritt an der Konsole eine Zeitüberschreitung auf, und sie wird automatisch nach 10 Minuten ausbleibender Aktivität beendet (optional). Geben Sie zum Entfernen der Zeitüberschreitung **set console timeout 0** ein.

Verwenden der WebUI

Zur Verwendung der WebUI muss sich die Arbeitsstation, von der aus das Gerät verwaltet wird, zunächst im selben Subnetz wie das Gerät befinden. Führen Sie zum Zugriff auf das Gerät mit der WebUI die folgenden Schritte aus:

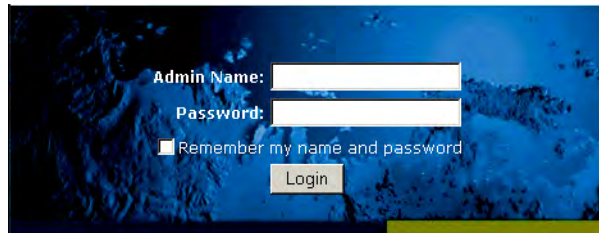
1. Stellen Sie für die Arbeitsstation eine Verbindung zum 0/2-0/4-Anschluss am Gerät her (bgroup0-Schnittstelle in der Trust Zone).
2. Stellen Sie sicher, dass die Arbeitsstation für Dynamic Host Configuration Protocol (DHCP) oder statisch mit einer IP-Adresse im Subnetz 192.168.1.0/24 konfiguriert ist.

3. Starten Sie den Browser, geben Sie die IP-Adresse für die bgroup0-Schnittstelle ein (die standardmäßige IP-Adresse lautet 192.168.1.1/24), und drücken Sie anschließend die **ENTER**.

HINWEIS: Beim ersten Zugriff auf das Gerät über die WebUI erscheint der Assistent für die Anfangskonfiguration (ICW). Möchten Sie Ihr Gerät mit diesem Assistenten konfigurieren, erhalten Sie unter „Assistent für die Anfangskonfiguration“ auf Seite 63 die entsprechenden Informationen.

Die WebUI-Anwendung zeigt die Anmeldeaufforderung entsprechend der Abbildung 14 an.

Abbildung 14: WebUI-Anmeldeaufforderung



4. Wenn Sie die Standardanmeldung für den Administratortypen und das Kennwort noch nicht geändert haben, geben Sie bei den Eingabeaufforderungen „admin name“ und „password“ **netscreen** ein. (Verwenden Sie nur Kleinbuchstaben. Für die Felder „login“ und „password“ muss die Groß-/Kleinschreibung beachtet werden.)

Verwenden von Telnet

Führen Sie zum Herstellen einer Telnet-Verbindung die folgenden Schritte aus:

1. Stellen Sie für die Arbeitsstation eine Verbindung zum 0/2-0/4-Anschluss am Gerät her (bgroup0-Schnittstelle in der Trust Zone).
2. Stellen Sie sicher, dass die Arbeitsstation für DHCP oder statisch mit einer IP-Adresse im Subnetz 192.168.1.0/24 konfiguriert ist.
3. Starten Sie mithilfe der IP-Adresse eine Telnet-Clientanwendung für die bgroup0-Schnittstelle (die standardmäßige IP-Adresse lautet 192.168.1.1). Geben Sie z.B. **telnet 192.168.1.1** ein.

Die Telnet-Anwendung zeigt die Anmeldeaufforderung an.

4. Wenn Sie die Standardanmeldung für den Anmeldenamen und das Kennwort noch nicht geändert haben, geben Sie bei den Eingabeaufforderungen „login“ und „password“ **netscreen** ein. (Verwenden Sie nur Kleinbuchstaben. Für die Felder „login“ und „password“ muss die Groß-/Kleinschreibung beachtet werden.)
5. Standardmäßig tritt an der Konsole eine Zeitüberschreitung auf, und sie wird automatisch nach 10 Minuten ausbleibender Aktivität beendet (optional). Geben Sie zum Entfernen der Zeitüberschreitung **set console timeout 0** ein.

Standardmäßige Geräteeinstellungen

In diesem Abschnitt werden die standardmäßigen Einstellungen und der Betrieb eines SSG 20-Geräts erläutert.

Tabelle 5 zeigt die standardmäßigen Zonenbindungen für Anschlüsse an den Geräten.

Tabelle 5: Standardmäßige physikalische Schnittstelle zu Zonenbindungen

Anschlussbeschriftung	Schnittstelle	Zone
10/100-Ethernet-Anschlüsse:		
0/0	ethernet0/0	Untrust
0/1	ethernet0/1	DMZ
0/2	bgroup0 (ethernet0/2)	Trust
0/3	bgroup0 (ethernet0/3)	Trust
0/4	bgroup0 (ethernet0/4)	Trust
AUX	serial0/0	Null
WAN-Mini-PIM-Anschlüsse (x = Mini-PIM-Steckplatz 1 oder 2):		
ADSL2/2 + (Annex A)	adsl(x/0)	Untrust
ADSL2/2 + (Annex B)	adsl(x/0)	Untrust
T1	serial(x/0)	Untrust
E1	serial(x/0)	Untrust
ISDN	bri(x/0)	Untrust
V.92	serial(x/0)	Null

Eine Bridge-Gruppe (bgroup) ermöglicht Netzwerkbenutzern das Wechseln zwischen per Kabel und drahtlos übertragenem Datenverkehr ohne Neukonfiguration oder Neustart des Geräts. Standardmäßig sind die ethernet0/2-ethernet0/4-Schnittstellen (die am Gerät als Anschlüsse 0/2-0/4 gekennzeichnet sind) zusammen als bgroup0-Schnittstelle gruppiert. Zudem verfügen die Schnittstellen über die IP-Adresse 192.168.1.1/24 und sind an die Trust Sicherheitszone gebunden. Bis zu vier bgroups können konfiguriert werden.

Soll eine Ethernet- oder Wireless-Schnittstelle in einer bgroup eingerichtet werden, muss sich die Ethernet- oder Wireless-Schnittstelle in der Null Sicherheitszone befinden. Nach dem Löschen der sich in einer bgroup befindenden Ethernet- bzw. Wireless-Schnittstelle wird die Schnittstelle in der Null Sicherheitszone angeordnet. Nach Zuweisung zur Null Sicherheitszone kann die Ethernet-Schnittstelle an eine Sicherheitszone gebunden und einer anderen IP-Adresse zugewiesen werden.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um ethernet0/3 aus bgroup0 zu löschen und diese Schnittstelle mit der statischen IP-Adresse 192.168.3.1/24 der Trust Zone zuzuweisen:

WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port: Deaktivieren Sie **ethernet0/3**, und klicken Sie anschließend auf **Apply**.

List > Edit (ethernet0/3): Geben Sie Folgendes ein, und klicken Sie dann auf **Apply**:

Zone Name: Trust (select)
IP Address/Netmask: 192.168.3.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
set interface ethernet0/3 zone trust
set interface ethernet0/3 ip 192.168.3.1/24
save
```

Tabelle 6: Wireless-Bindungen und Bindungen für logische Schnittstellen

SSG 20-WLAN	Schnittstelle	Zone
Wireless-Schnittstelle	wireless0/0 (die Standard-IP-Adresse lautet 192.168.2.1/24).	Trust
Gibt eine Wireless-Schnittstelle an, die für den Betrieb in einem Frequenzband mit 2,4 GHz und/oder 5GHz konfiguriert werden kann.	wireless0/1-0/3.	Null
Logische Schnittstellen		
Layer-2-Schnittstelle	vlan1 gibt die für die Verwaltung und die VPN-Datenverkehrsbeendigung verwendeten logischen Schnittstellen an, während sich das Gerät im transparenten Modus befindet.	Nicht zutreffend
Tunnelschnittstellen	Tunnel.n gibt eine logische Tunnelschnittstelle an. Diese Schnittstelle ist für VPN-Datenverkehr vorgesehen.	Nicht zutreffend

Die Standard-IP-Adresse auf der bgroup0-Schnittstelle kann so geändert werden, dass sie den Adressen im LAN und WLAN entspricht. Unter „Grundlegende Wireless-Konfiguration“ auf Seite 37 erhalten Sie Informationen zur Konfiguration einer Wireless-Schnittstelle für eine bgroup.

HINWEIS: Die bgroup-Schnittstelle ist im transparenten Modus nicht verwendbar, wenn darin eine Wireless-Schnittstelle enthalten ist.

Zusätzliche Informationen und Beispiele zu bgroup erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.

Auf anderen Ethernet- oder Wireless-Schnittstellen auf einem Gerät sind keine anderen Standard-IP-Adressen konfiguriert; IP-Adressen müssen den anderen Schnittstellen (einschließlich der WAN-Schnittstellen) zugewiesen werden.

Grundlegende Gerätekonfiguration

In diesem Abschnitt werden folgende grundlegende Konfigurationseinstellungen beschrieben:

- Administrator auf Stammebene – Name und Kennwort
- Datum und Uhrzeit
- Bridge-Gruppenschnittstellen
- Administratorzugriff
- Verwaltungsdienste
- Host- und Domänenname
- Standardroute
- Adresse der Verwaltungsschnittstelle
- Konfiguration der Untrust Sicherungsschnittstelle

Administrator auf Stammebene – Name und Kennwort

Der als Administrator auf Stammebene angemeldete Benutzer verfügt über vollständige Berechtigungen für die Konfiguration eines SSG 20-Geräts. Es wird empfohlen, den Standardnamen und das Kennwort des Administrators auf Stammebene umgehend zu ändern (beides **netscreen**).

Verwenden Sie zum Ändern des Namens und des Kennworts für den Administrator auf Stammebene die WebUI oder die Befehlszeilenschnittstelle folgendermaßen:

WebUI

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

Administrator Name:
Old Password: netscreen
New Password:
Confirm New Password:

HINWEIS: Kennwörter werden auf der WebUI nicht angezeigt.

CLI

```
set admin name name
set admin password pswd_str
save
```


Datum und Uhrzeit

Die auf einem SSG 20-Gerät festgelegte Uhrzeit nimmt beeinflusst Ereignisse wie die Einrichtung von VPN-Tunnels. Die einfachste Möglichkeit zum Festlegen des Datums und der Uhrzeit auf dem Gerät besteht darin, über die WebUI die Gerätesystemuhr mit der Arbeitsstationsuhr zu synchronisieren.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um das Datum und die Uhrzeit auf einem Gerät zu konfigurieren:

WebUI

1. Configuration > Date/Time: Klicken Sie auf die Schaltfläche **Sync Clock with Client**.

Sie werden gefragt, ob Sie die Sommer-/Winterzeitoption auf Ihrer Arbeitsstation 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 Befehlszeilenbefehl **set clock** in einer Telnet- oder Konsolensitzung verwenden, um das Datum und die Uhrzeit für das Gerät manuell einzugeben.

Bridge-Gruppenschnittstellen

Standardmäßig verfügt das SSG 20-Gerät über die in der Trust Sicherheitszone zusammengruppierten Ethernet-Schnittstellen vom Typ ethernet0/2-ethernet0/4. Durch Gruppieren der Schnittstellen werden diese in einem Subnetz angeordnet. Eine Schnittstelle kann aus einer Gruppe gelöscht und einer anderen Sicherheitszone zugewiesen werden. Schnittstellen müssen sich in der Null Sicherheitszone befinden, bevor sie einer Gruppe zugewiesen werden können. Verwenden Sie zum Anordnen einer gruppierten Schnittstelle in der Null Sicherheitszone den Befehlszeilenbefehl **unset interface interface port interface**.

Die SSG 20-WLAN-Geräte ermöglichen die Gruppierung von Ethernet- und Wireless-Schnittstellen unter einem Subnetz.

HINWEIS: In einer bgroup können nur Wireless- und Ethernet-Schnittstellen festgelegt werden.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um eine Gruppe mit Ethernet- und Wireless-Schnittstellen zu konfigurieren:

WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port: Deaktivieren Sie **ethernet0/3** und **ethernet0/4**, und klicken Sie anschließend auf **Apply**.

Edit (bgroup1) > Bind Port: Wählen Sie **ethernet0/3**, **ethernet0/4** und **wireless0/2** aus, und klicken Sie anschließend auf **Apply**.

> Basic: Geben Sie Folgendes ein, und klicken Sie dann auf **Apply**:

Zone Name: DMZ (select)
IP Address/Netmask: 10.0.0.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
unset interface bgroup0 port ethernet0/4
set interface bgroup1 port ethernet0/3
set interface bgroup1 port ethernet0/4
set interface bgroup1 port wireless0/2
set interface bgroup1 zone DMZ
set interface bgroup1 ip 10.0.0.1/24
save
```

Administratorzugriff

Standardmäßig kann jeder Benutzer im Netzwerk ein Gerät verwalten, sofern er den Anmeldenamen und das Kennwort kennt.

Verwenden Sie die WebUI und die Befehlszeilenschnittstelle folgendermaßen, um das Gerät so zu konfigurieren, dass es nur von einem bestimmten Host im Netzwerk verwaltet werden kann:

WebUI

Configuration > Admin > Permitted IPs: Geben Sie Folgendes ein, und klicken Sie dann auf **Add**:

IP Address/Netmask: *ip_addr/mask*

CLI

```
set admin manager-ip ip_addr/mask
save
```

Verwaltungsdienste

ScreenOS bietet Dienste für die Konfiguration und die Verwaltung des Geräts (z.B. SNMP, SSL und SSH), die für jede Schnittstelle einzeln aktiviert werden können.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um die Verwaltungsdienste im Gerät zu konfigurieren:

WebUI

Network > Interfaces > List > Edit (für ethernet0/0): Wählen Sie unter **Management Services** die auf der Schnittstelle zu verwendenden Dienste aus, bzw. löschen Sie diese, und klicken Sie anschließend auf **Apply**.

CLI

```
set interface ethernet0/0 manage web
unset interface ethernet0/0 manage snmp
save
```

Host- und Domänenname

Der Domänenname definiert das Netzwerk oder das Subnetzwerk, zu dem das Gerät gehört, wohingegen sich der Hostname auf ein bestimmtes Gerät bezieht. Anhand des Hostnamens und des Domännennamens wird das Gerät im Netzwerk eindeutig identifiziert.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um den Host- und den Domännennamen auf einem Gerät zu konfigurieren:

WebUI

Network > DNS > Host: Geben Sie Folgendes ein, und klicken Sie dann auf **Apply**:

Host Name: *name*
Domain Name: *name*

CLI

```
set hostname name
set domain name
save
```

Standardroute

Bei der Standardroute handelt es sich um eine statische Route, über die Pakete weitergeleitet werden, die an nicht ausdrücklich in der Routentabelle aufgeführte Netzwerke adressiert sind. Geht ein Paket beim Gerät mit einer Adresse ein, für die dem Gerät keine Routeninformationen vorliegen, sendet das Gerät das Paket an das von der Standardroute angegebene Ziel.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um die Standardroute auf dem Gerät zu konfigurieren:

WebUI

Network > Routing > Destination > New (trust-vr): Geben Sie Folgendes ein, und klicken Sie dann auf **OK**:

IP Address/Netmask: 0.0.0.0/0.0.0.0
Next Hop
Gateway: (select)
Interface: ethernet0/2 (ausgewählt)
Gateway IP Address: *ip_addr*

Befehlszeilenschnittstelle

```
set route 0.0.0.0/0 interface ethernet0/2 gateway ip_addr
save
```

Adresse der Verwaltungsschnittstelle

Die Trust Schnittstelle besitzt die Standard-IP-Adresse 192.168.1.1/24 und ist für die Verwaltungsdienste konfiguriert. Werden die Anschlüsse 0/2-0/4 am Gerät mit einer Arbeitsstation verbunden, kann das Gerät über eine Arbeitsstation im Subnetzwerk 192.168.1.1/24 mithilfe eines Verwaltungsdienstes wie Telnet konfiguriert werden.

Die Standard-IP-Adresse kann auf der Trust Schnittstelle geändert werden. Möglicherweise möchten Sie die Schnittstelle ändern, um die Übereinstimmung mit den bereits im LAN vorhandenen IP-Adressen zu gewährleisten.

Konfiguration der Untrust Sicherungsschnittstelle

Das SSG 20-Gerät ermöglicht die Konfiguration einer Sicherungsschnittstelle für einen nicht vertrauenswürdigen Failover. Führen Sie zum Festlegen der Sicherungsschnittstelle bei Auftreten eines nicht vertrauenswürdigen Failovers folgende Schritte aus:

1. Legen Sie die Sicherungsschnittstelle in der Null Sicherheitszone mithilfe des Befehlszeilenbefehls **unset interface interface [port interface]** fest.
2. Binden Sie mithilfe des Befehlszeilenbefehls **set interface interface zone zone_name** die Sicherungsschnittstelle an dieselbe Sicherheitszone wie die Primärschnittstelle.

HINWEIS: Die Primär- und Sicherungsschnittstellen müssen sich in derselben Sicherheitszone befinden. Eine Primärschnittstelle verfügt nur über eine Sicherungsschnittstelle und umgekehrt.

Zum Festlegen der ethernet0/4-Schnittstelle als Sicherungsschnittstelle für die ethernet0/0-Schnittstelle muss die WebUI oder die Befehlszeilenschnittstelle folgendermaßen verwendet werden:

WebUI

Network > Interfaces > Backup > Geben Sie Folgendes ein, und klicken Sie anschließend auf **Apply**.

Primary: ethernet0/0
Backup: ethernet0/4
Type: track-ip (select)

CLI

```
unset interface bgroup0 port ethernet0/4
set interface ethernet0/4 zone untrust
set interface ethernet0/0 backup interface ethernet0/4 type track-ip
save
```

Grundlegende Wireless-Konfiguration

In diesem Abschnitt finden Sie Informationen zur Konfiguration der Wireless-Schnittstelle am SSG 20-WLAN-Gerät. Wireless-Netzwerke (Drahtlosnetzwerke) bestehen aus Namen, die als Service Set Identifiers (SSIDs) bezeichnet werden. Das Festlegen von SSIDs ermöglicht das Anordnen von mehreren Wireless-Netzwerken am selben Ort, ohne dass es zu Konflikten kommt. Ein SSID-Name darf aus maximal 32 Zeichen bestehen. Ist ein Leerzeichen Teil des SSID-Namens, muss die Zeichenfolge in Anführungszeichen gesetzt werden. Nach

Festlegung des SSID-Namens können weitere SSID-Attribute konfiguriert werden. Zur Verwendung von Wireless Local Area Network (WLAN)-Funktionen am Gerät muss zumindest eine SSID konfiguriert und an eine Wireless-Schnittstelle gebunden werden.

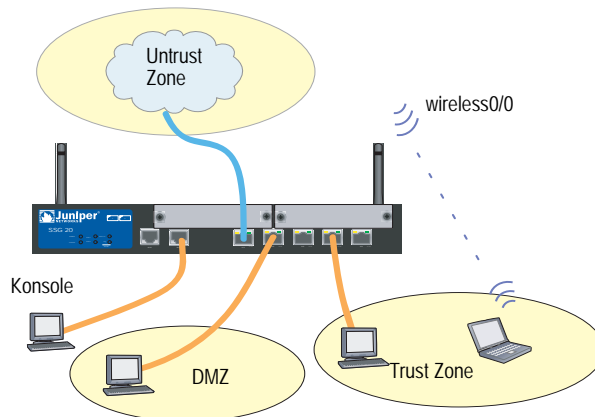
Das SSG 20-WLAN-Gerät ermöglicht das Erstellen von bis zu 16 SSIDs, von denen jedoch nur vier gleichzeitig verwendet werden können. Das Gerät kann für die Verwendung der vier 4 SSIDs auf einem der Transceiver oder für das Aufteilen der Verwendung auf beide Transceiver (z.B. drei WLAN 0 zugewiesene SSIDs und eine WLAN 1 zugewiesene SSID) konfiguriert werden. Legen Sie mit dem Befehlszeilenbefehl **set interface wireless_interface wlan {0 | 1 | both}** die Funktransceiver am SSG 20-WLAN-Gerät fest.

Sobald Sie eine SSID für die wireless0/0-Schnittstelle festgelegt haben, können Sie mithilfe der standardmäßigen IP-Adresse der wireless0/0-Schnittstelle auf das Gerät zugreifen (schrittweise Anleitungen hierzu finden Sie unter „Zugriff auf das Gerät“ auf Seite 28). Abbildung 15 zeigt die Standardkonfiguration für das SSG 20-WLAN-Gerät.

HINWEIS: Wird das SSG 20-WLAN-Gerät außerhalb Japans, Kanadas, Chinas, Taiwans, Koreas, Israels, Singapurs oder der Vereinigten Staaten betrieben, benötigen Sie den Befehlszeilenbefehl **set wlan country-code**, oder Sie müssen das Gerät auf der Wireless-WebUI-Seite > General Settings einrichten, um eine WLAN-Verbindung herstellen zu können. Durch diesen Befehl wird der auswählbare Kanalbereich und die Übertragungsleistung festgelegt.

Lautet Ihr Regionalcode ETSI, muss der korrekte Ländercode festgelegt werden, der den örtlichen Bestimmungen zu Funkbereichen entspricht.

Abbildung 15: Standardmäßige SSG 20-WLAN-Konfiguration



Standardmäßig wird die wireless0/0-Schnittstelle mit der IP-Adresse 192.168.2.1/24 konfiguriert. Alle Wireless-Clients, für die eine Verbindung zur Trust Zone hergestellt werden muss, benötigen eine IP-Adresse im Wireless-Subnetzwerk. Das Gerät kann auch so konfiguriert werden, dass das Gerät mit DHCP Ihren Geräten automatisch IP-Adressen im Subnetzwerk 192.168.2.1/24 zuweist.

Standardmäßig werden die wireless0/1-wireless0/3-Schnittstellen als Null definiert. Den Schnittstellen sind keine IP-Adressen zugewiesen. Möchten Sie eine beliebige der anderen Wireless-Schnittstellen verwenden, müssen Sie für die Schnittstelle eine IP-Adresse konfigurieren, dieser eine SSID zuweisen und sie an eine Sicherheitszone binden. In Tabelle 7 sind die Methoden zur Wireless-Authentifizierung und –Verschlüsselung aufgeführt.

Tabelle 7: Wireless-Authentifizierung und Verschlüsselungsoptionen

Authentifizierung	Verschlüsselung
Offen	Ermöglicht einem beliebigen Wireless-Client den Zugriff auf das Gerät.
Shared-key	WEP shared-key
WPA-PSK	AES/TKIP mit Pre-Shared Key
WPA	AES/TKIP mit Schlüssel von RADIUS-Server
WPA2-PSK	802.11i-kompatibel mit einem Pre-Shared Key
WPA2	802.11i-kompatibel mit einem RADIUS-Server
WPA-Auto-PSK	Lässt einen WPA- und einen WPA2-Typ mit Pre-Shared Key zu.
WPA-Auto	Lässt einen WPA- und einen WPA2-Typ mit RADIUS-Server zu.
802.1x	WEP mit Schlüssel von RADIUS-Server

Im *Concepts & Examples ScreenOS Reference Guide* finden Sie Konfigurationsbeispiele, SSID-Attribute und Befehlszeilenbefehle bzgl. Wireless-Sicherheitskonfigurationen.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um eine Wireless-Schnittstelle für grundlegende Verbindung zu konfigurieren:

WebUI

1. Legen Sie den WLAN-Ländercode und die IP-Adresse fest.

Wireless > General Settings > – Wählen Sie Folgendes aus, und klicken Sie anschließend auf **Apply**:

Country code: Select your code
IP Address/Netmask: *ip_add/netmask*

2. Legen Sie die SSID fest.

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

SSID:
Authentication:
Encryption:
Wireless Interface Binding:

3. Legen Sie den WEP-Schlüssel fest (optional).

SSID > WEP Keys: Wählen Sie die Schlüssel-ID aus, und klicken Sie anschließend auf **Apply**:

4. Legen Sie den WLAN-Modus fest.

Network > Interfaces > List > Edit (Wireless-Schnittstelle): Wählen Sie für den WLAN-Modus **Both** aus, und klicken Sie anschließend auf **Apply**.

5. Aktivieren Sie die Änderungen für die Wireless-Einstellungen.

Wireless > General Settings > Klicken Sie auf **Activate Changes**.

CLI

1. Legen Sie den WLAN-Ländercode und die IP-Adresse fest.

```
set wlan country-code { code_id }
set interface wireless_interface ip ip_addr/netmask
```

2. Legen Sie die SSID fest.

```
set ssid name name_str
set ssid name_str authentication auth_type encryption encryption_type
set ssid name_str interface interface
set ssid name_str key-id number (optional)
```

3. Legen Sie den WLAN-Modus fest.

```
set interface wireless_interface wlan both
```

4. Aktivieren Sie die Änderungen für die Wireless-Einstellungen.

```
save
exec wlan reactivate
```

Eine SSID kann so konfiguriert werden, dass er im selben Subnetz wie das verkabelte Subnetz arbeitet. Dadurch haben Clients die Möglichkeit, ohne Wiederherstellen einer Verbindung in einem anderen Subnetz auf beiden Schnittstellen zu arbeiten.

Verwenden Sie zum Festlegen einer Ethernet- und einer Wireless-Schnittstelle für dieselbe Bridge-Gruppenschnittstelle wie folgt die WebUI oder die Befehlszeilenschnittstelle:

WebUI

Network > Interfaces > List > Edit (*bgroup_name*) > Bind Port: Wählen Sie die Wireless- und die Ethernet-Schnittstellen aus, und klicken Sie anschließend auf **Apply**:

CLI

```
set interface bgroup_name port wireless_interface
set interface bgroup_name port wireless_interface
```

HINWEIS: *Bgroup_name* kann bgroup0-bgroup3 sein.

Ethernet_interface kann ethernet0/0-ethernet0/4 sein.

Wireless_interface kann wireless0/0-wireless0/3 sein.

Ist eine Wireless-Schnittstelle konfiguriert, muss das WLAN mit dem Befehlszeilenbefehl **exec wlan reactivate** neu aktiviert werden. Alternativ dazu können Sie auch auf der WebUI-Seite „Wireless > General Settings“ auf **Activate Changes** klicken.

Konfiguration des Mini-PIM

In diesem Abschnitt wird die Konfiguration der Mini Physical Interface Modules (PIMs) erläutert:

- ADSL2/2 + -Schnittstelle
- ISDN ISDN-Schnittstelle
- T1-Schnittstelle
- E1-Schnittstelle
- V.92 Modemschnittstelle

ADSL2/2+-Schnittstelle

Ihr Netzwerk verwendet die ADSL2/2 + -Schnittstelle **adslx/0** (wobei x den Steckplatz des Mini-PIM (1 oder 2) bezeichnet) am Gerät, um über eine virtuelle Asynchronous Transfer Mode (ATM)-Verbindung eine Verbindung zum Dienstanbieter herzustellen. Zusätzliche virtuelle Verbindungen können durch Erstellen von ADSL2/2 + -Subschnittstellen konfiguriert werden. Weitere Informationen hierzu finden Sie unter „Virtuelle Verbindungen“ auf Seite 42.

Wechseln Sie auf der WebUI zur Seite Network > Interfaces > List um eine Liste der aktuellen Schnittstellen im NetScreen-Gerät anzuzeigen. Wenn Sie eine Telnet- oder Konsolensitzung verwenden, geben Sie den Befehlszeilenbefehl **get interface** ein. Die adslx/0-Schnittstelle ist an die Untrust Zone gebunden.

Bei Verwendung der ADSL2/2 + -Schnittstelle zur Herstellung einer Verbindung zum Dienstnetzwerk des Anbieters muss die adsl(x/0)-Schnittstelle konfiguriert werden. 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 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

Virtuelle Verbindungen

Zum Hinzufügen von virtuellen Verbindungen erstellen Sie Subschnittstellen für die ADSL2/2 + -Schnittstelle. Sie können bis zu zehn ADSL2/2 + -Subschnittstellen erstellen. Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um z..B. eine neue Subschnittstelle mit der Bezeichnung **adsl1/0.1** zu erstellen, die an die vordefinierte Zone mit der Bezeichnung **Untrust** gebunden ist:

WebUI

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

Interface Name: adsl1/0.1
 VPI/VCI: 0/35
 Zone Name: Untrust (auswählen)

CLI

```
set interface adsl 1/0.1 pvc 0 35 zone Untrust
save
```

Eine ADSL2/2 + -Subschnittstelle muss auf die gleiche Weise konfiguriert werden wie die ADSL2/2 + -Hauptschnittstelle, d.h., Sie müssen auch wie unter „ADSL2/2 + -Schnittstelle“ auf Seite 41 beschrieben, die VPI/VCI-Werte einstellen. ADSL2/2 + -Subschnittstellen können unabhängig von der ADSL2/2 + -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 ADSL2/2 + -Hauptschnittstelle nicht über eine statische IP-Adresse verfügt.

VPI/VCI und Multiplexingmethode

Ihr Dienstanbieter ordnet für jede virtuelle Verbindung ein VPI/VCI-Wertepaar zu. Sie können z.B. das VPI/VCI-Paar 1/32 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.

Gehen Sie zum Konfigurieren des VPI/VCI-Paars 1/32 auf der adsl1/0-Schnittstelle mithilfe der WebUI oder der Befehlszeilenschnittstelle folgendermaßen vor:

WebUI

Network > Interfaces > List > Edit (für die adsl1/0-Schnittstelle): Geben Sie ins Feld VPI/VCI 1/32 ein, und klicken Sie auf **Apply**.

CLI

```
set interface adsl1/0 pvc 1 32
save
```

Standardmäßig verwendet das Gerät für jede virtuelle Verbindung Logical Link Control (LLC)-basiertes Multiplexing.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um das VPI/VCI 1/32 auf der adsl1/0-Schnittstelle zu konfigurieren und die LLC-Einkapselung für die virtuelle Verbindung zu verwenden:

WebUI

Network > Interfaces > List > Edit (für die adsl1/0-Schnittstelle): Geben Sie Folgendes ein, und klicken Sie dann auf **Apply**:

VPI/VCI: 1 / 32
Multiplexing Method: LLC (selected)

CLI

```
set interface adsl1/0 pvc 1 32 mux llc
save
```

PPPoE oder PPPoA

Das SSG 20-Gerät enthält sowohl PPPoE- als auch PPPoA-Clients zum Herstellen einer Verbindung mit dem Netzwerk des Dienstanbieters 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 Gerät beendet werden können. Damit das Gerät eine Verbindung mit dem Netzwerk des Dienstanbieters herstellen kann, müssen Sie den vom Dienstanbieter zugeordneten Benutzernamen und das zugehörige Kennwort konfigurieren. Die Konfiguration für PPPoA ähnelt der Konfiguration für PPPoE.

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

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um den Benutzernamen **roswell** und das Kennwort **area51** für PPPoE zu konfigurieren und die PPPoE-Konfiguration an die adsl1/0-Schnittstelle zu binden:

WebUI

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

PPPoE Instance: poe1
Bound to Interface: adsl1/0 (select)
Username: roswell
Password: area51

CLI

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1/0
save
```

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

Statische IP-Adresse und Netzmaske

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

Sie müssen wie unter „PPPoE oder PPPoA“ auf Seite 43 beschrieben eine PPPoE- oder PPPoA-Instanz konfigurieren und an die adsl1/0-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.

So konfigurieren Sie mithilfe der WebUI oder der Befehlszeilenschnittstelle die statische IP-Adresse 1.1.1.1/24 für das Netzwerk:

WebUI

Network > Interfaces > List > Edit (für die adsl1/0-Schnittstelle): Geben Sie Folgendes ein, und klicken Sie dann auf **Apply**:

```
IP Address/Netmask: 1.1.1.1/24
Static IP: (select)
```

CLI

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

oder

```
set interface adsl1/0 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 Gerät über PPPoE oder PPPoA eine IP-Adresse für die ADSL2/2+ -Schnittstelle zugewiesen wird, erhält es automatisch auch IP-Adressen für die DNS-Server. Weist der DHCP-Server im Gerät den Computern im Netzwerk ihre IP-Adressen zu, erhalten die Computer auch diese DNS-Serveradressen.

Wenn Sie der ADSL2/2+ -Schnittstelle eine statische IP-Adresse zuordnen, muss Ihnen der Diensteanbieter 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-Serveradresse für jeden Computer bereitstellt.

So konfigurieren Sie mithilfe der WebUI oder der Befehlszeilenschnittstelle den DHCP-Server auf der bgroup0-Schnittstelle zum Bereitstellen der DNS-Serveradresse 1.1.1.152 für Computer im Netzwerk:

WebUI

Network > DHCP > Edit (für die bgroup0-Schnittstelle) > DHCP Server: Geben Sie **1.1.1.152** für DNS1 ein, und klicken Sie dann auf **Apply**.

CLI

```
set interface bgroup0 dhcp server option dns1 1.1.1.152
save
```

Weitere Informationen zur Konfiguration der ADSL- und ADSL2/2+ -Schnittstellen erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.

ISDN ISDN-Schnittstelle

Bei Integrated Services Digital Network (ISDN) handelt es sich um Standards für die digitale Übertragung über verschiedene vom Consultative Committee for International Telegraphy and Telephone (CCITT) und von der International Telecommunications Union (ITU) erstellte Medien. Als Dial-on-Demand-Dienst bietet ISDN einen schnellen Verbindungsaufbau sowie niedrige Latenz und ermöglicht zudem hochwertige Sprach-, Daten- und Videoübertragungen. ISDN ist überdies ein leitungsvermittelter Dienst, der sowohl für Multipoint- als auch auf Point-to-Point-Verbindungen verwendet werden kann. ISDN bietet einen Dienstrouter mit einer Multilink Point-to-Point Protocol (PPP)-Verbindung für Netzwerkschnittstellen. Die ISDN-Schnittstelle wird normalerweise zum Zugriff auf externe Netzwerke als Sicherungsschnittstelle der Ethernet-Schnittstelle konfiguriert.

So konfigurieren Sie die ISDN-Schnittstelle mithilfe der WebUI oder der Befehlszeilenschnittstelle:

WebUI

Network > Interfaces > List > Edit (bri1/0): Geben Sie Folgendes ein (bzw. wählen Sie Folgendes aus), und klicken Sie dann auf **OK**:

```
BRI-Mode: Dial Using BRI
Primary Number: 123456
WAN Encapsulation: PPP
PPP Profile: isdnprofile
```

CLI

```
set interface bri1/0 dialer-enable
set interface bri1/0 primary-number "123456"
set interface bri1/0 encaps ppp
set interface bri1/0 ppp profile isdnprofile
save
```

Informationen zum Konfigurieren der ISDN-Schnittstelle als Sicherungsschnittstelle erhalten Sie unter „Konfiguration der Untrust Sicherungsschnittstelle“ auf Seite 37.

Weitere Informationen zur Konfiguration der ISDN-Schnittstelle erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.

T1-Schnittstelle

Die T1-Schnittstelle ist ein grundlegendes Physical Layer-Protokoll, das in Nordamerika von der Digital Signal Level 1 (DS-1)-Multiplexingmethode verwendet wird. Eine T1-Schnittstelle arbeitet mit einer Bitrate von 1,544 MBit/s oder erreicht eine Geschwindigkeit von 24 DS0-Kanälen.

Die Geräte unterstützen die folgenden T1 DS-1-Standards:

- ANSI T1.107, T1.102
- GR 499-core, GR 253-core
- AT&T Pub 54014
- ITU G.751, G.703

So konfigurieren Sie das T1-Mini-PIM mithilfe der WebUI oder der Befehlszeilenschnittstelle:

WebUI

Network > Interfaces > List > Edit (serial1/0): Geben Sie Folgendes ein (bzw. wählen Sie Folgendes aus), und klicken Sie dann auf **OK**:

WAN Configure: main link (Hauptverknüpfung)
 WAN Encapsulation: cisco-hdlc
 Klicken Sie auf **Apply**.
 Fixed IP: (select)
 IP Address/Netmask: 172.18.1.1/24

CLI

```
set interface serial1/0 encap cisco-hdlc
set interface serial1/0 ip 172.18.1.1/24
```

Weitere Informationen zur Konfiguration der T1-Schnittstelle erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.

E1-Schnittstelle

Die E1-Schnittstelle ist ein standardmäßiges digitales Kommunikationsformat für Wide Area Network (WAN), das über Kupfervorrichtungen mit einer Rate von 2,048 MBit/s arbeitet. E1 ist ein grundlegendes Zeitmultiplexschema zum Übertragen digitaler Verbindungen, das sich außerhalb Nordamerikas großer Beliebtheit erfreut.

Die Geräte unterstützen die folgenden E1-Standards:

- ITU-T G.703
- ITU-T G0,751
- ITU-T G0,775

So konfigurieren Sie das E1-Mini-PIM mithilfe der WebUI oder der Befehlszeilenschnittstelle:

WebUI

Network > Interfaces > List > Edit (serial1/0): Geben Sie Folgendes ein (bzw. wählen Sie Folgendes aus), und klicken Sie dann auf **OK**:

WAN Configure: main link
 WAN Encapsulation: PPP
 Binding a PPP Profile: junipertest
 Klicken Sie auf **Apply**.
 Fixed IP: (select)
 IP Address/Netmask: 172.18.1.1/24

CLI

```
set interface serial1/0 encapsulation ppp
set ppp profile "junipertest" static-ip
set ppp profile "junipertest" auth type chap
set ppp profile "junipertest" auth local-name "juniper"
set ppp profile "junipertest" auth secret "password"
set interface serial1/0 ppp profile "junipertest"
set interface serial1/0 ip 172.18.1.1/24
set user "server" type wan
set user "server" password "server"
```

Weitere Informationen zur Konfiguration der E1-Schnittstelle erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.

V.92 Modemschnittstelle

Die V.92-Schnittstelle verfügt über ein internes analoges Modem zum Herstellen einer PPP-Verbindung zu einem Dienstanbieter. Die serielle Schnittstelle kann als Primär- oder Sicherungsschnittstelle konfiguriert werden, die beim Failover einer Schnittstelle verwendet wird.

HINWEIS: Die V.92-Schnittstelle funktioniert im transparenten Modus nicht.

So konfigurieren Sie die V.92-Schnittstelle mithilfe der WebUI oder der Befehlszeilenschnittstelle:

WebUI

Network > Interfaces > List > Edit (for serial1/0): Geben Sie Folgendes ein, und klicken Sie dann auf **OK**:

Zone Name: untrust (select)

ISP: Geben Sie Folgendes ein, und klicken Sie dann auf **OK**:

ISP Name: isp_juniper
 Primary Number: 1234567
 Login Name: juniper
 Login Password: juniper

Modem: Geben Sie Folgendes ein, und klicken Sie dann auf **OK**:

Modem Name: mod1
 Init String: AT&FS7=255S32=6
 Active Modem setting
 Inactivity Timeout: 20

CLI

```
set interface serial1/0 zone untrust
set interface serial1/0 modem isp isp_juniper account login juniper password
juniper
set interface serial1/0 modem isp isp_juniper primary-number 1234567
set interface serial1/0 modem idle-time 20
set interface serial1/0 modem settings mod1 init-strings AT&FS7=255S32=6
set interface serial1/0 modem settings mod1 active
```

Weitere Informationen zur Konfiguration der V.92-Modemschnittstelle erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.

Grundlegender Firewallschutz

Die Geräte werden mit einer Standardrichtlinie konfiguriert, die Arbeitsstationen in der Trust Zone des Netzwerks den Zugriff auf eine beliebige Ressource in der Untrust Sicherheitszone gestattet, wohingegen externe Computer mit den Arbeitsstationen nicht auf Sitzungen zugreifen oder diese starten dürfen. Sie können Richtlinien konfigurieren, damit das Gerät externen Computern das Starten bestimmter Sitzungstypen mit Ihren Computern erlaubt. Informationen zum Erstellen oder Ändern von Richtlinien erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.

Das SSG 20-Gerät bietet verschiedene Erkennungsmethoden und Verteidigungsmechanismen zur Bekämpfung von Spionage und Angriffen, durch die ein Netzwerk oder eine Netzwerkressource gefährdet oder beschädigt werden soll.

- Die ScreenOS SCREEN-Optionen sichern eine Zone, indem sie alle über eine Schnittstelle laufenden Verbindungsversuche zu dieser Zone überprüfen und dann zulassen oder verweigern. Sie können in der Untrust Zone z.B. einen Port-Scan-Schutz anwenden, um eine Quelle aus einem Remotenetzwerk am Erkennen von Diensten zu hindern, die u. U. Gegenstand weiterer Angriffe werden sollen.
- Das Gerät wendet Firewallrichtlinien, die ggf. Komponenten für Inhaltsfilterung und Eindringungserkennung und -verhinderung (Intrusion Detection and Prevention, IDP) beinhalten, für den Datenverkehr an, der zonenübergreifend die SCREEN-Filter durchläuft. Standardmäßig darf durch das Gerät kein Datenverkehr zonenübergreifend geleitet werden. Erstellen Sie eine Richtlinie zum Deaktivieren des Standardverhaltens, um Datenverkehr ein zonenübergreifendes Durchlaufen des Geräts zu gestatten.

Legen Sie ScreenOS SCREEN-Optionen für eine Zone folgendermaßen mithilfe der WebUI oder der Befehlszeilenschnittstelle fest:

WebUI

Screening > Screen: Wählen Sie die Zone aus, für die die Optionen Gültigkeit besitzen. Wählen Sie die gewünschten SCREEN-Optionen aus, und klicken Sie anschließend auf **Apply**:

CLI

```
set zone zone screen option
save
```

Weitere Informationen zur Konfiguration der in ScreenOS verfügbaren Netzwerksicherheitsoptionen erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.

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 Browser, und geben Sie den folgenden URL ein: www.juniper.net.

Zurücksetzen eines Geräts auf die werkseitigen Standardeinstellungen

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



WARNHINWEIS: Durch das Zurücksetzen des Geräts werden alle vorhandenen Konfigurationseinstellungen gelöscht und alle vorhandenen Firewall- und VPN-Dienste deaktiviert.

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

- Verwenden einer Konsolenverbindung. Zusätzliche Informationen erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.
- Verwenden des Reset-Stiftlochs an der Rückseite des Geräts wie im folgenden Abschnitt beschrieben.

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 28 beschrieben eine Konsolensitzung starten.

Führen Sie zum Zurücksetzen und Wiederherstellen der Standardeinstellungen mithilfe des Reset-Stifts die folgenden Schritte aus:

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 rot. 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 überprüft die zweite Zurücksetzung. Die Status-LED leuchtet kurz rot auf und blinkt anschließend wieder grün.

Das Gerät wird dann auf seine ursprünglichen Werkseinstellungen zurückgesetzt. Beim Zurücksetzen des Geräts leuchtet die Status-LED kurz rot auf und leuchtet anschließend 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 grün. Der Anmeldename und das Kennwort lauten **netscreen**.

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.

Kapitel 4

Warten des Geräts

In diesem Kapitel werden die Wartungsmaßnahmen für SSG 20-Geräte erläutert. Der Anhang umfasst die folgenden Abschnitte:

- „Erforderliche Werkzeuge und Teile“ auf dieser Seite
- „Ersetzen eines Mini-Physical Interface Module“ auf dieser Seite
- „Erweitern des Arbeitsspeichers“ auf Seite 54

HINWEIS: Sicherheitshinweise und Anweisungen finden Sie im *Security Products Safety Guide* von Juniper Networks. Dieses Handbuch enthält Informationen zu 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.

Erforderliche Werkzeuge und Teile

Zum Ersetzen einer Komponente eines SSG 20-Geräts benötigen Sie folgende Werkzeuge und Teile:

- Abschirmbeutel zum Schutz vor elektrostatischer Entladung oder antistatische Matte
- Erdungsarmband zum Schutz vor elektrostatischer Entladung (Electrostatic Discharge, ESD)
- Kreuzschlitzschraubenzieher (3 mm)

Ersetzen eines Mini-Physical Interface Module

Beide SSG 20-Modelle verfügen am Bedienfeld über zwei Steckplätze für Wide Area Network Mini Physical Interface Modules (WAN-Mini-PIMs). Mini-PIMs in einem SSG 20-Gerät können eingebaut und ersetzt werden. Das Gerät muss vor dem Entfernen oder Einbauen eines Mini-PIM ausgeschaltet werden.



VORSICHT: Stellen Sie sicher, dass das Gerät beim Entfernen eines Mini-PIM ausgeschaltet ist. Die Mini-PIMs sind nicht „hot-swappable“, d.h. der Austausch von Komponenten ist nicht möglich, während der Computer läuft.

Entfernen einer unbeschrifteten Frontscheibe

Zur Gewährleistung einer ausreichenden Belüftung des SSG 20-Geräts sollten unbeschriftete Frontscheiben über Steckplätzen angebracht werden, die keine Mini-PIMs enthalten. Entfernen Sie eine unbeschriftete Frontscheibe nur, wenn Sie ein Mini-PIM in den leeren Steckplatz einbauen.

Führen Sie zum Entfernen einer unbeschrifteten Frontscheibe die folgenden Schritte aus:

1. Legen Sie einen Abschirmbeutel gegen elektrostatische Entladung oder eine antistatische Matte auf einen flachen, festen Untergrund, auf dem Sie das Mini-PIM abstellen möchten.
2. Schnallen Sie zum Schutz vor elektrostatischer Entladung ein Erdungsband um Ihr Handgelenk, und stellen Sie eine Verbindung zwischen dem Band und dem ESD-Punkt auf dem Gehäuse oder einem externen ESD-Punkt her, falls das SSG 20-Gerät nicht geerdet ist.
3. Entfernen Sie den Stromadapter vom Gerät. Überprüfen Sie, ob die Strom-LED aus ist.
4. Lösen Sie mit einem Schraubenzieher die Schrauben auf jeder Seite der Frontscheibe.
5. Entfernen Sie die Frontscheibe, und legen Sie die Frontscheibe anschließend in den Abschirmbeutel oder auf die antistatische Matte.

Entfernen eines Mini-PIM

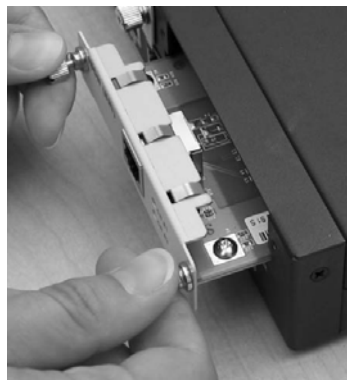
Mini-PIMs werden im Bedienfeld des SSG 20-Geräts eingebaut. Ein Mini-PIM wiegt unter 110 g.

Führen Sie zum Entfernen eines Mini-PIM die folgenden Schritte aus:

1. Legen Sie einen Abschirmbeutel oder eine antistatische Matte auf einen flachen, festen Untergrund, auf dem Sie das Mini-PIM abstellen möchten.
2. Schnallen Sie zum Schutz vor elektrostatischer Entladung ein Erdungsband um Ihr Handgelenk, und stellen Sie eine Verbindung zwischen dem Band und dem ESD-Punkt auf dem Gehäuse oder einem externen ESD-Punkt her, falls das SSG 20-Gerät nicht geerdet ist.
3. Entfernen Sie den Stromadapter vom Gerät. Überprüfen Sie, ob die Strom-LED aus ist.
4. Beschriften Sie die an das Mini-PIM angeschlossenen Kabel, damit Sie später jedes Kabel wieder an das entsprechende PIM anschließen können.
5. Entfernen Sie die Kabel aus dem Mini-PIM.
6. Ordnen Sie das Kabel ggf. so an, dass ein Herausgleiten des Kabels oder das Entstehen von Stresspunkten verhindert wird:
 - a. Bringen Sie die Kabel so an, dass sie beim Herunterhängen nicht ihr eigenes Gewicht stützen müssen.

- b. Legen Sie zu lange Kabel sorgfältig zu einer Schleife zusammen, und räumen Sie diese beiseite.
 - c. Fixieren Sie die Kabel mithilfe von Klemmen.
- 7. Lösen Sie auf jeder Seite der Mini-PIM-Frontscheibe die Schrauben mit einem Schraubenzieher.
- 8. Ergreifen Sie die Schrauben auf jeder Seite der Frontscheibe des Mini-PIM, und lassen Sie das Mini-PIM aus dem Gerät hinausgleiten. Legen Sie das Mini-PIM im Abschirmbeutel oder auf der antistatischen Matte ab.

Abbildung 16: Entfernen eines Mini-PIM



- 9. Wenn Sie das Mini-PIM nicht mehr in den leeren Steckplatz einbauen, bringen Sie über dem Steckplatz eine unbeschriftete Frontscheibe an, um eine ausreichende Belüftung zu gewährleisten.

Einbauen eines Mini-PIM

Führen Sie zum Einbauen eines Mini-PIM die folgenden Schritte aus:

- 1. Schnallen Sie zum Schutz vor elektrostatischer Entladung ein Erdungsband um Ihr Handgelenk, und stellen Sie eine Verbindung zwischen dem Band und dem ESD-Punkt auf dem Gehäuse oder einem externen ESD-Punkt her, falls das SSG 20-Gerät nicht geerdet ist.
- 2. Entfernen Sie den Stromadapter vom Gerät. Überprüfen Sie, ob die Strom-LED aus ist.

3. Ergreifen Sie die Schrauben auf jeder Seite der Frontscheibe des Mini-PIM, und richten Sie die Einkerbungen auf dem Stecker an der Hinterseite des Mini-PIM an den Einkerbungen im Steckplatz des Mini-PIM im SSG 20-Gerät aus. Schieben Sie das Mini-PIM anschließend hinein, bis es fest im Gerät einrastet.

Abbildung 17: Einbauen eines Mini-PIM



VORSICHT: Schieben Sie das Mini-PIM direkt in den Steckplatz, um die Komponenten der Mini-PIM nicht zu beschädigen.

4. Ziehen Sie die Schrauben auf jeder Seite der Frontscheibe des Mini-PIM mit einem 3 mm-Schlitzschraubenzieher fest.
5. Stecken Sie die entsprechenden Kabel in die Kabelanschlüsse am Mini-PIM ein.
6. Ordnen Sie das Kabel ggf. so an, dass ein Herausgleiten des Kabels oder das Entstehen von Stresspunkten verhindert wird:
 - a. Bringen Sie die Kabel so an, dass sie beim Herunterhängen nicht ihr eigenes Gewicht stützen müssen.
 - b. Legen Sie zu lange Kabel sorgfältig zu einer Schleife zusammen, und räumen Sie diese beiseite.
 - c. Fixieren Sie die Kabel mithilfe von Klemmen.
7. Entfernen Sie den Stromadapter vom Gerät. Überprüfen Sie, ob die Strom-LED nach Drücken des Einschaltknopfs ständig grün leuchtet.
8. Überprüfen Sie, ob die PIM-Status-LED auf dem Systemdashboard ständig grün leuchtet. Dadurch wird angezeigt, dass das Mini-PIM online ist.

Erweitern des Arbeitsspeichers

Das einem SSG 20-Gerät zur Verfügung stehende 128 MB umfassende Dual Inline Memory Module (DIMM) Dynamic Random Access Memory (DRAM) kann auf 256 MB DIMM DRAM erweitert werden.

Gehen Sie zum Erweitern des Arbeitsspeichers eines SSG 20-Geräts folgendermaßen vor:

1. Schnallen Sie zum Schutz vor elektrostatischer Entladung ein Erdungsband um Ihr Handgelenk, und stellen Sie eine Verbindung zwischen dem Band und dem ESD-Punkt auf dem Chassis oder einem externen ESD-Punkt her, falls das Gerät nicht geerdet ist.
2. Stecken Sie das Wechselstromkabel aus.

3. Drehen Sie das Gerät um, damit die Oberseite auf einem ebenen Untergrund liegt.
4. Entfernen Sie die Schrauben mit einem Kreuzschlitzschraubenzieher von der Speicherkartenabdeckung. Legen Sie die Schrauben neben sich ab, um damit später wieder die Abdeckung zu fixieren.
5. Entfernen Sie die Speicherkartenabdeckung.

Abbildung 18: Unterseite des Geräts



6. Drücken Sie auf jeder Seite des Moduls mit den Daumen außen auf die Sperrriegel. Diese gleiten daraufhin vom Modul weg, und Sie können den 128 MB DIMM DRAM entnehmen.

Abbildung 19: Entriegeln des Arbeitsspeichermoduls



7. Ergreifen Sie die lange Kante des Arbeitsspeichermoduls, und lassen Sie dieses hinausgleiten. Legen Sie das Modul neben sich ab.

Abbildung 20: Entfernen der Modulsteckplätze



8. Setzen Sie den 256 MB DIMM DRAM in den Steckplatz ein. Üben Sie mit beiden Daumen einen gleichmäßigen Druck auf die obere Kante des Moduls aus, und drücken Sie das Modul nach unten, bis die Sperrriegel in der vorgesehenen Position einrasten.

Abbildung 21: Einsetzen des Arbeitsspeichermoduls



9. Platzieren Sie die Speicherkartenabdeckung über dem Steckplatz.
10. Ziehen Sie die Schrauben mit einem Kreuzschlitzschraubenzieher fest, und fixieren Sie die Abdeckung am Gerät.

Anhang A

Technische Daten

Dieser Anhang beinhaltet allgemeine technische Systemdaten für ein SSG 20-Gerät.
Der Anhang umfasst die folgenden Abschnitte:

- „Physisch“ auf Seite 58
- „Elektrik“ auf Seite 58
- „Umgebungstoleranz“ auf Seite 58
- „Zertifizierungen“ auf Seite 59
- „Stecker“ auf Seite 60

Physisch

Tabelle 8: SSG 20 – Physische Daten

Beschreibung	Wert
Chassisabmessungen	294 mm x 194,8 mm x 44 mm
Gewicht des Geräts	1,53 kg ohne eingebaute PIMs
ISDN-PIM	70 g
Annex A-PIM für ADSL	106 g
Annex B-PIM für ADSL	106 g
T1-PIM	75 g
E1-PIM	75 g
V.92-PIM	79 g

Elektrik

Tabelle 9: SSG 20 – Elektrische Daten

Physikalische Größe	Technische Daten
Eingangsgleichspannung	12 V
Zulässige Höchstspannung des Gleichspannungssystems	3 - 4,16 A

Umgebungstoleranz

Tabelle 10: SSG 20-Umgebungstoleranz

Beschreibung	Wert
Höhe über NN	Keine Beeinträchtigung der Leistung bis zu einer Höhe von 2.000 m
Relative Luftfeuchtigkeit	Bei einer relativen Luftfeuchtigkeit zwischen 10 und 90 Prozent (nicht kondensierend) ist eine ordnungsgemäße Funktion gesichert.
Temperatur	In einem Temperaturbereich zwischen 32°F (0°C) und 104°F (40°C) ist eine ordnungsgemäße Funktion sichergestellt. Zulässiger Temperaturbereich für die Lagerung des Geräts: -4°F (-20°C) bis 158°F (70°C)

Zertifizierungen

Sicherheit

- CAN/CSA-C22.2 Nr. 60950-1-03/UL 60950-1, Sicherheit von Informationstechnologiegeräten
- EN 60950-1 (2000) Dritte Ausgabe, Sicherheit von Informationstechnologiegeräten
- IEC 60950-1 (1999) Dritte Ausgabe, Sicherheit von Informationstechnologiegeräten

EMC-Emissionen

- FCC Teil 15 Klasse B (USA)
- EN 55022 Klasse B (Europa)
- AS 3548 Klasse B (Australien)
- VCCI Klasse B (Japan)

EMC-Störfestigkeit

- EN 55024
- EN-61000-3-2 – Netzoberwellen
- EN-61000-3-3 – Netzoberwellen
- EN-61000-4-2 – ESD (elektrostatische Entladung)
- EN-61000-4-3 – Störfestigkeit gegen Strahlung
- EN-61000-4-4 – EFT (schnelle transiente Störgrößen)
- EN-61000-4-5 – Stoßspannungen
- EN-61000-4-6 – Allgemeine Störfestigkeit gegen niedrige Frequenzen
- EN-61000-4-11 – Spannungseinbrüche und -schwankungen

ETSI

European Telecommunications Standards Institute (ETSI) EN-3000386-2: Netzwerkgeräte für Telekommunikation. Anforderungen für elektromagnetische Kompatibilität; (Gerätekategorie – Unterschied zu Telekommunikationscentern)

T1-Schnittstelle

- FCC Teil 68 – TIA 968
- Industry Canada CS-03
- UL 60950-1 – Geltende Anforderungen für TNV-Verbindungen mit einem externen Leitungsanschluss

Stecker

Abbildung 22 zeigt die Position der Pins auf einem RJ-45-Stecker.

Abbildung 22: RJ-45-Kontaktanordnungen

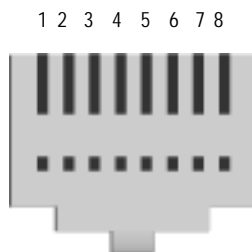


Tabelle 11 beinhaltet eine Auflistung der Kontaktanordnungen der RJ-45-Stecker.

Tabelle 11: Kontaktanordnungen der RJ-45-Stecker

Pin	Name	E/A	Beschreibung
1	RTS Out	O	Sendeaufforderung (Request To Send)
2	DTR Out	O	Endgerät betriebsbereit (Data Terminal Ready)
3	TxD	O	Daten übertragen (Transmit Data)
4	GND	Nicht zutreffend	Chassismasse (Chassis Ground)
5	GND	Nicht zutreffend	Chassismasse (Chassis Ground)
6	RxD	I	Daten empfangen (Receive Data)
7	DSR	I	Datensatz bereit (Data Set Ready)
8	CTS	I	Sendebereitschaft (Clear To Send)

Abbildung 23 zeigt die Position der Pins auf einer DB-9-Buchse.

Abbildung 23: DB-9-Buchse

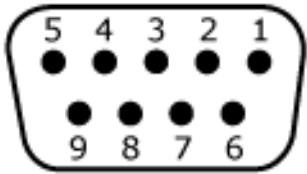


Tabelle 12 beinhaltet eine Auflistung der Kontaktanordnungen der DB-9-Stecker.

Tabelle 12: Kontaktanordnungen der DB-9-Stecker

Pin	Name	E/A	Beschreibung
1	DCD	I	Trägersignal erkannt (Carrier Detect)
2	RxD	I	Daten empfangen (Receive Data)
3	TxD	O	Daten übertragen (Transmit Data)
4	DTR	O	Endgerät betriebsbereit (Data Terminal Ready)
5	GND	Nicht zutreffend	Signalerde (Signal Ground)
6	DSR	I	Datensatz bereit (Data Set Ready)
7	RTS	O	Sendeaufforderung (Request To Send)
8	CTS	I	Sendebereitschaft (Clear To Send)
9	RING	I	Anrufanzeige (Ring Indicator)

Anhang B

Assistent für die Anfangskonfiguration

Dieser Anhang beinhaltet detaillierte Informationen zum Assistenten für die Anfangskonfiguration (Initial Configuration Wizard, ICW) für SSG 20-Geräte.

Verwenden Sie nach dem Anschluss des Geräts an das Netzwerk den ICW zur Konfiguration der auf dem Gerät installierten Schnittstellen.

In diesem Abschnitt werden die folgenden ICW-Fenster behandelt:

- Fenster für die Schnellkonfiguration auf Seite 64
- Fenster für die Administratoranmeldung auf Seite 64
- Fenster für den WLAN-Zugriffspunkt auf Seite 65
- Fenster für die Konfiguration der physischen Schnittstelle auf Seite 65
- ADSL2/2+ Interface – Fenster auf Seite 66
- Fenster für die Konfiguration der T1-Schnittstelle auf Seite 68
- Fenster für die Konfiguration der E1-Schnittstelle auf Seite 73
- Fenster für die Konfiguration der ISDN-Schnittstelle auf Seite 76
- Fenster für die Konfiguration der V.92-Modemschnittstelle auf Seite 79
- Eth0/0 Interface (Untrust Zone) – Fenster auf Seite 80
- Eth0/1 Interface (DMZ Zone) – Fenster auf Seite 81
- Bgroup0 Interface (Trust Zone) – Fenster auf Seite 82
- Fenster für die Konfiguration der Wireless0/0-Schnittstelle (Trust Zone) auf Seite 83
- Fenster für die Schnittstellenzusammenfassung auf Seite 84
- Fenster für die Konfiguration der physischen Ethernet-DHCP-Schnittstelle auf Seite 85
- Fenster für die Konfiguration der Wireless-DHCP-Schnittstelle auf Seite 85
- Bestätigungsfenster auf Seite 86

1. Fenster für die Schnellkonfiguration

Abbildung 24: Fenster für die Schnellkonfiguration

Arbeitet das Netzwerk mit NetScreen-Security Manager (NSM) kann das Configlet für die Schnellkonfiguration zur automatischen Konfiguration des Geräts eingesetzt werden. Sie erhalten ein Configlet vom NSM-Administrator, wählen Sie **Yes, Load Configlet from:**, und navigieren Sie zum Speicherort der Datei. Klicken Sie anschließend auf **Next**. Das Configlet richtet das Gerät für Sie ein, sodass Sie zum Konfigurieren des Geräts die folgenden Schritte nicht ausführen müssen.

Wenn Sie den ICW umgehen und direkt zur WebUI wechseln möchten, wählen Sie die letzte Option, und klicken Sie anschließend auf **Next**.

Wenn Sie zum Konfigurieren des Geräts kein Configlet, sondern den ICW verwenden möchten, wählen Sie die erste Option, und klicken Sie anschließend auf **Next**. Die ICW-Willkommensseite wird angezeigt. Klicken Sie auf **Next**. Das Fenster für die Administratoranmeldung wird angezeigt.

2. Fenster für die Administratoranmeldung

Geben Sie einen neuen Administratoranmeldenamen und ein neues Kennwort ein, und klicken Sie auf **Next**.

Abbildung 25: Fenster für die Administratoranmeldung

3. Fenster für den WLAN-Zugriffspunkt

Bei Verwendung des Geräts in der Regulierungsdomäne WORLD oder ETSI müssen Sie einen Ländercode auswählen. Wählen Sie die entsprechenden Optionen, und klicken Sie anschließend auf **Next**.

Abbildung 26: Fenster für die Konfiguration des Ländercodes für den Wireless-Zugriffspunkt

The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. The main area has a light blue background. The text 'How do you want to configure the wireless access point?' is at the top. Below it, there are four dropdown menus: 'Regulatory Domain' set to 'WORLD', 'Country Code' set to 'NO_COUNTRY_SET', '2.4G Mode' set to '802.11b/g', and '5G Mode' set to '802.11a'. At the bottom, there is a checkbox labeled 'Configure wireless0/0 interface in trust zone.' which is checked. Below the checkbox are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

4. Fenster für die Konfiguration der physischen Schnittstelle

Auf dem Bildschirm für Schnittstellen-Zonenbindungen legen Sie die Schnittstelle fest, an die die Untrust Sicherheitszone gebunden werden soll. Bgroup0 ist vorab an die Trust Sicherheitszone gebunden. Eth0/1 ist an die DMZ-Sicherheitszone gebunden, dabei jedoch optional.

Abbildung 27: Fenster für die Angabe der physischen Schnittstelle

The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. The main area has a light blue background. The text 'Please choose one interface for untrust, dmz and trust zone respectively.' is at the top. Below it, there are three dropdown menus: 'Untrust Zone' set to 'eth0/0', 'DMZ Zone' set to 'eth0/1', and 'Trust Zone' set to 'bgroup0'. At the bottom are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Sie können nach dem Binden einer Schnittstelle an eine Zone die Schnittstelle konfigurieren. Die auf dem Sicherheitsgerät installierten Mini-PIMs bestimmen darüber, welche Konfigurationsfenster anschließend angezeigt werden. Klicken Sie zum Fortsetzen der Konfiguration mithilfe des ICW auf **Next**.

5. ADSL2/2+ Interface – Fenster

Wenn auf dem Gerät das ADSL2/2 + -Mini-PIM installiert ist, können Sie über das folgende Fenster die adslx/0-Schnittstelle konfigurieren.

HINWEIS: Sind auf dem Gerät zwei ADSL2/2 + -Mini-PIMs installiert, kann die Mehrfachverbindungsfunktion mit dem ICW nicht verwendet werden. Informationen zum Konfigurieren von ML ADSL finden Sie im *Concepts & Examples ScreenOS Reference Guide*.

Abbildung 28: Fenster für die Konfiguration der ADSL-Schnittstelle

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20. The window has a blue header with the title 'Initial Configuration Wizard'. Below the header is a Juniper logo and the text 'SSG 20'. A red text prompt says: 'Please click the following links or the above figure to configure interfaces.' Below this are three links: 'adsl1/0(Untrust Zone)', 'bgroup0(Trust Zone)', and 'eth0/1(DMZ Zone)'. The main configuration area is titled 'How does the Juniper device connect to the outside via adsl1/0 interface?'. It contains several fields and radio buttons: 'VPI/VCI:' with input boxes for '8' and '35'; 'Multiplexing Method:' with a dropdown menu set to 'LLC'; 'RFC1483 Protocol Mode:' with radio buttons for 'Bridged' (selected) and 'Routed'; 'Operating Mode:' with radio buttons for 'Auto' (selected), 'ANSI DMT', 'ITU DMT', 'Adsl2', and 'Adsl2+'. Below these are three sections for dynamic IP configuration: 'Dynamic IP via DHCP', 'Dynamic IP via PPPoA' (with fields for Username, Password, and Confirm), and 'Dynamic IP via PPPoE' (with fields for Username, Password, and Confirm). The 'Static IP' section is selected with a radio button and contains fields for 'Interface IP:', 'Netmask:', and 'Gateway:'. At the bottom are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Tabelle 13: Felder im Fenster für die Konfiguration der ADSL-Schnittstelle

Feld	Beschreibung
Informationen vom Diensteanbieter:	
VPI/VCI	VPI/VCI-Werte zum Identifizieren der dauerhaften virtuellen Verbindung.
Multiplexing Method	ATM-Multiplexingmethode (Standardeinstellung: LLC).
RFC1483 Protocol Mode	Protokollmoduseinstellung (Standardeinstellung: Bridged).
Operating Mode	Betriebsmodus für die physische Leitung (Standardeinstellung: Auto).
IP-Konfigurationseinstellungen	<ul style="list-style-type: none"> ■ Aktivieren Sie Dynamic IP via DHCP, damit das Gerät eine IP-Adresse für die ADSL-Schnittstelle von einem Diensteanbieter empfangen kann. ■ Aktivieren Sie Dynamic IP via PPPoA, damit das Gerät als PPPoA-Client arbeiten kann. Geben Sie den vom Diensteanbieter zugewiesenen Benutzernamen und das zugewiesene Kennwort ein. ■ Aktivieren Sie Dynamic IP via PPPoE, damit das Gerät als PPPoE-Client arbeiten kann. Geben Sie den vom Diensteanbieter zugewiesenen Benutzernamen und das zugewiesene Kennwort ein. ■ Wählen Sie zum Zuweisen einer eindeutigen und festen IP-Adresse zur ADSL-Schnittstelle die Option Static IP aus. Geben Sie die IP-Adresse der Schnittstelle, die Netzmaske und das Gateway ein (die Gateway-Adresse ist die IP-Adresse des mit dem Gerät verbundenen Routeranschlusses).

Sind Ihnen diese Einstellungen nicht bekannt, schlagen Sie in der mit dem Diensteanbietergerät mitgelieferten Dokument *Common Settings for Service Providers* nach.

6. Fenster für die Konfiguration der T1-Schnittstelle

Ist auf dem Gerät das T1-Mini-PIM installiert und wurde die Option **Frame Relay** ausgewählt, werden die folgenden Fenster angezeigt:

- Fenster für die Konfiguration der T1-Schnittstelle mit der Registerkarte „Physical Layer“
- Fenster für die Konfiguration der T1-Schnittstelle – Registerkarte „Frame Relay“

HINWEIS: Sind auf dem Gerät zwei T1-Mini-PIMs installiert und Sie wählen die Option für die Mehrfachverbindungen, werden zwei mit Physical Layer bezeichnete Registerkarten angezeigt.

Abbildung 29: Fenster für die Konfiguration der T1-Schnittstelle mit der Registerkarte „Physical Layer“

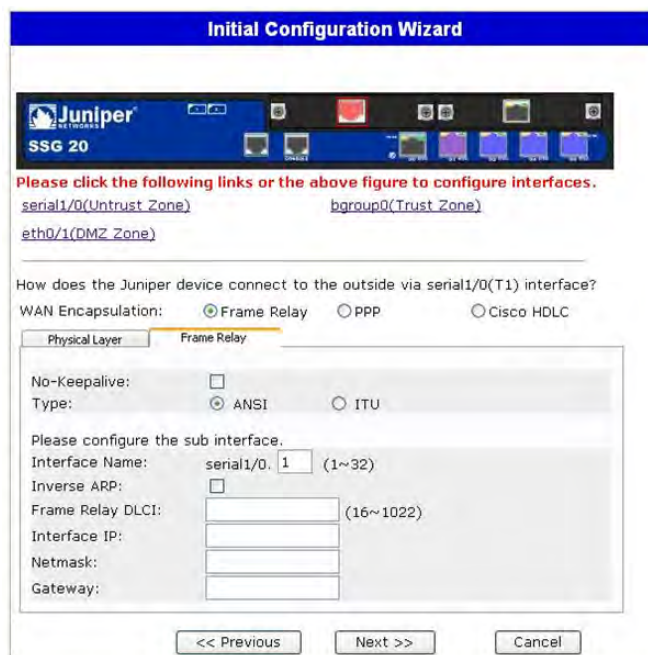
The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20. The main window has a blue header with the Juniper logo and 'SSG 20'. Below the header, there's a section titled 'Please click the following links or the above figure to configure interfaces.' with links for 'serial1/0(Untrust_Zone)', 'bggroup0(Trust_Zone)', and 'eth0/1(DMZ_Zone)'. The next question is 'How does the Juniper device connect to the outside via serial1/0(T1) interface?'. The 'WAN Encapsulation' options are 'Frame Relay' (selected), 'PPP', and 'Cisco HDLC'. Below this, there are two tabs: 'Physical Layer' (active) and 'Frame Relay'. The 'Physical Layer' tab contains the following settings:

- Clocking: ☒ External, ☐ Internal (Lab Use Only)
- Line Buildout: 0~132 Feet (dropdown)
- Line Encoding: ☐ AMI (Auto Mark Inversion), ☒ B8ZS (8-bits Zero Suppression)
- Byte Encoding: ☐ 7-bits per byte, ☒ 8-bits per byte
- Frame Checksum: ☒ 16-bits, ☐ 32-bits
- Framing Mode: ☐ Super Frame, ☒ Extended Super Frame
- Idle Cycles Flag: ☒ 0x7E, ☐ 0xFF(All Ones)
- Start/End Flags: ☒ Filler, ☐ Share
- Invert data: ☐
- Loopback Respond: ☐
- Time Slots: 0 (dropdown), (0(all active), 1..24(e.g. 2,7-9))

At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Tabelle 14: Felder im Fenster für die Konfiguration der T1-Schnittstelle mit der Registerkarte „Physical Layer“

Feld	Beschreibung
Clocking	Stellt den Übertragungstakt der Schnittstelle ein.
Line Buildout	Legt die Entfernung fest, bis zu der über eine Schnittstelle eine Verbindung aufrechterhalten werden kann. Die Standardeinstellung ist 0 - 132 Feet (ca. 0-40 m).
Line Encoding	Legt das Leitungsver schlüsselungsformat der Schnittstelle fest: <ul style="list-style-type: none"> ■ Auto Mark Inversion ■ 8-bits Zero Suppression
Byte Encoding	Legt die Byte-Verschlüsselung der T1-Schnittstelle auf 7 Bit/Byte oder 8 Bit/Byte fest. Standardmäßig sind 8 Bit/Byte ausgewählt.
Frame Checksum	Legt die Größe der Prüfsumme fest. Der Standardwert ist 16 .
Framing Mode	Legt das Rahmenformat fest. Standardmäßig ist der erweiterte Modus ausgewählt.
Idle Cycles Flag	Legt den Wert fest, der während Zyklen ohne Aktivität von der Schnittstelle übertragen wird. Standardmäßig ist 0x7E ausgewählt: <ul style="list-style-type: none"> ■ 0x7E (Flags) ■ 0xFF (Einsen)
Start/End Flags	Für die Übertragung der Start- und Endflags kann Filler oder Shared ausgewählt werden. Standardmäßig ist Filler ausgewählt.
Invert Data – Kontrollkästchen	Ermöglicht die invertierte Übertragung nicht verwendeter Datenbits.
Loopback Respond – Kontrollkästchen	Ermöglicht das Loopback auf der T1-Schnittstelle von der Remote-CSU (Channel Service Unit).
Time Slots	Legt die Verwendung von Zeitsteckplätzen einer T1-Schnittstelle fest. Die Standardeinstellung ist 0 , alle 24 Zeitsteckplätze werden verwendet.

Abbildung 30: Fenster für die Konfiguration der T1-Schnittstelle – Registerkarte „Frame Relay“**Tabelle 15: Felder auf der Registerkarte „Frame Relay“ im Fenster für die Konfiguration der T1-Schnittstelle**

Feld	Beschreibung
No-Keepalive – Kontrollkästchen	Aktiviert No-Keepalives.
Type	Legt den Frame-Relay-LMI-Typ fest: <ul style="list-style-type: none"> ■ ANSI: American National Standards Institute unterstützt Downstream-Datenraten von bis zu 8 MBit/s und Upstream-Datenraten von bis zu 1 MBit/s. ■ ITU: International Telecommunications Union unterstützt Downstream-Datenraten von 6,144 MBit/s und Upstream-Datenraten von 640 KBit/s.
Interface Name	Legt den Namen der Subschnittstelle fest.
Inverse ARP	Ermöglicht das umgekehrte ARP (Address Resolution Protocol) für die Subschnittstelle.
Frame Relay DLCI	Weist der Subschnittstelle einen DLCI (Data Link Connection Identifier) zu.
Interface IP	Legt die IP-Adresse für die Subschnittstelle fest.
Netmask	Legt die Netzmaske für die Subschnittstelle fest.
Gateway	Legt die Gateway-Adresse für die Subschnittstelle fest.

Ist auf dem Gerät das T1-Mini-PIM installiert und wurde die Option „PPP“ ausgewählt, werden die folgenden zusätzlichen Fenster angezeigt:

- Fenster für die Option „PPP“ mit der Registerkarte „PPP“
- Fenster für die Option „PPP“ mit der Registerkarte „Peer User“

Abbildung 31: Fenster für die Option „PPP“ mit der Registerkarte „PPP“

Initial Configuration Wizard

Juniper
SSG 20

Please click the following links or the above figure to configure interfaces.
[serial1/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

How does the Juniper device connect to the outside via serial1/0(T1) interface?
 WAN Encapsulation: ☐ Frame Relay ☒ PPP ☐ Cisco HDLC

Physical Layer **PPP** Peer User

Please create the PPP profile.

PPP Profile Name:

Authentication: ☒ Any ☐ CHAP ☐ PAP ☐ None

Local User:

Password:

Static IP: ☒

Please configure the serial1/0 interface.

Interface IP:

Netmask:

Gateway:

<< Previous Next >> Cancel

Tabelle 16: Felder im Fenster für die Option „PPP“ mit der Registerkarte „PPP“

Feld	Beschreibung
PPP Profile Name	Legt den Namen des PPP-Profiles fest.
Authentication	Legt den Authentifizierungstyp fest.
Local User	Legt den Namen des lokalen Benutzers fest.
Password	Legt das Kennwort für den lokalen Benutzer fest.
Static IP – Kontrollkästchen	Ermöglicht eine statische IP-Adresse.
Interface IP	Legt die IP-Adresse für die serialx/0-Schnittstelle fest.
Netmask	Legt die serialx/0-Netzmaske fest.
Gateway	Legt die serialx/0-Gateway-Adresse fest.

Abbildung 32: Fenster für die Option „PPP“ mit der Registerkarte „Peer User“

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20. At the top, there's a blue header with the Juniper logo and 'SSG 20'. Below it, a network diagram shows various interfaces. A red text prompt says: 'Please click the following links or the above figure to configure interfaces.' with links for 'serial1/0(Untrust Zone)', 'eth0/1(DMZ Zone)', and 'hgroup0(Trust Zone)'. The main question is 'How does the Juniper device connect to the outside via serial1/0(T1) interface?'. Under 'WAN Encapsulation', there are three radio buttons: 'Frame Relay' (unselected), 'PPP' (selected), and 'Cisco HDLC' (unselected). Below this, there are three tabs: 'Physical Layer', 'PPP', and 'Peer User'. The 'Peer User' tab is active and highlighted in yellow. It contains three input fields: 'Peer User:', 'Password:', and 'Status:'. The 'Status' field has two radio buttons: 'Enable' (selected) and 'Disable' (unselected). At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Tabelle 17: Felder im Fenster für die Option „PPP“ mit der Registerkarte „Peer User“

Feld	Beschreibung
Peer User	Legt den Namen des Peer-Benutzers fest.
Password	Legt das Kennwort für den im Textfeld Peer User angegebenen Peer-Benutzer fest.
Status	Aktiviert bzw. deaktiviert PPP.

Ist auf dem Gerät das T1-Mini-PIM installiert und wurde die Option Cisco HDLC ausgewählt, wird das folgende Fenster angezeigt:

Abbildung 33: Fenster für die Option „Cisco HDLC“ mit der Registerkarte „Cisco HDLC“



Tabelle 18: Felder im Fenster mit Option „Cisco HDLC“ und Registerkarte „Cisco HDLC“

Feld	Beschreibung
Interface IP	Legt die IP-Adresse für die T1 Cisco HDLC-Schnittstelle fest.
Netmask	Legt die Netzmaske für die T1 Cisco HDLC-Schnittstelle fest.
Gateway	Legt die Gateway-Adresse für die T1 Cisco HDLC-Schnittstelle fest.

7. Fenster für die Konfiguration der E1-Schnittstelle

Ist auf dem Gerät das E1-Mini-PIM installiert und wurde Option Frame Relay ausgewählt, werden die folgenden Fenster angezeigt:

- Fenster für die Konfiguration der E1-Schnittstelle mit der Registerkarte „Physical Layer“
- Fenster für die Konfiguration der E1-Schnittstelle mit der Registerkarte „Frame Relay“

HINWEIS: Sind auf dem Gerät zwei E1-Mini-PIMs installiert und wird die Option für die Mehrfachverbindungen ausgewählt, werden zwei der mit Physical Layer bezeichneten Registerkarten angezeigt.

Abbildung 34: Fenster für die Konfiguration der E1-Schnittstelle mit der Registerkarte „Physical Layer“



Tabelle 19: Felder im Fenster für die Konfiguration der E1-Schnittstelle mit der Registerkarte „Physical Layer“

Feld	Beschreibung
Clocking	Stellt den Übertragungstakt der Schnittstelle ein.
Frame Checksum	Legt die Größe der Prüfsumme fest. Der Standardwert ist 16 .
Framing Mode	Legt das Rahmenformat fest. Die Standardeinstellung ist without CRC4 .
Idle Cycles Flag	Legt den Wert fest, der während Zyklen ohne Aktivität von der Schnittstelle übertragen wird. Standardmäßig ist 0x7E ausgewählt: <ul style="list-style-type: none"> ■ 0x7E (Flags) ■ 0xFF (Einsen)
Start/End Flags	Für die Übertragung der Start- und Endflags kann Filler oder Shared ausgewählt werden. Standardmäßig ist Filler ausgewählt.
Invert Data – Kontrollkästchen	Ermöglicht die invertierte Übertragung nicht verwendeter Datenbits.
Time Slots	Legt die Verwendung von Zeitsteckplätzen einer T1-Schnittstelle fest. Die Standardeinstellung ist 0 , alle 32 Zeitsteckplätze werden verwendet.

Abbildung 35: Fenster für die Konfiguration der E1-Schnittstelle mit der Registerkarte „Frame Relay“



Tabelle 20: Felder auf der Registerkarte „Frame Relay“ im Fenster für die Konfiguration der E1-Schnittstelle

Feld	Beschreibung
No-Keepalive – Kontrollkästchen	Aktiviert No-Keepalives.
Type	Legt den Frame-Relay-LMI-Typ fest: <ul style="list-style-type: none"> ■ ANSI: American National Standards Institute unterstützt Downstream-Datenraten von bis zu 8 MBit/s und Upstream-Datenraten von bis zu 1 MBit/s. ■ ITU: International Telecommunications Union unterstützt Downstream-Datenraten von 6,144 MBit/s und Upstream-Datenraten von 640 Bit/s.
Interface Name	Legt den Namen der Subschnittstelle fest.
Inverse ARP – Kontrollkästchen	Ermöglicht das umgekehrte ARP (Address Resolution Protocol) für die Subschnittstelle.
Frame Relay DLCI	Weist der Subschnittstelle einen DLCI zu.
Interface IP	Legt die IP-Adresse für die Subschnittstelle fest.
Netmask	Legt die Netzmaske für die Subschnittstelle fest.
Gateway	Legt die Gateway-Adresse für die Subschnittstelle fest.

Informationen zum Konfigurieren der E1-Schnittstelle mit PPP-Optionen finden Sie unter „Fenster für die Option „PPP“ mit der Registerkarte „PPP““ auf Seite 71.

Informationen zum Konfigurieren der E1-Schnittstelle mit der Option Cisco HDLC finden Sie unter „Fenster für die Option „Cisco HDLC“ mit der Registerkarte „Cisco HDLC““ auf Seite 73.

8. Fenster für die Konfiguration der ISDN-Schnittstelle

Wenn auf dem Gerät das ISDN-Mini-PIM installiert ist, können Sie über das folgende Fenster die bri1/0 (Untrust)-Schnittstelle konfigurieren.

HINWEIS: Sind auf dem Gerät zwei ISDN-Mini-PIMs installiert und wurde die Option für die Mehrfachverbindungen ausgewählt, werden zwei der mit Physical Layer bezeichneten Registerkarten angezeigt.

Abbildung 36: Fenster für die Konfiguration der ISDN-Schnittstelle mit der Registerkarte „Physical Layer“

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20 device. At the top, there's a blue header with the Juniper logo and 'SSG 20'. Below it, a network diagram shows various interfaces. A red text prompt says: 'Please click the following links or the above figure to configure interfaces.' followed by three links: [bri1/0\(Untrust_Zone\)](#), [bgroup0\(Trust_Zone\)](#), and [eth0/1\(DMZ_Zone\)](#).

Below the links, a question asks: 'How does the Juniper device connect to the outside via bri1/0 interface?'. There are two options: 'Leased Line Mode (128Kbps):' with an unchecked checkbox, and 'Dial Using BRI:' with an unchecked checkbox.

The 'Physical Layer' tab is selected. It contains the following fields:

- Switch Type: A dropdown menu set to 'European Variants'.
- SPID1: A text input field followed by '(Optional)'.
- SPID2: A text input field followed by '(Optional)'.
- TEI Negotiation: Two radio buttons, 'First Call' (which is selected) and 'Power UP'.
- Calling Number: A text input field followed by '(Optional)'.
- Sending Complete: An unchecked checkbox.

At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Tabelle 21: Felder auf der Registerkarte „Physical Layer“ im Fenster für die Konfiguration der ISDN-Schnittstelle

Feld	Beschreibung
Switch Type	Legt den Vermittlungstyp des Dienstanbieters fest: <ul style="list-style-type: none"> ■ att5e: At&T 5ESS ■ ntdms100: Nortel DMS 100 ■ ins-net: NTT INS-Net ■ etsi: European variants ■ ni1: National ISDN-1
SPID1	Dienstanbieter-ID, normalerweise eine siebenstellige Telefonnummer mit einigen optionalen Nummern. Nur für die Vermittlungstypen DMS-100 und NI1 sind SPIDs erforderlich. Dem Vermittlungstyp DMS-100 sind zwei SPIDs zugewiesen, einer für jeden B-Kanal.
SPID2	Sicherungsdienstanbieter-ID.
TEI Negotiation	Gibt an, wann die TEI ausgehandelt werden soll (beim Start oder beim ersten Anruf). Diese Einstellung wird normalerweise für ISDN-Dienstangebote in Europa und Verbindungen zu DMS-100-Switches verwendet, die für das Initialisieren der TEI-Aushandlung vorgesehen sind.
Calling Number	Rechnungsnummer für das ISDN-Netzwerk.
Sending Complete – Kontrollkästchen	Ermöglicht das Senden vollständiger Informationen an ausgehende Installationsmeldung. Wird normalerweise nur in Hongkong und Taiwan verwendet.

Bei der bri1/0-Schnittstelle kann eine Verbindung mithilfe der Wählhilfe, der Wählhilfe für Mehrfachverbindungen, einer geleasteten Leitung oder durch Einwahl mithilfe von BRI hergestellt werden. Wird keine oder eine Option oder werden beide Optionen ausgewählt, sieht das daraufhin angezeigte Fenster etwa folgendermaßen aus:

Abbildung 37: Fenster für die Konfiguration der ISDN-Schnittstelle mit der Registerkarte „Connection“

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20 device. The 'Dialer Interface' tab is active. The wizard prompts the user to create a PPP profile. The configuration fields include:

- PPP Profile Name:** A text input field.
- Authentication:** Radio buttons for Any (selected), CHAP, PAP, and None.
- Local User:** A text input field.
- Password:** A text input field.
- Static IP:** A checked checkbox.
- Interface Name:** A dropdown menu showing 'dialer 1'.
- Encapsulation Type:** Radio buttons for ppp (selected) and Multi-Link PPP.
- Primary Number:** A text input field.
- Alternative Number:** A text input field with '(Optional)' next to it.
- Dialer Pool:** A text input field.
- Interface IP:** A text input field.
- Netmask:** A text input field.
- Gateway:** A text input field.

Navigation buttons at the bottom include '<< Previous', 'Next >>', and 'Cancel'.

Tabelle 22: Felder auf der Registerkarte „Connection“ im Fenster für die Konfiguration der ISDN-Schnittstelle

Feld	Beschreibung
PPP Profile Name	Legt für die ISDN-Schnittstelle einen PPP-Profilnamen fest.
Authentication	Legt den PPP-Authentifizierungstyp fest: <ul style="list-style-type: none"> ■ Any ■ CHAP: Challenge Handshake Authentication Protocol ■ PAP: Password Authentication Protocol ■ None
Local User	Legt den lokalen Benutzer fest.
Password	Legt das Kennwort für den lokalen Benutzer fest.
Static IP – Kontrollkästchen	Aktiviert eine statische IP-Adresse für die Schnittstelle.
Interface IP	Legt die IP-Adresse für die Schnittstelle fest.
Interface Name (nur Wählhilfe)	Legt den Schnittstellennamen der Wählhilfe fest. Der Standardwert ist dialer.1 .
Encapsulation Type	Legt den Einkapselungstyp für die Wählhilfe und für BRI-Schnittstellen verwendende Wählhilfen fest. Der Standardwert ist PPP .
Primary Number	Legt die primäre Nummer für Wählhilfen und für BRI-Schnittstellen verwendende Wählhilfen fest.

Feld	Beschreibung
Alternative Number	Legt die alternative (sekundäre) Nummer fest, die verwendet werden soll, wenn die primäre Nummer für die Verbindungsherstellung nicht verwendet werden kann.
Dialer Pool (nur Wählhilfe)	Legt den Poolnamen der Wählhilfe für die Schnittstelle der Wählhilfe fest.
Netmask	Legt die Netzmaske fest.
Gateway	Legt die Gateway-Adresse fest.

9. Fenster für die Konfiguration der V.92-Modemschnittstelle

Wenn auf dem Gerät das V.92-Mini-PIM installiert ist, können Sie über das folgende Fenster die serialx/0 (Modem)-Schnittstelle konfigurieren:

Abbildung 38: Fenster für die Konfiguration der Modemschnittstelle

Tabelle 23: Felder im Fenster für die Konfiguration der Modemschnittstelle

Feld	Beschreibung
Modem Name	Legt den Namen für die Modemschnittstelle fest.
Init String	Legt die Initialisierungszeichenfolge für das Modem fest.
ISP Name	Weist dem Dienstanbieter einen Namen zu.
Primary Number	Gibt die Telefonnummer zum Zugreifen auf den Dienstanbieter an.
Alternative Number (optional)	Gibt eine alternative Telefonnummer zum Zugreifen auf den Dienstanbieter an, wenn mithilfe der primären Nummer keine Verbindung hergestellt werden kann.
Login Name	Legt den Anmeldenamen für das Dienstanbieterkonto fest.
Password	Legt das Kennwort für den Anmeldenamen fest.
Confirm	Bestätigt das ins Feld für das Kennwort eingegebene Kennwort.

10. Eth0/0 Interface (Untrust Zone) – Fenster

Der eth0/0-Schnittstelle kann über DHCP oder PPPoE eine statische oder dynamische IP-Adresse zugewiesen werden.

Abbildung 39: Fenster für die Konfiguration der Eth0/0-Schnittstelle

Initial Configuration Wizard

Juniper
SSG 20

Please click the following links or the above figure to configure interfaces.
[eth0/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

Enter the IP address and netmask for the interface eth0/0(untrust zone).

☐ Dynamic IP via DHCP
☐ Dynamic IP via PPPoE
 Username:
 Password:
 Confirm:
☒ Static IP
 Interface IP:
 Netmask:
 Gateway:

<< Previous Next >> Cancel

Tabelle 24: Felder im Fenster für die Konfiguration der Eth0/0-Schnittstelle

Feld	Beschreibung
Dynamic IP via DHCP	Ermöglicht den Empfang einer IP-Adresse für die Schnittstelle der Untrust Zone von einem Dienstanbieter.
Dynamic IP via PPPoE	Das Gerät kann als PPPoE-Client fungieren und empfängt eine IP-Adresse für die Schnittstelle der Untrust Zone von einem Dienstanbieter. Geben Sie den vom Dienstanbieter zugewiesenen Benutzernamen und das zugewiesene Kennwort ein.
Static IP	Weist der Schnittstelle der Untrust Zone eine eindeutige und feste IP-Adresse zu. Geben Sie die IP-Adresse der Schnittstelle der Untrust Zone, die Netzmaske und die Gateway-Adresse ein.

11. Eth0/1 Interface (DMZ Zone) – Fenster

Der eth0/1-Schnittstelle kann über DHCP eine statische oder dynamische IP-Adresse zugewiesen werden.

Abbildung 40: Fenster für die Konfiguration der Eth0/1-Schnittstelle



Tabelle 25: Felder im Fenster für die Konfiguration der Eth0/1-Schnittstelle

Feld	Beschreibung
Dynamic IP via DHCP	Ermöglicht den Empfang einer IP-Adresse für die DMZ-Schnittstelle von einem Dienstanbieter.
Static IP	Weist der DMZ-Schnittstelle eine eindeutige und feste IP-Adresse zu. Geben Sie die IP-Adresse der DMZ-Schnittstelle und eine Netzmaske ein.

12. Bgroup0 Interface (Trust Zone) – Fenster

Der bgroup0-Schnittstelle kann über DHCP eine statische oder dynamische IP-Adresse zugewiesen werden.

Die Standard-IP-Adresse für Schnittstellen ist **192.168.1.1**, und die Netzmaske lautet **255.255.255.0** oder **24**.

Abbildung 41: Fenster für die Konfiguration der Bgroup0-Schnittstelle



Tabelle 26: Felder im Fenster für die Konfiguration der Bgroup0-Schnittstelle

Feld	Beschreibung
Dynamic IP via DHCP	Ermöglicht den Empfang einer IP-Adresse für die Schnittstelle der Trust Zone von einem Dienstanbieter.
Static IP	Weist der Schnittstelle der Trust Zone eine eindeutige und feste IP-Adresse zu. Geben Sie die IP-Adresse der Schnittstelle der Trust Zone und eine Netzmaske ein.

13. Fenster für die Konfiguration der Wireless0/0-Schnittstelle (Trust Zone)

Beim Konfigurieren des SSG 20-WLAN-Geräts müssen Sie vor dem Aktivieren der wireless0/0-Schnittstelle eine Service Set Identifier (SSID) festlegen. Detaillierte Anweisungen zum Konfigurieren der Wireless-Schnittstellen finden Sie im *Concepts & Examples ScreenOS Reference Guide*.

Abbildung 42: Fenster für die Konfiguration der Wireless0/0-Schnittstelle



Tabelle 27: Felder im Fenster für die Konfiguration der Wireless0/0-Schnittstelle

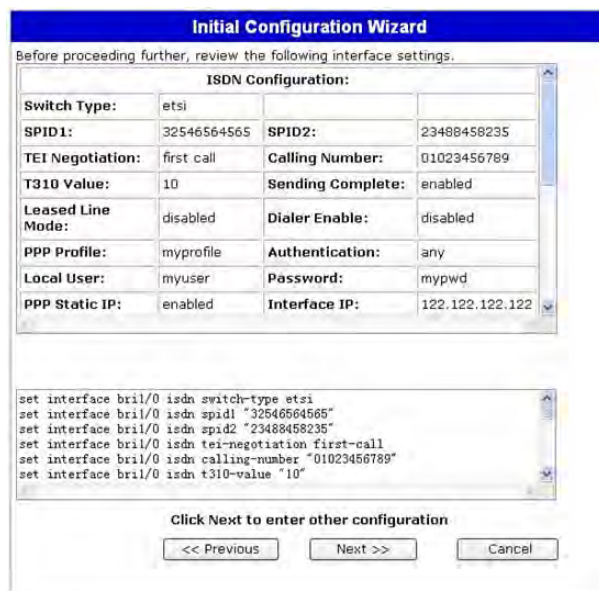
Feld	Beschreibung
Wlan Mode	Legt den WLAN-Funkmodus fest: <ul style="list-style-type: none">■ 5 G (802.11a)■ 2.4 G (802.11b/g)■ Both (802.11a/b/g)
SSID	Legt den SSID-Namen fest.

Feld	Beschreibung
Authentication and Encryption	<p>Legt die Authentifizierung und Verschlüsselung der WLAN-Schnittstelle fest:</p> <ul style="list-style-type: none"> ■ Mit der Standardeinstellung Open für die Authentifizierung kann jeder auf das Gerät zugreifen. Für diese Authentifizierungsoption steht keine Verschlüsselung zur Verfügung. ■ Der Authentifizierungstyp WPA Pre-Shared Key legt den Pre-Shared Key (PSK) oder die Passphrase fest, die beim Zugreifen auf eine Wireless-Verbindung eingegeben werden muss. Für den PSK können Sie einen HEX- oder ASCII-Wert eingeben. Für einen HEX PSK muss ein 256-Bit-HEX-Wert (64 Textzeichen) eingegeben werden. Eine ASCII-Passphrase muss zwischen 8 und 63 Textzeichen enthalten. Als Verschlüsselungstyp für diese Option muss Temporal Key Integrity Protocol (TKIP) oder Advanced Encryption Standard (AES) ausgewählt werden. Wählen Sie alternativ Auto aus, um beide Optionen zuzulassen. ■ WPA2 Pre-Shared Key. ■ WPA Auto Pre-Shared Key
Interface IP	Legt die IP-Adresse für die WLAN-Schnittstelle fest.
Netmask	Legt die Netzmaske für die WLAN-Schnittstelle fest.

14. Fenster für die Schnittstellenzusammenfassung

Nach dem Konfigurieren der WAN-Schnittstellen wird das Fenster für die Schnittstellenzusammenfassung angezeigt.

Abbildung 43: Fenster für die Schnittstellenzusammenfassung



Überprüfen Sie die Schnittstellenkonfiguration, und klicken Sie anschließend zum Fortfahren auf **Next**. Das Fenster für die Konfiguration der physischen Ethernet-DHCP-Schnittstelle wird angezeigt.

15. Fenster für die Konfiguration der physischen Ethernet-DHCP-Schnittstelle

Wählen Sie **Yes**, damit das Gerät dem verdrahteten Netzwerk über DHCP IP-Adressen zuweisen kann. Geben Sie den IP-Adressbereich ein, innerhalb dessen Clients im Netzwerk vom Gerät IP-Adressen zugewiesen werden können, und klicken Sie anschließend auf **Next**.

Abbildung 44: Fenster für die Konfiguration der physischen Ethernet-DHCP-Schnittstelle

The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. The main area has a light blue background. The text reads: 'Do you want the Juniper device to dynamically assign IP addresses to your local **wired** hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses.' Below this, there are two radio buttons: 'Yes' and 'No'. The 'No' button is selected. To the right of the 'Yes' button, there are four input fields: 'IP Address Range Start' (192.168.1.33), 'End' (192.168.1.126), 'DNS Server 1 (optional)', and 'DNS Server 2 (optional)'. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

16. Fenster für die Konfiguration der Wireless-DHCP-Schnittstelle

Wählen Sie **Yes**, damit das Gerät dem Wireless-Netzwerk über DHCP IP-Adressen zuweisen kann. Geben Sie den IP-Adressbereich ein, innerhalb dessen Clients im Netzwerk vom Gerät IP-Adressen zugewiesen werden können, und klicken Sie anschließend auf **Next**.

Abbildung 45: Fenster für die Konfiguration der Wireless-DHCP-Schnittstelle

The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. The main area has a light blue background. The text reads: 'Do you want the Juniper device to dynamically assign IP addresses to your local **wireless** hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses.' Below this, there are two radio buttons: 'Yes' and 'No'. The 'No' button is selected. To the right of the 'Yes' button, there are four input fields: 'IP Address Range Start' (192.168.2.33), 'End' (192.168.2.126), 'DNS Server 1 (optional)', and 'DNS Server 2 (optional)'. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

17. Bestätigungsfenster

Bestätigen Sie die Gerätekonfiguration, und nehmen Sie ggf. Änderungen vor. Klicken Sie zum Speichern auf **Next**, starten Sie das Gerät neu, und führen Sie anschließend die Konfiguration aus.

Abbildung 46: Bestätigungsfenster

Initial Configuration Wizard

Before proceeding further, review the following all device settings.

Admin Login:	netscreen		Password:	*****	
Device is in NAT mode.					
ISDN Configuration:					
Switch Type:	etsi		SPID1:	32546564565	SPID2: 23488458235
TEI Negotiation:	first call		Calling Number:	01023456789	
T310 Value:	10		Sending Complete:	enabled	
Leased Line Mode:	disabled		Dialer Enable:	disabled	
PPP Profile:	myprofile		Authentication:	any	

```

set admin password "netscreen"
set interface bri1/0 isdn switch-type etsi
set interface bri1/0 isdn spid1 "32546564565"
set interface bri1/0 isdn spid2 "23488458235"
set interface bri1/0 isdn tei-negotiation first-call
set interface bri1/0 isdn calling-number "01023456789"
  
```

Click Next to save CLI into device.

<< Previous Next >> Cancel

Nach dem Starten mit der gespeicherten Systemkonfiguration wird die WebUI-Anmeldeaufforderung angezeigt. Informationen zum Zugreifen auf das Gerät mithilfe der WebUI finden Sie unter „Verwenden der WebUI“ auf Seite 29.

Index

A

AAL5-Multiplexing	41
ADSL	
Anschluss verbinden	24
Kabel anschließen	24
Schnittstelle konfigurieren	41
Annex A	24
Annex B	24
Antennen	26
ATM Adaptation Layer 5	41

F

Funktransceiver	
WLAN 0	16
WLAN 1	16

I

IP-Adresse und Netzmaske des Internetdienstanbieters (ISP)	44
---	----

K

Kabel	
ADSL	24
Basisnetzwerkverbindungen	23
seriell	24
Konfiguration	
Administratorname und -kennwort	33
Administratorzugriff	35
ADSL 2/2 + -Mini-PIM	41
Bridge-Gruppen (bgroup)	34
Datum und Uhrzeit	34
E1-Mini-PIM	47
Host- und Domänenname	36
ISDN-Mini-PIM	45
Mini-PIM für V.92-Modem	47
Standardroute	36
T1-Mini-PIM	46
Untrust Sicherungsschnittstelle	37
USB	17
Verwaltungsadresse	36
Verwaltungsdienste	35
Virtuelle Verbindungen	42
VPI/VCI-Paar	42
Wireless und Ethernet (kombiniert)	40
Wireless-Authentifizierung und -Verschlüsselung	39

L

LEDs	
Activity Link auf Ethernet-Anschlüssen	13
PIM 1	12
PIM 2	12
POWER	12
STATUS	12

M

Mini-PIM	
Einbau	53
Entfernen	52
Unbeschriftete Frontscheibe	52
Multiplexing, konfigurieren	42

P

Point-to-Point-Protokoll über ATM	
<i>Siehe</i> PPPoA	
Point-to-Point-Protokoll über Ethernet	
<i>Siehe</i> PPPoE	
PPPoA	42
PPPoE	42

R

Reset-Stiftloch, Verwenden	49
----------------------------------	----

S

Sicherungsschnittstelle für die Untrust Zone	37
Standard-IP-Adressen	32
statische IP-Adresse	42

U

Untrust Zone, Konfigurieren einer Sicherungsschnittstelle	37
--	----

V

Verbindung, Basisnetzwerk	23
Verwaltung	
über die WebUI	29
über eine Konsole	28
über eine Telnet-Verbindung	30
Virtuelle Pfad-ID/Virtuelle Kanal-ID	
<i>Siehe</i> VPI/VCI	
Vorgehensweise beim Erweitern des Arbeitsspeichers	54

VPI/VCI	
konfigurieren.....	42
Werte	41

W

Wireless	
Antennen.....	26
Verwenden der Standardschnittstelle	26
WLAN-LEDs	
802.11a.....	12
b/g.....	12

Z

Zertifizierungen	
EMC (Emissionen)	59
EMC-Störfestigkeit	59
European Telecommunications Standards	
Institute (ETSI).....	59
Sicherheit.....	59
T1-Schnittstelle	60

Contenido

Acerca de este manual	5
Organización.....	6
Convenciones de la interfaz gráfica (WebUI)	6
Convenciones CLI	7
Cómo obtener documentación y soporte técnico	8
Capítulo 1 Presentación del hardware	9
Conectores de alimentación y puertos	10
Panel frontal	11
LED de estado del sistema	11
Descripciones de los puertos	13
Puertos ethernet.....	13
Puerto de la consola.....	13
Puerto AUX	14
Descripciones del puerto del módulo de mini interfaz física.....	14
Panel trasero.....	16
Adaptador de alimentación.....	16
Transceptores de radio	16
Terminador de conexión a tierra	17
Tipos de antenas	17
Puerto USB	17
Capítulo 2 Instalación y conexión del dispositivo	19
Antes de empezar	20
Equipo de instalación	20
Conexión de los cables de la interfaz a un dispositivo	22
Conexión de la alimentación.....	22
Conexión de un dispositivo a una red	23
Conexión del dispositivo a una red no fiable	23
Puertos ethernet.....	24
Puertos serie (AUX/consola)	24
Conexión de mini PIM a una red no fiable.....	24
Mini PIM ADSL2/2 +	24
Mini PIM RDSI, T1, E1 y V.92.....	25
Conexión del dispositivo a una red interna o una estación de trabajo.....	25
Puertos Ethernet	26
Antenas inalámbricas.....	26
Capítulo 3 Configuración del dispositivo	27
Acceso al dispositivo	28
Utilización de una conexión de consola	28
Utilización de la WebUI	29

Utilización de Telnet	30
Ajustes predeterminados del dispositivo	31
Configuración básica del dispositivo	33
Contraseña y nombre del administrador raíz.....	33
Fecha y hora.....	34
Interfaces de grupos en puente.....	34
Acceso administrativo	35
Servicios de administración.....	35
Nombre de host y nombre de dominio.....	36
Ruta predeterminada.....	36
Dirección de interfaz de administración	36
Configuración de la interfaz Untrust de respaldo	37
Configuración inalámbrica básica	37
Configuración de mini PIM.....	41
Interfaz ADSL2/2 +	41
Circuitos virtuales.....	42
Método VPI/VCI y multiplexado.....	42
PPPoE o PPPoA.....	43
Dirección IP estática y máscara de red.....	44
Interfaz RDSI	45
Interfaz T1	45
Interfaz E1	46
Interfaz del módem V.92	47
Protecciones básicas del cortafuegos	48
Verificación de la conectividad externa.....	49
Restablecimiento de los ajustes predeterminados de fábrica.....	49
Capítulo 4 Servicio del dispositivo	51
Piezas y herramientas requeridas	51
Reemplazo de un mini módulo de interfaz física	51
Extracción de una placa frontal	52
Extracción de un mini PIM	52
Instalación de un mini PIM.....	53
Actualización de memoria.....	54
Apéndice A Especificaciones	57
Características físicas	58
Características eléctricas	58
Tolerancia ambiental	58
Certificaciones	59
Seguridad	59
Emisiones EMC.....	59
Inmunidad EMC.....	59
ETSI.....	59
Interfaz T1	60
Conectores.....	60
Apéndice B Asistente de configuración inicial	63
Índice	87

Acerca de este manual

El dispositivo de la puerta de enlace de servicios seguros (SSG) 20 de Juniper Networks es una plataforma de cortafuegos y enrutador integrada que proporciona una red privada virtual (VPN) de seguridad de protocolo de Internet (IPSec) y servicios de cortafuegos para una sucursal o establecimiento minorista.

Juniper Networks ofrece dos modelos del dispositivo SSG 20:

- SSG 20, que admite conectividad auxiliar (AUX)
- SSG 20-WLAN, que admite normas inalámbricas 802.11 a/b/g integradas

Ambos dispositivos SSG 20 admiten almacenamiento de bus serie universal (USB) y dos ranuras de módulo de mini interfaz física (PIM) que soportan cualquiera de los PIM. Los dispositivos también proporcionan conversiones de protocolo entre redes de área local (LAN) y redes de área extensa (WAN).

NOTA: Los ejemplos e instrucciones de configuración incluidos en este documento se basan en la funcionalidad de un dispositivo que ejecuta ScreenOS 5.4. Es posible que su dispositivo funcione diferente dependiendo de la versión de ScreenOS instalada. Para obtener la última documentación del dispositivo, consulte el sitio Web de publicaciones técnicas de Juniper Networks en <http://www.juniper.net/techpubs/hardware>. Para ver cuáles versiones de ScreenOS están disponibles actualmente para su dispositivo, consulte el sitio Web de soporte de Juniper Networks en <http://www.juniper.net/customers/support/>.

Organización

Este manual contiene las siguientes secciones:

- El capítulo 1, “Presentación del hardware,” describe el chasis y componentes de un dispositivo SSG 20.
- El capítulo 2 “Instalación y conexión del dispositivo,” describe cómo instalar un dispositivo SSG 20 y conectar los cables y alimentación al dispositivo.
- El capítulo 3 “Configuración del dispositivo,” describe cómo configurar y administrar un dispositivo SSG 20 y cómo realizar algunas tareas de configuración básica.
- El capítulo 4 “Servicio del dispositivo,” describe los procedimientos de servicio y mantenimiento para el dispositivo SSG 20.
- El apéndice A “Especificaciones,” proporciona especificaciones generales del sistema para el dispositivo SSG 20.
- El apéndice B “Asistente de configuración inicial,” proporciona información detallada sobre cómo utilizar el asistente de configuración inicial (ICW) en un dispositivo SSG 20.

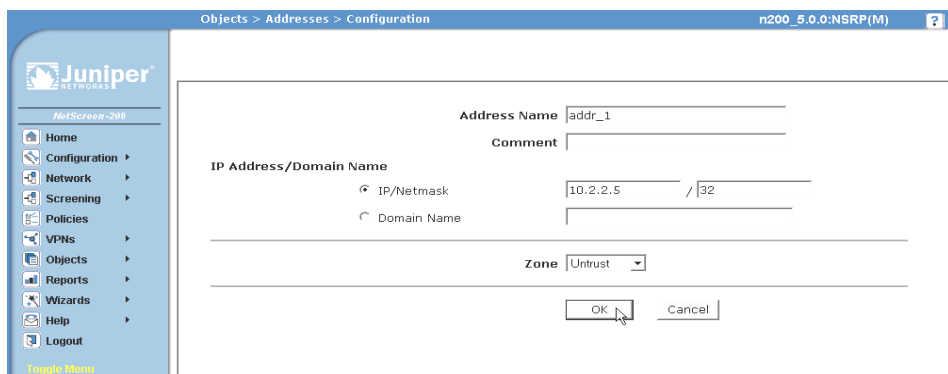
Convenciones de la interfaz gráfica (WebUI)

Para llevar a cabo una tarea en la WebUI, en primer lugar debe navegar al cuadro de diálogo apropiado, donde podrá definir objetos y establecer parámetros. Una comilla angular (>) muestra la secuencia de navegación a través de WebUI, a la que puede llegar mediante un clic en las opciones de menú y vínculos. El conjunto de instrucciones de cada tarea se divide en ruta de navegación y ajustes de configuración.

La siguiente figura muestra la ruta al cuadro de diálogo de configuración de direcciones con los siguientes ajustes de configuración de muestra:

Objects > Addresses > List > New: Introduzca los siguientes datos y luego haga clic en **OK**:

Address Name: addr_1
IP Address/Domain Name:
 IP/Netmask: (seleccione), 10.2.2.5/32
Zone: Untrust

Figura 1: Ruta de navegación y ajustes de configuración

Convenciones CLI

Las siguientes convenciones se utilizan para presentar la sintaxis de los comandos CLI en ejemplos y dentro del texto.

En ejemplos:

- Los elementos entre corchetes [] son opcionales.
- Los elementos entre llaves { } son obligatorios.
- Si existen dos o más opciones, 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*:

```
set admin user nombre1 password xyz
```

En texto:

- Los comandos aparecen en **negrita**.
- Las variables aparecen en *cursiva*.

NOTA: Para introducir palabras clave, debe introducir los primeros caracteres para identificar la palabra de forma inequívoca. Por ejemplo, es suficiente introducir **set admin user kathleen j12fmt54** para que el sistema reconozca el comando **set admin user kathleen j12fmt54**. Aunque este método se puede utilizar para introducir comandos, en la presente documentación todos ellos se presentan en su forma original.

Cómo obtener documentación y soporte técnico

Para obtener documentación técnica sobre cualquier producto 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 este documento, póngase en contacto con nosotros a través de la siguiente dirección de correo electrónico:

techpubs-comments@juniper.net

Capítulo 1

Presentación del hardware

En este capítulo se describe de forma detallada el chasis SSG 20 y sus componentes. Incluye las siguientes secciones:

- “Conectores de alimentación y puertos” en la página 10
- “Panel frontal” en la página 11
- “Panel trasero” en la página 16

Conectores de alimentación y puertos

Esta sección describe e indica la ubicación de los conectores de alimentación y puertos incorporados. Consulte la siguiente figura para obtener la información de ubicaciones de puertos incorporados y la Tabla 1 para obtener las descripciones de los conectores de alimentación.

Figura 2: Puerto incorporado y ubicación de los mini PIM

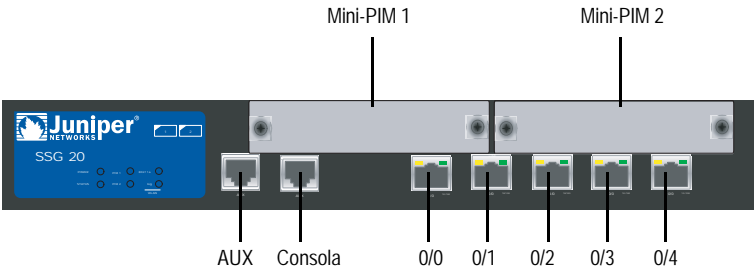


Tabla 1: Conectores de alimentación y puertos SSG 20

Puerto	Descripción	Conector	Velocidad/protocolo
0/0-0/4	Permite conectar directamente estaciones de trabajo o una LAN a través de un conmutador o concentrador. Esta conexión también permite manejar el dispositivo a través de una sesión Telnet o de la WebUI.	RJ-45	Ethernet 10/100 Mbps Detección automática de dúplex y auto MDI/MDIX
USB	Permite la conexión 1.1 USB con el sistema.	N/A	12M (velocidad completa) ó 1.5M (velocidad baja)
Consola	Permite la conexión serie con el sistema. Utilizada en la conectividad de emulación de terminal para ejecutar sesiones de CLI.	RJ-45	Serie 9600 bps/RS-232C
AUX	Permite una conexión a Internet serie asíncrona RS-232 de respaldo a través de un módem externo.	RJ-45	Serie 9600 bps — 115 Kbps/RS-232C
Mini PIM			
ADSL 2/2 +	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 (solamente Anexo A) ITU G.992.1 (G.dmt) ITU G.992.3 (ADSL2) ITU G.992.5 (ADSL2 +)
Módem V.92	Permite una conexión de red no fiable o Internet de respaldo o principal con un proveedor de servicio	RJ-11	Detección automática de polaridad y dúplex serie 9600 bps — 115 Kbps/RS-232
T1	Habilita una conexión a la línea T1 de la red no fiable.	RJ-45	1,544 Mbps (intervalos de tiempo completo)
E1	Habilita una conexión a la línea E1 de la red no fiable.	RJ-45	2,048 Mbps (intervalos de tiempo completo)

Puerto	Descripción	Conector	Velocidad/protocolo
RDSI	Permite el uso de la línea RDSI como interfaz untrust o de respaldo. (S/T)	RJ-45	Canales B a 64 Kbps Línea arrendada a 128 Kbps
Antena A y B (SSG 20-WLAN)	Permite conectar directamente estaciones de trabajo próximas a una conexión de radio inalámbrica.	RPSMA	802.11 a (54 Mbps en una banda de radio de 5 GHz) 802.11 b (11 Mbps en una banda de radio de 2,4 GHz) 802.11 g (54 Mbps en una banda de radio de 2,4 GHz) 802.11 superG (108 Mbps en bandas de radio de 2,4 GHz y 5 GHz)

Panel frontal

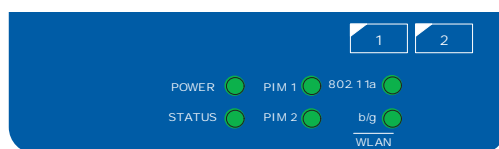
Esta sección describe los siguientes elementos en el panel frontal de un dispositivo SSG 20:

- LED de estado del sistema
- Descripciones de los puertos
- Descripciones del puerto del módulo de mini interfaz física

LED de estado del sistema

Los LED de estado del sistema muestran información sobre funciones fundamentales del dispositivo. La Figura 3 ilustra la posición de cada LED de estado en la parte delantera del dispositivo SSG 20-WLAN. Los LED de WLAN solamente están presentes en el dispositivo SSG 20-WLAN.

Figura 3: LED de estado



Cuando el sistema se enciende, el LED POWER cambia de apagado a verde intermitente y el LED STATUS cambia en la siguiente secuencia: Rojo, verde, verde intermitente. El arranque toma aproximadamente dos minutos para completarse. Si desea apagar y encender el sistema de nuevo, le recomendamos que espere unos segundos mientras lo apaga y lo vuelve a encender. La Tabla 2 proporciona el nombre, color, estado y descripción de cada LED de estado del sistema.

Tabla 2: Descripciones de LED de estado

Nombre	Color	Estado	Descripción
POWER (alimentación)	Verde	Encendido sin parpadear	Indica que el sistema recibe alimentación.
		Apagado	Indica que el sistema no está recibiendo alimentación.
	Rojo	Encendido sin parpadear	Indica que el dispositivo no está funcionando normalmente.
		Apagado	Indica que el dispositivo está funcionando normalmente.
STATUS (estado)	Verde	Encendido sin parpadear	Indica que el sistema está arrancando o realizando diagnósticos.
		Parpadeo	Indica que el dispositivo está funcionando normalmente.
	Rojo	Parpadeo	Indica que se detectó un error.
PIM 1	Verde	Encendido sin parpadear	Indica que el mini PIM está funcionando.
		Parpadeo	Indica que el mini PIM está pasando tráfico.
		Apagado	Indica que el mini PIM no está funcionando.
PIM 2	Verde	Encendido sin parpadear	Indica que el mini PIM está funcionando.
		Parpadeo	Indica que el mini PIM está pasando tráfico.
		Apagado	Indica que el mini PIM no está funcionando.
WLAN (solamente en el dispositivo WLAN)			
802.11a	Verde	Encendido sin parpadear	Indica que se ha establecido una conexión inalámbrica pero no hay actividad de conexión.
		Parpadeo lento	Indica que se ha establecido una conexión inalámbrica. La velocidad de transmisión es proporcional a la actividad de la conexión.
		Apagado	Indica que no se ha establecido una conexión inalámbrica.
b/g	Verde	Encendido sin parpadear	Indica que se ha establecido una conexión inalámbrica pero no hay actividad de conexión.
		Parpadeo lento	Indica que se ha establecido una conexión inalámbrica. La velocidad de transmisión es proporcional a la actividad de la conexión.
		Apagado	Indica que no se ha establecido una conexión inalámbrica.

Descripciones de los puertos

En esta sección se explica el propósito y función de los siguientes puertos:

- Puertos ethernet
- Puerto de la consola
- Puerto AUX

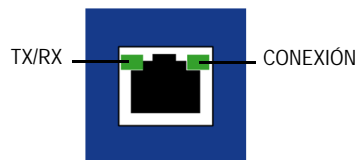
Puertos ethernet

Cinco puertos de Ethernet 10/100 proporcionan conexiones LAN a concentradores, conmutadores, servidores locales y estaciones de trabajo. También puede designar un puerto Ethernet para el tráfico administrativo. Los puertos están etiquetados **0/0** a **0/4**. Consulte, “Ajustes predeterminados del dispositivo” en la página 31 para obtener los enlaces de zona predeterminados para cada puerto Ethernet.

Al configurar uno de los puertos, haga referencia al nombre de interfaz que corresponde a la ubicación del puerto. De izquierda a derecha en el panel frontal, los nombres de interfaz de los puertos son **ethernet0/0** a **ethernet0/4**.

La Figura 4 muestra la ubicación de los LED en cada puerto Ethernet.

Figura 4: Ubicación de los LED de actividad de conexión



La Tabla 3 describe los LED del puerto Ethernet.

Tabla 3: LED del puerto LAN

Nombre	Color	Estado	Descripción
CONEXIÓN	Verde	Encendido sin parpadear Apagado	El puerto está en línea. El puerto está fuera de línea.
TX/RX	Verde	Parpadeo Apagado	El tráfico está pasando. La velocidad de transmisión es proporcional a la actividad de la conexión. El puerto podría estar encendido, pero no recibe datos.

Puerto de la consola

El puerto de la consola es un puerto serie RJ-45 cableado como equipo de terminación de circuitos de datos (DCE) que se puede utilizar para la administración local. Utilícelo como un cable directo al utilizar una conexión de terminal y un cable de conexión directa al conectarse a otro dispositivo DCE. Se proporciona un adaptador RJ-45 a DB-9.

Consulte “Conectores” en la página 60 para obtener información sobre las patillas de salida del conector RJ-45.

Puerto AUX

El puerto auxiliar (AUX) es un puerto serie RJ-45 cableado como equipo de terminal de datos (DTE) que se puede conectar a un módem para permitir una administración remota. No recomendamos el uso de este puerto para una administración remota regular. El puerto AUX está asignado típicamente como una interfaz serie de respaldo. La velocidad de transmisión es ajustable de 9600 bps a 115200 bps y requiere control de flujo de hardware. Utilícelo como un cable directo al conectar a un módem y cable de conexión directa al conectarse a otro dispositivo DTE.






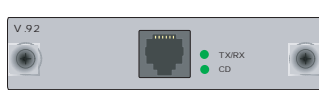
Consulte “Conectores” en la página 60 para obtener información sobre las patillas de salida del conector RJ-45.

Descripciones del puerto del módulo de mini interfaz física

Cada módulo de mini interfaz física (PIM) admitido en un dispositivo tiene los siguientes componentes:

- Puerto de conector de un cable, acepta un conector de medios de red. La Figura 5 muestra los mini PIM disponibles. Puede instalar hasta dos mini PIM en un dispositivo.

Figura 5: Mini PIM para el SSG 20

	ADSL2/2+ Annex B
	ADSL2/2+ Annex A
	ISDN BRI
	T1
	E1
	V.92

- Dos o tres LED de estado, indican el estado del puerto. La Tabla 4 describe el significado de los estados de LED.

Tabla 4: Estados del LED de PIM en el SSG 20

Tipo	Nombre	Color	Estado	Descripción
ADSL 2/2 + (anexo A y B)	SYNC	Verde	Encendido sin parpadear	Indica que la interfaz ADSL está capacitada
			Parpadeo	Indica que la capacitación está en progreso
			Apagado	Indica que la interfaz está inactiva
	TX/RX	Verde	Parpadeo	Indica que el tráfico está pasando.
			Apagado	Indica que el tráfico no está pasando.
ISDN (BRI)	CH B1	Verde	Encendido sin parpadear	Indica que el canal B 1 está activo
			Apagado	Indica que el canal B 1 no está activo
	CH B2	Verde	Encendido sin parpadear	Indica que el canal B 2 está activo
			Apagado	Indica que el canal B 2 no está activo
T1/E1	ALARM	Amarillo	Encendido sin parpadear	Indica que hay una alarma remota o local; el dispositivo detectó un fallo
			Apagado	Indica que no hay alarmas o fallas
	LOOP BACK	Amarillo	Encendido sin parpadear	Indica que se detectó un estado de línea o bucle invertido
			Apagado	Indica que el bucle invertido no está activo.
	CD	Verde	Encendido sin parpadear	Indica que se detectó una portadora y el DSU/CSU interno en el mini PIM se está comunicando con otro DSU/CSU
			Apagado	Indica que la portadora no está activa.
V.92	CD	Verde	Encendido sin parpadear	Indica que la conexión está activa.
			Apagado	Indica que la interfaz serie no está en servicio
	TX/RX	Verde	Parpadeo	Indica que el tráfico está pasando.
			Apagado	Indica que el tráfico no está pasando.



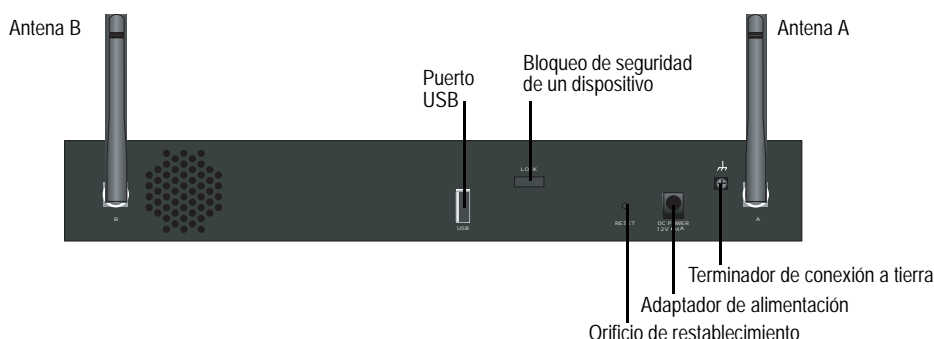
PRECAUCIÓN: Mini PIM que no se pueden intercambiar cuando están activos. Debe instalarlos en las ranuras del panel frontal antes de encender el dispositivo.

Panel trasero

Esta sección describe los siguientes elementos en el panel trasero de un dispositivo SSG 20:

- Adaptador de alimentación
- Transceptores de radio
- Terminador de conexión a tierra
- Tipos de antenas
- Puerto USB

Figura 6: Panel trasero de un dispositivo SSG 20-WLAN



Adaptador de alimentación

El LED POWER que se encuentra en el panel frontal de un dispositivo se enciende en verde o está apagado. Verde indica una función correcta y apagado indica un fallo del adaptador de alimentación o que el dispositivo está apagado.

Transceptores de radio

El SSG 20-WLAN contiene dos transceptores de radio de conectividad inalámbrica, que admiten las normas 802.11a/b/g. El primer transceptor (WLAN 0) utiliza la banda de radio 2,4 GHz, que admite la norma 802.11b a 11 Mbps y la norma 802.11g a 54 Mbps y la norma SuperG 802.11 a 108 Mbps. El segundo transceptor de radio (WLAN 1) utiliza una banda de radio de 5 GHz que admite la norma 802.11a a 54 Mbps. Para obtener más información sobre la configuración de la banda de radio inalámbrica, consulte “Configuración inalámbrica básica” en la página 37.

Terminador de conexión a tierra

Un terminador de conexión a tierra de un agujero se proporciona en la parte trasera del chasis para conectar el dispositivo a tierra (consulte la Figura 6).

Para conectar a tierra el dispositivo antes de conectar la alimentación, conecte un cable de conexión a tierra a tierra y después conecte el cable al terminador en la parte trasera del chasis.

Tipos de antenas

El dispositivo SSG 20-WLAN admite tres tipos de antenas de radio fabricadas de acuerdo con las especificaciones del cliente.

- **Antenas de diversidad:** Las antenas de diversidad proporcionan una cobertura direccional 2dBi y un nivel bastante uniforme de fuerza de la señal dentro del área de cobertura y son adecuadas para la mayoría de instalaciones. Este tipo de antenas se envía con el dispositivo.
- **Antena omnidireccional externa:** Las antenas externas proporcionan 2dBi de cobertura omnidireccional. A diferencia de las antenas de diversidad, que funcionan como un par, una antena externa funciona para eliminar un efecto de eco que puede ocurrir algunas veces por causa de características de un leve retardo en la recepción de la señal cuando hay dos en uso.
- **Antena direccional externa:** La antena direccional externa proporciona cobertura unidireccional 2dBi y es apropiada para ubicaciones como corredores o paredes exteriores (con la antena orientada hacia adentro).

Puerto USB

El puerto USB que se encuentra en el panel trasero de un dispositivo SSG 20 acepta un dispositivo de almacenamiento de bus serie universal (USB) o un adaptador de dispositivo de almacenamiento USB con un disco flash compacto instalado, como se define en la *Especificación de CompactFlash* publicada por la Asociación CompactFlash. Cuando el dispositivo de almacenamiento USB está instalado y configurado, éste automáticamente actúa como un dispositivo de inicio secundario si el disco flash compacto principal falla al arranque.

El puerto USB permite transferencias de archivos como configuraciones de dispositivo, certificaciones de usuario e imágenes de versión de actualización entre un dispositivo de almacenamiento USB externo y el almacenamiento flash interno ubicado en el dispositivo de seguridad. El puerto USB admite la especificación USB 1.1 en cualquier transferencia de archivos de velocidad baja (1,5 M) o velocidad completa (12 M).

Para transferir archivos entre el dispositivo de almacenamiento USB y un SSG 20, realice los siguientes pasos:

1. Inserte el dispositivo de almacenamiento USB en el puerto USB del dispositivo de seguridad.
2. Guarde los archivos del dispositivo de almacenamiento USB en el almacenamiento flash interno por medio del comando CLI **save {software | config | image-key} from usb nombearchivo to flash**.
3. Antes de retirar el dispositivo de almacenamiento USB, detenga el puerto USB con el comando CLI **exec usb-device stop**.
4. Ahora es seguro retirar el dispositivo de almacenamiento USB.

Si desea borrar un archivo del dispositivo de almacenamiento USB, utilice el comando CLI **delete file usb:/nombearchivo**.

Si desea ver la información de archivos guardados en el dispositivo de almacenamiento USB o en el almacenamiento flash interno, utilice el comando de CLI **get file**.

Capítulo 2

Instalación y conexión del dispositivo

Este capítulo describe cómo instalar un dispositivo SSG 20 y conectar los cables y alimentación al dispositivo. Este capítulo consta de las siguientes secciones:

- “Antes de empezar” en la página 20
- “Equipo de instalación” en la página 20
- “Conexión de los cables de la interfaz a un dispositivo” en la página 22
- “Conexión de la alimentación” en la página 22
- “Conexión de un dispositivo a una red” en la página 23

NOTA: Para obtener información sobre las advertencias e instrucciones de seguridad, consulte el *Manual de seguridad de productos Juniper Networks*. Antes de utilizar cualquier equipo, debe tener en cuenta los peligros que entraña el sistema de circuitos eléctricos y familiarizarse con las prácticas habituales de prevención de accidentes.

Antes de empezar

La ubicación del chasis, el diseño del equipo de montaje y la seguridad de su sala de cableado son muy importantes para el funcionamiento correcto del sistema.



ADVERTENCIA: Para evitar el abuso e intrusión de personal no autorizado, instale el dispositivo SSG 20 en un entorno seguro.

El cumplimiento de las siguientes precauciones puede evitar apagones, fallos de equipo y lesiones:

- Antes de la instalación, revise siempre que el suministro de alimentación esté desconectado de cualquier fuente de alimentación.
- Asegúrese que la habitación en la que utilizará el dispositivo tenga circulación de aire adecuada y que la temperatura del cuarto no exceda 104°F (40°C).
- No coloque el dispositivo en un soporte para bastidor de equipo que bloquee un puerto de escape o entrada. Asegúrese de que los bastidores tengan ventiladores y lados con rejillas.
- Corrija estas condiciones peligrosas antes de realizar cualquier instalación: Pisos húmedos o mojados, fugas, cables eléctricos pelados o sin conexión a tierra o falta de tomas de tierra de seguridad.

Equipo de instalación

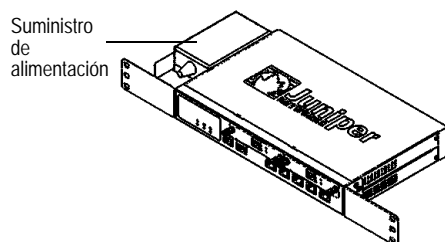
Puede instalar un dispositivo SSG 20 en un bastidor, en una pared o en un escritorio. Los kits de montaje se pueden comprar por separado.

Para instalar un dispositivo SSG 20, necesita un destornillador phillips número 2 (no incluido) y tornillos que sean compatibles con el bastidor del equipo (incluidos en el kit)

NOTA: Al instalar un dispositivo, asegúrese que esté dentro del alcance de una toma de corriente.

Para instalar un dispositivo SSG 20 en un bastidor de equipo estándar de 19 pulgadas, realice los siguientes pasos:

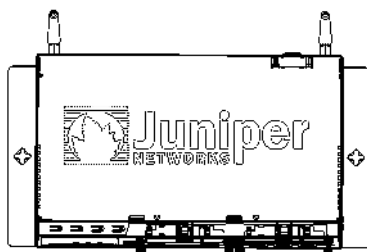
Figura 7: Instalación del SSG 20 en bastidor



1. Alinee la lengüeta de instalación en el bastidor de suministro de alimentación con el borde frontal izquierdo del dispositivo.
2. Coloque los tornillos en los agujeros y utilice un destornillador phillips para asegurarlos.
3. Alinee la otra lengüeta de instalación en el bastidor con el borde frontal derecho del dispositivo.
4. Coloque los tornillos en los agujeros y utilice un destornillador phillips para asegurarlos.
5. Instale el dispositivo en el bastidor con los tornillos que se proporcionan.
6. Conecte el suministro de alimentación en la toma de corriente.

Para instalar un dispositivo SSG 20 en una pared, realice los siguientes pasos:

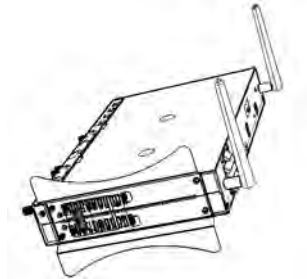
Figura 8: Instalación del SSG 20 en una pared



1. Alinee las lengüetas para instalación en una pared con el dispositivo.
2. Coloque los tornillos en los agujeros y utilice un destornillador phillips para asegurarlos.
3. Asegúrese que la pared que utilizará sea lisa, plana, seca y sólida.
4. Instale el dispositivo en la pared con los tornillos que se proporcionan.
5. Conecte el suministro de alimentación en la toma de corriente.

Para instalar un dispositivo SSG 20 en un escritorio, realice los siguientes pasos:

Figura 9: Instalación del SSG 20 en un escritorio



1. Fije el soporte para escritorio en un lateral del dispositivo. Recomendamos utilizar el lateral más cercano al adaptador de alimentación.
2. Una vez montado el dispositivo, colóquelo en el escritorio.
3. Enchufe el adaptador de alimentación y conecte la fuente de alimentación a la toma de corriente.

Conexión de los cables de la interfaz a un dispositivo

Para conectar el cable de la interfaz al dispositivo, realice los siguientes pasos:

1. Tenga listo un trozo de cable de la longitud necesaria y del tipo adecuado para la interfaz.
2. Inserte el conector del cable en el puerto correspondiente en la placa frontal de la interfaz.
3. Coloque el cable de la siguiente manera para evitar que se desprenda o se desarrollen puntos de tensión:
 - a. Asegure el cable de manera que no sostenga su propio peso mientras cuelga hacia el suelo.
 - b. Quite de enmedio el cable sobrante en un bucle bien enrollado.
 - c. Utilice bridas para mantener la forma de los bucles de cable.

Conexión de la alimentación

Para conectar la alimentación al dispositivo, realice los siguientes pasos:

1. Enchufe el extremo del conector de CC del cable de alimentación al receptáculo de alimentación CC en la parte posterior del dispositivo.
2. Conecte el extremo del adaptador de CA del cable de alimentación a la fuente de alimentación de CA.



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

Conexión de un dispositivo a una red

Un dispositivo SSG 20 proporciona protección de cortafuegos y seguridad general para las redes cuando se coloca entre las redes internas y la red no fiable. En esta sección se describe lo siguiente:

- Conexión del dispositivo a una red no fiable
- Conexión del dispositivo a una red interna o una estación de trabajo

Conexión del dispositivo a una red no fiable

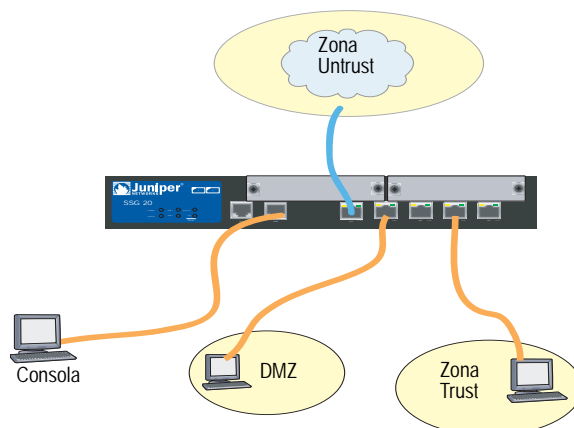
Puede conectar su dispositivo SSG 20 a una red no fiable de una de las siguientes maneras:

- Puertos ethernet
- Puertos serie (AUX/consola)
- Conexión de mini PIM a una red no fiable

La Figura 10 muestra el SSG 20 con conexiones de cableado de red básica con dos puertos de Ethernet 10/100 y mini PIM en blanco cableados de la siguiente manera:

- El puerto etiquetado 0/0 (interfaz ethernet 0/0) está conectado a la red no fiable.
- El puerto etiquetado 0/1 (interfaz ethernet 0/1) está conectado a una estación de trabajo en la zona de seguridad DMZ.
- El puerto etiquetado 0/3 (interfaz bgrou0) está conectado a una estación de trabajo en la zona de seguridad Trust.
- El puerto de la consola está conectado a una terminal serie para el acceso de administración.

Figura 10: Ejemplo de un sistema de redes básico



Puertos ethernet

Para establecer una conexión de alta velocidad, conecte el cable Ethernet que se proporciona del puerto Ethernet marcado 0/0 en el dispositivo SSG 20 al enrutador externo. El dispositivo detecta automáticamente los ajustes de velocidad, dúplex y MDI/MDIX correctas.

Puertos serie (AUX/consola)

Puede conectarse a la red no fiable con un cable de serie directo RJ-45 y un módem externo.



ADVERTENCIA: Asegúrese de no conectar por error los puertos de la consola, AUX o Ethernet del dispositivo a la toma de teléfono.

Conexión de mini PIM a una red no fiable

Esta sección explica la manera en que debe conectar los mini PIM a una red no fiable.

Mini PIM ADSL2/2+

Conecte el cable ADSL que se proporciona desde el mini PIM ADSL2/2+ hasta 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.

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 como parte del equipo que conecta las líneas telefónicas del lugar a la red del proveedor.

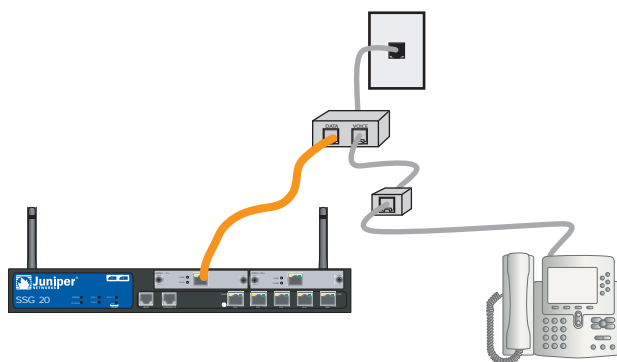
Hay separadores que los usuarios pueden instalar por sí mismos, según los equipos de los proveedores del servicio. Si instala un separador de este tipo por sí mismo,

conecte el cable ADSL desde el dispositivo 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 realiza un filtrado por ruidos de alta frecuencia en la línea telefónica. Instale el microfiltro en la línea telefónica entre el teléfono, el fax, contestador automático o módem analógico y el conector de voz del separador.

La Figura 11 muestra un ejemplo de instalación de un microfiltro y un separador. El proveedor de telefonía debe proporcionarle los microfiltros o separadores adecuados.

Figura 11: Microfiltro y separador en su conexión de red



Mini PIM RDSI, T1, E1 y V.92

Para conectar los mini PIM al dispositivo, realice los siguientes pasos:

1. Tenga listo un trozo de cable de la longitud necesaria y del tipo adecuado para la interfaz.
2. Inserte el conector del cable en el puerto correspondiente en la placa frontal de la interfaz.
3. Coloque el cable de la siguiente manera para evitar que se desprenda o se desarrollen puntos de tensión:
 - a. Asegure el cable de manera que no sostenga su propio peso mientras cuelga hacia el suelo.
 - b. Quite de enmedio el cable sobrante en un bucle bien enrollado.
 - c. Utilice bridas para mantener la forma de los bucles de cable.

Para configurar los mini PIM RDSI, E1, T1 o V.92, consulte “Configuración de mini PIM” en la página 41.

Conexión del dispositivo a una red interna o una estación de trabajo

Puede conectar su red de área local (LAN) o estación de trabajo con las interfaces Ethernet o inalámbrica.

Puertos Ethernet

Un dispositivo SSG 20 contiene cinco puertos Ethernet. 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 o un concentrador. Puede utilizar cables cruzados o directos para conectar los puertos Ethernet a otros dispositivos. Consulte “Ajustes predeterminados del dispositivo” en la página 31 para obtener los enlaces de zona a interfaz predeterminados.

Antenas inalámbricas

Si utiliza la interfaz inalámbrica, deberá conectar las antenas proporcionadas con el dispositivo. Si dispone de las antenas de diversidad 2dB estándar, utilice tornillos para sujetarlas a los postes marcados A y B en la parte posterior del dispositivo. Doble cada antena por su parte curva, teniendo cuidado de no ejercer presión sobre los conectores de mamparo.

Figura 12: Ubicación de las antenas SSG 20-WLAN



Si está utilizando la antena externa opcional, siga las instrucciones de conexión incluidas con esa antena.

Capítulo 3

Configuración del dispositivo

El software de ScreenOS viene ya instalado en el dispositivo SSG 20. Cuando el dispositivo se enciende, está ya listo para configurarse. Si bien el dispositivo tiene una configuración de fábrica predeterminada que permite su conexión inicial, es necesario configurar otros ajustes para cumplir con los requisitos específicos de su red.

Este capítulo consta de las siguientes secciones:

- “Acceso al dispositivo” en la página 28
- “Ajustes predeterminados del dispositivo” en la página 31
- “Configuración básica del dispositivo” en la página 33
- “Configuración inalámbrica básica” en la página 37
- “Configuración de mini PIM” en la página 41
- “Protecciones básicas del cortafuegos” en la página 48
- “Verificación de la conectividad externa” en la página 49
- “Restablecimiento de los ajustes predeterminados de fábrica” en la página 49

NOTA: Después que configure un dispositivo y verifique la conectividad a través de la red remota, deberá registrar su producto en www.juniper.net/support/ para que en el dispositivo se puedan activar determinados servicios de ScreenOS, tales como servicio de inspección detallada de firmas y antivirus (se adquieren por separado). Después de registrar el producto, utilice la WebUI para obtener la suscripción al servicio. Para obtener más información acerca del registro de su producto y obtención de las suscripciones para los servicios específicos, consulte el volumen *Fundamentos del Manual de referencia de ScreenOS: Conceptos y ejemplos* para la versión de ScreenOS que se ejecuta en el dispositivo.

Acceso al dispositivo

Puede configurar y administrar el dispositivo de diversas formas:

- **Consola:** El puerto de consola del dispositivo le permite acceder al dispositivo a través de un cable serie conectado a su estación de trabajo o terminal. Para configurar el dispositivo, debe introducir los comandos de la interfaz de línea de comandos (CLI) de ScreenOS en su terminal o en un programa de emulación de terminal en la estación de trabajo.
- **WebUI:** La interfaz del usuario Web (WebUI) de ScreenOS es una interfaz gráfica que está disponible a través de un explorador. Para utilizar inicialmente la WebUI, la estación de trabajo donde usa el explorador debe estar en la misma subred que el dispositivo. También puede obtener acceso a WebUI a través de un servidor seguro utilizando el nivel de sockets seguro (SSL) con HTTP seguro (S-HTTP).
- **Telnet/SSH:** Telnet y SSH son aplicaciones que le permiten acceder a dispositivos a través de una red IP. Para configurar el dispositivo, introduzca los comandos de la CLI de ScreenOS en una sesión Telnet desde la estación de trabajo. Para obtener más información, consulte el volumen *Administración del Manual de referencia de ScreenOS: Conceptos y ejemplos*.
- **NetScreen-Security Manager:** NetScreen-Security Manager es una aplicación de administración a nivel corporativo de Juniper Networks que le permite controlar y administrar el cortafuegos de Juniper Networks/dispositivos VPN IPSec. Para obtener las instrucciones sobre la manera de administrar su dispositivo con NetScreen-Security Manager, consulte el *Manual del administrador de NetScreen-Security Manager*.

Utilización de una conexión de consola

NOTA: Utilice un cable serie directo RJ-45 CAT5 con un conector macho RJ-45 para conectarlo al puerto de la consola del dispositivo.

Para establecer una conexión de consola, realice los siguientes pasos:

1. Inserte el conector hembra del adaptador DB-9 proporcionado en el puerto serie de su estación de trabajo. (Asegúrese de que el DB-9 esté debidamente colocado y fijo.) La Figura 13 muestra el tipo de conector DB-9 que se requiere.

Figura 13: Adaptador DB-9

2. Conecte el conector macho del cable serie RJ-45 CAT5 en el puerto de la consola del SSG 20. (Asegúrese de que el otro extremo del cable CAT5 esté debidamente colocado y fijo al adaptador DB-9.)
3. Inicie un programa de emulación de terminal serie en su estación de trabajo. Los ajustes requeridos para iniciar una sesión de consola son los siguientes:
 - Velocidad de transferencia: 9600
 - Paridad: Ninguna
 - Bits de datos: 8
 - Bit de parada: 1
 - Control de flujo: Ninguno
4. Si todavía no ha modificado el inicio de sesión predeterminado para el nombre de administrador y la contraseña, escriba **netscreen** en los campos login y password. (Utilice sólo letras en minúscula. Los campos login y password distinguen entre mayúsculas y minúsculas).

Para obtener información sobre la manera de configurar el dispositivo con los comandos CLI, consulte el *Manual de referencia de ScreenOS: Conceptos y ejemplos*.
5. (Opcional) De forma predeterminada, el tiempo de espera de la consola vence y se termina automáticamente después de 10 minutos de tiempo de inactividad. Para eliminar el tiempo de espera, introduzca **set console timeout 0**.

Utilización de la WebUI

Para utilizar la WebUI, la estación de trabajo desde donde maneja el dispositivo debe estar en la misma subred que el dispositivo inicialmente. Para acceder al dispositivo con la WebUI, lleve a cabo los pasos siguientes:

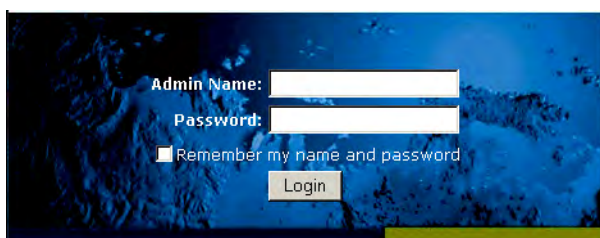
1. Conecte su estación de trabajo al puerto 0/2 — 0/4 (interfaz bgroup0 en la zona Trust) del dispositivo.
2. Asegúrese de que su estación de trabajo esté configurada para el protocolo de configuración dinámica de host (DHCP) o configurada estáticamente con una dirección IP en la subred 192.168.1.0/24.

3. Inicie el explorador, introduzca la dirección IP de la interfaz bgrou0 (la dirección IP predeterminada es 192.168.1.1/24), luego presione **Enter**.

NOTA: Cuando accede por primera vez al dispositivo a través de la WebUI, aparece el asistente de configuración inicial (ICW). Si decide utilizar el ICW para configurar su dispositivo, consulte “Asistente de configuración inicial” en la página 63.

La aplicación de WebUI muestra el mensaje de solicitud de inicio de sesión como aparece en la Figura 14.

Figura 14: Mensaje de solicitud de inicio de sesión de WebUI



4. Si todavía no ha modificado el inicio de sesión predeterminado para el nombre de administrador y la contraseña, escriba **netscreen** en los campos admin name y password. (Utilice sólo letras en minúscula. Los campos login y password distinguen entre mayúsculas y minúsculas).

Utilización de Telnet

Para establecer una conexión de Telnet, realice los siguientes pasos:

1. Conecte su estación de trabajo al puerto 0/2 — 0/4 (interfaz bgrou0 en la zona Trust) del dispositivo.
2. Asegúrese de que su estación de trabajo esté configurada para DHCP o configurada estáticamente con una dirección IP en la subred 192.168.1.0/24.
3. Inicie una aplicación de cliente Telnet en la dirección IP para la interfaz bgrou0 (la dirección IP predeterminada es 192.168.1.1). Por ejemplo, introduzca **telnet 192.168.1.1**.

La aplicación Telnet muestra el mensaje de solicitud de inicio de sesión.

4. Si todavía no ha modificado el inicio de sesión predeterminado para el inicio de sesión y la contraseña, escriba **netscreen** en los campos login y password. (Utilice sólo letras en minúscula. Los campos login y password distinguen entre mayúsculas y minúsculas).
5. (Opcional) De forma predeterminada, el tiempo de espera de la consola vence y se termina automáticamente después de 10 minutos de tiempo de inactividad. Para eliminar el tiempo de espera, introduzca **set console timeout 0**.

Ajustes predeterminados del dispositivo

Esta sección describe los ajustes predeterminados y el funcionamiento de un dispositivo SSG 20.

La Tabla 5 muestra los enlaces de zona predeterminados para los puertos de los dispositivos.

Tabla 5: Interfaz física predeterminada a enlaces de zona

Etiqueta de puerto	Interfaz	Zona
Puertos Ethernet 10/100:		
0/0	ethernet0/0	Untrust
0/1	ethernet0/1	DMZ
0/2	bgroup0 (ethernet0/2)	Trust
0/3	bgroup0 (ethernet0/3)	Trust
0/4	bgroup0 (ethernet0/4)	Trust
AUX	serial0/0	Null
Puertos de mini PIM WAN (x = ranura mini PIM 1 ó 2):		
ADSL2/2 + (anexo A)	adsl(x/0)	Untrust
ADSL2/2 + (anexo B)	adsl(x/0)	Untrust
T1	serial(x/0)	Untrust
E1	serial(x/0)	Untrust
ISDN	bri(x/0)	Untrust
V.92	serial(x/0)	Null

Los grupos puente (bgroup) están diseñados para permitir que los usuarios de la red cambien entre el tráfico inalámbrico y el tráfico con cable sin tener que reconfigurar o reiniciar el dispositivo. De manera predeterminada, las interfaces ethernet0/2 — ethernet0/4, etiquetadas como puertos 0/2 — 0/4 en el dispositivo, están agrupadas juntas como la interfaz bgroup0, tienen la dirección IP 192.168.1.1/24 y están enlazadas a la zona de seguridad Trust. Puede configurar hasta cuatro bgroups.

Si desea configurar una interfaz Ethernet o inalámbrica en un bgroup, primero debe asegurarse de que la interfaz Ethernet o inalámbrica esté en la zona de seguridad Null. Al desactivar la interfaz Ethernet o inalámbrica que está en un bgroup, la interfaz se coloca en la zona de seguridad Null. Una vez asignada a la zona de seguridad Null, la interfaz Ethernet se puede enlazar a una zona de seguridad y asignar a una dirección IP diferente.

Para desactivar ethernet0/3 del bgroup0 y asignarlo a la zona Trust con una dirección IP estática de 192.168.3.1/24, utilice la WebUI o CLI como sigue:

WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port: anule la selección **ethernet0/3**, luego haga clic en **Apply**.

List > Edit (ethernet0/3): Introduzca los siguientes datos, luego haga clic en **Apply**:

Zone Name: Trust (seleccione)
IP Address/Netmask: 192.168.3.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
set interface ethernet0/3 zone trust
set interface ethernet0/3 ip 192.168.3.1/24
save
```

Tabla 6: Enlaces de interfaz inalámbrica y lógica

SSG 20-WLAN	Interfaz	Zona
Interfaz inalámbrica Especifica una interfaz inalámbrica, la cual se puede configurar para que funcione en radio 2,4 G o 5 G	wireless0/0 (la dirección IP predeterminada es 192.168.2.1/24).	Trust
	wireless0/1-0/3.	Null
Interfaces lógicas		
Interfaz de capa 2	vlan1 especifica las interfaces lógicas que se utilizan para la administración y terminación del tráfico VPN mientras el dispositivo está en el modo transparente.	N/A
Interfaces de túnel	tunnel.n especifica una interfaz de túnel lógica. Esta interfaz sirve para el tráfico VPN.	N/A

Puede cambiar la dirección IP predeterminada en la interfaz bgroup0 para que coincida con las direcciones de su red LAN y WLAN. Para realizar la configuración de una interfaz inalámbrica en un bgroup, consulte “Configuración inalámbrica básica” en la página 37.

NOTA: La interfaz de bgroup no funciona en el modo transparente cuando cuenta con una interfaz inalámbrica.

Para obtener información adicional sobre bgroup y algunos ejemplos, consulte el *Manual de referencia de ScreenOS: Conceptos y ejemplos*.

No hay otras direcciones IP predeterminadas, configuradas en otras interfaces Ethernet o inalámbricas en un dispositivo; debe asignar las direcciones IP a las demás interfaces, incluso las interfaces WAN.

Configuración básica del dispositivo

Esta sección describe los siguientes ajustes de configuración básica:

- Contraseña y nombre del administrador raíz
- Fecha y hora
- Interfaces de grupos en puente
- Acceso administrativo
- Servicios de administración
- Nombre de host y nombre de dominio
- Ruta predeterminada
- Dirección de interfaz de administración
- Configuración de la interfaz Untrust de respaldo

Contraseña y nombre del administrador raíz

El usuario administrador raíz posee privilegios completos para la configuración de un dispositivo SSG 20. Le recomendamos que cambie de inmediato el nombre del administrador raíz y contraseña predeterminados (ambos **netscreen**).

Para cambiar el nombre del administrador raíz y la contraseña, utilice WebUI o CLI como se muestra a continuación:

WebUI

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

Administrator Name:
Old Password: netscreen
New Password:
Confirm New Password:

NOTA: Las contraseñas no se muestran en la WebUI.

CLI

```
set admin name nombre
set admin password contraseña
save
```

Fecha y hora

La hora establecida en un dispositivo SSG 20 afecta a los eventos tales como la configuración de los túneles de VPN. La manera más fácil de configurar la fecha y hora en el dispositivo es utilizar la WebUI para sincronizar el reloj del sistema del dispositivo con el reloj de la estación de trabajo.

Para configurar la fecha y hora en un dispositivo, utilice WebUI o CLI como se muestra a continuación:

WebUI

1. Configuration > Date/Time: Haga clic en el botón Sync Clock with Client.

Aparecerá un mensaje emergente solicitándole que especifique si tiene habilitada la opción del horario de verano en el reloj de la estación de trabajo.

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

Interfaces de grupos en puente

De forma predeterminada, el dispositivo SSG 20 tiene agrupadas las interfaces Ethernet ethernet0/2 —ethernet0/4 en la zona de seguridad Trust. Las interfaces agrupadas se establecen en una subred. Puede desactivar una interfaz de un grupo y asignarla a una zona de seguridad diferente. Las interfaces deben estar en la zona de seguridad Null antes que se puedan asignar a un grupo. Para colocar una interfaz agrupada en la zona de seguridad Null, utilice el comando CLI **unset interface interfaz port interfaz**.

Los dispositivos SSG 20-WLAN permiten que las interfaces Ethernet e inalámbricas se agrupen en una subred.

NOTA: Sólo las interfaces inalámbricas y de Ethernet se pueden configurar en un bgroup.

Para configurar un grupo con interfaces Ethernet e inalámbricas, utilice WebUI o CLI como sigue:

WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port: anule la selección **ethernet0/3** y **ethernet0/4**, luego haga clic en **Apply**.

Edit (bgroup1) > Bind Port: seleccione **ethernet0/3**, **ethernet0/4** y **wireless0/2**, luego haga clic en **Apply**.

> Basic: Introduzca los siguientes datos, luego haga clic en **Apply**:

Zone Name: DMZ (seleccione)
IP Address/Netmask: 10.0.0.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
unset interface bgroup0 port ethernet0/4
set interface bgroup1 port ethernet0/3
set interface bgroup1 port ethernet0/4
set interface bgroup1 port wireless0/2
set interface bgroup1 zone DMZ
set interface bgroup1 ip 10.0.0.1/24
save
```

Acceso administrativo

De forma predeterminada, todos los usuarios de la red pueden administrar un dispositivo siempre que conozcan el inicio de sesión y la contraseña.

Para configurar el dispositivo para poderlo manejar sólo desde un host específico en su red, utilice la WebUI o CLI como sigue:

WebUI

Configuration > Admin > Permitted IPs: Introduzca los siguientes datos y haga clic en **Add**:

IP Address/Netmask: *dir_ip/máscara*

CLI

```
set admin manager-ip dir_ip/máscara
save
```

Servicios de administración

ScreenOS proporciona servicios para configurar y administrar el dispositivo, tales como SNMP, SSL y SSH, que es posible habilitar mediante la interfaz.

Para configurar los servicios de administración en el dispositivo, utilice WebUI o CLI como se muestra a continuación:

WebUI

Network > Interfaces > List > Edit (para ethernet0/0): En **Management Services**, seleccione o borre los servicios de administración que desea utilizar en la interfaz, luego haga clic en **Apply**.

CLI

```
set interface ethernet0/0 manage web
unset interface ethernet0/0 manage snmp
save
```


Nombre de host y nombre de dominio

El nombre del dominio define la red o subred a la cual pertenece el dispositivo, mientras que el nombre de host se refiere a un dispositivo específico. El nombre de host y el nombre de dominio identifican de manera única al dispositivo en la red.

Para configurar el nombre de host y nombre de dominio en un dispositivo, utilice WebUI o CLI como se muestra a continuación:

WebUI

Network > DNS > Host: Introduzca los siguientes datos, luego haga clic en **Apply**:

Host Name: *nombre*
Domain Name: *nombre*

CLI

```
set hostname nombre
set domain nombre
save
```

Ruta predeterminada

La ruta predeterminada es una ruta estática que se utiliza para dirigir los paquetes a las redes que no están explícitamente enumeradas en la tabla de enrutamiento. Si un paquete llega al dispositivo con una dirección para la cual el dispositivo no tiene información de enrutamiento, el dispositivo envía el paquete al destino especificado por la ruta predeterminada.

Para configurar la ruta predeterminada en el dispositivo, utilice WebUI o CLI como se muestra a continuación:

WebUI

Network > Routing > Destination > New (trust-vr): Introduzca los siguientes datos y haga clic en **OK**:

IP Address/Netmask: 0.0.0.0/0.0.0.0
Next Hop
Gateway: (seleccione)
Interface: ethernet0/2 (seleccione)
Gateway IP Address: *dir_ip*

CLI

```
set route 0.0.0.0/0 interface ethernet0/2 gateway dir_ip
save
```

Dirección de interfaz de administración

La interfaz Trust tiene la dirección IP predeterminada 192.168.1.1/24 y está configurada para los servicios de administración. Si conecta los puertos 0/2 — 0/4 del dispositivo a una estación de trabajo, puede configurar el dispositivo de una estación de trabajo en la subred 192.168.1.1/24 utilizando un servicio de administración tal como Telnet.

Puede cambiar la dirección IP predeterminada en la interfaz Trust. Por ejemplo, tal vez desee cambiar la interfaz para que coincida con las direcciones IP ya existentes en LAN.

Configuración de la interfaz Untrust de respaldo

El dispositivo SSG 20 le permite configurar una interfaz de respaldo en caso de fallo de untrust. Para establecer una interfaz de respaldo en caso de fallo de untrust, lleve a cabo los siguientes pasos:

1. Configure la interfaz de respaldo en la zona de seguridad Null con el comando CLI **unset interface** *interfaz* [**port** *interfaz*].
2. Enlace la interfaz de respaldo a la misma zona de seguridad como la interfaz principal con el comando CLI **set interface** *interfaz* **zone** *nombre_zona*.

NOTA: Las interfaces principal y de respaldo deben estar en la misma zona de seguridad. Una interfaz principal tiene sólo una interfaz de respaldo y una interfaz de respaldo únicamente tiene una interfaz principal.

Para configurar la interfaz ethernet0/4 como la interfaz de respaldo para la interfaz ethernet0/0, utilice la WebUI o CLI como se muestra a continuación:

WebUI

Network > Interfaces > Backup > Introduzca los siguientes datos, luego haga clic en **Apply**.

Primary: ethernet0/0
Backup: ethernet0/4
Type: track-ip (seleccione)

CLI

```
unset interface bgroup0 port ethernet0/4
set interface ethernet0/4 zone untrust
set interface ethernet0/0 backup interface ethernet0/4 type track-ip
save
```

Configuración inalámbrica básica

En esta sección se proporciona información para la configuración de la interfaz inalámbrica del dispositivo SSG 20-WLAN. Las redes inalámbricas están formadas por nombres conocidos como identificadores de conjunto de servicios (SSID). Al especificar los SSID, podrá tener varias redes inalámbricas en la misma ubicación sin que éstas interfieran entre sí. Un nombre de SSID puede tener un máximo de 32 caracteres. Si un espacio es parte de la cadena de nombres de SSID, entonces la cadena se debe colocar entre comillas. Una vez que configure el nombre de SSID, podrá configurar más atributos de SSID. Para utilizar las capacidades de la red de área local inalámbrica (WLAN) en el dispositivo, debe configurar por lo menos un SSID y enlazarlo a una interfaz inalámbrica.

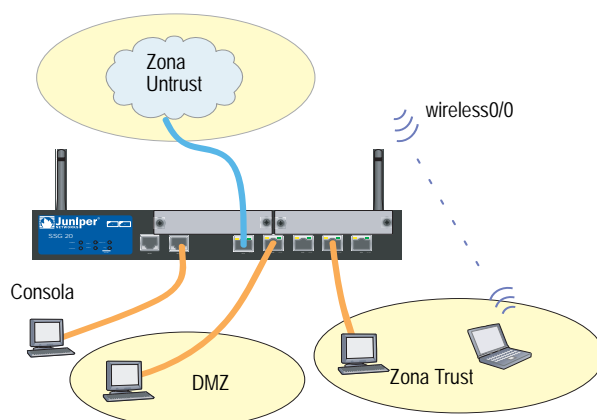
El dispositivo SSG 20-WLAN le permite crear hasta 16 SSID, pero sólo 4 de ellos se pueden utilizar simultáneamente. Puede configurar el dispositivo para utilizar los 4 SSID en cualquiera de los transceptores o dividir su utilización en ambos (por ejemplo, 3 SSID asignados a WLAN 0 y 1 SSID asignado a WLAN 1). Utilice el comando CLI **set interface** *interfaz_inalámbrica* **wlan** {0 | 1 | both} para configurar los transceptores de radio en el dispositivo SSG 20-WLAN.

Una vez que ha definido un SSID para la interfaz wireless0/0, puede acceder al dispositivo mediante la dirección IP de la interfaz wireless0/0 predeterminada descrita en los pasos proporcionados en “Acceso al dispositivo” en la página 28. La Figura 15 muestra la configuración predeterminada para el dispositivo SSG 20-WLAN.

NOTA: Si está utilizando el dispositivo SSG 20-WLAN en un país que no es Estados Unidos, Japón, Canadá, China, Taiwán, Corea, Israel o Singapur, entonces debe utilizar el comando CLI **set wlan country-code** o configurarlo en la página de WebUI Wireless > General Settings antes que se pueda establecer una conexión WLAN. Este comando ajusta el intervalo de canales que se pueden seleccionar y el nivel de potencia de la transmisión.

Si su código regional es ETSI, debe configurar el código de país correcto que cumple con las normativas de espectro de radio local.

Figura 15: Configuración predeterminada de SSG 20-WLAN



De manera predeterminada, la interfaz wireless0/0 está configurada con la dirección IP 192.168.2.1/24. Todos los clientes que utilizan servicios inalámbricos y que necesiten conectarse a la zona Trust, deben tener una dirección IP en la subred inalámbrica. También puede configurar el dispositivo para utilizar DHCP con el fin de que asigne direcciones IP de forma automática en la subred 192.168.2.1/24 a sus dispositivos.

De manera predeterminada, las interfaces wireless0/1 – wireless0/3 están definidas como Null y no tienen direcciones IP asignadas. Si desea utilizar cualquiera de las otras interfaces inalámbricas, debe configurar una dirección IP para ello, asignarle un SSID y enlazarla a una zona de seguridad. La Tabla 7 muestra la autenticación inalámbrica y los métodos de encriptación.

Tabla 7: Opciones de autenticación inalámbrica y encriptación

Autenticación	Encriptación
Open	Permite que cualquier cliente que utiliza el servicio inalámbrico tenga acceso al dispositivo
Shared-key	Clave compartida de WEP
WPA-PSK	AES/TKIP con clave previamente compartida
WPA	AES/TKIP con clave del servidor RADIUS
WPA2-PSK	802.11i, compatible con una clave previamente compartida
WPA2	802.11i, compatible con un servidor RADIUS
WPA-Auto-PSK	Permite usar WPA y WPA2 con la clave previamente compartida
WPA-Auto	Permite usar WPA y WPA2 con el servidor RADIUS
802.1x	WEP con clave del servidor RADIUS

Consulte el *Manual de referencia de ScreenOS: Conceptos y ejemplos* para ver ejemplos de configuración, atributos de SSID y comandos de CLI relacionados con las configuraciones de seguridad inalámbrica.

Para configurar una interfaz inalámbrica para la conectividad básica, utilice WebUI o CLI como se muestra a continuación:

WebUI

1. Configure el código de país WLAN y la dirección IP.

Wireless > General Settings > Seleccione los siguientes datos, luego haga clic en **Apply**:

Country code: Select your code
IP Address/Netmask: *dir_ip/máscara_red*

2. Configure el SSID.

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

SSID:
Authentication:
Encryption:
Wireless Interface Binding:

3. (Opcional) configure la clave WEP.

SSID > WEP Keys: Seleccione la ID de clave, luego haga clic en **Apply**.

4. Configure el modo WLAN.

Network > Interfaces > List > Edit (interfaz inalámbrica): Seleccione **Both** para el modo WLAN, luego haga clic en **Apply**.

5. Active los cambios inalámbricos.

Wireless > General Settings > Haga clic en **Activate Changes**.

CLI

1. Configure el código de país de WLAN y la dirección IP.

```
set wlan country-code { code_id }
set interface interfaz_inalámbrica ip dir_ip/máscara_red
```

2. Configure SSID.

```
set ssid name cadena_nombre
set ssid cadena_nombre authentication tipo_autorización encryption tipo_cifrado
set ssid cadena_nombre interface interfaz
(opcional) set ssid cadena_nombre key-id number
```

3. Configure el modo WLAN.

```
set interface interfaz_inalámbrica wlan both
```

4. Active los cambios inalámbricos.

```
save
exec wlan reactivate
```

Puede configurar un SSID para que funcione en la misma subred que la subred con cables. Esta acción permite a los clientes trabajar en una interfaz sin tener que volver a conectarse a otra subred.

Para establecer una interfaz inalámbrica y Ethernet para la misma interfaz de grupo en puente, utilice WebUI o CLI como se muestra a continuación:

WebUI

Network > Interfaces > List > Edit (*nombre_bgroup*) > Bind Port: Seleccione las interfaces inalámbrica y Ethernet, luego haga clic en **Apply**.

CLI

```
set interface nombre_bgroup port interfaz_inalámbrica
set interface nombre_bgroup port interfaz_Ethernet
```

NOTA: El *Nombre_bgroup* puede ser bgroup0—bgroup3.

La *Interfaz_Ethernet* puede ser ethernet0/0—ethernet0/4.

La *Interfaz_inalámbrica* puede ser wireless0/0—wireless0/3.

Si configura una interfaz inalámbrica, luego deberá reactivar la WLAN con el comando CLI **exec wlan reactivate** o hacer clic en **Activate Changes** en la página de WebUI Wireless > General Settings.

Configuración de mini PIM

Esta sección explica la manera de configurar los mini módulos de interfaz física (PIM):

- Interfaz ADSL2/2 +
- Interfaz RDSI
- Interfaz T1
- Interfaz E1
- Interfaz del módem V.92

Interfaz ADSL2/2+

Su red utiliza la interfaz ADSL2/2 + **adslx/0**, donde la x representa la ranura del mini PIM (1 ó 2) en el dispositivo para conectarlo a la red del proveedor de servicios a través de un circuito virtual de modo de transferencia asíncrona (ATM). Puede configurar circuitos virtuales adicionales creando subinterfases ADSL2/2 + . Para obtener más información, consulte “Circuitos virtuales” en la página 42.

En la WebUI, acceda a la página Network > Interfaces > List para ver una lista de las interfaces disponibles en el dispositivo. Si utiliza una sesión Telnet o de consola, introduzca el comando CLI **get interface**. Debe comprobar que la interfaz adslx/0 está enlazada a la zona Untrust.

Si utiliza la interfaz ADSL2/2 + para conectarse a la red de servicios del proveedor, debe configurar la interfaz adsl(x/0). Para ello, el proveedor de servicios le tiene que proporcionar la siguiente información:

- Valores del identificador de trayecto virtual y del identificador de canal virtual (VPI/VCI)
- Método de multiplexado de capa de adaptación ATM 5 (AAL5), que puede ser una de las siguientes opciones:
 - Multiplexado con base en el circuito virtual, 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 de servicios para conectarse a la red del proveedor mediante el protocolo punto a punto a través de Ethernet (PPPoE) o el protocolo punto a punto a través de ATM (PPPoA).
- Método de autenticación, si hubiera, que se proporciona a la conexión PPPoE o PPPoA
- Opcionalmente, una dirección IP estática y un valor de máscara de red para la red

Circuitos virtuales

Para agregar circuitos virtuales, debe crear subinterfaces en la interfaz ADSL2/2 + . Puede crear un máximo de 10 subinterfaces ADSL2/2 + . Por ejemplo, para crear una nueva subinterfaz denominada **adsl1/0.1** enlazada a la zona predeterminada que se conoce como **Untrust**, utilice la WebUI o CLI como se muestra a continuación:

WebUI

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

Interface Name: adsl1/0.1
VPI/VCI: 0/35
Zone Name: Untrust (seleccione)

CLI

```
set interface adsl 1/0.1 pvc 0 35 zone Untrust
save
```

Debe configurar una subinterfaz ADSL 2/2 + de la misma manera que la interfaz ADSL2/2 + principal, incluyendo el ajuste de los valores VPI/VCI, tal y como se describe en “Interfaz ADSL2/2 + ” en la página 41 . Las subinterfaces ADSL2/2 + se configuran independientemente de la interfaz ADSL2/2 + principal. Esto quiere decir que va a configurar un método de multiplexado, VPI/VCI, y un cliente PPP diferentes de los de la interfaz ADSL2/2 + principal. También puede configurar una dirección IP estática en una subinterfaz, aunque la interfaz ADSL2/2 + principal no disponga de una dirección IP estática.

Método VPI/VCI y multiplexado

El proveedor de servicios asigna un par de VPI/VCI a cada conexión de circuito virtual. Por ejemplo, puede obtener el valor 1/32 para el par VPI/VCI, lo que asigna un valor VPI de 1 y un valor VCI de 32. 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 1/32 VPI/VCI en la interfaz adsl1/0, utilice la WebUI o CLI como se muestra a continuación:

WebUI

Network > Interfaces > List > Edit (para la interfaz adsl1/0): Introduzca **1/32** en el campo VPI/VCI, luego haga clic en **Apply**.

CLI

```
set interface adsl1/0 pvc 1 32
save
```

De manera predeterminada, el dispositivo utiliza el multiplexado con base en el control de enlaces lógico (LLC) para cada circuito virtual.

Para configurar el par VPI/VCI 1/32 en la interfaz adslx/0 y utilizar el encapsulado LLC en el circuito virtual, utilice la WebUI o CLI como sigue:

WebUI

Network > Interfaces > List > Edit (para la interfaz adsl1/0): Introduzca los siguientes datos, luego haga clic en **Apply**:

VPI/VCI: 1 / 32
 Multiplexing Method: LLC (seleccionado)

CLI

```
set interface adsl1/0 pvc 1 32 mux llc
save
```

PPPoE o PPPoA

Un dispositivo SSG 20 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 host de la red. PPPoA se utiliza principalmente para los servicios empresariales, ya que las sesiones PPP se pueden finalizar en el dispositivo. Para permitir conectar el dispositivo a la red del proveedor de servicios, debe 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 sólo admite una sesión PPPoE en cada circuito virtual.

Para configurar el nombre de usuario **roswell** y la contraseña **area51** para PPPoE y enlazar la configuración PPPoE a la interfaz adsl1/0, utilice la WebUI o CLI como sigue:

WebUI

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

PPPoE Instance: poe1
 Bound to Interface: adsl1/0 (seleccione)
 Username: roswell
 Password: area51

CLI

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1/0
save
```

Hay otros parámetros PPPoE o PPPoA que puede configurar en el dispositivo, incluyendo el método de autenticación (de forma predeterminada, el dispositivo admite el protocolo de autenticación de establecimiento de conexión por desafío o bien el protocolo de autenticación mediante contraseña), 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.

Dirección IP estática y máscara de red

Si su proveedor de servicio le proporcionó una dirección IP fija y una máscara de red para la red, entonces configure la dirección IP y máscara de red para la red y la dirección IP del puerto del enrutador conectado al dispositivo. También deberá especificar que el dispositivo utiliza una dirección IP estática. (Por lo general, el dispositivo actúa como un cliente PPPoE o PPPoA y recibe una dirección IP para la interfaz ADSL mediante negociaciones con el servidor PPPoE o PPPoA.)

Debe configurar una instancia PPPoE o PPPoA y enlazarla a la interfaz `adsl1/0`, tal y como se describe en “PPPoE o PPPoA” en la página 43. Asegúrese de seleccionar **Obtain IP using PPPoE** u **Obtain IP using PPPoA** y el nombre de la instancia PPPoE o PPPoA.

Para configurar la dirección IP estática `1.1.1.1/24` para la red, utilice la WebUI o CLI como se muestra a continuación:

WebUI

Network > Interfaces > List > Edit (para la interfaz `adsl1/0`): Introduzca los siguientes datos, luego haga clic en **Apply**:

IP Address/Netmask: `1.1.1.1/24`
Static IP: (seleccione)

CLI

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

o bien

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoa name poa1 static-ip
save
```

Para utilizar el sistema de nombres de dominios (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 recibe una dirección IP para la interfaz `ADSL2/2 +` mediante PPPoE o PPPoA, entonces también 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, estos equipos también obtendrán las direcciones de estos servidores DNS.

Si asigna una dirección IP estática a la interfaz `ADSL2/2 +`, 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 para que proporcione la dirección del servidor DNS a cada equipo.

Para configurar el servidor DHCP en la interfaz `bgroup0` con el fin de que proporcione la dirección `1.1.1.152` del servidor DNS a los equipos de la red, utilice la WebUI o CLI como se muestra a continuación:

WebUI

Network > DHCP > Edit (para la interfaz bgroup0) > DHCP Server: Introduzca **1.1.1.152** para DNS1, luego haga clic en **Apply**.

CLI

```
set interface bgroup0 dhcp server option dns1 1.1.1.152
save
```

Para obtener más información sobre la manera de configurar las interfaces ADSL y ADSL2/2 + , consulte el *Manual de referencia de ScreenOS: Conceptos y ejemplos*.

Interfaz RDSI

Las redes digitales de servicios integrados (RDSI) son un conjunto de normas para la transmisión digital a través de medios diferentes creadas por el Comité Consultivo para la Telegrafía y Telefonía Internacional (CCITT) y la Unión Internacional de Telecomunicaciones (ITU). Como un servicio de acceso telefónico de demanda, tiene configuración de llamada rápida y latencia baja, así como la capacidad de transmitir voz, datos y transmisiones de vídeo de alta calidad. RDSI también es un servicio conmutado de circuitos que se puede utilizar tanto en conexiones multipunto como de punto a punto. RDSI proporciona un enrutador de servicio con una conexión múltiple del protocolo de punto a punto (PPP) para las interfaces de red. La interfaz RDSI generalmente se configura como la interfaz de respaldo de la interfaz Ethernet para acceder a las redes externas.

Para configurar la interfaz RDSI, utilice la WebUI o CLI como se muestra a continuación:

WebUI

Network > Interfaces > List > Edit (bri1/0): Introduzca o seleccione los siguientes datos, luego haga clic en **OK**:

```
BRI Mode: Dial Using BRI
Primary Number: 123456
WAN Encapsulation: PPP
PPP Profile: isdnprofile
```

CLI

```
set interface bri1/0 dialer-enable
set interface bri1/0 primary-number "123456"
set interface bri1/0 encaps ppp
set interface bri1/0 ppp profile isdnprofile
save
```

Para configurar la interfaz RDSI como la interfaz de respaldo, consulte “Configuración de la interfaz Untrust de respaldo” en la página 37.

Para obtener más información sobre la manera de configurar la interfaz RDSI, consulte el *Manual de referencia de ScreenOS: Conceptos y ejemplos*.

Interfaz T1

La interfaz T1 es un protocolo de capa física que utiliza el método de multiplexado (DS-1) de nivel 1 de señal digital en Norteamérica. Una interfaz T1 funciona a una velocidad de bits de 1,544 Mbps o hasta de 24 canales DS0.

El dispositivo admite las siguientes normas T1 DS-1:

- ANSI T1.107, T1.102
- GR 499-core, GR 253-core
- AT&T Pub 54014
- ITU G.751, G.703

Para configurar el mini PIM T1, utilice la WebUI o CLI como se muestra a continuación:

WebUI

Network > Interfaces > List > Edit (serial1/0): Introduzca o seleccione los siguientes datos, luego haga clic en **OK**:

WAN Configure: main link
 WAN Encapsulation: cisco-hdlc
 Haga clic en **Apply**
 Fixed IP: (seleccione)
 IP Address/Netmask: 172.18.1.1/24

CLI

```
set interface serial1/0 encap cisco-hdlc
set interface serial1/0 ip 172.18.1.1/24
```

Para obtener información sobre la manera de configurar la interfaz T1, consulte el *Manual de referencia de ScreenOS: Conceptos y ejemplos*.

Interfaz E1

La interfaz E1 es un formato de comunicaciones digitales de la red de área extensa estándar (WAN) diseñado para funcionar a través de cables de cobre a una velocidad de 2,048 Mbps. Ampliamente utilizada fuera de Norteamérica, la interfaz E1 es un esquema de multiplexado de división de tiempo básico que se usa para transportar circuitos digitales.

El dispositivo admite las siguientes normas E1:

- ITU-T G.703
- ITU-T G.751
- ITU-T G.775

Para configurar el mini PIM E1, utilice la WebUI o CLI como se muestra a continuación:

WebUI

Network > Interfaces > List > Edit (serial1/0): Introduzca o seleccione los siguientes datos, luego haga clic en **OK**:

WAN Configure: main link
 WAN Encapsulation: PPP
 Binding a PPP Profile: junipertest
 Haga clic en **Apply**
 Fixed IP: (seleccione)
 IP Address/Netmask: 172.18.1.1/24

CLI

```
set interface serial1/0 encapsulation ppp
set ppp profile "junipertest" static-ip
set ppp profile "junipertest" auth type chap
set ppp profile "junipertest" auth local-name "juniper"
set ppp profile "junipertest" auth secret "password"
set interface serial1/0 ppp profile "junipertest"
set interface serial1/0 ip 172.18.1.1/24
set user "server" type wan
set user "server" password "server"
```

Para obtener información sobre la manera de configurar la interfaz E1, consulte el *Manual de referencia de ScreenOS: Conceptos y ejemplos*.

Interfaz del módem V.92

La interfaz V.92 proporciona un módem analógico interno para establecer una conexión PPP con un proveedor de servicios. Puede configurar la interfaz serie como una interfaz principal o de respaldo, la cual se utiliza si ocurre un cambio por fallo de la interfaz.

NOTA: La interfaz V.92 no funciona en el modo transparente.

Para configurar la interfaz V.92, utilice la WebUI o CLI como se muestra a continuación:

WebUI

Network > Interfaces > List > Edit (para serial1/0): Introduzca los siguientes datos y haga clic en **OK**:

Zone Name: untrust (seleccione)

ISP: Introduzca los siguientes datos y haga clic en **OK**:

ISP Name: isp_juniper
 Primary Number: 1234567
 Login Name: juniper
 Login Password: juniper

Modem: Introduzca los siguientes datos y haga clic en **OK**:

Modem Name: mod1
 Init String: AT&FS7=255S32=6
 Active Modem setting
 Inactivity Timeout: 20

CLI

```

set interface serial1/0 zone untrust
set interface serial1/0 modem isp isp_juniper account login juniper password
juniper
set interface serial1/0 modem isp isp_juniper primary-number 1234567
set interface serial1/0 modem idle-time 20
set interface serial1/0 modem settings mod1 init-strings AT&FS7=255S32=6
set interface serial1/0 modem settings mod1 active

```

Para obtener información sobre la manera de configurar la interfaz de módem V.92, consulte el *Manual de referencia de ScreenOS: Conceptos y ejemplos*.

Protecciones básicas del cortafuegos

Los dispositivos están configurados con una directiva predeterminada que permite utilizar estaciones de trabajo en la zona Trust de su red para acceder a cualquier recurso en la zona de seguridad Untrust, mientras que los equipos externos no cuentan con el permiso para acceder o iniciar sesiones con sus estaciones de trabajo. Puede configurar directivas que obliguen al dispositivo a permitir que los equipos externos inicien determinado tipo de sesiones con los equipos de la red. Para obtener información sobre la manera de crear o modificar las directivas, consulte el *Manual de referencia de ScreenOS: Conceptos y ejemplos*.

El dispositivo SSG 20 proporciona varios métodos de detección y mecanismos de defensa para combatir rastreos y ataques con los que se pretende comprometer o dañar una red o un recurso de red:

- Las opciones SCREEN de ScreenOS aseguran una zona inspeccionando y luego permitiendo o rechazando todo intento de conexión que necesite atravesar una interfaz enlazada a dicha zona. Por ejemplo, puede aplicar la protección de análisis de puertos a la zona Untrust para detener un origen desde una red remota que intenta identificar servicios con el fin de llevar a cabo ataques futuros.
- El dispositivo aplica directivas de cortafuegos, que pueden contener componentes para el filtrado de contenidos y la detección así como prevención de intrusiones (IDP), al tráfico que pasa por los filtros SCREEN de una zona a otra. De manera predeterminada, no se permite que ningún tráfico pase por el dispositivo de una zona a otra. Para permitir que el tráfico pase por el dispositivo de una zona a otra, debe crear una directiva que anule el comportamiento predeterminado.

Para configurar las opciones SCREEN de ScreenOS para una zona, utilice la WebUI o CLI como se muestra a continuación:

WebUI

Screening > Screen: Seleccione la zona para la cual aplican las opciones. Seleccione las opciones SCREEN que desee, luego haga clic en **Apply**:

CLI

```

set zone zona screen opción
save

```

Para obtener más información sobre la manera de configurar las opciones de seguridad de red en ScreenOS, consulte el *Manual de referencia de ScreenOS: Conceptos y ejemplos*.

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 desde cualquier estación de la red e introduzca la siguiente URL: www.juniper.net.

Restablecimiento de los ajustes predeterminados de fábrica

Si pierde la contraseña de administrador, puede restablecer los ajustes predeterminados del dispositivo. De este modo destruirá la configuración existente, pero restablecerá el acceso al dispositivo.



ADVERTENCIA: Al restablecer el dispositivo, se eliminan todos los ajustes de configuración existentes y se deshabilitan todos los servicios existentes del cortafuegos y VPN.

Puede restaurar los ajustes predeterminados del dispositivo mediante uno de los siguientes procedimientos:

- Por medio de una conexión de consola. Para obtener información adicional, consulte el *Manual de referencia de ScreenOS: Conceptos y ejemplos*.
- Mediante el orificio de restablecimiento situado en el panel posterior del dispositivo tal como se describe en la siguiente sección.

Puede restablecer el dispositivo y restaurar los ajustes predeterminados de fábrica insertando un objeto punzante en el orificio de restablecimiento y al presionar ligeramente. Para realizar esta operación, es necesario ver los LED de estado del dispositivo que se encuentran en el panel frontal o iniciar una sesión de consola tal como se describe en “Utilización de una conexión de consola” en la página 28.

Para utilizar el orificio de restablecimiento para restablecer los ajustes predeterminados, lleve a cabo los siguientes pasos:

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.

El LED de estado parpadea con luz roja. 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 del segundo restablecimiento. 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 de restablecimiento y presione hacia dentro entre cuatro y seis segundos.

El mensaje de la consola verifica el segundo restablecimiento. El LED de estado se enciende con luz roja durante medio segundo y luego la luz pasa a verde intermitente.

Luego, se restablecen los ajustes originales de fábrica del dispositivo. Cuando el dispositivo se restablece, el LED de estado se enciende con luz roja durante medio segundo y luego 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 host de captura SNMP o SYSLOG configurados.

Una vez reiniciado el dispositivo, la consola muestra el mensaje de solicitud de inicio de sesión del dispositivo. El LED de estado parpadea con luz verde. El inicio de sesión y la contraseña son **netscreen**.

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 restableció, se enviará una alerta SNMP para confirmar el fallo.

Capítulo 4

Servicio del dispositivo

Este capítulo describe los procedimientos de servicio y mantenimiento para un dispositivo SSG 20. Incluye las siguientes secciones:

- “Piezas y herramientas requeridas” en esta página
- “Reemplazo de un mini módulo de interfaz física” en esta página
- “Actualización de memoria” en la página 54

NOTA: Para obtener información sobre las advertencias e instrucciones de seguridad, consulte el *Manual de seguridad de productos Juniper Networks*. Las instrucciones incluidas en el manual advierten sobre situaciones que podrían provocar lesiones físicas. Antes de utilizar cualquier equipo, debe tener en cuenta los peligros que entraña el sistema de circuitos eléctricos y familiarizarse con las prácticas habituales de prevención de accidentes.

Piezas y herramientas requeridas

Para reemplazar un componente en un dispositivo SSG 20, necesita las siguientes herramientas y piezas:

- Bolsa electrostática o alfombra antiestática
- Muñequera de tierra para protección contra descargas electrostáticas (ESD)
- Destornillador Phillips de 1/8 de pulgada

Reemplazo de un mini módulo de interfaz física

Ambos modelos SSG 20 tienen dos ranuras en el panel frontal para los mini módulos de interfaz física de red de área extensa (mini PIM WAN). Los mini PIM de un dispositivo SSG 20 se pueden instalar y reemplazar. El dispositivo se debe apagar antes de poder desinstalar o instalar un mini PIM.



PRECAUCIÓN: Asegúrese de que la alimentación está apagada hacia el dispositivo al desinstalar un mini PIM. Estos no se pueden intercambiar cuando están activos.

Extracción de una placa frontal

Para mantener el flujo de aire correcto a través del dispositivo SSG 20, las placas frontales deben permanecer en las ranuras que no contienen mini PIM. No desinstale una placa frontal a menos que instale un mini PIM en esa ranura vacía.

Para desinstalar una placa frontal, realice los siguientes pasos:

1. Coloque una bolsa electrostática o una alfombra antiestática en una superficie plana y estable en la que piense colocar el mini PIM.
2. Asegure una muñequera de tierra ESD a su muñeca, directamente sobre la piel, y conecte la muñequera al punto ESD en el chasis o a un punto ESD exterior si el dispositivo SSG 20 está desconectado de la conexión a tierra.
3. Desenchufe el adaptador de alimentación del dispositivo. Verifique que el LED POWER (alimentación) está apagado.
4. Afloje y retire los tornillos de cada lado de la placa frontal con un destornillador.
5. Desinstale la placa frontal, después coloque la placa frontal en la bolsa electrostática o en la alfombra antiestática.

Extracción de un mini PIM

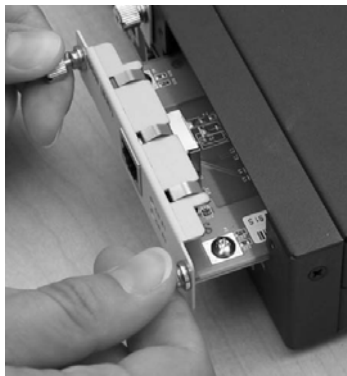
Los mini PIM se instalan en el panel frontal del dispositivo SSG 20. Un mini PIM pesa menos de 106 gramos (0,2 libras).

Para desinstalar un mini PIM, realice los siguientes pasos:

1. Coloque una bolsa electrostática o una alfombra antiestática en una superficie plana y estable en la que piense colocar el mini PIM.
2. Asegure una muñequera de tierra ESD a su muñeca, directamente sobre la piel, y conecte la muñequera al punto ESD en el chasis o a un punto ESD exterior si el dispositivo SSG 20 está desconectado de la conexión a tierra.
3. Desenchufe el adaptador de alimentación del dispositivo. Verifique que el LED POWER está apagado.
4. Etiquete los cables conectados al mini PIM de manera que pueda volver a conectarlos más adelante al mini PIM correcto.
5. Desconecte los cables del mini PIM.
6. Si es necesario, coloque los cables para evitar que se desprendan o se desarrollen puntos de tensión:
 - a. Asegure los cables de manera que no sostengan su propio peso mientras cuelgan hacia el suelo.
 - b. Quite de enmedio el exceso de cable en un bucle bien enrollado.
 - c. Utilice bridas para mantener la forma de los bucles de cable.

7. Afloje y retire los tornillos de cada lado de la placa frontal del mini PIM con un destornillador.
8. Agarre los tornillos de cada lado de la placa frontal del mini PIM y deslice el mini PIM fuera del dispositivo. Coloque el mini PIM en la bolsa electrostática o en la alfombra antiestática.

Figura 16: Desinstalación de un mini PIM



9. Si no está instalando de nuevo un mini PIM en la ranura vacía, instale una placa frontal en la ranura para mantener el flujo de aire correcto.

Instalación de un mini PIM

Para instalar un mini PIM, realice los siguientes pasos:

1. Asegure una muñequera de tierra ESD a su muñeca, directamente sobre la piel, y conecte la muñequera al punto ESD en el chasis o a un punto ESD exterior si el dispositivo SSG 20 está desconectado de la conexión a tierra.
2. Desenchufe el adaptador de alimentación del dispositivo. Verifique que el LED POWER está apagado.
3. Agarre los tornillos de cada lado de la placa frontal del mini PIM y alinee las muescas del conector en la parte trasera del mini PIM con las muescas de la ranura del mini PIM en el dispositivo SSG 20. Después, deslice el mini PIM hasta que se asegure firmemente en el dispositivo.

Figura 17: Instalación de un mini PIM



PRECAUCIÓN: Deslice el mini PIM en dirección recta en la ranura para evitar ocasionar daños a los componentes del mini PIM.

4. Apriete los tornillos de cada lado de la placa frontal del mini PIM con un destornillador ranurado de 1/8 de pulgada.

5. Inserte los cables apropiados en los conectores de cable del mini PIM.
6. Si es necesario, arregle los cables para evitar que se desprendan o se desarrollen puntos de tensión:
 - a. Asegure los cables de manera que no sostengan su propio peso mientras cuelgan hacia el suelo.
 - b. Quite de enmedio el exceso de cable en un bucle bien enrollado.
 - c. Utilice bridas para mantener la forma de los bucles de cable.
7. Desenchufe el adaptador de alimentación del dispositivo. Verifique que el LED POWER se enciende en verde, sin parpadear, mientras presiona el botón de encendido.
8. Verifique que el LED de estado del PIM en el tablero del sistema se enciende en verde, sin parpadear, para confirmar que el mini PIM está en línea.

Actualización de memoria

Puede actualizar un dispositivo SSG 20 desde un único módulo doble de memoria en línea (DIMM) de 128 MB de memoria de acceso aleatorio dinámica (DRAM) a un DIMM DRAM de 256 MB.

Para actualizar la memoria de un dispositivo SSG 20, realice los siguientes pasos:

1. Asegure la muñequera de tierra ESD a su muñeca, directamente sobre la piel, y conecte la muñequera al punto ESD en el chasis o a un punto ESD exterior si el dispositivo está desconectado de la conexión a tierra.
2. Desenchufe el cordón de CA de la toma de corriente.
3. Voltee el dispositivo de manera que la parte superior esté sobre una superficie plana.
4. Utilice un destornillador Phillips para retirar los tornillos de la cubierta de la tarjeta de memoria. Mantenga los tornillos cerca para usarlos cuando asegure la cubierta más adelante.
5. Retire la cubierta de la tarjeta de memoria.

Figura 18: Parte inferior del dispositivo



- Libere la DIMM DRAM de 128 MB presionando con sus dedos pulgares hacia afuera en las lengüetas de bloqueo de cada lado del módulo de manera que las lengüetas se salgan del módulo.

Figura 19: Desbloqueo del módulo de memoria



- Agarre el borde largo del módulo de memoria y deslícelo hacia afuera. Colóquelo a un lado.

Figura 20: Extracción de las ranuras del módulo



- Introduzca la DIMM DRAM de 256 MB en la ranura. Aplicando presión uniforme con los pulgares en el borde superior del módulo, presione el módulo hacia abajo hasta que las lengüetas de bloqueo traben en su lugar.

Figura 21: Introducción del módulo de memoria



- Coloque la cubierta de la tarjeta de memoria en la ranura.
- Utilice el destornillador Phillips para apretar los tornillos y asegure la cubierta al dispositivo.

Apéndice A

Especificaciones

En este apéndice se muestran las especificaciones de sistema generales para un dispositivo SSG 20. Incluye las siguientes secciones:

- “Características físicas” en la página 58
- “Características eléctricas” en la página 58
- “Tolerancia ambiental” en la página 58
- “Certificaciones” en la página 59
- “Conectores” en la página 60

Características físicas

Tabla 8: Especificaciones físicas del SSG 20

Descripción	Valor
Dimensiones del chasis	294 mm x 194,8 mm x 44 mm (11,5 pulgadas x 7,7 pulgadas x 2 pulgadas)
Peso del dispositivo	1,53 kg (3,3 libras) sin PIM instalados
PIM RDSI	70 gramos
PIM ADSL, anexo A	106 gramos
PIM ADSL, anexo B	106 gramos
PIM T1	75 gramos
PIME1	75 gramos
PIM V.92	79 gramos

Características eléctricas

Tabla 9: Especificaciones eléctricas del SSG 20

Elemento	Especificaciones
Voltaje entrada CC	12 V
Clasificación de corriente del sistema CC	3 - 4,16 Amps

Tolerancia ambiental

Tabla 10: Tolerancia ambiental del SSG 20

Descripción	Valor
Altitud	No hay degradación de rendimiento a 6.600 pies (2.000 m)
Humedad relativa	El funcionamiento normal está garantizado en un rango de humedad relativa de 10 a 90 por ciento, sin condensación
Temperatura	El funcionamiento normal está garantizado en un rango de temperatura de 32°F (0°C) a 104°F (40°C) Temperatura de almacenamiento sin funcionamiento en el embalaje para transporte: -4°F (-20°C) a 158°F (70°C)

Certificaciones

Seguridad

- CAN/CSA-C22.2 No. 60950-1-03/UL 60950-1 Seguridad del equipo de tecnología de información
- EN 60950-1 (2000) Tercera edición, Seguridad del equipo de tecnología de información
- IEC 60950-1 (1999) Tercera edición, Seguridad del equipo de tecnología de información

Emisiones EMC

- FCC Parte 15 Clase B (EE.UU.)
- EN 55022 Clase B (Europa)
- AS 3548 Clase B (Australia)
- VCCI Clase B (Japón)

Inmunidad EMC

- EN 55024
- Armónica de la línea de alimentación EN-61000-3-2
- Armónica de la línea de alimentación EN-61000-3-3
- EN-61000-4-2 ESD
- Inmunidad irradiada EN-61000-4-3
- EN-61000-4-4 EFT
- Sobretensión EN-61000-4-5
- Inmunidad común de baja frecuencia EN-61000-4-6
- Caídas y pérdidas de voltaje EN-61000-4-11

ETSI

Instituto Europeo de Normas en Telecomunicaciones (ETSI) EN-3000386-2: Equipo de red de telecomunicación. Requisitos de compatibilidad electromagnética; (categoría del equipo-Distinto a centro de telecomunicación)

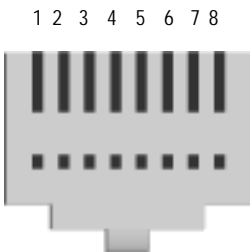
Interfaz T1

- FCC Parte 68 - T1A 968
- Industria de Canadá CS-03
- UL 60950-1 Requisitos aplicables para circuito TNV con conexión de conductor de planta exterior

Conectores

La Figura 22 muestra la ubicación de las patillas del conector RJ-45.

Figura 22: Patillas de salida RJ-45



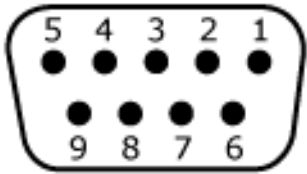
La Tabla 11 enumera las patillas de salida del conector RJ-45.

Tabla 11: Patillas de salida del conector RJ-45

Patilla	Nombre	E/S	Descripción
1	Salida RTS	S	Solicitud para enviar
2	Salida DTR	S	Terminal de datos lista
3	TxD	S	Transmisión de datos
4	GND	N/A	Tierra del chasis
5	GND	N/A	Tierra del chasis
6	RxD	E	Recepción de datos
7	DSR	E	Datos listos
8	CTS	E	Listo para enviar

La Figura 23 muestra la ubicación de las patillas del conector hembra DB-9.

Figura 23: Conector hembra DB-9



La Tabla 12 proporciona las patillas de salida del conector DB-9.

Tabla 12: Patillas de salida del conector DB-9

Patilla	Nombre	E/S	Descripción
1	DCD	E	Detección de portadora
2	RxD	E	Recepción de datos
3	TxD	S	Transmisión de datos
4	DTR	S	Terminal de datos lista
5	GND	N/A	Tierra de la señal
6	DSR	E	Datos listos
7	RTS	S	Solicitud para enviar
8	CTS	E	Listo para enviar
9	RING	E	Indicador de llamada

Apéndice B

Asistente de configuración inicial

Este apéndice proporciona información detallada sobre el asistente de configuración inicial (ICW) para un dispositivo SSG 20.

Después de conectar físicamente su dispositivo a la red, podrá utilizar el ICW para configurar las interfaces que están instaladas en su dispositivo.

Esta sección describe las siguientes ventanas de ICW:

- Ventana Rapid Deployment en la página 64
- Ventana Administrator Login en la página 64
- Ventana WLAN Access Point en la página 65
- Ventana Physical Interface en la página 65
- Ventana ADSL2/2 + Interface en la página 66
- Ventanas T1 Interface en la página 68
- Ventanas E1 Interface en la página 73
- Ventanas ISDN Interface en la página 75
- Ventana V.92 Modem Interface en la página 78
- Ventana Eth0/0 Interface (Untrust Zone) en la página 79
- Ventana Eth0/1 Interface (DMZ Zone) en la página 80
- Ventana Bgroup0 Interface (Trust Zone) en la página 81
- Ventana Wireless0/0 Interface (Trust Zone) en la página 82
- Ventana Interface Summary en la página 83
- Ventana Physical Ethernet DHCP Interface en la página 84
- Ventana Wireless DHCP Interface en la página 84
- Ventana Confirmation en la página 85

1. Ventana Rapid Deployment

Figura 24: Ventana Rapid Deployment

Si su red utiliza NetScreen-Security Manager (NSM), puede utilizar un configlet de implementación rápida para configurar el dispositivo automáticamente. Obtenga un configlet de su administrador NSM, seleccione **Yes**, seleccione **Load Configlet from:**, busque la ubicación del archivo y luego haga clic en **Next**. El configlet configura el dispositivo para usted, de manera que no es necesario que utilice los siguientes pasos para configurarlo.

Si no desea utilizar el ICW sino ir directamente a la WebUI, seleccione la última opción, luego haga clic en **Next**.

Si no utiliza un configlet para configurar el dispositivo y desea utilizar el ICW, seleccione la primera opción, luego haga clic en **Next**. Aparece la pantalla ICW Welcome. Haga clic en **Next**. Aparece la ventana Administrator Login.

2. Ventana Administrator Login

Introduzca un nuevo nombre de inicio de sesión de administrador y contraseña, luego haga clic en **Next**.

Figura 25: Ventana Administrator Login

3. Ventana WLAN Access Point

Si utiliza el dispositivo en el dominio regulador WORLD o ETSI, debe escoger un código de país. Seleccione las opciones adecuadas, luego haga clic en **Next**.

Figura 26: Ventana Wireless Access Point Country Code

The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. Below the title bar, the text 'How do you want to configure the wireless access point?' is displayed. The window contains several configuration options: 'Regulatory Domain' is set to 'WORLD'; 'Country Code' is set to 'NO_COUNTRY_SET'; '2.4G Mode' is set to '802.11b/g'; and '5G Mode' is set to '802.11a'. There is a checkbox labeled 'Configure wireless0/0 interface in trust zone.' which is checked. At the bottom of the window, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

4. Ventana Physical Interface

En la pantalla de enlaces de interfaz a zona, establecerá la interfaz en la que desea enlazar la zona de seguridad Untrust. El Bgroup0 viene ya enlazado a la zona de seguridad Trust. Eth0/1 está enlazada a la zona de seguridad DMZ, pero esto es opcional.

Figura 27: Ventana Physical Interface

The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. Below the title bar, the text 'Please choose one interface for untrust, dmz and trust zone respectively.' is displayed. The window contains three configuration options: 'Untrust Zone' is set to 'eth0/0'; 'DMZ Zone' is set to 'eth0/1'; and 'Trust Zone' is set to 'bgroup0'. At the bottom of the window, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Después de enlazar una interfaz a una zona, podrá configurar la interfaz. Las ventanas de configuración que se muestran después de este punto dependen de los mini PIM instalados en su dispositivo de seguridad. Para continuar con la configuración de su dispositivo con el ICW, haga clic en **Next**.

5. Ventana ADSL2/2+ Interface

Si tiene el mini PIM de ADSL2/2 + instalado en su dispositivo, puede configurar la interfaz adslx/0 por medio de la siguiente ventana.

NOTA: Si tiene dos mini PIM de ADSL2/2 + instalados en su dispositivo, no puede configurar la función de conexión múltiple con el ICW. Para configurar ML ADSL, consulte el *Manual de referencia de ScreenOS: Conceptos y ejemplos*.

Figura 28: Ventana ADSL Interface Configuration

Initial Configuration Wizard

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.
[adsl1/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

How does the Juniper device connect to the outside via adsl1/0 interface?

VPI/VCI: 8 / 35

Multiplexing Method: LLC

RFC1483 Protocol Mode: ☒ Bridged ☐ Routed

Operating Mode: ☒ Auto ☐ ANSI DMT ☐ ITU DMT ☐ Adsl2 ☐ Adsl2+

☐ Dynamic IP via DHCP

☐ Dynamic IP via PPPoA

Username:

Password:

Confirm:

☐ Dynamic IP via PPPoE

Username:

Password:

Confirm:

☒ Static IP

Interface IP:

Netmask:

Gateway:

<< Previous Next >> Cancel

Tabla 13: Campos de la ventana ADSL Interface Configuration

Campo	Descripción
Información del proveedor de servicios:	
VPI/VCI	Valores VPI/VCI para identificar el circuito virtual permanente.
Multiplexing Method	Método de multiplexado ATM (LLC es el ajuste predeterminado).
RFC1483 Protocol Mode	Ajuste del modo de protocolo (Bridged es el ajuste predeterminado).
Operating Mode	Modo de funcionamiento para la línea física (Auto es el ajuste predeterminado).
IP configuration settings	<ul style="list-style-type: none"> ■ Seleccione Dynamic IP via DHCP para que el dispositivo pueda recibir una dirección IP para la interfaz ADSL por medio del proveedor de servicios. ■ Seleccione Dynamic IP via PPPoA para que el dispositivo pueda actuar como un cliente PPPoA. Introduzca el nombre de usuario y la contraseña asignados por el proveedor de servicio. ■ Seleccione Dynamic IP via PPPoE para que el dispositivo pueda actuar como un cliente PPPoE. Introduzca el nombre de usuario y la contraseña que el proveedor de servicio asignó. ■ Seleccione Static IP para asignar una dirección IP única y fija a la interfaz ADSL. Introduzca la dirección IP de interfaz, máscara de red y puerta de enlace (la dirección de la puerta de enlace es la dirección IP del puerto del enrutador conectado al dispositivo).

Si no conoce estos ajustes, consulte el documento *Common Settings for Service Providers* que se incluye con el dispositivo del proveedor de servicios.

6. Ventanas T1 Interface

Si tiene el mini PIM T1 instalado en su dispositivo y seleccionó la opción de retransmisión de trama, aparecerán las siguientes ventanas:

- Ventana T1, ficha Physical Layer
- Ventana T1, ficha Frame Relay

NOTA: Si tiene dos mini PIM T1 instalados en su dispositivo y selecciona la opción de conexión múltiple, verá dos fichas Physical Layer.

Figura 29: Ventana T1, ficha Physical Layer

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20 device. At the top, there's a header with the Juniper logo and 'SSG 20'. Below it, a message says: 'Please click the following links or the above figure to configure interfaces.' followed by links: [serial1/0\(Untrust_Zone\)](#), [hgroup0\(Trust_Zone\)](#), and [eth0/1\(DMZ_Zone\)](#).

The main section is titled 'How does the Juniper device connect to the outside via serial1/0(T1) interface?'. It has three radio buttons for 'WAN Encapsulation': ☒ Frame Relay, ☐ PPP, and ☐ Cisco HDLC.

Below this, there are two tabs: 'Physical Layer' (selected) and 'Frame Relay'. The 'Physical Layer' tab contains the following settings:

- Clocking:** ☒ External, ☐ Internal (Lab Use Only)
- Line Buildout:** 0~132 Feet (dropdown menu)
- Line Encoding:** ☐ AMI (Auto Mark Inversion), ☒ B8ZS (8-bits Zero Suppression)
- Byte Encoding:** ☐ 7-bits per byte, ☒ 8-bits per byte
- Frame Checksum:** ☒ 16-bits, ☐ 32-bits
- Framing Mode:** ☐ Super Frame, ☒ Extended Super Frame
- Idle Cycles Flag:** ☒ 0x7E, ☐ 0xFF(All Ones)
- Start/End Flags:** ☒ Filler, ☐ Share
- Invert data:** ☐
- Loopback Respond:** ☐
- Time Slots:** 0 (dropdown menu), (0(all active), 1..24(e.g. 2,7-9))

At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Tabla 14: Campos de la ventana T1, ficha Physical Layer

Campo	Descripción
Clocking	Establece el reloj de transmisión en la interfaz.
Line Buildout	Establece la distancia en la cual una interfaz dirige una línea. El ajuste predeterminado es de 0 a 132 pies.
Line Encoding	Establece el formato de codificación de línea en la interfaz: <ul style="list-style-type: none"> ■ Inversión de marca automática ■ Supresión de cero de 8 bits
Byte Encoding	Establece la codificación de bytes en la interfaz T1 para utilizar 7 bits por byte u 8 bits por byte. El ajuste predeterminado es 8 bits por byte.
Frame Checksum	Establece el tamaño de la suma de comprobación. El ajuste predeterminado es 16 .
Framing Mode	Establece el formato de trama. El ajuste predeterminado es Extended mode .
Idle Cycles Flag	Establece el valor que transmite la interfaz durante los ciclos de inactividad. El ajuste predeterminado es 0x7E : <ul style="list-style-type: none"> ■ 0x7E (indicadores) ■ 0xFF (unos)
Start/End Flags	Establece la transmisión de los indicadores de inicio y final ya sea en lleno o compartido. El ajuste predeterminado es filler .
Casilla Invert Data	Habilita la transmisión invertida de los bits de datos sin utilizar.
Casilla Loopback Respond	Habilita el bucle invertido en la interfaz T1 desde la unidad de servicio del canal remoto (CSU).
Time Slots	Establece el uso de intervalos de tiempo en una interfaz T1. El ajuste predeterminado es 0 , se utilizan los 24 intervalos de tiempo.

Figura 30: Ventana T1, ficha Frame Relay

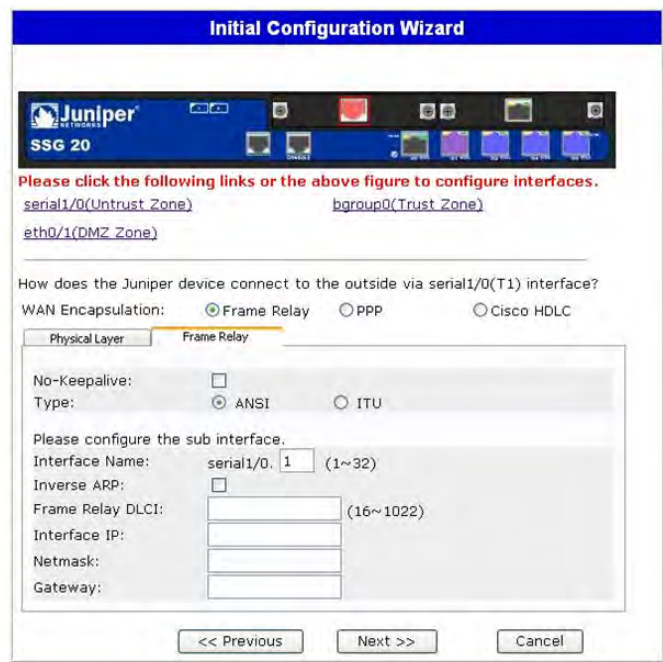


Tabla 15: Campos de la ventana T1, ficha Frame Relay

Campo	Descripción
Casilla No-Keepalive	Habilita la opción sin mantenimientos de conexión.
Type	Establece el tipo de LMI de retransmisión de trama: <ul style="list-style-type: none">■ ANSI: El Instituto nacional de normas de Estados Unidos admite velocidades de datos de hasta 8 Mbps en sentido descendente y 1 Mbps en sentido ascendente.■ ITU: La Unión internacional de telecomunicaciones admite velocidades de datos de 6,144 Mbps en sentido descendente y 640 kbps en sentido ascendente.
Interface Name	Establece el nombre de la subinterfaz.
Inverse ARP	Habilita el protocolo de resolución de direcciones inversas para la subinterfaz.
Frame Relay DLCI	Asigna un identificador de conexión de la conexión de datos (DLCI) a la subinterfaz.
Interface IP	Establece la dirección IP para la subinterfaz.
Netmask	Establece la máscara de red para la subinterfaz.
Gateway	Establece la dirección de la puerta de enlace para la subinterfaz.

Si tiene el mini PIM T1 instalado en su dispositivo y seleccionó la opción PPP, aparecerán las siguientes ventanas adicionales:

- Ventana PPP Option, ficha PPP
- Ventana PPP Option, ficha Peer User

Figura 31: Ventana PPP Option, ficha PPP

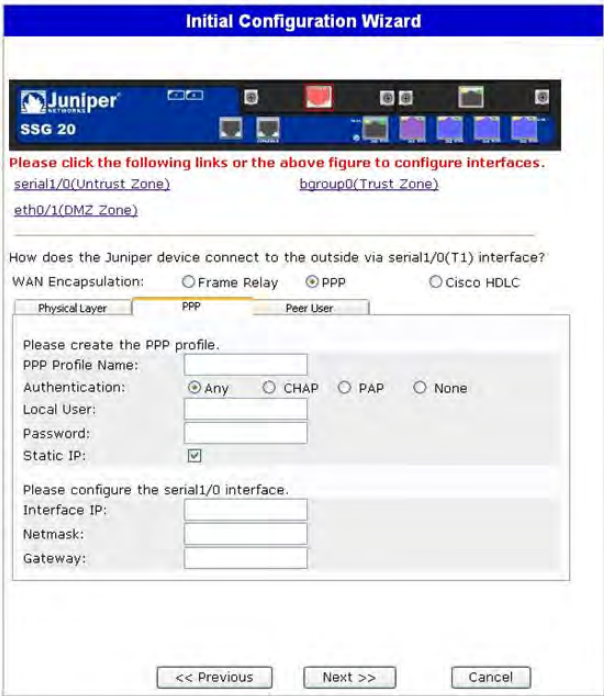


Tabla 16: Campos de la ventana PPP Option, ficha PPP

Campo	Descripción
PPP Profile Name	Establece el nombre del perfil PPP
Authentication	Establece el tipo de autenticación
Local User	Establece el nombre del usuario local
Password	Establece la contraseña del usuario local
Casilla Static IP	Habilita una dirección IP estática
Interface IP	Establece la dirección IP de la interfaz serialx/0
Netmask	Establece la máscara de red serialx/0
Gateway	Establece la dirección de la puerta de enlace serialx/0

Figura 32: Ventana PPP Option, ficha Peer User

Initial Configuration Wizard

Please click the following links or the above figure to configure interfaces.

[serial1/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)

[eth0/1\(DMZ Zone\)](#)

How does the Juniper device connect to the outside via serial1/0(T1) interface?

WAN Encapsulation: ☐ Frame Relay ☒ PPP ☐ Cisco HDLC

Physical Layer **PPP** Peer User

Peer User: []

Password: []

Status: ☒ Enable ☐ Disable


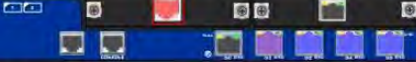
Tabla 17: Campos de la ventana PPP Option, ficha Peer User

Campo	Descripción
Peer User	Establece el nombre del interlocutor
Password	Establece la contraseña para el interlocutor especificado en el campo de texto Peer User
Status	Habilita o deshabilita PPP

Si tiene el mini PIM T1 instalado en su dispositivo y seleccionó la opción Cisco HDLC, aparecerá la siguiente ventana:

Figura 33: Ventana Cisco HDLC Option, ficha Cisco HDLC

Initial Configuration Wizard

Please click the following links or the above figure to configure interfaces.

[serial1/0\(Untrust_Zone\)](#)

[bgroup0\(Trust_Zone\)](#)

[eth0/1\(DMZ_Zone\)](#)

How does the Juniper device connect to the outside via serial1/0(T1) interface?

WAN Encapsulation: ☐ Frame Relay ☐ PPP ☒ Cisco HDLC

Physical Layer
Cisco HDLC

Interface IP:

Netmask:

Gateway:

<< Previous
Next >>
Cancel

Tabla 18: Campos de la ventana Cisco HDLC Option, ficha Cisco HDLC

Campo	Descripción
Interface IP	Establece la dirección IP para la interfaz T1 Cisco HDLC
Netmask	Establece la máscara de red para la interfaz T1 Cisco HDLC
Gateway	Establece la dirección de la puerta de enlace para la interfaz T1 Cisco HDLC

7. Ventanas E1 Interface

Si tiene el mini PIM E1 instalado en su dispositivo y seleccionó la opción de retransmisión de trama, aparecerán las siguientes ventanas:

- Ventana E1, ficha Physical Layer
- Ventana E1, ficha Frame Relay

NOTA: Si tiene dos mini PIM E1 instalados en su dispositivo y selecciona la opción de conexión múltiple, verá dos fichas Physical Layer.

Figura 34: Ventana E1, ficha Physical Layer



Tabla 19: Campos de la ventana E1, ficha Physical Layer

Campo	Descripción
Clocking	Establece el reloj de transmisión en la interfaz.
Frame Checksum	Establece el tamaño de la suma de comprobación. El ajuste predeterminado es 16 .
Framing Mode	Establece el formato de trama. El ajuste predeterminado es without CRC4 .
Idle Cycles Flag	Establece el valor que transmite la interfaz durante los ciclos de inactividad. El ajuste predeterminado es 0x7E : <ul style="list-style-type: none">■ 0x7E (indicadores)■ 0xFF (unos)
Start/End Flags	Establece la transmisión de los indicadores de inicio y final con valor de relleno compartido. El ajuste predeterminado es de relleno .
Casilla Invert Data	Habilita la transmisión invertida de los bits de datos sin utilizar.
Time Slots	Establece el uso de intervalos de tiempo en una interfaz T1. El ajuste predeterminado es 0 , se utilizan los 32 intervalos de tiempo.

Figura 35: Ventana E1, ficha Frame Relay

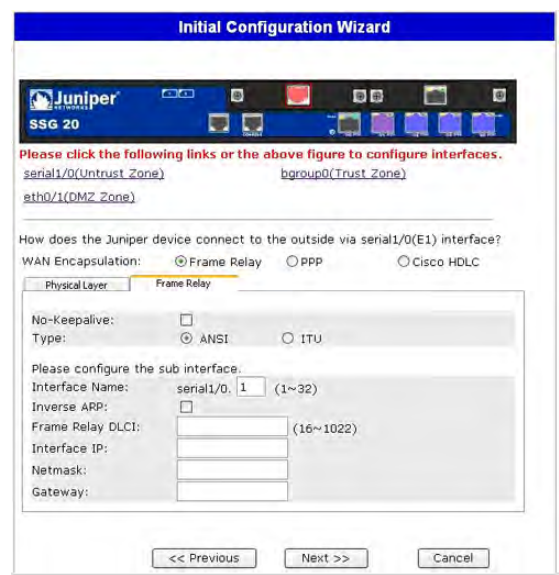


Tabla 20: Campos de la ventana E1, ficha Frame Relay

Campo	Descripción
Casilla No-Keepalive	Habilita la opción sin mantenimientos de conexión.
Type	Establece el tipo de LMI de retransmisión de trama: <ul style="list-style-type: none">■ ANSI: El Instituto nacional de normas de Estados Unidos admite velocidades de datos de hasta 8 Mbps en sentido descendente y 1 Mbps en sentido ascendente.■ ITU: La Unión internacional de telecomunicaciones admite velocidades de datos de 6,144 Mbps en sentido descendente y 640 kbps en sentido ascendente.
Interface Name	Establece el nombre de la subinterfaz.

Campo	Descripción
Casilla Inverse ARP	Habilita el protocolo de resolución de direcciones inversas (ARP) para la subinterfaz.
Frame Relay DLCI	Asigna un DLCI a la subinterfaz.
Interface IP	Establece la dirección IP para la subinterfaz
Netmask	Establece la máscara de red para la subinterfaz
Gateway	Establece la dirección de la puerta de enlace para la subinterfaz

Para configurar la interfaz E1 con las opciones PPP, consulte “Ventana PPP Option, ficha PPP” en la página 71.

Para configurar la interfaz E1 con Cisco HDLC, consulte “Ventana Cisco HDLC Option, ficha Cisco HDLC” en la página 72.

8. Ventanas ISDN Interface

Si tiene el mini PIM de ISDN instalado en su dispositivo, puede configurar la interfaz brix/0 (Untrust) utilizando la ventana siguiente.

NOTA: Si tiene dos mini PIM ISDN instalados en su dispositivo y seleccionó la opción de conexión múltiple, verá dos fichas Physical Layer.

Figura 36: Ventana ISDN, ficha Physical Layer

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20 device. The wizard is titled 'Initial Configuration Wizard' and displays the Juniper logo and 'SSG 20'. Below the title bar, there is a navigation bar with icons for various configuration steps. The main content area is titled 'Please click the following links or the above figure to configure interfaces.' and lists three links: [bri1/0\(Untrust_Zone\)](#), [bgroup0\(Trust_Zone\)](#), and [eth0/1\(DMZ_Zone\)](#). Below the links, there is a question: 'How does the Juniper device connect to the outside via bri1/0 interface?'. There are two checkboxes: 'Leased Line Mode (128Kbps):' and 'Dial Using BRI:'. The 'Physical Layer' tab is selected, and the 'Dialer Interface' tab is also visible. Under the 'Physical Layer' tab, there are several configuration options: 'Switch Type:' with a dropdown menu set to 'European Variants', 'SPID1:' and 'SPID2:' with text input fields and '(Optional)' labels, 'TEI Negotiation:' with radio buttons for 'First Call' (selected) and 'Power UP', 'Calling Number:' with a text input field and '(Optional)' label, and 'Sending Complete:' with a checkbox. At the bottom of the wizard, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Tabla 21: Campos de la ventana ISDN, ficha Physical Layer

Campo	Descripción
Switch Type	Establece el tipo de conmutador del proveedor de servicio: <ul style="list-style-type: none"> ■ att5e: At&T 5ESS ■ ntdms100: Nortel DMS 100 ■ ins-net: NTT INS-Net ■ etsi: European variants ■ ni1: National ISDN-1
SPID1	Un ID del proveedor de servicios es, por lo general, un número telefónico de siete dígitos con algunos números opcionales. Únicamente los tipos de conmutador DMS-100 y NI1 requieren SPID. El tipo de conmutador DMS-100 tiene dos SPID asignados, uno para cada canal B.
SPID2	ID del proveedor de servicio de respaldo.
TEI Negotiation	Especifica cuándo negociar TEI, ya sea al inicio o en la primera llamada. Normalmente, este ajuste se utiliza para las ofertas del servicio RDSI en Europa y conexiones a conmutadores DMS-100 que están designados para iniciar la negociación TEI.
Calling Number	Número de facturación de la red RDSI.
Casilla ending Complete	Habilita el envío de información completa al mensaje de configuración saliente. Por lo general sólo se utiliza en Hong Kong y Taiwán.

Puede seleccionar la interfaz bri1/0 para conectarse por medio del uso de marcador, marcador de conexión múltiple, línea arrendada o marcado con BRI. Si no selecciona ninguna de las opciones, o si selecciona una o ambas, aparecerá una ventana similar a la siguiente.

Figura 37: Ventana ISDN, ficha Connection

Initial Configuration Wizard

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.
[bri1/0\(Untrust_Zone\)](#) [bggroup0\(Trust_Zone\)](#)
[eth0/1\(DMZ_Zone\)](#)

How does the Juniper device connect to the outside via bri1/0 interface?
 Leased Line Mode (128kbps): ☐
 Dial Using BRI: ☐

Physical Layer **Dialer Interface**

Please create the PPP profile.

PPP Profile Name:
 Authentication: ☒ Any ☐ CHAP ☐ PAP ☐ None
 Local User:
 Password:
 Static IP: ☒
 Interface Name: dialer 1
 Encapsulation Type: ☒ ppp ☐ Multi-Link PPP
 Primary Number:
 Alternative Number: (Optional)
 Dialer Pool:
 Interface IP:
 Netmask:
 Gateway:

<< Previous Next >> Cancel

Tabla 22: Campos de la ventana ISDN, ficha Connection

Campo	Descripción
PPP Profile Name	Establece un nombre de perfil PPP en la interfaz ISDN.
Authentication	Establece el tipo de autenticación PPP: <ul style="list-style-type: none"> ■ Ninguna ■ CHAP: Protocolo de autenticación de establecimiento de conexión por desafío ■ PAP: Protocolo de autenticación de contraseña ■ Ninguno
Local User	Establece el usuario local.
Password	Establece la contraseña del usuario local.
Casilla Static IP	Habilita una dirección IP estática para la interfaz.
Interface IP	Establece la dirección IP de la interfaz
Interface Name (Dialer only)	Establece el nombre de la interfaz del marcador. El ajuste predeterminado es dialer.1 .
Encapsulation Type	Establece el tipo de encapsulado en el marcador, y el marcador utilizando la interfaz BRI. El ajuste predeterminado es PPP .
Primary Number	Establece el número principal para el marcador, y el marcador utilizando las interfaces BRI.

Campo	Descripción
Alternative Number	Establece el número alternativo (secundario) a utilizar cuando el número principal no se pueda utilizar para la conectividad.
Dialer Pool (Dialer only)	Establece el nombre del conjunto de marcador para la interfaz de marcador.
Netmask	Establece la máscara de red.
Gateway	Establece la dirección de la puerta de enlace.

9. Ventana V.92 Modem Interface

Si tiene el mini PIM V.92 instalado en su dispositivo, puede configurar la interfaz serialx/0 (módem) por medio de la siguiente ventana:

Figura 38: Ventana Modem Interface



Tabla 23: Campos de la ventana Modem Interface

Campo	Descripción
Modem Name	Establece el nombre para la interfaz de módem
Init String	Establece la cadena de inicialización para el módem
ISP Name	Asigna un nombre al proveedor de servicios
Primary Number	Especifica el número telefónico para obtener acceso al proveedor de servicios
Alternative Number (optional)	Especifica un número telefónico alternativo para obtener acceso al proveedor de servicios si el número principal no conecta
Login Name	Establece el nombre de inicio de sesión para la cuenta del proveedor de servicios
Password	Establece la contraseña para el nombre de inicio de sesión
Confirm	Confirma la contraseña introducida en el campo Password

10. Ventana Eth0/0 Interface (Untrust Zone)

La interfaz eth0/0 puede tener una dirección IP estática o dinámica, asignada a través de DHCP o PPPoE.

Figura 39: Ventana Eth0/0 Interface



Tabla 24: Campos de la ventana Eth0/0 Interface

Campo	Descripción
Dynamic IP via DHCP	Habilita el dispositivo para que reciba una dirección IP para la interfaz de zona Untrust desde un proveedor de servicios.
Dynamic IP via PPPoE	Habilita el dispositivo para que actúe como un cliente PPPoE, recibiendo una dirección IP para la interfaz de zona Untrust desde un proveedor de servicios. Introduzca el nombre de usuario y la contraseña que el proveedor de servicio asignó.
Static IP	Asigna una dirección IP única y fija a la interfaz de zona Untrust. Introduzca la dirección IP de interfaz de zona Untrust, máscara de red y dirección de puerta de enlace.

11. Ventana Eth0/1 Interface (DMZ Zone)

La interfaz eth0/1 puede tener una dirección IP estática o dinámica asignada a través de DHCP.

Figura 40: Ventana Eth0/1 Interface

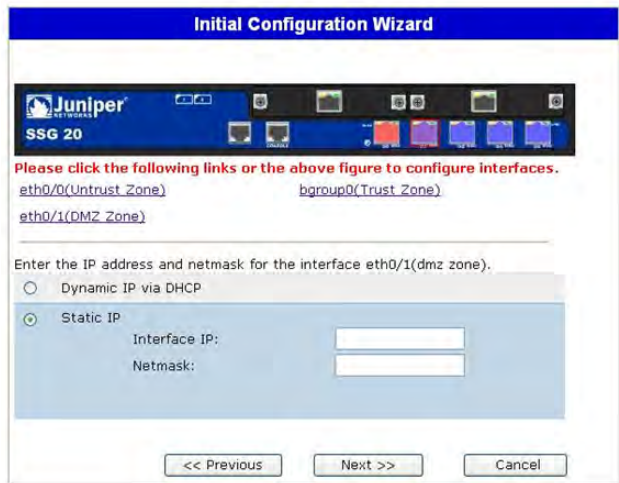


Tabla 25: Campos de la ventana Eth0/1 Interface

Campo	Descripción
Dynamic IP via DHCP	Habilita el dispositivo para que reciba una dirección IP para la interfaz DMZ desde un proveedor de servicios.
Static IP	Asigna una dirección IP única y fija a la interfaz DMZ. Introduzca IP de interfaz DMZ y máscara de red.

12. Ventana Bgroup0 Interface (Trust Zone)

La interfaz bgroup0 puede tener una dirección IP estática o dinámica asignada a través de DHCP.

La dirección IP de la interfaz predeterminada es **192.168.1.1** con una máscara de red de **255.255.255.0** ó **24**.

Figura 41: Ventana Bgroup0 Interface



Tabla 26: Campos de la ventana Bgroup0 Interface

Campo	Descripción
Dynamic IP via DHCP	Habilita el dispositivo para que reciba una dirección IP para la interfaz de zona Trust desde un proveedor de servicios.
Static IP	Asigna una dirección IP única y fija a la interfaz de zona Trust. Introduzca la dirección IP de interfaz de zona Trust y máscara de red.

13. Ventana Wireless0/0 Interface (Trust Zone)

Si está configurando el dispositivo SSG 20-WLAN, debe establecer un identificador de conjunto de servicios (SSID) para que la interfaz wireless0/0 se pueda activar. Para obtener instrucciones detalladas acerca de la configuración de sus interfaces inalámbricas, consulte el *Manual de referencia de ScreenOS: Conceptos y ejemplos*.

Figura 42: Ventana Wireless0/0 Interface

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20 device. At the top, there's a header with the Juniper logo and 'SSG 20'. Below it, a red text prompt says 'Please click this wlan radio to configure wireless.' with a small icon of a wireless radio. A toolbar contains various icons for configuration. Below the toolbar, a red text prompt says 'Please click the following links or the above figure to configure interfaces.' followed by four links: [eth0/0\(Untrust_Zone\)](#), [hgroup0\(Trust_Zone\)](#), [eth0/1\(DMZ_Zone\)](#), and [wireless0/0\(Trust_Zone\)](#). The main section is titled 'How do you want to configure wireless0/0 interface(trust zone)?'. It includes a 'Wlan Mode:' dropdown set to '2.4G(802.11b/g)'. Below this is an 'SSID:' text field. There are two main radio buttons: 'Open' (selected) and 'WPA-PSK'. Under 'Open', there's a 'No Encryption' option. Under 'WPA-PSK', there are three options: 'Passphrase(8~63 ASCII):' (selected), 'PSK(64 hexadecimal):', and 'Encryption Type:' with radio buttons for 'Auto' (selected), 'TKIP', and 'AES'. Each of these options has a 'Confirm:' field. At the bottom, there are 'Interface IP:' and 'Netmask:' text fields with values '192.168.2.1' and '255.255.255.0' respectively. Navigation buttons at the bottom are '<< Previous', 'Next >>', and 'Cancel'.

Tabla 27: Campos de la ventana Wireless0/0 Interface

Campo	Descripción
Wlan Mode	Configure el modo de radio WLAN: <ul style="list-style-type: none"> ■ 5G (802.11a). ■ 2.4G (802.11b/g). ■ Ambos (802.11a/b/g).
SSID	Establece el nombre de SSID.
Authentication and Encryption	Establece la autenticación y encriptación de la interfaz WLAN: <ul style="list-style-type: none"> ■ La autenticación open, el ajuste predeterminado, permite que cualquier persona tenga acceso al dispositivo. No hay encriptación para esta opción de autenticación. ■ La autenticación WPA Pre-Shared Key establece la clave previamente compartida (PSK) o contraseña que debe introducir al acceder a una conexión inalámbrica. Puede elegir introducir un valor HEX o ASCII para la PSK. Una PSK HEX debe ser un valor HEX de 256 bits (64 caracteres de texto). Una contraseña ASCII debe tener de 8 a 63 caracteres de texto. Debe seleccionar el protocolo de integridad de clave temporal (TKIP) o estándar de encriptación avanzada (AES) como el tipo de encriptación para esta opción, o bien seleccione Auto para utilizar cualquiera de las opciones. ■ Clave previamente compartida WPA2. ■ Clave previamente compartida automática WPA.
Interface IP	Establece la dirección IP de la interfaz WLAN.
Netmask	Establece la máscara de red de la interfaz WLAN.

14. Ventana Interface Summary

Después de configurar las interfaces WAN, verá la ventana Interface Summary.

Figura 43: Ventana Interface Summary

Initial Configuration Wizard

Before proceeding further, review the following interface settings.

ISDN Configuration:			
Switch Type:	etsi		
SPID1:	32546564565	SPID2:	23488458235
TEI Negotiation:	first call	Calling Number:	01023456789
T310 Value:	10	Sending Complete:	enabled
Leased Line Mode:	disabled	Dialer Enable:	disabled
PPP Profile:	myprofile	Authentication:	any
Local User:	myuser	Password:	mypwd
PPP Static IP:	enabled	Interface IP:	122.122.122.122

```

set interface bril/0 isdn switch-type etsi
set interface bril/0 isdn spid1 "32546564565"
set interface bril/0 isdn spid2 "23488458235"
set interface bril/0 isdn tei-negotiation first-call
set interface bril/0 isdn calling-number "01023456789"
set interface bril/0 isdn t310-value "10"

```

Click Next to enter other configuration

<< Previous Next >> Cancel

Revise la configuración de su interfaz, luego haga clic en **Next** cuando esté listo para continuar. Aparece la ventana Physical Ethernet DHCP Interface.

15. Ventana Physical Ethernet DHCP Interface

Seleccione **Yes** para que su dispositivo pueda asignar direcciones IP a su red de cables a través de DHCP. Introduzca el rango de dirección IP que desea que su dispositivo asigne a los clientes utilizando su red, luego haga clic en **Next**.

Figura 44: Ventana Physical Ethernet DHCP Interface

The screenshot shows a window titled "Initial Configuration Wizard". The text inside asks: "Do you want the Juniper device to dynamically assign IP addresses to your local **wired** hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses." There are two radio buttons: "Yes" and "No". The "No" button is selected. Below the "Yes" option, there are input fields for "IP Address Range Start" (192.168.1.33), "End" (192.168.1.126), "DNS Server 1 (optional)", and "DNS Server 2 (optional)". At the bottom, there are three buttons: "<< Previous", "Next >>", and "Cancel".

16. Ventana Wireless DHCP Interface

Seleccione **Yes** para que su dispositivo pueda asignar direcciones IP a su red inalámbrica a través de DHCP. Introduzca el rango de dirección IP que desea que su dispositivo asigne a los clientes por medio de su red, luego haga clic en **Next**.

Figura 45: Ventana Wireless DHCP Interface

The screenshot shows a window titled "Initial Configuration Wizard". The text inside asks: "Do you want the Juniper device to dynamically assign IP addresses to your local **wireless** hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses." There are two radio buttons: "Yes" and "No". The "No" button is selected. Below the "Yes" option, there are input fields for "IP Address Range Start" (192.168.2.33), "End" (192.168.2.126), "DNS Server 1 (optional)", and "DNS Server 2 (optional)". At the bottom, there are three buttons: "<< Previous", "Next >>", and "Cancel".

17. Ventana Confirmation

Confirma la configuración de su dispositivo y permite cambiarla según sea necesario. Haga clic en **Next** para guardar, reiniciar el dispositivo y ejecutar la configuración.

Figura 46: Ventana Confirmation

Initial Configuration Wizard

Before proceeding further, review the following all device settings.

Admin Login:	netscreen	Password:	*****
Device is in NAT mode.			
ISDN Configuration:			
Switch Type:	etsi	SPID2:	23488458235
SPID1:	32546564565	TEI Negotiation:	first call
TEI Negotiation:	first call	Calling Number:	01023456789
T310 Value:	10	Sending Complete:	enabled
Leased Line Mode:	disabled	Dialer Enable:	disabled
PPP Profile:	myprofile	Authentication:	any

```

set admin password "netscreen"
set interface bri1/0 isdn switch-type etsi
set interface bri1/0 isdn spid1 "32546564565"
set interface bri1/0 isdn spid2 "23488458235"
set interface bri1/0 isdn tei-negotiation first-call
set interface bri1/0 isdn calling-number "01023456789"
  
```

Click Next to save CLI into device.

<< Previous Next >> Cancel

Después de que el dispositivo se reinicie con la configuración del sistema almacenada, aparece el mensaje de petición de inicio de sesión de WebUI. Para obtener información sobre la manera de obtener acceso al dispositivo utilizando la WebUI, consulte “Utilización de la WebUI” en la página 29.

Índice

A

Actualización de memoria, procedimiento	54
Administración	
a través de la WebUI	29
a través de una conexión de Telnet	30
a través de una consola	28
ADSL	
conexión al puerto	24
conexión del cable	24
configuración de la interfaz	41
Anexo A	24
Anexo B	24
antenas	26

C

Cables	
conexiones de red básica	23
serie	24
cables	
ADSL	24
Capa de adaptación ATM 5	41
Certificaciones	
EMC (emisiones)	59
inmunidad EMC	59
Instituto Europeo de Normas en Telecomunicaciones (ETSI)	59
interfaz T1	60
seguridad	59
Conexión, red básica	23
Configuración	
acceso administrativo	35
autenticación inalámbrica y encriptación	38
circuitos virtuales	42
dirección de administración	36
fecha y hora	34
grupos en puente (bgroup)	34
inalámbrica y Ethernet combinadas	40
interfaz untrust de respaldo	37
Mini PIM ADSL 2/2 +	41
mini PIM de módem V.92	47
Mini PIM E1	46
Mini PIM RDSI	45
Mini PIM T1	46
nombre de administrador y contraseña	33
nombre de host y dominio	36

par VPI/VCI	42
ruta predeterminada	36
servicios de administración	35
USB	17

D

Dirección IP de ISP y máscara de red	44
Dirección IP estática	41
Direcciones IP predeterminadas	32

I

Identificador de trayecto virtual/Identificador de canal virtual	
<i>Véase</i> VPI/VCI	
inalámbrico	
antenas	26
utilización de la interfaz predeterminada	26
Interfaz de respaldo en la zona Untrust	37

L

LED	
conexión de actividad en puertos Ethernet	13
PIM 1	12
PIM 2	12
POWER (alimentación)	12
STATUS (estado)	12
LED de WLAN	
802.11a	12
b/g	12

M

Mini PIM	
desinstalación	52
instalación	53
placa frontal	52
Multiplexado AAL5	41
Multiplexado, configuración	42

P

PPPoA	41
PPPoE	41
Protocolo punto a punto a través de ATM	
<i>Véase</i> PPPoA	
Protocolo punto a punto a través de Ethernet	
<i>Véase</i> PPPoE	

R

Restablecimiento, uso del orificio 49

T

Transceptores de radio

WLAN 0..... 16

WLAN 1..... 16

V

VPI/VCI

configuración 42

valores..... 41

Z

Zona Untrust, configuración de la interfaz

de respaldo..... 37

目次

	本ガイドについて	5
	構成	6
	WebUI 使用上の注意	6
	CLI 使用上の注意	7
	ドキュメントとテクニカルサポートの問い合わせ	7
第 1 章	ハードウェアの概要	9
	ポートと電源のコネクタ	9
	フロントパネル	10
	システムステータス LED	10
	ポート	12
	イーサネットポート	12
	コンソールポート	13
	AUX ポート	13
	ミニ物理インターフェースモジュールポート	13
	バックパネル	15
	電源アダプタ	15
	無線トランシーバ	15
	接地ラグ	16
	アンテナのタイプ	16
	USB ポート	16
第 2 章	SSG 20 の取り付けと接続	17
	使用準備	17
	機器の設置	18
	SSG 20 とインターフェースケーブルの接続	19
	電源の接続	19
	ネットワークと SSG 20 の接続	20
	SSG 20 と Untrust ネットワークの接続	20
	イーサネットポート	21
	シリアル (AUX/ コンソール) ポート	21
	Mini PIM と Untrust ネットワークの接続	21
	ADSL2/2 + Mini PIM	21
	ISDN、T1、E1、V.92 Mini PIM	22
	SSG 20 と内部ネットワークまたはワークステーションとの接続	22
	イーサネットポート	22
	ワイヤレスアンテナ	23

第 3 章	SSG 20 の構成	25
	SSG 20 のアクセス.....	26
	コンソール接続の使用	26
	WebUI の使用.....	27
	Telnet の使用.....	28
	SSG 20 のデフォルト設定	29
	SSG 20 の基本構成.....	31
	ルート管理者名とパスワード	31
	日付と時刻	31
	ブリッジグループインターフェース	32
	管理アクセス	33
	管理サービス	33
	ホスト名とドメイン名	33
	デフォルトルート	34
	管理インターフェースのアドレス	34
	バックアップ Untrust インターフェースの構成	34
	基本ワイヤレス構成	35
	Mini PIM 構成	39
	ADSL2/2+ インターフェース	39
	仮想回路.....	39
	VPI/VCI と複合方式	40
	PPPoE または PPPoA	41
	静的 IP アドレスおよびネットマスク	42
	ISDN インターフェース	43
	T1 インターフェース	43
	E1 インターフェース	44
	V.92 モデム インターフェース	45
	基本的ファイアウォール保護	46
	外部との接続性の確認	46
	SSG 20 の出荷時のデフォルト設定へのリセット	46
第 4 章	SSG 20 の点検	49
	必要なツールとパーツ	49
	ミニ物理インターフェースモジュールの交換	49
	ブランク面板の取り外し	50
	Mini PIM の取り外し	50
	Mini PIM の取り付け	51
	メモリのアップグレード	52
付録 A	仕様	55
	物理的仕様.....	55
	電氣的仕様.....	55
	環境耐性	56
	保証.....	56
	安全性	56
	EMC エミッション.....	56
	EMC (イミュニティ)	56
	ETSI	57
	T1 インターフェース	57
	コネクタ	57

付録 B	Initial Configuration Wizard （初期構成ウィザード）	59
	索引	83

本ガイドについて

Juniper Networks Secure Services Gateway (SSG) 20 は統合ルーター / ファイアウォールプラットフォームであり、支店や販売店向けのインターネットプロトコルセキュリティ (IPSec) 仮想プライベートネットワーク (VPN) とファイアウォールサービスを提供します。

SSG 20 には、次の 2 つの モデルがあります。

- SSG 20: 補助 (AUX) 接続をサポートします。
- SSG 20-WLAN: 統合 802.11a/b/g ワイヤレス標準をサポートします。

どちらの SSG 20 モデルもユニバーサルシリアルバス (USB) ストレージと、あらゆる Mini PIM を収容できるミニ物理インターフェースモジュール (PIM) スロットを 2 スロットサポートしています。SSG 20 モデルはローカルエリアネットワーク (LAN) とワイドエリアネットワーク (WAN) 間のプロトコル変換もサポートしています。

メモ： 本書で紹介する構成手順と例では、ScreenOS 5.4 で SSG 20 を実行したときの機能を基準としています。使用する ScreenOS バージョンによっては、SSG 20 の機能が異なることがあります。SSG 20 の最新ドキュメントについては、<http://www.juniper.net/techpubs/hardware> の Juniper Networks Technical Publications Web サイトを参照してください。お手元の SSG 20 に、使用できるどの ScreenOS バージョンについては、<http://www.juniper.net/customers/support/> の Juniper Networks Support Web サイトを参照してください。

構成

本ガイドは次の章で構成されています。

- 第 1 章、「ハードウェアの概要」では、SSG 20 のシャーシとコンポーネントについて説明します。
- 第 2 章、「SSG 20 の取り付けと接続」では、SSG 20 の取り付け方法と、ケーブルと電源の接続方法を説明します。
- 第 3 章、「SSG 20 の構成」では、SSG 20 の構成方法と管理方法、および基本的な構成作業の方法を説明します。
- 第 4 章、「SSG 20 の点検」では、SSG 20 のサービスとメンテナンス手順について説明します。
- 付録第 A 章、「仕様」では、SSG 20 の一般的なシステム仕様を紹介します。
- 付録 B、「Initial Configuration Wizard（初期構成ウィザード）」では、SSG 20 用の ICW (Initial Configuration Wizard) の使用方法を紹介します。

WebUI 使用上の注意

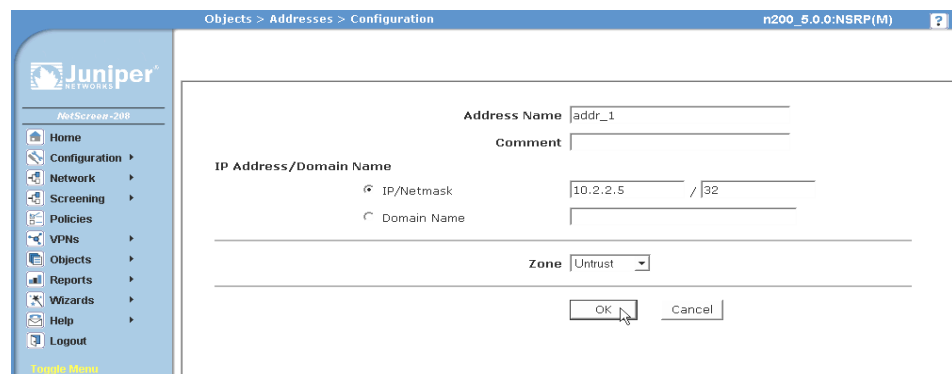
WebUI で作業を行うには、まず目的のダイアログボックスを呼び出してオブジェクトを定義し、パラメータを設定します。シェvron (>) は、WebUI でメニューオプションやリンクをクリックする操作手順を示します。各作業の操作指示は、操作手順と構成設定値に分かれています。

次に、アドレス構成ダイアログボックスを呼び出すための手順と構成設定値の例を示します。

Objects > Addresses > List > New: 次のように入力してから **OK** をクリックします。

Address Name: addr_1
 IP Address/Domain Name:
 IP/Netmask: (選択), 10.2.2.5/32
 Zone: Untrust

図 1: 操作手順と構成設定値



CLI 使用上の注意

次の規則は、例や本文中で CLI コマンド構文を使用するときの表記に適用します。

例では、次のように表記します。

- 角括弧 [] 内はすべてオプションです。
- 中括弧 { } 内はすべて必須です。
- 選択肢が複数ある場合、選択肢同士はパイプ (|) で区切ります。例：

```
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。

- 変数は斜体で表示します。

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

本文では、次のように表記します。

- コマンドは太字で表記します。
- 変数は斜体で表記します。

メモ： キーワードは、一意の識別に必要なだけの文字数を入力すればあとは省略できます。たとえば、コマンド **set admin user kathleen j12fmt54** は、**set adm u kath j12fmt54** と入力するだけですべて画面に表示されます。コマンド入力にはこのショートカットが使用できますが、本書で紹介するコマンドはすべて完全な形式で記載しています。

ドキュメントとテクニカルサポートの問い合わせ

Juniper Networks 製品のテクニカルドキュメントの入手方法については、www.juniper.net/techpubs/ を参照してください。

テクニカルサポートについては、<http://www.juniper.net/support/> にある Case Manager リンクでサポート事例を開くか、1-888-314-JTAC（米国内）または 1-408-745-9500（その他の国）までお問い合わせください。

本書に間違いや欠落があった場合は、次の E メールアドレスまでお知らせください。

techpubs-comments@juniper.net

第 1 章 ハードウェアの概要

本章では、SSG 20 シャーシとそのコンポーネントについて解説します。本章は、以下の節で構成されています。

- 9 ページの「ポートと電源のコネクタ」
- 10 ページの「フロントパネル」
- 15 ページの「バックパネル」

ポートと電源のコネクタ

本節では、内蔵ポートと電源のコネクタの解説とともにその配置を示します。内蔵ポートの配置と表 1 電源コネクタについては次の図を参照してください。

図 2: 内蔵ポートと Mini PIM の配置

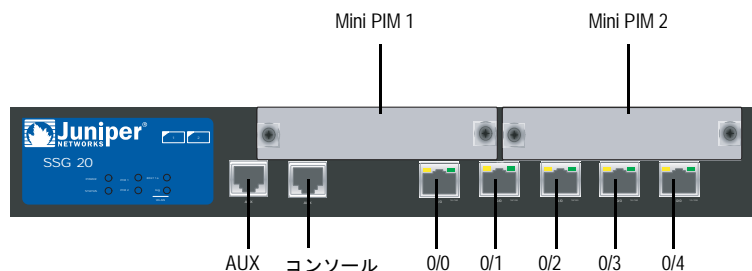


図 1: SSG 20 のポートと電源コネクタ

ポート	説明	コネクタ	速度 / プロトコル
0/0-0/4	ワークステーションとの直接接続またはスイッチやハブ経由の LAN 接続用のポートです。このポートでは Telnet セッションや WebUI で SSG 20 を管理することもできます。	RJ-45	10/100 Mbps イーサネット オートセンシング全二重と自動 MDI/MDIX
USB	システムとの 1.1 USB 接続用のポートです。	該当なし	12M（全速時）または 1.5M（低速時）
コンソール	システムとのシリアル接続用のポートです。CLI セッションを起動するターミナルエミュレーション接続に使用します。	RJ-45	9600 bps/RS-232C シリアル
AUX	外部モデム経由によるバックアップ RS-232 非同期シリアルインターネット接続用のポートです。	RJ-45	9600 bps — 115 Kbps/RS-232C シリアル

ポート	説明	コネクタ	速度 / プロトコル
Mini PIM			
ADSL 2/2 +	ADSL データリンク経由のインターネット接続用のポートです。	RJ-11 (Annex A) RJ-45 (Annex B)	ANSI T1.413 Issue 2 (Annex A のみ) ITU G.992.1 (G.dmt) ITU G.992.3 (ADSL2) ITU G.992.5 (ADSL2+)
V.92 モデム	サービスプロバイダとの、パリティまたはバックアップインターネット接続または Untrust ネットワークとの接続用のポートです。	RJ-11	9600 bps — 115 Kbps/RS-232 シリアル オートセンシング二重と極性
T1	T1 回線経由の Untrust ネットワークとの接続用のポートです。	RJ-45	1.544 Mbps (フルタイムスロット)
E1	E1 回線経由の Untrust ネットワークとの接続用のポートです。	RJ-45	2.048 Mbps (フルタイムスロット)
ISDN	ISDN 回線を Untrust インターフェースまたはバックアップインターフェースとして利用するためのポートです。(S/T)	RJ-45	64 Kbps B チャンネル 128 Kbps 専用回線
アンテナ A と B (SSG 20-WLAN)	ワイヤレス無線接続近隣のワークステーションとの直接接続用のポートです。	RPSMA	802.11a (5GHz 無線バンドで 54 Mbps) 802.11b (2.4 GHz 無線バンドで 11 Mbps) 802.11g (2.4 GHz 無線バンドで 54 Mbps) 802.11 superG (2.4 GHz および 5GHz 無線バンドで 108 Mbps)

フロントパネル

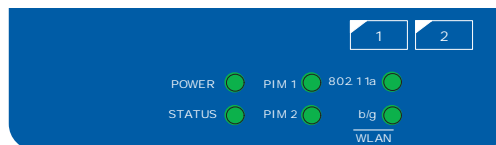
この節では、SSG 20 のフロントパネル上の次の要素について説明します。

- システムステータス LED
- ポート
- ミニ物理インターフェースモジュールポート

システムステータス LED

通常、システムステータス LED は、SSG 20 の重要機能に関する情報を表示します。図 3 は、SSG 20-WLAN のフロントパネル上の各ステータス LED の配置です。WLAN LED は、SSG 20-WLAN 専用の LED です。

図 3: ステータス LED



システムの電源を入れると、消灯していた POWER LED が緑で点滅し始め、STATUS LED は赤、緑、緑の点滅という順序で変化します。起動に約 2 分かかります。システムの電源をいったん切って、再び投入するときは、電源を切ってから 2、3 分待って電源を投入してください。表 2 は、各システムステータス LED の名前、色、ステータス、説明をまとめた表です。

表 2: ステータス LED

名前	色	ステータス	説明
POWER	緑	点灯	システムに電源が供給中であることを示します。
		消灯	システムに電源が供給されていないことを示します。
	赤	点灯	SSG 20 が正常に機能していないことを示します。
		消灯	SSG 20 が正常に機能していることを示します。
STATUS	緑	点灯	システムが起動中か、診断実施中であることを示します。
		点滅	SSG 20 が正常に機能していることを示します。
	赤	点滅	エラーが検出されたことを示します。
PIM 1	緑	点灯	Mini PIM が機能していることを示します。
		点滅	Mini PIM がトラフィックを中継中であることを示します。
		消灯	Mini PIM が停止していることを示します。
PIM 2	緑	点灯	Mini PIM が機能していることを示します。
		点滅	Mini PIM がトラフィックを中継中であることを示します。
		消灯	Mini PIM が停止していることを示します。
WLAN (WLAN SSG 20 専用)			
802.11a	緑	点灯	ワイヤレス接続は成立していますが、リンクアクティビティがないことを示します。
		低速点滅	ワイヤレス接続が成立していることを示します。ボーレートはリンクアクティビティと比例します。
		消灯	ワイヤレス接続が成立していないことを示します。
b/g	緑	点灯	ワイヤレス接続は成立していますが、リンクアクティビティがないことを示します。
		低速点滅	ワイヤレス接続が成立していることを示します。ボーレートはリンクアクティビティと比例します。
		消灯	ワイヤレス接続が成立していないことを示します。

ポート

この節では、次のポートの目的と機能を説明します。

- イーサネットポート
- コンソールポート
- AUX ポート

イーサネットポート

5 箇所の 10/100 イーサネットポートで、ハブ、スイッチ、ローカルサーバー、ワークステーションに LAN 接続を提供します。また、管理トラフィック用にイーサネットポートを指定することもできます。ポートのラベルは **0/0** から **0/4** です。各イーサネットポートのデフォルトゾーンバインディングについては、29 ページの「SSG 20 のデフォルト設定」を参照してください。

ポートのどれかを構成するときは、ポート位置に対応するインターフェース名を確認してください。フロントパネルの左から右に、ポートのインターフェース名は、**ethernet0/0** から **ethernet0/4** となっています。

図 4 は、各イーサネットポートの LED の場所を示します。

図 4: アクティビティリンク LED の場所

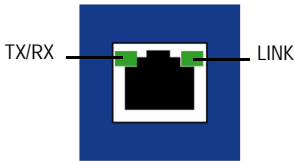


表 3 は、イーサネットポート LED の解説をまとめたものです。

表 3: LAN ポート LED

名前	色	ステータス	説明
LINK	緑	点灯 消灯	ポートがオンラインです。 ポートがオフラインです。
TX/RX	緑	点滅 消灯	トラフィックを中継中です。ボーレートはリンク アクティビティと比例します。 ポートがアクティブの可能性はありますが、デー タは受信していません。

コンソールポート

コンソールポートは、ローカル管理に使用できるデータ回路終端装置（DCE）として配線した RJ-45 シリアルポートです。ターミナル接続にはストレートケーブルを使用し、別の DCE 装置を追加するときはクロスオーバーケーブルを使用してください。RJ-45 対 DB-9 のアダプタを用意しています。

RJ-45 コネクタのピン配列については、57 ページの「コネクタ」を参照してください。

AUX ポート

補助（AUX）ポートは、RJ-45 シリアルポートです。リモート管理のためにモデムに接続できるデータターミナル装置（DTE）として配線されています。通常のリモート管理には、このポートを使用しないでください。AUX ポートは通常バックアップシリアルインターフェースとして割り当てます。ボーレートは、9600 bps から 115200 bps の範囲で調節できます。ハードウェアフロー制御が必要です。モデムに接続するときはストレートケーブルを使用し、別の DTE 装置を追加するときはクロスオーバーケーブルを使用してください。

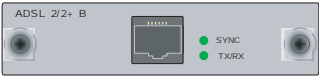
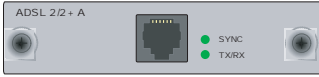




RJ-45 コネクタのピン配列については、57 ページの「コネクタ」を参照してください。

ミニ物理インターフェースモジュールポート

SSG 20 でサポートしているミニ物理インターフェースモジュール（PIM）には、それぞれのコンポーネントがあります。

- ケーブルコネクタポート 1 翼 | ネットワークメディアコネクタを接続します。図5 は利用できる Mini PIM をまとめたものです。Mini PIM は、SSG 20 ごとに最大 2 基を装着できます。

図 5: SSG 20 の Mini PIM

	ADSL2/2+ Annex B
	ADSL2/2+ Annex A
	ISDN BRI
	T1
	E1
	V.92

- 2 つから 3 つのステータス LED 翼 | ートステータスを示します。表 4 は、LED 状態の意味をまとめたものです。

表 4: SSG 20 の Mini PIM LED の状態

タイプ	名前	色	状態	説明
ADSL 2/2 + (Annex A と B)	SYNC	緑	点灯	ADSL インターフェースがトレーニング中であることを示します。
			点滅	トレーニングが進行中であることを示します。
			消灯	インターフェースがアイドル状態であることを示します。
	TX/RX	緑	点滅	トラフィックが中継中であることを示します。
			消灯	中継中のトラフィックがないことを示します。
ISDN (BRI)	CH B1	緑	点灯	B-Channel 1 がアクティブであることを示します。
			消灯	B-Channel 1 がアクティブでないことを示します。
	CH B2	緑	点灯	B-Channel 2 がアクティブであることを示します。
			消灯	B-Channel 2 がアクティブでないことを示します。
T1/E1	ALARM	黄	点灯	ローカルアラームまたはリモートアラームがあることを示します。SSG 20 が障害を検出しました。
			消灯	アラームや障害がないことを示します。
	LOOP BACK	黄	点灯	ループバックまたは回線の状態が検出されたことを示します。
			消灯	ループバックがアクティブでないことを示します。
	CD	緑	点灯	キャリアが検出され、Mini PIM の内部 DSU/CSU が別の DSU/CSU と通信中であることを示します。
			消灯	キャリア検出がアクティブでないことを示します。
	V.92	緑	点灯	リンクがアクティブであることを示します。
			消灯	シリアルインターフェースが停止していることを示します。
	TX/RX	緑	点滅	トラフィックが中継中であることを示します。
			消灯	中継中のトラフィックがないことを示します。



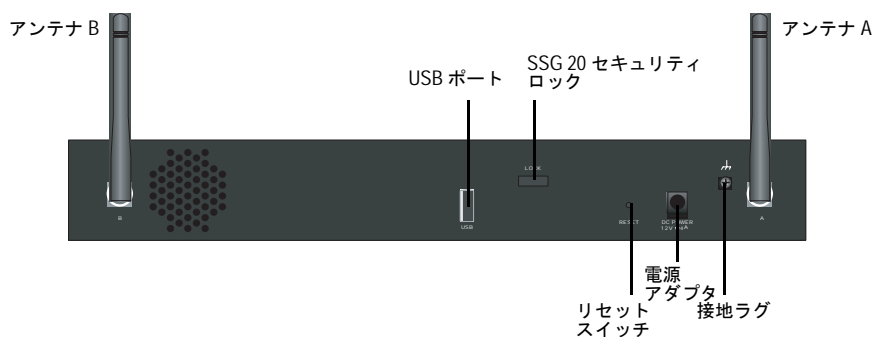
注意: Mini PIM はホストスワップابلではありません。SSG 20 の電源は、Mini PIM を装着してから入れてください。

バックパネル

この節では、SSG 20 のバックパネル上の次の要素について説明します。

- 電源アダプタ
- 無線トランシーバ
- 接地ラグ
- アンテナのタイプ
- USB ポート

図 6: SSG 20-WLAN のバックパネル



電源アダプタ

SSG 20 のフロントパネルの POWER LED のステータスは、緑に点灯しているか消灯しているかのいずれかです。緑に点灯しているときは正常に機能していることを示し、消灯しているときは電源アダプタに障害があるか、SSG 20 の電源が入っていないことを示します。

無線トランシーバ

SSG 20-WLAN には、2 基のワイヤレス接続無線トランシーバが組み込まれており、802.11a/b/g の各標準に準拠しています。最初のトランシーバ (WLAN 0) は 2.4 GHz 無線バンドを使用します。これは、11 Mbps で 802.11b 標準に、54 Mbps で 802.11g 標準に、そして 108 Mbps で 802.11 SuperG に準拠しています。第 2 の無線トランシーバ (WLAN 1) は、5GHz 無線バンドを使用します。これは、54 Mbps で 802.11a 標準に準拠しています。ワイヤレス無線バンドの構成方法については、35 ページの「基本ワイヤレス構成」を参照してください。

接地ラグ

シャーシのバックパネルにはワンホール接地ラグがあり、これで SSG 20 をアース接地に接続します (図 6 参照)。

電源投入前に SSG 20 を接地するには、接地ケーブルをアース接地に接続し、シャーシのバックパネルのラグにケーブルを接続します。

アンテナのタイプ

SSG 20-WLAN は、3 タイプのカスタムビルド無線アンテナをサポートしています。

- **ダイバーシティーアンテナ** — ダイバーシティーアンテナは 2dBi の指向性有効範囲を備え、範囲内では極めて均一レベルの信号強度を発揮でき、ほとんどのインストレーションに最適です。SSG 20 に同梱のアンテナはこのタイプです。
- **外部無指向性アンテナ** — この外部アンテナは 2dBi の無指向性有効範囲を備えています。ペアで使用するダイバーシティーアンテナとは異なり、2 つのタイプのアンテナの使用時の外部アンテナの目的は信号受信時の若干の遅延特性に起因するエコー効果を排除することです。
- **外部指向性アンテナ** — 外部指向性アンテナは、2dBi の単一指向性の有効範囲を備えています。通路や外壁のある場所に最適です (アンテナは内側に向けます)。

USB ポート

CompactFlash Association が公開している *CompactFlash Specification* に定められているように、SSG 20 のバックパネルの USB ポートには、ユニバーサルシリアルバス (USB) ストレージデバイスまたはコンパクトフラッシュディスクをインストールした USB ストレージアダプタを接続します。USB ストレージデバイスをインストールして構成しておけば、スタートアップ時にプライマリコンパクトフラッシュディスクに障害が発生しても、USB ストレージデバイスは自動的にセカンダリブートデバイスとして機能します。

USB ポートでは、外部 USB ストレージデバイスとセキュリティデバイス内にある内部フラッシュストレージ間で、デバイス構成、ユーザー認証、アップデートバージョンイメージなどのファイルを転送できます。USB ポートは、低速 (1.5M) と全速 (12M) のいずれのファイル転送でも USB 1.1 仕様をサポートしています。

USB ストレージデバイスと SSG 20 間のファイル転送手順を次に示します。

1. セキュリティデバイスの USB ポートに USB ストレージデバイスを挿入します。
2. **save {software | config | image-key} from usb filename to flash** CLI コマンドで、USB ストレージデバイスから SSG 20 の内部フラッシュストレージにファイルを保存します。
3. USB ストレージデバイスを取り外す前に、**exec usb-device stop** CLI コマンドで USB ポートを停止します。
4. これで安全に USB ストレージデバイスを取り出すことができます。

USB ストレージデバイスからファイルを削除するときは、**delete file usb:/filename** CLI コマンドを使用します。

USB ストレージデバイスまたは内部フラッシュストレージに保存してあるファイル情報を表示するには、**get file** CLI コマンドを使用します。

第 2 章

SSG 20 の取り付けと接続

本章では、SSG 20 の取り付け方法と、ケーブルや電源の接続方法を説明します。本章は、次の節で構成されています。

- 17 ページの「使用準備」
- 18 ページの「機器の設置」
- 19 ページの「SSG 20 とインターフェースケーブルの接続」
- 19 ページの「電源の接続」
- 20 ページの「ネットワークと SSG 20 の接続」

メモ： 安全上の注意と手順については、『*Juniper Networks Security Products Safety Guide*』を参照してください。機器の操作にあたっては、電気回路にともなう危険性をよく認識し、事故防止のための一般的な対策を理解しておいてください。

使用準備

システムを正しく運用するためには、シャーシの位置、監視装置の配置、配線室のセキュリティが重要です。



警告： 誤用や無用な者の侵入を防ぐため、SSG 20 は、安全な環境に設置してください。

システムのシャットダウン、機器の障害、けがを防ぐため、次の注意事項に従ってください。

- 設置前には、電源が入っていないことを確認してください。
- SSG 20 を設置する部屋は、適切な換気があり、部屋の温度が 104°F (40°C) を超えないことを確認してください。
- 吸気ポートや排気ポートがふさがれるおそれのある機器ラックフレームに SSG 20 を設置しないでください。密閉型ラックの場合はファンがあり、側面にルーバーがあることを確認してください。
- 湿気のある床面や濡れた床面、漏電、接地されていない電源ケーブルやすり切れた電源ケーブル、安全用接地の欠落など、危険な状態は修復しておいてください。

機器の設置

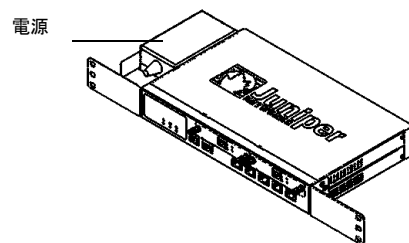
SSG 20 の取り付け方法には、壁面取り付け、机上取り付けがあります。取り付けキットは別途販売です。

SSG 20 の取り付けには、プラスドライバの 2 番（未同梱）と、機器ラック（キットに同梱）と互換性のあるネジが必要です。

メモ： SSG 20 の取り付けは、電源コンセントが手の届く範囲にあることを確認して行ってください。 .

標準 19 インチ機器ラックに SSG 20 を前面取り付けするには、次の手順に従ってください。

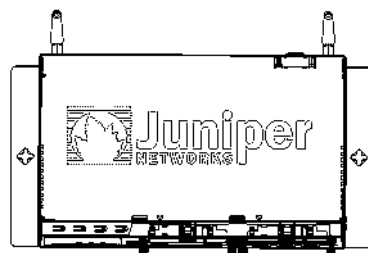
図 7: SSG 20 の前面取り付け



1. 電源ラック マウントの耳を SSG 20 の左前端に合わせます。
2. ネジ穴にネジを入れて、プラスドライバで締めます。
3. もう一方の電源ラック マウントの耳を SSG 20 の右前端に合わせます。
4. ネジ穴にネジを入れて、プラス ドライバで締めます。
5. 同梱のネジでラックに SSG 20 を取り付けます。
6. 電源コンセントに電源を差し込みます。

SSG 20 を壁面取り付けするには、次の手順に従ってください。

図 8: SSG 20 の壁面取り付け

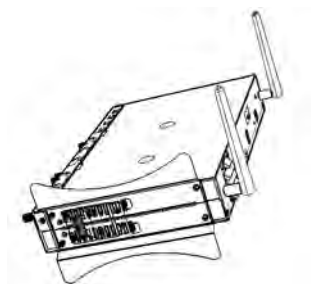


1. 壁面取り付けの耳を SSG 20 に合わせます。
2. ネジ穴にネジを入れて、プラスドライバで締めます。
3. SSG 20 は、凹凸がなく滑らかで、乾燥していて頑丈な壁に取り付けてください。

4. 同梱のネジで壁に SSG 20 を固定します。
5. 出力に電源を差し込みます。

SSG 20 を机に取り付けするには、次の手順に従ってください。

図 9: SSG 20 の机に取り付け



1. デスクトップスタンドを SSG 20 の側面に取り付けます。その際、電源アダプタに近い側面を使用してください。
2. デスクトップに SSG 20 を置きます。
3. 電源アダプタを差し込み、電源を電源コンセントに接続します。

SSG 20 とインターフェースケーブルの接続

インターフェースケーブルは次の手順で SSG 20 に接続します。

1. インターフェースに使用する所定の長さのケーブルを用意します。
2. インターフェース面板のケーブルコネクタポートにケーブルコネクタを挿入します。
3. ケーブルが外れたり、ストレスポイントができないように、次の手順でケーブルを固定します。
 - a. ケーブルが床に垂れて自重がかからないようケーブルを固定します。
 - b. 余分な長さのケーブルはコイルに巻いて整理します。
 - c. ケーブルループが崩れないようファスナで固定します。

電源の接続

電源は次の手順で SSG 20 に接続します。

1. 電源ケーブルの DC コネクタ側を SSG 20 背後の DC 電源コンセントに差し込みます。
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：電源接続にはサージ保安器を使用してください。

ネットワークと SSG 20 の接続

SSG 20 には、内部ネットワークと Untrust ネットワーク間に配置するときのファイアウォール機能と、一般的な対ネットワークセキュリティ機能があります。この節の内容を次に示します。

- SSG 20 と Untrust ネットワークの接続
- SSG 20 と内部ネットワークまたはワークステーションとの接続

SSG 20 と Untrust ネットワークの接続

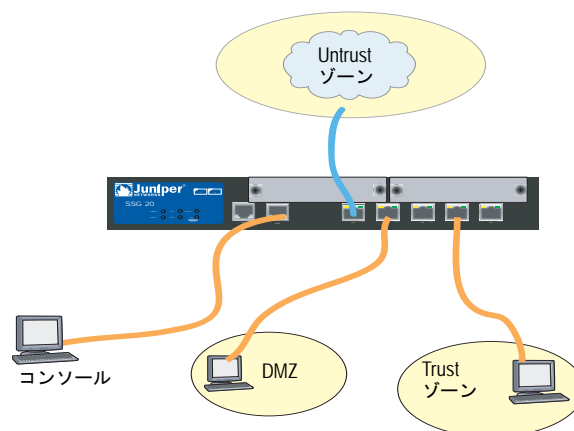
SSG 20 は、次のいずれかの方法で Untrust ネットワークに接続できます。

- イーサネットポート
- シリアル (AUX/ コンソール) ポート
- Mini PIM と Untrust ネットワークの接続

図 10 は、10/100 イーサネットポート接続による基本的なネットワーク配線の SSG 20 です。Mini PIM が 2 基ブランクになっています。

- ラベル 0/0 (ethernet0/0 インターフェース) のポートは、Untrust ネットワークに接続します。
- ラベル 0/1 (ethernet0/1 インターフェース) のポートは、DMZ セキュリティゾーンのワークステーションに接続します。
- ラベル 0/3 (bgroup0 インターフェース) のポートは、Trust セキュリティゾーンのワークステーションに接続します。
- コンソールポートは、管理アクセス用のシリアルターミナルに接続します。

図 10: 基本ネットワークの例



イーサネットポート

高速接続については、SSG 20 のラベル 0/0 のイーサネットポートから外部ルーターに、同梱のイーサネットケーブルを接続します。SSG 20 が、指定速度、全二重、MDI/MDIX 設定値を自動的に検出します。

シリアル (AUX/ コンソール) ポート

Untrust ネットワークとは、RJ-45 ストレートシリアルケーブルと外部モデムで接続できます。



警告：SSG 20 のコンソール、AUX、またはイーサネットの各ポートからは電話線に接続しないでください。

Mini PIM と Untrust ネットワークの接続

この節では、SSG 20 の Mini PIM を Untrust ネットワークに接続する方法を説明します。

ADSL2/2+ Mini PIM

同梱の ADSL ケーブルを、ADSL2/2+ Mini PIM から電話線に接続します。SSG 20 の Annex A バージョンの ADSL ポートでは RJ-11 コネクタを使用しますが、Annex B バージョンでは RJ-45 コネクタを使用します。Annex B モデルの場合、ADSL ポートを電話線に結ぶ接続ケーブルは、ストレート 10 Base-T イーサネットケーブルと外見は同じです。

スプリッタとマイクロフィルタの接続

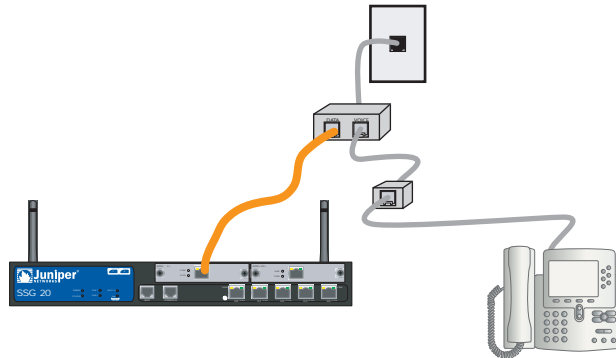
信号スプリッタは、音声通話用の低周波音声信号とデータ通信用の高周波データ信号に電話信号を分割します。通常、サービスプロバイダが設置するスプリッタは、屋内電話回線をプロバイダネットワークに接続する機器に組み込まれています。

サービスプロバイダの機器によっては、ユーザー自身が設置できるスプリッタもあります。スプリッタを自分自身で設置する場合は、SSG 20 と電話線の ADSL ケーブルをスプリッタ上の該当するコネクタ（例、「データ」または「音声」）に接続してください。スプリッタのもう一方の終端は電話線に接続します。

場合によっては、ADSL 回線に接続した電話、ファックス、留守番電話、またはアナログモデムのそれぞれ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。マイクロフィルタは、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回線に設置します。

図 11 は、サイトに設置したマイクロフィルタやスプリッタの例です。（マイクロフィルタやスプリッタはサービスプロバイダから入手してください。）

図 11: ネットワーク接続上のマイクロフィルタとスプリッタは



ISDN、T1、E1、V.92 Mini PIM

Mini PIM は次の手順で SSG 20 に接続します。

1. インターフェースに使用する所定の長さのケーブルを用意します。
2. インターフェース面板のケーブルコネクタポートにケーブルコネクタを挿入します。
3. ケーブルが外れたり、ストレスポイントができないように、次の手順でケーブルを固定します。
 - a. ケーブルが床に垂れて自重がかからないような状態にケーブルを固定します。
 - b. 余分な長さのケーブルはコイルに巻いて整理します。
 - c. ケーブルループが崩れないよう、ファスナで固定します。

ISDN、E1、T1 または V.92 Mini PIM の構成方法については、39 ページの「Mini PIM 構成」を参照してください。

SSG 20 と内部ネットワークまたはワークステーションとの接続

ローカルエリアネットワーク（LAN）やワークステーションは、イーサネットとワイヤレスインターフェースのいずれかまたは両方に接続できます。

イーサネットポート

SSG 20 にはイーサネットポートが 5 つあります。スイッチやハブ経由で LAN との接続には、これらのポートを 1 つまたは複数使用できます。ハブやスイッチを介せずに、これらポートの 1 つまたはすべてをワークステーションに直接接続することもできます。クロスケーブルとストレートケーブルのどちらでも、イーサネットポートと他の装置は接続できます。デフォルトのゾーン対インターフェースのバインドについては、29 ページの「SSG 20 のデフォルト設定」を参照してください。

ワイヤレスアンテナ

ワイヤレスインターフェースを使用する場合、SSG 20 に同梱のアンテナを接続してください。標準 2dB ダイバーシティーアンテナが手元にある場合は、SSG 20 背面のマーク A と B のポストにねじ止めしてください。バルクヘッドコネクタに圧力がかからないよう、アンテナを L 字形に曲げます。

図 12: SSG 20-WLAN アンテナの位置



オプションの外部アンテナを使用する場合は、そのアンテナに同梱の接続指示に従ってください。

第 3 章

SSG 20 の構成

SSG 20 には、出荷時に ScreenOS ソフトウェアがインストールされています。SSG 20 の電源を入れると、構成準備が整います。SSG 20 には、SSG 20 との初期接続のためのデフォルト構成を出荷時に済ませていますが、使用するネットワークの要件に応じて追加構成をする必要があります。

本章は、次の節で構成されています。

- 26 ページの「SSG 20 のアクセス」
- 29 ページの「SSG 20 のデフォルト設定」
- 31 ページの「SSG 20 の基本構成」
- 35 ページの「基本ワイヤレス構成」
- 39 ページの「Mini PIM 構成」
- 46 ページの「基本的ファイアウォール保護」
- 46 ページの「外部との接続性の確認」
- 46 ページの「SSG 20 の出荷時のデフォルト設定へのリセット」

メモ： SSG 20 を構成し、リモートネットワークによる接続ができることを確認したら、www.juniper.net/support/ で製品を登録してください。SSG 20 で、Deep Inspection Signature Service と アンチウイルスソフトウェア（別途購入）などの ScreenOS サービスを受けるためです。製品を登録したら、WebUI でサービスを申し込みます。製品の登録とサービスの申込みの詳細については、使用する SSG 20 で実行するバージョンの ScreenOS に対応する『*概念と用例 ScreenOS リファレンス ガイド*』の「基本」の部を参照してください。

SSG 20 のアクセス

SSG 20 には、次の構成方法や管理方法があります。

- コンソール: SSG 20 のコンソールポートからは、ワークステーションやターミナルに接続したシリアルケーブル経由で SSG 20 をアクセスできます。SSG 20 を構成するには、ターミナルから、またはワークステーションで実行しているターミナルエミュレーションプログラムから ScreenOS コマンドラインインターフェース (CLI) コマンドを入力します。
- WebUI: ScreenOS Web ユーザーインターフェース (WebUI) は、ブラウザで利用できるグラフィカルインターフェースです。初めて WebUI を使用するときは、ブラウザを実行するワークステーションを、SSG 20 と同じサブネットワークに接続してください。WebUI は、セキュア HTTP (S-HTTP) によるセキュアソケットレイヤー (SSL) を利用してセキュアサーバーでもアクセスできます。
- Telnet/SSH: Telnet と SSH は、IP ネットワークで SSG 20 をアクセスできるアプリケーションです。SSG 20 を構成するには、ワークステーションから Telnet セッションで ScreenOS CLI コマンドを入力します。詳細については、『*概念と用例 ScreenOS リファレンス ガイド*』の「管理」の部を参照してください。
- NetScreen-Security Manager: NetScreen-Security Manager は、Juniper Networks ファイアウォール /IPSec VPN の構成、管理を行うための Juniper Networks 業務用管理アプリケーションです。NetScreen-Security Manager による SSG 20 の管理方法については、『*NetScreen-Security Manager 2004 Administrator's Guide*』を参照してください。

コンソール接続の使用

メモ: SSG 20 のコンソールポートとの接続には、オス RJ-45 コネクタ付きのストレート RJ-45 CAT5 シリアルケーブルを使用します。

コンソールは次の手順で接続します。

1. 同梱の DB-9 アダプタのメス側をワークステーションのシリアルポートに差し込みます (DB-9 は正しく、確実に差し込んでください)。図 13 は、使用するタイプの DB-9 コネクタです。

図 13: DB-9 アダプタ



2. SSG 20 のコンソールポートにシリアルケーブルの RJ-45 オス側を差し込みます (CAT5 ケーブルのもう一方の端は、正しく、確実に、DB-9 アダプタに差し込んでください)。

- ワークステーションで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
コンソールセッションの開始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
- フロー制御：なし

- 管理者名とパスワードのデフォルトログインを変更していない場合は、ログインプロンプトとパスワードプロンプトの両方に **netScreen** と入力します（小文字以外使用しないでください。ログインフィールドとパスワードフィールドのいずれも、大文字小文字を区別します）。

CLI コマンドによる SSG 20 の構成方法については、『*概念と用例 ScreenOS リファレンス ガイド*』を参照してください。

- （オプション）アイドルタイムが 10 分続くとコンソールはデフォルトでタイムアウトになり、自動的に終了します。タイムアウトの設定を削除するには、**set console timeout 0** と入力します。

WebUI の使用

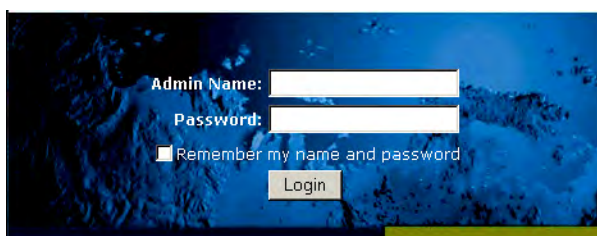
WebUI を使用するには、SSG 20 と同じサブネットワークに、SSG 20 を管理するワークステーションを配置してください。WebUI で SSG 20 をアクセスするには、次のように操作します。

- SSG 20 の 0/2 — 0/4 ポート（Trust ゾーンの bgroup0 インターフェース）にワークステーションを接続します。
- ワークステーションが動的ホスト構成プロトコル（DHCP）対応で構成されているか、192.168.1.0/24 サブネットの IP アドレスで静的に構成されていることを確認します。
- ブラウザを起動して bgroup0 インターフェースの IP アドレス（デフォルト IP アドレスは 192.168.1.1/24）を入力し、**Enter** を押します。

メモ： WebUI による初めての SSG 20 のアクセスでは、Initial Configuration Wizard (ICW) が表示されます。ICW で SSG 20 を構成する場合は、59 ページの「Initial Configuration Wizard（初期構成ウィザード）」を参照してください。

WebUI アプリケーションでは、図 14 のようにログインプロンプトが表示されます。

図 14: WebUI ログインプロンプト



4. 管理者名とパスワードのデフォルトログインを変更していない場合は、管理者名プロンプトとパスワードプロンプトの両方に **netscreen** と入力します（小文字以外使用しないでください。ログインフィールドとパスワードフィールドのいずれも、大文字小文字を区別します）。

Telnet の使用

Telnet は次の手順で接続します。

1. SSG 20 の 0/2 — 0/4 ポート（Trust ゾーンの bgroup0 インターフェース）にワークステーションを接続します。
2. ワークステーションが DHCP 対応で構成されているか、192.168.1.0/24 サブネットの IP アドレスで静的に構成されていることを確認します。
3. bgroup0 インターフェースの IP アドレス（デフォルト IP アドレスは 192.168.1.1）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、**telnet 192.168.1.1** と入力します。

Telnet アプリケーションにログインプロンプトが表示されます。

4. ログインとパスワードのデフォルトログインを変更していない場合は、ログインプロンプトとパスワードプロンプトの両方に **netscreen** と入力します（小文字以外使用しないでください。ログインフィールドとパスワードフィールドのいずれも、大文字小文字を区別します）。
5. （オプション）アイドルタイムが 10 分続くとコンソールはデフォルトでタイムアウトになり、自動的に終了します。タイムアウトの設定を削除するには、**set console timeout 0** と入力します。

SSG 20 のデフォルト設定

この節では、SSG 20 のデフォルト設定と動作について説明します。

表 5 は、SSG 20 のデフォルトゾーンバインディングです。

表 5: デフォルトの物理インターフェースからゾーンへのバインディング

ポートラベル	インターフェース	ゾーン
10/100 イーサネットポート:		
0/0	ethernet0/0	Untrust
0/1	ethernet0/1	DMZ
0/2	bgroup0 (ethernet0/2)	Trust
0/3	bgroup0 (ethernet0/3)	Trust
0/4	bgroup0 (ethernet0/4)	Trust
AUX	serial0/0	Null
WAN Mini PIM ポート (x = Mini PIM スロット 1 か 2):		
ADSL2/2 + (Annex A)	adsl(x/0)	Untrust
ADSL2/2 + (Annex B)	adsl(x/0)	Untrust
T1	serial(x/0)	Untrust
E1	serial(x/0)	Untrust
ISDN	bri(x/0)	Untrust
V.92	serial(x/0)	Null

ブリッジグループ (bgroup) は、SSG 20 を再構成やリブートせずに、ネットワークユーザーが有線トラフィックとワイヤレストラフィック間で切り換えるためのグループです。SSG 20 でポート 0/2 からポート 0/4 というラベルが付いている ethernet0/2 から ethernet0/4 のインターフェースには、デフォルトで IP アドレス 192.168.1.1/24 が割り当てられ、Trust セキュリティゾーンにバインドされます。bgroup は最大 4 つまで指定できます。

イーサネットインターフェースやワイヤレスインターフェースを bgroup に設定する場合、まずイーサネットインターフェースやワイヤレスインターフェースがヌルセキュリティゾーンにあることを確認してください。bgroup に所属しているイーサネットインターフェースやワイヤレスインターフェースの設定を解除すると、それらのインターフェースはヌルセキュリティゾーンに配置されます。ヌルセキュリティゾーンに割り当てると、イーサネットインターフェースはセキュリティゾーンにバインドでき、別の IP アドレスを割り当てることができます。

ethernet0/3 を bgroup0 から設定解除し、静的 IP アドレス 192.168.3.1/24 の Trust ゾーンに割り当てするには、WebUI か CLI を次のように操作します。

WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port: **ethernet0/3** を選択解除し、**Apply** をクリックします。

List > Edit (ethernet0/3): 次の値を入力して、**Apply** をクリックします。

Zone Name: Trust (選択)
IP Address/Netmask: 192.168.3.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
set interface ethernet0/3 zone trust
set interface ethernet0/3 ip 192.168.3.1/24
save
```

表 6: ワイヤレスインターフェースと論理インターフェースのバインディング

SSG 20-WLAN	インターフェース	ゾーン
ワイヤレスインターフェース ワイヤレスインターフェースを指定します。2.4 G と 5 G 無線の両方またはいずれかで動作する構成が可能です。	wireless0/0 (デフォルト IP アドレスは 192.168.2.1/24)	Trust
	wireless0/1-0/3.	Null
論理インターフェース		
レイヤー 2 インターフェース	vlan1 は、SSG 20 がトランスパレントモードのときに、管理と VPN トラフィックの終了に使用する論理インターフェースを指定します。	該当なし
トンネルインターフェース	tunnel.n は、論理トンネルインターフェースを指定します。このインターフェースは、VPN トラフィック用です。	該当なし

bgroup0 インターフェースのデフォルト IP アドレスは、LAN や WLAN のアドレスに合わせて変更できます。bgroup に対するワイヤレスインターフェースの構成方法については、「35 ページの「基本ワイヤレス構成」」を参照してください。

メモ: ワイヤレスインターフェースを構成した bgroup インターフェースはトランスパレントモードでは機能しません。

bgroup の詳細と例については、『*概念と用例 ScreenOS リファレンス ガイド*』を参照してください。

SSG 20 の他のイーサネットインターフェースやワイヤレスインターフェースにはデフォルト IP アドレスは構成されていません。WAN インターフェースをはじめ、他のインターフェースには IP アドレスを割り当ててください。

SSG 20 の基本構成

この節では、次の基本構成設定について説明します。

- ルート管理者名とパスワード
- 日付と時刻
- ブリッジグループインターフェース
- 管理アクセス
- 管理サービス
- ホスト名とドメイン名
- デフォルトルート
- 管理インターフェースのアドレス
- バックアップ Untrust インターフェースの構成

ルート管理者名とパスワード

ルート管理者には、SSG 20 の構成に必要なすべての管理権限があります。デフォルトのルート管理者名とパスワード (いずれも **netscreen**) はすみやかに変更してください。

ルート管理者名とパスワードを変更するには、WebUI か CLI を次のように操作します。

WebUI

Configuration > Admin > Administrators > Edit (NetScreen 管理者名の値): 次のように入力してから **OK** をクリックします。

Administrator Name:
Old Password: netscreen
New Password:
Confirm New Password:

メモ: WebUI にパスワードは表示されません。

CLI

```
set admin name name
set admin password pswd_str
save
```

日付と時刻

SSG 20 で設定した時刻は VPN トンネルのセットアップなどさまざまなイベントに反映されます。日付と時刻は、WebUI で SSG 20 のシステムクロックをワークステーションクロックに同期すれば簡単に SSG 20 に設定できます。

SSG 20 に日付と時刻を設定するには、WebUI か CLI を次のように操作します。

WebUI

1. Configuration > Date/Time: Sync Clock with Client ボタンをクリックします。

ワークステーションクロックで夏時間オプションを有効にしたかどうかの指定を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、夏時間に合わせてシステムクロックを同期化します。**No** をクリックすると、夏時間との調整なしで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 **set clock** CLI 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。

ブリッジグループインターフェース

デフォルトで、SSG 20 では、イーサネットインターフェース ethernet0/2 から ethernet0/4 が Trust セキュリティゾーンにグループとしてまとめられています。グループ化したインターフェースは、1 つのサブネットになります。グループのインターフェースをグループから取り出して、別のセキュリティゾーンに割り当てることもできます。グループに割り当てられるのはヌルセキュリティゾーンのインターフェースだけです。グループ化したインターフェースをヌルセキュリティゾーンに配置するには、**unset interface interface port interface** CLI コマンドを使用します。

SSG 20-WLAN では、イーサネットインターフェースとワイヤレスインターフェースを 1 サブネットとしてグループにまとめることができます。

メモ： bgroup のグループにまとめられるのはワイヤレスインターフェースとイーサネットインターフェースだけです。

イーサネットインターフェースとワイヤレスインターフェースでグループを構成するには、WebUI か CLI を次のように操作します。

WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port: **ethernet0/3** と **ethernet0/4** の選択を解除し、**Apply** をクリックします。

Edit (bgroup1) > Bind Port: **ethernet0/3**、**ethernet0/4**、**wireless0/2** を選択し、**Apply** をクリックします。

> Basic: 次の値を入力して、**Apply** をクリックします。

Zone Name: DMZ (選択)
IP Address/Netmask: 10.0.0.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
unset interface bgroup0 port ethernet0/4
set interface bgroup1 port ethernet0/3
set interface bgroup1 port ethernet0/4
set interface bgroup1 port wireless0/2
set interface bgroup1 zone DMZ
set interface bgroup1 ip 10.0.0.1/24
save
```

管理アクセス

デフォルトでは、ログインとパスワードがわかっているならば、ネットワークの誰でも SSG 20 を管理できます。

SSG 20 を管理できるホストを、ネットワークの特定のホストに限定するには、WebUI か CLI を次のように操作します。

WebUI

Configuration > Admin > Permitted IPs: 次のように入力してから **Add** をクリックします。

IP Address/Netmask: *ip_addr/mask*

CLI

```
set admin manager-ip ip_addr/mask
save
```

管理サービス

ScreenOS には、SNMP、SSL、SSH など、SSG 20 の構成と管理のためのサービス機能があり、これらはインターフェース単位で有効にできます。

SSG 20 で管理サービスを構成するには、WebUI か CLI を次のように操作します。

WebUI

Network > Interfaces > List > Edit (ethernet0/0): **Management Services** で、インターフェースで使用する管理サービスを選択するか、選択解除し、**Apply** をクリックします。

CLI

```
set interface ethernet0/0 manage web
unset interface ethernet0/0 manage snmp
save
```

ホスト名とドメイン名

ドメイン名は、SSG 20 が所属するネットワークやサブネットワークを定義します。ホスト名は特定の SSG 20 の名前です。ホスト名とドメイン名を組み合わせるとネットワークの SSG 20 を一意で識別できます。

SSG 20 にホスト名とドメイン名を構成するには、WebUI か CLI を次のように操作します。

WebUI

Network > DNS > Host: 次の値を入力して、**Apply** をクリックします。

Host Name: *名前*
Domain Name: *名前*

CLI

```
set hostname 名前
```

```
set domain 名前
save
```

デフォルトルート

デフォルトルートとは、ルーティングテーブルに明示的にリストされていないネットワークにアドレス指定されたパケットのパスを示す静的ルートです。SSG 20 にルーティング情報がないアドレスを持ったパケットが SSG 20 に到着すると、SSG 20 はデフォルトルートで指定された宛先にそのパケットを送信します。

SSG 20 でデフォルトルートを構成するには、WebUI か CLI を次のように操作します。

WebUI

Network > Routing > Destination > New (trust-vr): 次のように入力してから **OK** をクリックします。

```
IP Address/Netmask: 0.0.0.0/0.0.0.0
Next Hop
  Gateway: ( 選択 )
  Interface: ethernet0/2 ( 選択 )
  Gateway IP Address: IP アドレス
```

CLI

```
set route 0.0.0.0/0 interface ethernet0/2 gateway IP アドレス
save
```

管理インターフェースのアドレス

Trust インターフェースには、デフォルト IP アドレス 192.168.1.1/24 が割り当てられており、管理サービス用に構成されています。装置の 0/2 — 0/4 ポートをワークステーションに接続すると、Telnet などの管理サービスを利用して、192.168.1.1/24 サブネットワークでワークステーションから装置を構成できます。

Trust インターフェースのデフォルト IP アドレスは変更できます。たとえば、LAN 上の既存の IP アドレスがある場合、そのアドレスに合わせて、インターフェースを変更できます。

バックアップUntrust インターフェースの構成

SSG 20 では、Untrust フェイルオーバー用のバックアップインターフェースを構成できます。Untrust フェイルオーバー用のバックアップインターフェースは、次の手順で設定します。

1. **unset interface interface [port interface]** CLI コマンドでヌルセキュリティゾーンにバックアップインターフェースを設定します。
2. **set interface interface zone zone_name** CLI コマンドで、同じセキュリティゾーンにプライマリインターフェースとしてバックアップインターフェースをバインドします。

メモ： プライマリインターフェースとバックアップインターフェースは同じセキュリティゾーンに構成してください。1 つのプライマリインターフェースに割り当てられるバックアップインターフェースは 1 つだけであり、バックアップインターフェース 1 つにつきプライマリインターフェースは 1 つしか割り当てられません。

ethernet0/0 インターフェースに ethernet0/4 インターフェースをバックアップインターフェースとして設定するには、次のように WebUI か CLI を使用します。

WebUI

Network > Interfaces > Backup > 次の値を入力し、**Apply** をクリックします。

Primary: ethernet0/0
Backup: ethernet0/4
Type: track-ip (選択)

CLI

```
unset interface bgrouop0 port ethernet0/4
set interface ethernet0/4 zone untrust
set interface ethernet0/0 backup interface ethernet0/4 type track-ip
save
```

基本ワイヤレス構成

この節では、SSG 20-WLAN におけるワイヤレスインターフェースの構成方法について説明します。ワイヤレスネットワークは、SSID (Service Set Identifiers) として参照する名前で構成します。SSID を指定すると、同じロケーションに複数のワイヤレスネットワークを配置しても互いに干渉することがありません。SSID 名は最長 32 文字です。SSID 名にスペースがある場合、名前は引用符で囲んでください。SSID 名を設定すると、さらに SSID 属性を構成できます。SSG 20 で WLAN (ワイヤレスローカルエリアネットワーク) 機能を使用するには、少なくとも SSID を 1 つ構成し、それをワイヤレスインターフェースにバインドしてください。

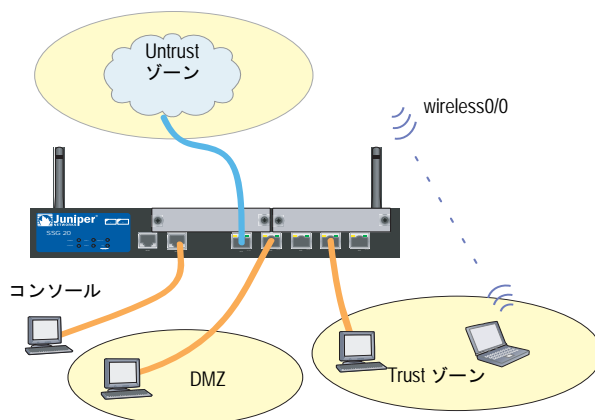
SSG 20-WLAN では、最大 16 の SSID を作成できますが、同時に使用できるのはその内の 4 つだけです。SSG 20-WLAN では、1 台のトランシーバで 4 つすべての SSID を使用する構成と、両方に分けた構成が可能です (例: 3 つの SSID を WLAN 0 に割り当て、1 つの SSID を WLAN 1 に割り当てるなど)。SSG 20-WLAN に無線トランシーバの設定には、**set interface wireless_interface wlan {0 | 1 | both}** CLI コマンドを使用します。

wireless0/0 インターフェースに SSID を設定すれば、「26 ページの「SSG 20 のアクセス」」の手順に従ってデフォルトの wireless0/0 インターフェース IP アドレスで SSG 20-WLAN をアクセスできます。図 15 は、SSG 20-WLAN のデフォルト構成です。

メモ: 米国、日本、カナダ、中国、台湾、韓国、イスラエル、シンガポール以外で SSG 20-WLAN を使用する場合は、**set wlan country-code** CLI コマンドを実行するか、Wireless > General Settings WebUI ページで設定しないと WLAN 接続はできません。このコマンドでは、チャンネルの選択範囲と送信出力レベルを設定できます。

地域コードが ETSI の場合、ローカル電波スペクトル規制に応じた国コードを設定してください。

図 15: デフォルト SSG 20-WLAN 構成



デフォルトで、wireless0/0 インターフェースの構成は IP アドレス 192.168.2.1/24 になっています。Trust ゾーンに接続する必要があるワイヤレスクライアントはいずれもワイヤレスサブネットワークに IP アドレスを登録しておく必要があります。SSG 20 は DHCP で自動的に 192.168.2.1/24 サブネットワークにおける IP アドレスを他の SSG 20 に割り当てる構成も可能です。

デフォルトで、wireless0/1 インターフェースから wireless0/3 インターフェースはヌルに定義され、IP アドレスは割り当てられません。他のワイヤレスインターフェースのどれかを使用する場合は、その IP アドレスを構成し、SSID を割り当てて、セキュリティゾーンにバインドしてください。表 7 は、ワイヤレス認証と暗号化の方式をまとめたものです。

表 7: ワイヤレス認証と暗号化オプション

認証	暗号化
オープン	すべてのワイヤレスクライアントで SSG 20 をアクセス可能
共有鍵	WEP 共有鍵
WPA-PSK	AES/TKIP (事前共有鍵使用)
WPA	AES/TKIP (RADIUS サーバーの鍵使用)
WPA2-PSK	802.11i 事前共有鍵準拠
WPA2	802.11i RADIUS サーバー準拠
WPA-Auto-PSK	WPA と WPA2 (事前共有鍵使用) が可能
WPA-Auto	WPA と WPA2 (RADIUS サーバー使用) が可能
802.1x	WEP (RADIUS サーバーの鍵使用)

構成例、SSID 属性、ワイヤレスセキュリティ構成に関する CLI コマンドについては、『*概念と用例/ScreenOS リファレンス ガイド*』を参照してください。

ワイヤレスインターフェースを基本接続に構成するには、WebUI か CLI を次のように操作します。

WebUI

1. WLAN 国コードと IP アドレスを設定します。

Wireless > General Settings > 次のように選択して、**Apply** をクリックします。

Country code: コードを選択します。
IP Address/Netmask: *ip_add/netmask*

2. SSID を設定します。

Wireless > SSID > New: 次のように入力してから **OK** をクリックします。

SSID:
Authentication:
Encryption:
Wireless Interface Binding:

3. (オプション) WEP 鍵を設定します。

SSID > WEP Keys: keyID を選択して **Apply** をクリックします。

4. WLAN モードを設定します。

Network > Interfaces > List > Edit (ワイヤレスインターフェース): WLAN モードに **Both** を選択し、**Apply** をクリックします。

5. ワイヤレス変更を有効にします。

Wireless > General Settings > **Activate Changes** をクリックします。

CLI

1. WLAN 国コードと IP アドレスを設定します。

```
set wlan country-code {code_id}
set interface wireless_interface ip ip_addr/netmask
```

2. SSID を設定します。

```
set ssid name name_str
set ssid name_str authentication auth_type encryption encryption_type
set ssid name_str interface interface
(オプション) set ssid name_str key-id number
```

3. WLAN モードを設定します。

```
set interface wireless_interface wlan both
```

4. ワイヤレス変更を有効にします。

```
save
exec wlan reactivate
```

同じサブネットでは有線サブネットとして機能するよう SSID を設定できます。こうしておけば、別のサブネットに接続を切り換えなくてもどちらのインターフェースでもクライアントを使用できます。

同じブリッジグループインターフェースにイーサネットとワイヤレスインターフェースを設定するには、WebUI か CLI で次のように操作します。

WebUI

Network > Interfaces > List > Edit (*bgroup_name*) > Bind Port: ワイヤレスインターフェースとイーサネットインターフェースを選択し、**Apply** をクリックします。

CLI

```
set interface bgroup_name port wireless_interface
set interface bgroup_name port ethernet_interface
```

メモ： *Bgroup_name* に指定できる値の範囲は、bgroup0 から bgroup3 です。

Ethernet_interface に指定できる値の範囲は、ethernet0/0 から ethernet0/4 です。

Wireless_interface に指定できる値の範囲は、wireless0/0 から wireless0/3 です。

ワイヤレスインターフェースを構成した場合は、**exec wlan reactivate** CLI コマンドで WLAN を有効にするか、Wireless > General Settings WebUI ページの **Activate Changes** をクリックしてください。

Mini PIM 構成

この節では、Mini PIM（ミニ物理インターフェース）の構成方法を説明します。

- ADSL2/2+ インターフェース
- ISDN インターフェース
- T1 インターフェース
- E1 インターフェース
- V.92 モデム インターフェース

ADSL2/2+ インターフェース

非同期転送モード (ATM) 仮想回路で SSG 20 からサービスプロバイダのネットワークに接続するとき、ネットワークでは ADSL2/2+ インターフェース **adslx/0** を使用します。ここで x は Mini PIM スロット (1 または 2) を表します。ADSL2/2+ サブインターフェースを作成すれば、さらに仮想回路を追加構成できます。詳細については、「39 ページの「仮想回路」」を参照してください。

SSG 20 の現在のインターフェース一覧については、WebUI で Network > Interfaces > List ページ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、**get interface** CLI コマンドを入力します。これで、adslx/0 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。

ADSL2/2+ インターフェースでプロバイダのサービスプロバイダに接続している場合は、adsl(x/0) インターフェースを構成してください。構成時には、サービスプロバイダから次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）多重化方式。
 - 仮想回路方式の多重化。各プロトコルは各 ATM 仮想回路に引き継がれます。
 - 論理リンク制御 (LLC) カプセル化。複数のプロトコルを同じ ATM VC に引き継ぐことができます（デフォルト多重化方式）。
- PPPoE (Point-to-Point Protocol over Ethernet) または PPPoA (Point-to-Point Protocol over ATM) によるサービスプロバイダのネットワークへの接続用にサービスプロバイダ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（ある場合。PPPoE または PPPoA 接続のいずれかに割り当てられたもの）
- オプションで、構内ネットワークの静的 IP アドレスとネットマスク値

仮想回路

仮想回路を追加するには、ADSL2/2+ 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。ADSL2/2+ 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、定義済みのゾーン **Untrust** にバインドされた新しいサブインターフェース **adsl1/0.1** を作成するには、WebUI か CLI を次のように操作します。

WebUI

Network > Interfaces > List > New ADSL Sub-IF: 次の値を入力して、**Apply** をクリックします。

Interface Name: adsl1/0.1
 VPI/VCI: 0/35
 Zone Name: Untrust (選択)

CLI

```
set interface adsl 1/0.1 pvc 0 35 zone Untrust
save
```

39 ページの「ADSL2/2+ インターフェース」に説明のあるように、ADSL2/2+ サブインターフェースは、VPI/VCI 値の設定も含めて、メイン ADSL2/2+ インターフェースと同じ方法で構成します。しかし、ADSL2/2+ サブインターフェースは、メイン ADSL2/2+ インターフェースとは別に構成してください。したがって、サブインターフェースには、メインの ADSL2/2+ インターフェースとは異なる多重化方式、VPI/VCI、PPP クライアントを構成できます。また、メインの ADSL2/2+ 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は静的 IP アドレスを構成できます。

VPI/VCI と複合方式

サービスプロバイダは、各仮想接続に VPI/VCI ペアを割り当てます。たとえば、VPI/VCI ペア 1/32 を受信した場合、VPI 値は 1、VCI 値は 32 です。これらの値は、サービスプロバイダが DSLAM (Digital Subscriber Line Access Multiplexer) の加入者側に構成した値と一致しているはずです。

VPI/VCI ペア 1/32 を adsl1/0 インターフェースに構成するには、WebUI か CLI を次のように操作します。

WebUI

Network > Interfaces > List > Edit (adsl1/0 インターフェース): VPI/VCI フィールドに **1/32** と入力して、**Apply** をクリックします。

CLI

```
set interface adsl1/0 pvc 1 32
save
```

デフォルトで SSG 20 は仮想回路ごとに論理リンク制御 (LLC) 方式の多重化を使用します。

adslx/0 インターフェースに VPI/VCI ペア 1/32 を構成し、仮想回路で LLC カプセル化を使用するには、WebUI か CLI を次のように操作します。

WebUI

Network > Interfaces > List > Edit (adsl1/0 インターフェース): 次の値を入力して、**Apply** をクリックします。

VPI/VCI: 1 / 32
 Multiplexing Method: LLC (選択されている)

CLI

```
set interface adsl1/0 pvc 1 32 mux llc
save
```

PPPoE または PPPoA

SSG 20 は、ADSL リンク経由でサービスプロバイダのネットワークに接続するため、PPPoE クライアントと PPPoA クライアントの両方を備えています。PPPoE は ADSL カプセル化の最も一般的な形式であり、ネットワーク上の各ホストにおける終了に利用します。PPP セッションは SSG 20 で終了できるため、PPPoA は主にビジネスクラスのサービスに利用します。SSG 20 をサービスプロバイダのネットワークに接続するには、サービスプロバイダに割り当てられ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。

メモ： SSG 20 がサポートするのは、仮想回路ごとに 1 つの PPPoE セッションです。

PPPoE にユーザー名 **roswell** とパスワード **area51** を構成し、PPPoE 構成を adsl1/0 インターフェイスにバインドするには、WebUI か CLI を次のように構成します。

WebUI

Network > PPP > PPPoE Profile > New: 次のように入力してから **OK** をクリックします。

PPPoE Instance: poe1
Bound to Interface: adsl1/0 (選択)
Username: roswell
Password: area51

CLI

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1/0
save
```

SSG 20 では、ほかにも構成可能な PPPoE パラメータや PPPoA パラメータがあります。たとえば認証方法（デフォルトサポートは、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）、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のサーバーとの通信用にその他の PPPoE パラメータや PPPoA のパラメータを構成する必要があるかどうか、サービスプロバイダに問い合わせてください。

静的 IP アドレスおよびネットマスク

ネットワーク用の固定 IP アドレスとネットマスクがサービスで割り当てられている場合、そのネットワークに IP アドレスとネットマスクを構成し、SSG 20 に接続したルーターポートの IP アドレスを構成してください。また、SSG 20 で静的 IP アドレスを使用する指定が必要です（通常、SSG 20 は PPPoE または PPPoA クライアントとして動作し、PPPoE サーバーまたは PPPoA サーバーとのネゴシエーションで ADSL インターフェースの IP アドレスを受け取ります）。

41 ページの「PPPoE または PPPoA」にあるように、PPPoE インスタンスまたは PPPoA インスタンスを構成して adsl1/0 インターフェースにバインドしてください。**Obtain IP using PPPoE** または **Obtain IP using PPPoA** を選択し、PPPoE インスタンスまたは PPPoA インスタンスの名前を選択してください。

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、WebUI か CLI で次のように操作します。

WebUI

Network > Interfaces > List > Edit (adsl1/0 インターフェース): 次の値を入力して、**Apply** をクリックします。

IP Address/Netmask: 1.1.1.1/24
Static IP: (選択)

CLI

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

or

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoa name poa1 static-ip
save
```

ドメイン名とアドレスの解決に 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に最低 1 つの DNS サーバーの IP アドレスを割り当てる必要があります。SSG 20 が PPPoE か PPPoA で ADSL2/2+ インターフェースの IP アドレスを受け取ると、SSG 20 は DNS サーバーの IP アドレスも自動的に受信します。ネットワーク上のコンピュータが SSG 20 の DHCP サーバーの IP アドレスを取得すると、コンピュータは DNS サーバーのアドレスも取得します。

ユーザーが ADSL2/2+ ADSL インターフェースに静的 IP アドレスを割り当てた場合、ユーザーはサービスプロバイダから DNS サーバーの IP アドレスを取得する必要があります。DNS サーバーのアドレスはネットワーク上の各コンピュータで構成します。あるいは、Trust ゾーンインターフェースで DHCP サーバーを構成すれば、Trust ゾーンインターフェースから各コンピュータに DNS サーバーのアドレスが通知されます。

bgroup0 インターフェースで DHCP サーバーを構成して DNS サーバー アドレス 1.1.1.152 をネットワークのコンピュータに通知するには、WebUI または CLI で次のように操作します。

WebUI

Network > DHCP > Edit (bgroup0 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 bgroup0 dhcp server option dns1 1.1.1.152
save
```

ADSL インターフェースと ADSL2/2+ インターフェースの構成方法の詳細については、『*概念と用例 ScreenOS リファレンス ガイド*』を参照してください。

ISDN インターフェース

統合サービスデジタル網（ISDN）は、国際電信電話諮問委員会（CCITT）と国際電気通信連合（ITU）が作成した、各種メディアによるデジタル通信のための標準です。ダイヤルオンデマンドサービスとして、ISDN は呼の設定が高速で待ち時間は短く、同時に高品質の音声、データ、ビデオ送信に対応します。ISDN はまた、マルチポイント接続とポイントツーポイント接続の両方で利用できる、回線交換サービスです。ISDN は、サービスルーターにマルチリンクポイントツーポイントプロトコル（PPP）接続を提供します。ISDN インターフェースは、通常、イーサネットインターフェースのバックアップインターフェースとして構成して外部ネットワークをアクセスします。

ISDN インターフェースを構成するには、WebUI か CLI を次のように操作します。

WebUI

Network > Interfaces > List > Edit (bri1/0): 次の値を入力するか選択して **OK** をクリックします。

```
BRI Mode: Dial Using BRI
Primary Number: 123456
WAN Encapsulation: PPP
PPP Profile: isdnprofile
```

CLI

```
set interface bri1/0 dialer-enable
set interface bri1/0 primary-number "123456"
set interface bri1/0 encap ppp
set interface bri1/0 ppp profile isdnprofile
save
```

バックアップインターフェースとして ISDN インターフェースを構成するには、「34 ページの「バックアップ Untrust インターフェースの構成」」を参照してください。

ISDN インターフェースの構成方法の詳細については、『*概念と用例 ScreenOS リファレンス ガイド*』を参照してください。

T1 インターフェース

T1 インターフェースは、北米で Digital Signal level 1 (DS-1) 多重化方式に使用されている基本物理レイヤープロトコルです。T1 インターフェースはビットレート 1.544 Mbps または最高通信速度 24 DS0 チャンネルで動作します。

SSG 20 は、次の T1 DS-1 標準をサポートしています。

- ANSI T1.107、T1.102
- GR 499-core、GR 253-core
- AT&T Pub 54014
- ITU G.751、G.703

T1 Mini PIM を構成するには、WebUI か CLI を次のように操作します。

WebUI

Network > Interfaces > List > Edit (serial1/0): 次の値を入力するか選択して **OK** をクリックします。

WAN Configure: main link
 WAN Encapsulation: cisco-hdlc
Apply をクリックします。
 Fixed IP: (選択)
 IP Address/Netmask: 172.18.1.1/24

CLI

```
set interface serial1/0 encaps cisco-hdlc
set interface serial1/0 ip 172.18.1.1/24
```

T1 インターフェースの構成方法については、『*概念と用例/ScreenOS リファレンス ガイド*』を参照してください。

E1 インターフェース

E1 インターフェースは、銅線で通信速度 2.048 Mbps で動作する標準ワイドエリアネットワーク (WAN) デジタル通信フォーマットです。北米以外で広く普及している E1 は、デジタル回路の搬送に使用されている基本的な時分割多重化スキームです。

SSG 20 は、次の E1 標準をサポートしています。

- ITU-T G.703
- ITU-T G.751
- ITU-T G.775

E1 Mini PIM を構成するには、WebUI か CLI を次のように操作します。

WebUI

Network > Interfaces > List > Edit (serial1/0): 次の値を入力するか選択して **OK** をクリックします。

WAN Configure: main link
 WAN Encapsulation: PPP
 Binding a PPP Profile: junipertest
Apply をクリックします。
 Fixed IP: (選択)
 IP Address/Netmask: 172.18.1.1/24

CLI

```
set interface serial1/0 encapsulation ppp
set ppp profile "junipertest" static-ip
set ppp profile "junipertest" auth type chap
set ppp profile "junipertest" auth local-name "juniper"
set ppp profile "junipertest" auth secret "password"
set interface serial1/0 ppp profile "junipertest"
set interface serial1/0 ip 172.18.1.1/24
```

```
set user "server" type wan
set user "server" password "server"
```

E1 インターフェースの構成方法については、『*概念と用例 ScreenOS リファレンス ガイド*』を参照してください。

V.92 モデム インターフェース

V.92 インターフェースには内蔵アナログモデムがあり、サービスプロバイダと PPP 接続ができます。シリアルインターフェースはプライマリインターフェースまたはバックアップインターフェースに構成でき、インターフェースフェイルオーバー時に使用できます。

メモ: V.92 インターフェースはトランスペアレントモードでは機能しません。

V.92 インターフェースを構成するには、WebUI か CLI を次のように操作します。

WebUI

Network > Interfaces > List > Edit (serial1/0): 次のように入力してから **OK** をクリックします。

Zone Name: untrust (選択)

ISP: 次のように入力してから **OK** をクリックします。

ISP Name: isp_juniper
Primary Number: 1234567
Login Name: juniper
Login Password: juniper

Modem: 次のように入力してから **OK** をクリックします。

Modem Name: mod1
Init String: AT&FS7=255S32=6
Active Modem setting
Inactivity Timeout: 20

CLI

```
set interface serial1/0 zone untrust
set interface serial1/0 modem isp isp_juniper account login juniper password
juniper
set interface serial1/0 modem isp isp_juniper primary-number 1234567
set interface serial1/0 modem idle-time 20
set interface serial1/0 modem settings mod1 init-strings AT&FS7=255S32=6
set interface serial1/0 modem settings mod1 active
```

V.92 モデム インターフェースの構成方法については、『*概念と用例 ScreenOS リファレンス ガイド*』を参照してください。

基本的ファイアウォール保護

SSG 20 は、デフォルトポリシーで構成してあります。このポリシーでは、ネットワーク上の Trust ゾーン内のワークステーションには Untrust セキュリティゾーンのどのリソースでもアクセスできますが、外部コンピュータはそのワークステーションにアクセスしたり、ワークステーションでセッションを開始することはできません。使用コンピュータとの特定のセッションを外部コンピュータから開始できるように SSG 20 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、『*概念と用例 ScreenOS リファレンス ガイド*』を参照してください。

ネットワークやネットワークリソースに脅威や害を与える目的の探査や攻撃に対抗するため、SSG 20 には各種の検出機能や防御機構が備わっています。

- ScreenOS SCREEN オプションでは、ゾーンとのインターフェース経由で接続しようとするアクセスをすべて検査して、許可か拒否で対応してゾーンを保護します。たとえば、Untrust ゾーンにポートスキャン保護を適用して、リモートネットワークのソースがサービスを特定して攻撃するのを防ぐことができます。
- SSG 20 では、SCREEN フィルタをゾーン間を移動するトラフィックにファイアウォールポリシーを適用します。このポリシーではコンテンツフィルタリングコンポーネントや IDP (Intrusion Detection and Prevention) コンポーネントを使用できます。デフォルトでは、トラフィックはゾーン間を移動できません。ゾーン間の移動で SSG 20 の通過をトラフィックに許可する場合は、デフォルト動作をオーバーライドするポリシーを作成してください。

ゾーンに ScreenOS SCREEN オプションを設定するには、次のように WebUI または CLI を操作します。

WebUI

Screening > Screen: オプションを適用するゾーンを選択します。目的の SCREEN オプションを選択し、**Apply** をクリックします。

CLI

```
set zone zone screen option
save
```

ScreenOS で使用できるネットワークセキュリティオプションの構成方法の詳細については、『*概念と用例 ScreenOS リファレンス ガイド*』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のリソースにアクセスできるかどうかを確認するには、ネットワークの任意のワークステーションからブラウザを起動し、URL: www.juniper.net を入力します。

SSG 20 の出荷時のデフォルト設定へのリセット

管理者パスワードがわからなくなったときは、SSG 20 をデフォルト設定にリセットしてください。既存の構成情報は失われますが、ブロックされていた SSG 20 のアクセスが解除されます。



警告： SSG 20 をリセットすると、既存構成の設定値がすべて削除され、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。

SSG 20 のデフォルト設定値は、次のいずれの方法で復元できます。

- コンソール接続による方法。詳細については、『*概念と用例 ScreenOS リファレンスガイド*』を参照してください。
- 次の節の説明に従って、SSG 20 背面パネルのリセットスイッチを操作する。

リセットスイッチを押すと SSG 20 がリセットされて工場出荷時のデフォルト設定値になります。この操作では、正面パネルの SSG 20 のステータス LED を確認するか、26 ページの「コンソール接続の使用」の説明に従ってコンソールセッションを開始します。

リセットスイッチでリセットしてデフォルト設定値を復元するには、次のように操作します。

1. リセットスイッチは背面パネルにあります。細くて固い針金（ゼムクリップなど）で小さな穴の奥のスイッチを 4 ～ 6 秒間押して離します。

ステータス LED が赤く点滅します。構成の消去プロセスが開始したことを知らせるメッセージがコンソールに表示されます。システムは SNMP/SYSLOG 警報を送信します。

2. 1 ～ 2 秒間待ちます。

最初のリセットが済むと、ステータス LED が緑に点滅して、SSG 20 で次のリセット準備が整ったことを知らせます。コンソールでは SSG 20 が次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 秒押します。

コンソールメッセージが 2 度目のリセットの実行を知らせます。ステータス LED が半秒間、赤く点灯してから、緑の点滅状態に戻ります。

SSG 20 の設定は、工場出荷時の値にリセットされます。SSG 20 がリセットすると、ステータス LED は半秒間、赤く点灯してから、緑の点灯状態に戻ります。コンソールには、SSG 20 の起動メッセージが表示されます。システムでは構成された SYSLOG または SNMP のトラップホストに SNMP と SYSLOG の警報を生成します。

SSG 20 が再起動すると、コンソールには SSG 20 のログインプロンプトが表示されます。ステータス LED が緑で点滅します。ログインとパスワードはいずれも **netscreen** です。

すべての手順を終了しないと、構成の変更なしでリセットプロセスがキャンセルされ、コンソールには構成の消去が中止された旨のメッセージが表示されます。ステータス LED は緑の点滅に戻ります。SSG 20 がリセットされなかった場合、障害を知らせる SNMP 警報が送信されます。

第 4 章

SSG 20 の点検

本章では、SSG 20 のサービスとメンテナンス手順について説明します。本章は、次の節で構成されています。

- 本ページの「必要なツールとパーツ」
- 本ページの「ミニ物理インターフェースモジュールの交換」
- 52 ページの「メモリのアップグレード」

安全上の注意事項と対応手順については、『Juniper Networks Security Products Safety Guide』を参照してください。このガイドには、身体に危害が及ぶ恐れのある状況に関する注意事項をまとめています。機器の操作にあたっては、電気回路にともなう危険性をよく認識し、事故防止のための一般的な対策を理解しておいてください。

必要なツールとパーツ

SSG 20 の机上取り付けには、次のツールとパーツが必要です。

- 帯電防止袋または静電防止マット
- 静電放電（ESD）接地リストストラップ
- 1/8 in. プラスドライバ

ミニ物理インターフェースモジュールの交換

SSG 20 のモデルにはいずれにも、ワイドエリアネットワークミニ物理インターフェースモジュール（WAN Mini PIM）用にフロントパネルに 2 スロットがあります。したがって SSG 20 では Mini PIM の取り付けや交換が可能です。Mini PIM の取り外しや取り付けは、SSG 20 の電源を切ってから行ってください。



注意：Mini PIM を取り外す際は、SSG 20 から電源が切り離されていることを確認してください。SSG 20 はホストスワップابلではありません。

ブランク面板の取り外し

SSG 20 内の適正な空気の流れを保つため、Mini PIM を装着していないスロットはブランク面板でカバーしておく必要があります。Mini PIM を空スロットに取り付ける場合を除き、ブランク面板は取り外さないでください。

ブランク面板は次の手順で取り外します。

1. Mini PIM を置く平らで安定した面に帯電防止袋または静電防止マットを置きます。
2. ESD 接地ストラップを手首に直に装着し、シャーシの ESD ポイントか外部 ESD ポイント（SSG 20 をアース接地から切り離している場合）にストラップをつなぎます。
3. SSG 20 から電源アダプタを切り離します。POWER LED が消灯していることを確認します。
4. 面板の両側のネジをドライバでゆるめて取り外します。
5. 取り外した面板は、帯電防止袋に入れるか、静電防止マットの上に置きます。

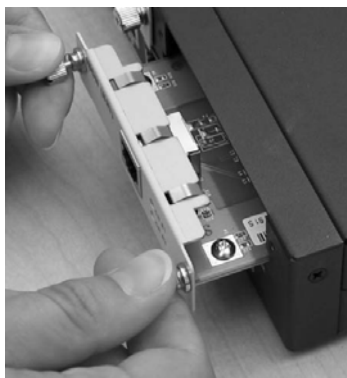
Mini PIM の取り外し

Mini PIM は、SSG 20 の正面パネルに取り付けます。Mini PIM の重量は 0.2 lb (106g) 未満です。

Mini PIM は次の手順で取り外します。

1. Mini PIM を置く場所として、平らで安定した面に帯電防止袋または静電防止マットを置きます。
2. ESD 接地ストラップを手首に直に装着し、シャーシの ESD ポイントか外部 ESD ポイント（SSG 20 をアース接地から切り離している場合）にストラップをつなぎます。
3. SSG 20 から電源アダプタを切り離します。POWER LED が消灯していることを確認します。
4. あとで正しい Mini PIM にケーブルを接続できるよう、Mini PIM に接続するケーブルにはラベルを付けておきます。
5. Mini PIM からケーブルを切り離します。
6. ケーブルが外れたり、ストレスポイントができないように、必要に応じてケーブルの位置を調整します。
 - a. ケーブルが床に垂れて自重がかからないような状態にケーブルを固定します。
 - b. 余分な長さのケーブルはコイルに巻いて整理します。
 - c. ケーブルループが崩れないようファスナで固定します。
7. Mini PIM 面板の両側のネジをドライバでゆるめて取り外します。
8. Mini PIM 面板の両側のネジを持って、SSG 20 から Mini PIM を取り出します。Mini PIM は、帯電防止袋に入れるか、静電防止マットの上に置きます。

図 16: Mini PIM の取り外し



9. Mini PIM を空スロットに戻さない場合は、筐体内の適正な空気の流れを維持するため、ブラック面板でスロットをカバーしてください。

Mini PIM の取り付け

Mini PIM は次の手順で取り付けます。

1. ESD 接地ストラップを手首に直に装着し、シャーシの ESD ポイントか外部 ESD ポイント（SSG 20 をアース接地から切り離している場合）にストラップをつなぎます。
2. SSG 20 から電源アダプタを切り離します。POWER LED が消灯していることを確認します。
3. Mini PIM 面板の両側のネジを持って、SSG 20 の Mini PIM スロットのノッチに Mini PIM 後部のコネクタのノッチを合わせます。SSG 20 に確実に収まるまで、Mini PIM を押し込みます。

図 17: Mini PIM の取り付け



注意：Mini PIM のコンポーネントが破損しないように気をつけて、Mini PIM をスロットにまっすぐ押し込みます。

4. Mini PIM 面板の両側のネジを 1/8 in. マイナスドライバで締めます。
5. Mini PIM のケーブルコネクタに所定のケーブルを挿入します。
6. ケーブルが外れたり、ストレスポイントができないように、必要に応じてケーブルの位置を調整します。
 - a. ケーブルが床に垂れて自重がかからないような状態にケーブルを固定します。
 - b. 余分な長さのケーブルはコイルに巻いて整理します。
 - c. ケーブルループが崩れないようファスナで固定します。

7. SSG 20 から電源アダプタを切り離します。電源ボタンを押すと POWER LED が緑に点灯することを確認します。
8. Mini PIM がオンラインになると、システムダッシュボードの PIM ステータス LED が緑に点灯したままになるのでそれを確認します。

メモリのアップグレード

SSG 20 は、128 MB DIMM（デュアルインラインメモリモジュール）DRAM（ダイナミックランダムアクセスメモリ）1 つから 256 MB DIMM DRAM 1 つにアップグレードできます。

SSG 20 のメモリをアップグレードするには、次の手順に従ってください。

1. ESD 接地ストラップを手首に直に装着し、シャーシの ESD ポイントか外部 ESD ポイント（SSG 20 をアース接地から切り離している場合）にストラップをつなぎます。
2. 電源コンセントから AC コードを切り離します。
3. SSG 20 をひっくり返して天板側から作業面に置きます。
4. メモリカードカバーのネジをプラスドライバで外します。あとでカバーを固定するときのためにネジは手近に保管します。
5. メモリカードカバーを取り外します。

図 18: SSG 20 の底面



6. モジュール両側のロック タブを親指で外側に押してタブをモジュールから外して 128 MB DIMM DRAM を取り外します。

図 19: メモリモジュールのロック解除



7. メモリモジュールの長辺を持って取り出します。脇によけておきます。

図 20: モジュールスロットの取り外し



8. スロットに 256 MB DIMM DRAM を挿入します。モジュールの上端に親指を当てて、ロック タブが所定の位置にカチッとハマるまで均等な力でモジュールを押し下げます。

図 21: メモリモジュールの挿入



9. スロットをメモ리카ードカバーでふさぎます。
10. プラスドライバでネジを締め、SSG 20 にカバーを固定します。

付録 A 仕様

本付録では、SSG 20 の総合的なシステム仕様を紹介します。本章は、以下の節で構成されています。

- 55 ページの「物理的仕様」
- 55 ページの「電氣的仕様」
- 56 ページの「環境耐性」
- 56 ページの「保証」
- 57 ページの「コネクタ」

物理的仕様

表 8: SSG 20 物理的仕様

説明	値
シャーシ寸法	294 mm x 194.8 mm x 44 mm (11.5 inches x 7.7 inches x 2 inches)
重量	1.53 kg (3.3 lbs)、PIM 未装着時
ISDN PIM	70g
ADSL Annex A PIM	106g
ADSL Annex B PIM	106g
T1 PIM	75g
E1 PIM	75g
V.92 PIM	79g

電氣的仕様

表 9: SSG 20 電氣的仕様

項目	仕様
DC 入力電圧	12V
DC システム定格電流	3 ~ 4.16 Amps

環境耐性

表 10: SSG 20 の環境耐性

説明	値
高度	最大 6,600 ft (2,000 m) までパフォーマンス低下なし
相対湿度	相対湿度 10 ～ 90 パーセントの範囲で正常動作を保証。結露なきこと。
温度	気温 32°F (0°C) ～ 104°F (40°C) の範囲で正常動作を保証。 発送用段ボール格納時の非動作時温度：-4°F (-20°C) ～ 158°F (70°C)

保証

安全性

- CAN/CSA-C22.2 No. 60950-1-03/UL 60950-1 Safety of Information Technology Equipment
- EN 60950-1 (2000) Third Edition Safety of Information Technology Equipment
- IEC 60950-1 (1999) Third Edition Safety of Information Technology Equipment

EMC エミッション

- FCC パート 15 クラス B (合衆国)
- EN 55022 クラス B (ヨーロッパ)
- AS 3548 クラス B (オーストラリア)
- VCCI クラス B (日本)

EMC (イミュニティ)

- EN 55024
- EN-61000-3-2 Power Line Harmonics
- EN-61000-3-3 Power Line Harmonics
- EN-61000-4-2 ESD
- EN-61000-4-3 Radiated Immunity
- EN-61000-4-4 EFT
- EN-61000-4-5 Surge
- EN-61000-4-6 Low Frequency Common Immunity
- EN-61000-4-11 Voltage Dips and Sags

ETSI

欧州電気通信標準化機構 (ETSI) EN-3000386-2: 電気通信網機器 電磁適合性 (機器カテゴリ。電気通信センターを除く)

T1 インターフェース

- FCC パート 68 - TIA 968
- Industry Canada CS-03
- UL 60950-1 Applicable requirements for TNV circuit with outside plant lead connection

コネクタ

図 22 は、使用する DB-45 コネクタのピン配列です。

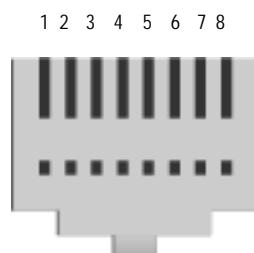
図 22: RJ-45 ピン配列

表 11 は、RJ-45 コネクタのピン配列です。

表 11: RJ-45 コネクタピン配列

ピン	名前	I/O	説明
1	RTS 出力	O	送信要求
2	DTR 出力	O	データターミナル準備完了
3	TxD	O	データ送信
4	接地	該当なし	シャーシ接地
5	接地	該当なし	シャーシ接地
6	RxD	I	データ受信
7	DSR	I	データセット準備完了
8	CTS	I	送信クリア

図 23 は、DB-9 メスコネクタのピン配列です。

図 23: DB-9 メスコネクタ

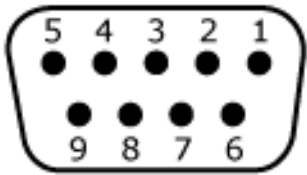


表 12 は、DB-9 コネクタのピン配列です。

表 12: DB-9 コネクタピン配列

ピン	名前	I/O	説明
1	DCD	I	搬送波検出
2	RxD	I	データ受信
3	TxD	O	データ送信
4	DTR	O	データターミナル準備完了
5	接地	該当なし	接地信号
6	DSR	I	データセット準備完了
7	RTS	O	送信要求
8	CTS	I	送信クリア
9	RING	I	リングインジケータ

付録 B

Initial Configuration Wizard (初期構成ウィザード)

本付録では、SSG 20 用の ICW (Initial Configuration Wizard、初期構成ウィザード) について解説します。

ネットワークに SSG 20 を物理的に接続すると、SSG 20 にインストールしたインターフェースを ICW で構成できます。

この節では、次の ICW について解説します。

- 60 ページの Rapid Deployment ウィンドウ
- 60 ページの Administrator Login ウィンドウ
- 61 ページの WLAN Access Point ウィンドウ
- 61 ページの Physical Interface ウィンドウ
- 62 ページの ADSL2/2+ Interface ウィンドウ
- 63 ページの T1 Interface ウィンドウ
- 69 ページの E1 Interface ウィンドウ
- 72 ページの ISDN Interface ウィンドウ
- 74 ページの V.92 Modem Interface インターフェース
- 75 ページの Eth0/0 Interface (Untrust Zone) ウィンドウ
- 76 ページの Eth0/1 Interface (DMZ Zone) ウィンドウ
- 77 ページの Bgroup0 Interface (Trust Zone) ウィンドウ
- 78 ページの Wireless0/0 Interface (Trust Zone) ウィンドウ
- 79 ページの Interface Summary ウィンドウ
- 79 ページの Physical Ethernet DHCP Interface ウィンドウ
- 80 ページの Wireless DHCP Interface ウィンドウ
- 81 ページの Confirmation ウィンドウ

1. Rapid Deployment ウィンドウ

図 24: Rapid Deployment ウィンドウ



Rapid Deployment Wizard

Welcome to the Rapid Deployment Wizard.

Do you have a Rapid Deployment Configlet file?

☒ No, use the Initial Configuration Wizard instead.

☐ Yes, use the following Rapid Deployment Configlet file:

Load Configlet from:

☐ No, skip the Wizard and go straight to the WebUI management session instead.

ネットワークで NetScreen-Security Manager (NSM) を使用していれば、SSG 20 はラピッドデプロイメントコンフィギュレットで自動的に構成できます。NSM 管理者からコンフィギュレットを入手し、**Yes** を選択し、**Load Configlet from:** を選択し、ファイルロケーションまでブラウズして、**Next** をクリックします。コンフィギュレットは、次の手順で SSG 20 を構成しなくてすむよう、ユーザーに代わって SSG 20 を構成してくれます。

ICW を使用せずに WebUI を直接呼び出した場合は、最後のオプションを選択して **Next** をクリックします。

SSG 20 の構成にコンフィギュレットを使用せず、ICW を使用する場合は、最初のオプションを選択し、**Next** をクリックします。ICW Welcome 画面が表示されます。**Next** をクリックします。Administrator Login ウィンドウが表示されます。

2. Administrator Login ウィンドウ

新しい管理者ログイン名とパスワードを入力し、**Next** をクリックします。

図 25: Administrator Login ウィンドウ



Initial Configuration Wizard

Enter the administrator's login name and password:

Administrator Login Name:

Password:

Confirm Password:

Note: You cannot retrieve the login name and password if you lose it. Please make sure you have a copy of this information in a secure location.

HTTP Redirect: ☐

Note: HTTP Redirect will redirect all HTTP traffic to HTTPS, ie, HTTPS is only way to manage the device through Web browsers.

3. WLAN Access Point ウィンドウ

WORLD または ETSI の規制ドメインを使用する場合は国コードを選択してください。該当するオプションを選択し、**Next** をクリックします。

図 26: Wireless Access Point Country Code ウィンドウ

4. Physical Interface ウィンドウ

インターフェースツリーゾーンバインディング画面で、Untrust セキュリティゾーンをバインドするインターフェースを設定します。Bgroup0 は Trust セキュリティゾーンにバインド済みです。Eth0/1 は、DMZ セキュリティゾーンにバインドされていますが、これはオプションです。

図 27: Physical Interface ウィンドウ

インターフェースをゾーンにバインドしたら、インターフェースを構成できます。以後表示される構成ウィンドウは、セキュリティ装置にインストールした Mini-PIM がどれかによって異なります。ICW で SSG 20 の構成を続けるには、**Next** をクリックします。

5. ADSL2/2+ Interface ウィンドウ

SSG 20 に ADSL2/2 + Mini PIM をインストールしてある場合、次のウィンドウで adslx/0 インターフェースを構成できます。

メモ： SSG 20 に ADSL2/2 + Mini PIM を 2 基インストールしてある場合、ICW ではマルチリンク機能を構成できません。ML ADSL の構成方法については、『*概念と用例 ScreenOS リファレンス ガイド*』を参照してください。

図 28: ADSL Interface ウィンドウ

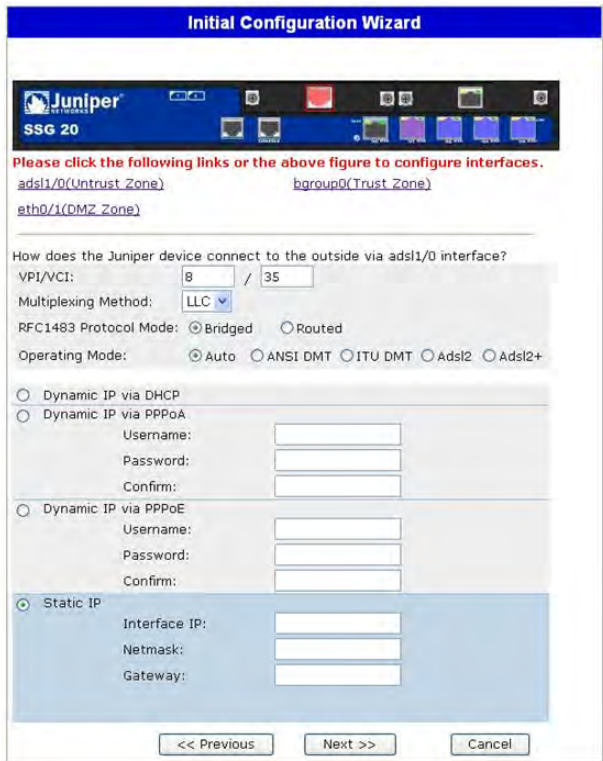


表 13: ADSL Interface ウィンドウのフィールド

フィールド	説明
サービスプロバイダから入手する情報：	
VPI/VCI	パーマネント仮想回路を識別する VPI/VCI 値
Multiplexing Method（多重化方式）	ATM 多重化方式（LLC がデフォルト）
RFC1483 Protocol Mode（プロトコルモード）	プロトコルモード設定（Bridged がデフォルト）
Operating Mode（動作モード）	物理回線の動作モード（Auto がデフォルト）

フィールド	説明
IP 構成設定値	<ul style="list-style-type: none"> ■ Dynamic IP via DHCP を選択して、SSG 20 で ADSL インターフェースの IP アドレスをサービスプロバイダから入手します。 ■ Dynamic IP via PPPoA を選択して SSG 20 を PPPoA クライアントとして使用します。サービスプロバイダによって割り当てられたユーザー名とパスワードを入力します。 ■ Dynamic IP via PPPoE を選択して SSG 20 を PPPoE クライアントとして使用します。サービスプロバイダによって割り当てられたユーザー名とパスワードを入力します。 ■ Static IP を選択して、一意の固定 IP アドレスを ADSL インターフェースに割り当てます。インターフェース IP アドレス、ネットマスク、ゲートウェイ（ゲートウェイアドレスは、SSG 20 に接続したルーターポートの IP アドレス）を入力します。

以上の設定値がわからない場合は、サービスプロバイダの装置に同梱の『*Common Settings for Service Providers*』ドキュメントを参照してください。

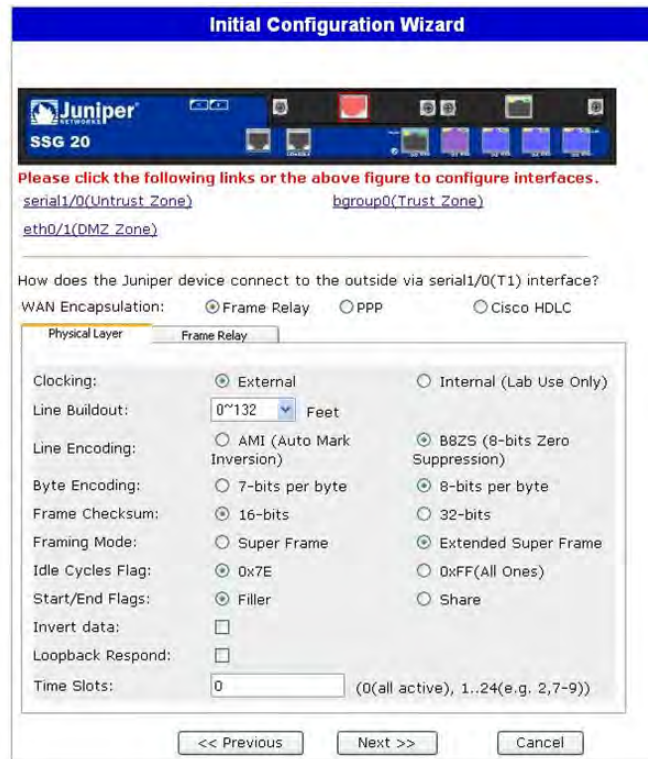
6. T1 Interface ウィンドウ

SSG 20 に T1 Mini-PIM をインストールして、Frame Relay オプションを選択すると、次のウィンドウが表示されます。

- T1 Physical Layer Tab ウィンドウ
- T1 Frame Relay Tab ウィンドウ

メモ： SSG 20 に T1 Mini-PIM を 2 基インストールして、Multi-link オプションを選択すると、Physical Layer タブが 2 つ表示されます。

図 29: T1 Physical Layer Tab ウィンドウ



The image shows the 'Initial Configuration Wizard' window for a Juniper SSG 20 device. The 'Physical Layer' tab is selected. The window includes a header with the Juniper logo and 'SSG 20'. Below the header, there are links for 'serial1/0(Untrust Zone)' and 'bggroup0(Trust Zone)'. A section titled 'How does the Juniper device connect to the outside via serial1/0(T1) interface?' shows 'WAN Encapsulation' with radio buttons for 'Frame Relay' (selected), 'PPP', and 'Cisco HDLC'. The 'Physical Layer' tab contains various configuration options: 'Clocking' (External selected, Internal (Lab Use Only) unselected), 'Line Buildout' (0*132 Feet), 'Line Encoding' (AMI (Auto Mark Inversion) unselected, B8ZS (8-bits Zero Suppression) selected), 'Byte Encoding' (7-bits per byte unselected, 8-bits per byte selected), 'Frame Checksum' (16-bits selected, 32-bits unselected), 'Framing Mode' (Super Frame unselected, Extended Super Frame selected), 'Idle Cycles Flag' (0x7E selected, 0xFF (All Ones) unselected), 'Start/End Flags' (Filler selected, Share unselected), 'Invert data' (checkbox unselected), 'Loopback Respond' (checkbox unselected), and 'Time Slots' (0, with a note '(0(all active), 1..24(e.g. 2,7-9))'). Navigation buttons at the bottom are '<< Previous', 'Next >>', and 'Cancel'.

Initial Configuration Wizard

Juniper
SSG 20

Please click the following links or the above figure to configure interfaces.
[serial1/0\(Untrust Zone\)](#) [bggroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

How does the Juniper device connect to the outside via serial1/0(T1) interface?
WAN Encapsulation: ☒ Frame Relay ☐ PPP ☐ Cisco HDLC

Physical Layer **Frame Relay**

Clocking: ☒ External ☐ Internal (Lab Use Only)

Line Buildout: 0*132 Feet

Line Encoding: ☐ AMI (Auto Mark Inversion) ☒ B8ZS (8-bits Zero Suppression)

Byte Encoding: ☐ 7-bits per byte ☒ 8-bits per byte

Frame Checksum: ☒ 16-bits ☐ 32-bits

Framing Mode: ☐ Super Frame ☒ Extended Super Frame

Idle Cycles Flag: ☒ 0x7E ☐ 0xFF (All Ones)

Start/End Flags: ☒ Filler ☐ Share

Invert data: ☐

Loopback Respond: ☐

Time Slots: 0 (0(all active), 1..24(e.g. 2,7-9))

<< Previous Next >> Cancel

表 14: T1 Physical Layer Tab ウィンドウのフィールド

フィールド	説明
Clocking (クロッキング)	インターフェースの送信クロックを設定します。
Line Buildout (回線ビルドアウト)	インターフェースが回線を駆動する距離を設定します。デフォルト設定値は 0 ~ 132 フィートです。
Line Encoding (回線エンコーディング)	インターフェースの回線エンコーディングフォーマットを設定します。 <ul style="list-style-type: none"> ■ Auto Mark Inversion (自動マーク反転) ■ 8 ビットゼロ抑止
Byte Encoding (バイトエンコーディング)	バイト当たり 7 ビットまたは 8 ビットを使用するよう T1 インターフェースのバイトエンコーディングを設定します。デフォルトはバイト当たり 8 ビットです。
Frame Checksum (フレームチェックサム)	チェックサムのサイズを設定します。デフォルトは 16 です。
Framing Mode (フレミングモード)	フレミングフォーマットを設定します。デフォルトは Extended mode (拡張モード) です。
Idle Cycles Flag (アイドルサイクルフラグ)	アイドルサイクルでインターフェースが送信する値を設定します。デフォルト設定値は 0x7E です。 <ul style="list-style-type: none"> ■ 0x7E (フラグ) ■ 0xFF (1)
Start/End Flags (開始 / 終了フラグ)	開始フラグと終了フラグの送信を filler (フィラー) か shared (共有) に設定します。デフォルトは filler (フィラー) です。
Invert Data checkbox (反転データ) チェックボックス	未使用データビットの反転送信を有効にします。
Loopback Respond checkbox (ループバック応答) チェックボックス	リモートチャンネルサービスユニット (CSU) からのループバックを T1 インターフェースで有効にします。
Time Slots (タイムスロット)	T1 インターフェースにおけるタイムスロットの使用を設定します。デフォルトは 0 です。この場合、24 すべてのタイムスロットを使用します。

図 30: T1 Frame Relay Tab ウィンドウ

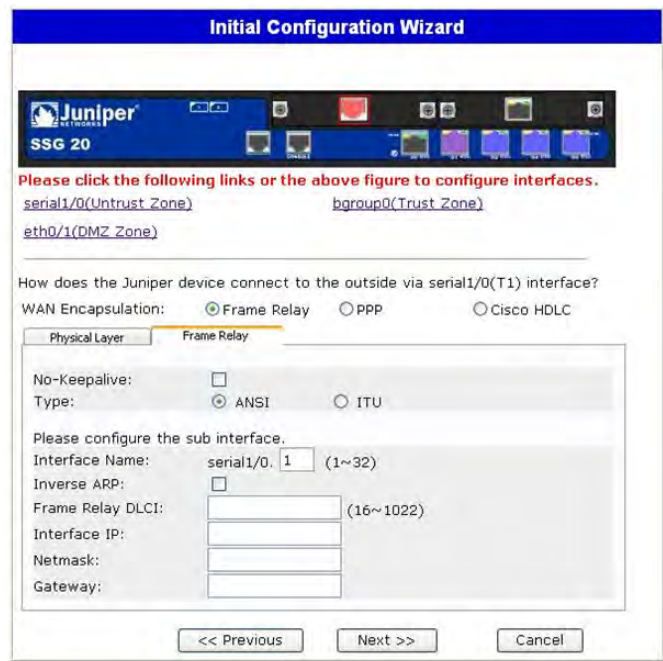


表 15: T1 Frame Relay Tab ウィンドウのフィールド

フィールド	説明
No-Keepalive checkbox (ノーキープアライブ) チェックボックス	ノーキープアライブを有効にします。
Type (タイプ)	フレームリレー LMI タイプを設定します。 <ul style="list-style-type: none">■ ANSI: American National Standards Institute (ANSI) は、ダウンストリームで最高 8 Mbps、アップストリームで最高 1 Mbps のデータ転送速度をサポートします。■ ITU: International Telecommunications Union (ITU) は、ダウンストリームで最高 6.144 Mbps、アップストリームで最高 640 kbps のデータ転送速度をサポートします。
Interface Name (インターフェース名)	サブインターフェース名を設定します。
Inverse ARP (逆 ARP)	サブインターフェースの逆アドレス解決プロトコルを有効にします。
Frame Relay DLCI (フレームリレー DLCI)	サブインターフェースにデータリンク接続識別子 (DLCI) を割り当てます。
Interface IP (インターフェース IP)	サブインターフェースの IP アドレスを設定します。
Netmask (ネットマスク)	サブインターフェースのネットマスクを設定します。
Gateway (ゲートウェイ)	サブインターフェースのゲートウェイアドレスを設定します。

SSG 20 に T1 Mini-PIM をインストールして、PPP オプションを選択すると、次の補助ウィンドウが表示されます。

- PPP Option with PPP Tab Window ウィンドウ
- PPP Option with Peer User Tab ウィンドウ

図 31: PPP Option with PPP Tab Window ウィンドウ

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20 device. The wizard is at the 'PPP' tab, which is selected under the 'Physical Layer' section. The 'WAN Encapsulation' is set to 'PPP'. The 'Please create the PPP profile' section includes fields for 'PPP Profile Name', 'Authentication' (set to 'Any'), 'Local User', 'Password', and a checked 'Static IP' checkbox. The 'Please configure the serial1/0 interface' section includes fields for 'Interface IP', 'Netmask', and 'Gateway'. Navigation buttons at the bottom are '<< Previous', 'Next >>', and 'Cancel'.

表 16: PPP Option with PPP Tab Window ウィンドウのフィールド

フィールド	説明
PPP Profile Name (PPP プロファイル名)	PPP プロファイルの名前を設定します。
Authentication (認証)	認証タイプを設定します。
Local User (ローカルユーザー)	ローカルユーザーの名前を設定します。
Password (パスワード)	ローカルユーザーのパスワードを設定します。
Static IP checkbox (静的 IP チェックボックス)	静的 IP アドレスを有効にします。
Interface IP (インターフェース IP)	serialx/0 インターフェース IP アドレスを設定します。

フィールド	説明
Netmask (ネットマスク)	serialx/0 ネットマスクを設定します。
Gateway (ゲートウェイ)	serialx/0 ゲートウェイアドレスを設定します。

図 32: PPP Option with Peer User Tab ウィンドウ

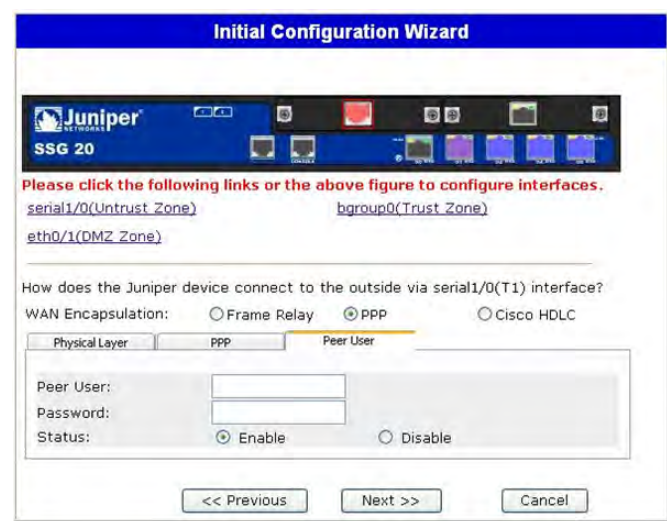


表 17: PPP Option with Peer User Tab ウィンドウのフィールド

フィールド	説明
Peer User (ピアユーザー)	ピアユーザーの名前を設定します。
Password (パスワード)	Peer User (ピアユーザー) テキストフィールドで指定したピアユーザーのパスワードを設定します。
Status (ステータス)	PPP の有効、無効を切り換えます。

SSG 20 に T1 Mini-PIM をインストールして、Cisco HDLC オプションを選択すると、次のウィンドウが表示されます。

図 33: Cisco HDLC Option with Cisco HDLC Tab ウィンドウ

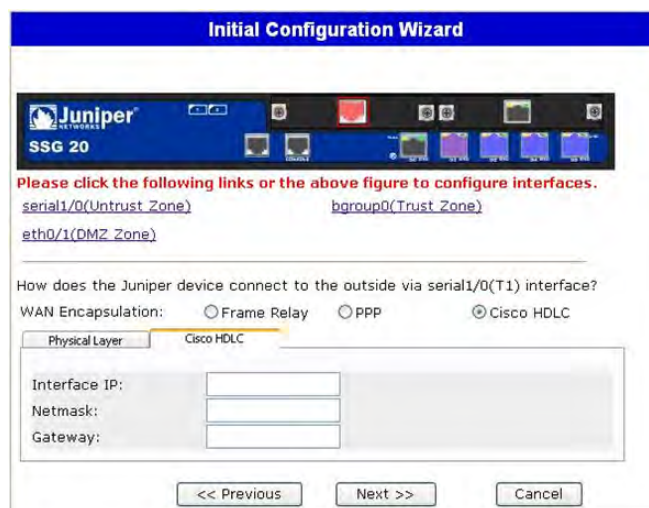


表 18: Cisco HDLC Option with Cisco HDLC Tab ウィンドウのフィールド

フィールド	説明
Interface IP (インターフェース IP)	T1 Cisco HDLC インターフェースの IP アドレスを設定します。
Netmask (ネットマスク)	T1 Cisco HDLC インターフェースのネットマスクを設定します。
Gateway (ゲートウェイ)	T1 Cisco HDLC インターフェースのゲートウェイアドレスを設定します。

7. E1 Interface ウィンドウ

SSG 20 に E1 Mini-PIM をインストールして、Frame Relay オプションを選択すると、次のウィンドウが表示されます。

- E1 Physical Layer Tab ウィンドウ
- E1 Frame Relay Tab ウィンドウ

メモ: SSG 20 に E1 Mini-PIM を 2 基インストールして、Multi-link (マルチリンク) オプションを選択すると、Physical Layer (物理レイヤー) が 2 つ表示されます。

図 34: E1 Physical Layer Tab ウィンドウ

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20. The 'Physical Layer' tab is selected. The wizard prompts the user to click links to configure interfaces: [serial1/0\(Untrust Zone\)](#), [bgroup0\(Trust Zone\)](#), and [eth0/1\(DM2 Zone\)](#). Below this, it asks 'How does the Juniper device connect to the outside via serial1/0(E1) interface?' with options for WAN Encapsulation: ☒ Frame Relay, ☐ PPP, and ☐ Cisco HDLC. The 'Physical Layer' sub-tab is active, showing settings for Clocking (External), Frame Checksum (16-bits), Framing Mode (with CRC4), Idle Cycles Flag (0x7E), Start/End Flags (Filler), Invert data (unchecked), and Time Slots (0). Navigation buttons '<< Previous', 'Next >>', and 'Cancel' are at the bottom.

表 19: E1 Physical Layer Tab ウィンドウのフィールド

フィールド	説明
Clocking (クロッキング)	インターフェースの送信クロックを設定します。
Frame Checksum (フレームチェックサム)	チェックサムのサイズを設定します。デフォルトは 16 です。
Framing Mode (フレーミングモード)	フレーミングフォーマットを設定します。デフォルトは without CRC4 です。
Idle Cycles Flag (アイドルサイクルフラグ)	アイドルサイクルでインターフェースが送信する値を設定します。デフォルト設定値は 0x7E です。 ■ 0x7E (フラグ) ■ 0xFF (1)
Start/End Flags (開始 / 終了フラグ)	開始フラグと終了フラグの送信を filler (フィラー) か shared (共有) に設定します。デフォルトは filler (フィラー) です。
Invert Data checkbox (反転データ) チェックボックス	未使用データビットの反転送信を有効にします。
Time Slots (タイムスロット)	T1 インターフェースにおけるタイムスロットの使用を設定します。デフォルトは 0 です。この場合、32 すべてのタイムスロットを使用します。

図 35: E1 Frame Relay Tab ウィンドウ

Initial Configuration Wizard

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.
[serial1/0\(Untrust Zone\)](#) [bgrou0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

How does the Juniper device connect to the outside via serial1/0(E1) interface?
 WAN Encapsulation: ☒ Frame Relay ☐ PPP ☐ Cisco HDLC

Physical Layer **Frame Relay**

No-Keepalive: ☐
 Type: ☒ ANSI ☐ ITU

Please configure the sub interface:
 Interface Name: serial1/0, 1 (1~32)
 Inverse ARP: ☐
 Frame Relay DLCI: (16~1022)
 Interface IP:
 Netmask:
 Gateway:

<< Previous Next >> Cancel

表 20: E1 Frame Relay Tab ウィンドウのフィールド

フィールド	説明
No-Keepalive checkbox (ノーキープアライブチェックボックス)	ノーキープアライブを有効にします。
Type (タイプ)	<p>フレームリレー LMI タイプを設定します。</p> <ul style="list-style-type: none"> ■ ANSI: American National Standards Institute (ANSI) は、ダウンストリームで最高 8 Mbps、アップストリームで最高 1 Mbps のデータ転送速度をサポートします。 ■ ITU: International Telecommunications Union (ITU) は、ダウンストリームで最高 6.144 Mbps、アップストリームで最高 640 kbps のデータ転送速度をサポートします。
Interface Name (インターフェース名)	サブインターフェース名を設定します。
Inverse ARP (逆 ARP) チェックボックス	サブインターフェースの逆アドレス解決プロトコル (ARP) を有効にします。
Frame Relay DLCI (フレームリレー DLCI)	サブインターフェースに DLCI を割り当てます。
Interface IP (インターフェース IP)	サブインターフェースの IP アドレスを設定します。
Netmask (ネットマスク)	サブインターフェースのネットマスクを設定します。
Gateway (ゲートウェイ)	サブインターフェースのゲートウェイアドレスを設定します。

PPP オプションで E1 インターフェースを構成するには、「67 ページの「PPP Option with PPP Tab Window ウィンドウ」」を参照してください。

Cisco HDLC で E1 インターフェースを構成するには、「69 ページの「Cisco HDLC Option with Cisco HDLC Tab ウィンドウ」」を参照してください。

8. ISDN Interface ウィンドウ

SSG 20 に ISDN Mini PIM をインストールしてある場合、次のウィンドウで brix/0 (Untrust) インターフェースを構成できます。

メモ： SSG 20 に ISDN Mini-PIM を 2 基インストールして、Multi-link（マルチリンク）オプションを選択すると、Physical Layer タブが 2 つ表示されます。

図 36: ISDN Physical Layer Tab ウィンドウ



表 21: ISDN Physical Layer Tab ウィンドウのフィールド

フィールド	説明
Switch Type	サービスプロバイダのスイッチタイプを設定します。 <ul style="list-style-type: none"> ■ att5e: At&T 5ESS ■ ntdms100: Nortel DMS 100 ■ ins-net: NTT INS-Net ■ etsi: European variants ■ ni1: National ISDN-1
SPID1	サービスプロバイダ ID は通常、オプションの番号を追加した 7 桁の電話番号です。SPID が必要なのは、DMS-100 と NI1 のスイッチタイプだけです。DMS-100 スwitchタイプには、2 つの SPID が B チャンネルに 1 つずつ割り当てられます。

フィールド	説明
SPID2	バックアップサービスプロバイダ ID
TEI Negotiation	スタートアップ時と最初の呼のどちらで TEI のネゴシエーションを行うかを指定します。通常、この設定は、ヨーロッパの ISDN サービスと、TEI ネゴシエーションを開始する DMS-100 スイッチとの接続に使用します。
Calling Number	ISDN ネットワークビリング番号
Sending Complete チェックボックス	発信セットアップメッセージに全情報の送信を有効にします。通常、香港や台湾以外では使用しません。

bri1/0 インターフェースはダイヤラ、マルチリンクダイヤラ、専用回線、BRI ダイアルによる接続に使用できます。オプションを選択しない、どちらかを選択する、あるいは両方を選択すると、次のようなウィンドウが表示されます。

図 37: ISDN Connection Tab ウィンドウ

Initial Configuration Wizard

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.

[bri1/0\(Untrust_Zone\)](#) [bgroup0\(Trust_Zone\)](#)
[eth0/1\(DMZ_Zone\)](#)

How does the Juniper device connect to the outside via bri1/0 interface?

Leased Line Mode (128Kbps): ☐

Dial Using BRI: ☐

Physical Layer **Dialer Interface**

Please create the PPP profile.

PPP Profile Name:

Authentication: ☒ Any ☐ CHAP ☐ PAP ☐ None

Local User:

Password:

Static IP: ☒

Interface Name: dialer 1

Encapsulation Type: ☒ PPP ☐ Multi-Link PPP

Primary Number:

Alternative Number: (Optional)

Dialer Pool:

Interface IP:

Netmask:

Gateway:

<< Previous Next >> Cancel

表 22: ISDN Connection Tab ウィンドウのフィールド

フィールド	説明
PPP Profile Name	ISDN インターフェースに PPP プロファイル名を設定します。
Authentication	PPP 認証タイプを設定します。 <ul style="list-style-type: none"> ■ Any ■ CHAP: チャレンジハンドシェイク式認証プロトコル ■ PAP: パスワード認証プロトコル ■ なし
Local User	ローカルユーザーを設定します。
Password	ローカルユーザーのパスワードを設定します。
Static IP チェックボックス	インターフェースの静的 IP アドレスを有効にします。
Interface IP	インターフェースの IP アドレスを設定します。
Interface Name (ダイヤラのみ)	ダイヤラインターフェース名を設定します。デフォルトは dialer.1 です。
Encapsulation Type	ダイヤラと BRI インターフェースによるダイヤラのカプセル化タイプを設定します。デフォルトは PPP です。
Primary Number	ダイヤラと BRI インターフェースによるダイヤラのプライマリ番号を設定します。
Alternative Number	プライマリ番号で接続できない場合に使用する代替 (セカンダリ) 番号を設定します。
Dialer Pool	ダイヤラインターフェースのダイヤラプール名を設定します。
Netmask	ネットマスクを設定します。
Gateway	ゲートウェイアドレスを設定します。

9. V.92 Modem Interface インターフェース

SSG 20 に V.92 Mini PIM をインストールしてある場合、次のウィンドウで serialx/0 (モデム) インターフェースを構成できます。

図 38: Modem Interface ウィンドウ

Initial Configuration Wizard

Juniper
SSG 20

Please click the following links or the above figure to configure interfaces.
[serial0/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

How does the Juniper device connect to the outside via serial0/0(Modem) interface?

Modem Name:

Init Strings:

ISP Name:

Primary Number:

Alternative Number: (Optional)

Login Name:

Password:

Confirm:

表 23: Modem Interface ウィンドウのフィールド

フィールド	説明
Modem Name	モデムインタフェース名を設定します。
Init String	モデムの初期化文字列を設定します。
ISP Name	サービスプロバイダに名前を割り当てます。
Primary Number	サービスプロバイダにアクセスするための電話番号を指定します。
Alternative Number	プライマリ番号で接続できない場合にサービスプロバイダにアクセスするための代替電話番号を指定します。
Login Name	サービスプロバイダアカウントのログイン名を設定します。
Password	ログイン名のパスワードを設定します。
Confirm	Password フィールドに入力したパスワードを確認します。

10. Eth0/0 Interface (Untrust Zone) ウィンドウ

eth0/0 インターフェースには、DHCP または PPPoE で静的 IP アドレスか動的 IP アドレスを割り当てることができます。

図 39: Eth0/0 Interface ウィンドウ

Initial Configuration Wizard

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.
[eth0/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

Enter the IP address and netmask for the interface eth0/0(untrust zone).

☐ Dynamic IP via DHCP
☐ Dynamic IP via PPPoE
 Username:
 Password:
 Confirm:
☒ Static IP
 Interface IP:
 Netmask:
 Gateway:

<< Previous Next >> Cancel

表 24: Eth0/0 Interface ウィンドウのフィールド

フィールド	説明
Dynamic IP via DHCP	サービスプロバイダから Untrust ゾーンの IP アドレスを受け取るよう SSG 20 を設定します。

フィールド	説明
Dynamic IP via PPPoE	PPPoE クライアントとして動作するように SSG 20 を設定し、サービスプロバイダから Untrust ゾーンインターフェースの IP アドレスを受け取ります。サービスプロバイダによって割り当てられたユーザー名とパスワードを入力します。
Static IP	Untrust ゾーンインターフェースに一意の固定 IP アドレスを割り当てます。Untrust ゾーンインタフェース IP アドレス、ネットマスク、ゲートウェイアドレスを入力します。

11. Eth0/1 Interface (DMZ Zone) ウィンドウ

eth0/1 インターフェースには、DHCP で静的 IP アドレスか動的 IP アドレスを割り当てるができます。

図 40: Eth0/1 Interface ウィンドウ

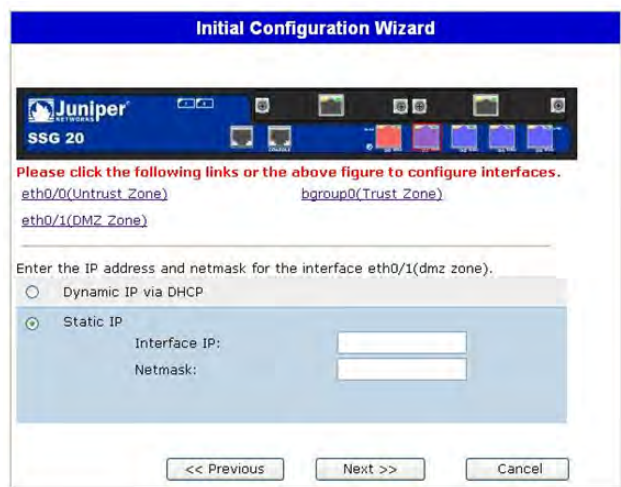


表 25: Eth0/1 Interface ウィンドウのフィールド

フィールド	説明
Dynamic IP via DHCP	サービスプロバイダから DMZ インターフェースの IP アドレスを受け取るよう SSG 20 を設定します。
Static IP	DMZ インターフェースに一意の固定 IP アドレスを割り当てます。DMZ インタフェース IP とネットマスクを入力します。

12. Bgroup0 Interface (Trust Zone) ウィンドウ

bgroup0 インターフェースには、DHCP で動的 IP アドレスを割り当てることができます。

デフォルトインターフェース IP アドレスは、**192.168.1.1** です。ネットマスクは **255.255.255.0** か **24** です。

図 41: Bgroup0 Interface ウィンドウ



表 26: Bgroup0 Interface ウィンドウのフィールド

フィールド	説明
Dynamic IP via DHCP	サービスプロバイダから Trust ゾーンの IP アドレスを受け取るよう SSG 20 を設定します。
Static IP	Trust ゾーンインターフェースに一意の固定 IP アドレスを割り当てます。Trust ゾーンインタフェース IP アドレスとネットマスクを入力します。

13. Wireless0/0 Interface (Trust Zone) ウィンドウ

SSG 20-WLAN を構成するときは、サービスセット識別子（SSID）を設定しないと wireless0/0 インターフェースを起動できません。ワイヤレスインターフェースの構成方法の詳細については、『*概念と用例 ScreenOS リファレンス ガイド*』を参照してください。

図 42: Wireless0/0 Interface ウィンドウ

The screenshot shows the 'Initial Configuration Wizard' for the 'Wireless0/0 Interface (Trust Zone)' on an SSG 20 device. The interface includes a Juniper logo and a status bar. The main configuration area has the following fields and options:

- Wlan Mode:** A dropdown menu currently set to '2.4G(802.11b/g)'.
- SSID:** A text input field.
- Authentication and Encryption:**
 - Open:** Selected by default, with 'No Encryption'.
 - WPA-PSK:** An option with a dropdown menu.
 - Passphrase(8~63 ASCII):** A text input field.
 - Confirm:** A text input field.
 - PSK(64 hexadecimal):** A text input field.
 - Confirm:** A text input field.
 - Encryption Type:** Radio buttons for 'Auto' (selected), 'TKIP', and 'AES'.
- Interface IP:** A text input field set to '192.168.2.1'.
- Netmask:** A text input field set to '255.255.255.0'.

At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

表 27: Wireless0/0 Interface ウィンドウのフィールド

フィールド	説明
Wlan Mode	WLAN 無線モードを設定します。 <ul style="list-style-type: none"> ■ 5 G (802.11a) ■ 2.4 G (802.11b/g) ■ 両方 (802.11a/b/g)
SSID	SSID 名を設定します。
Authentication and Encryption	WLAN インターフェース認証と暗号化を設定します。 <ul style="list-style-type: none"> ■ デフォルトの Open 認証では、誰でも SSG 20 をアクセスできます。この認証オプションに暗号化はありません。 ■ WPA Pre-Shared Key (WPA 事前共有鍵) 認証では、ワイヤレス接続のアクセス時に事前共有鍵 (PSK) またはパスフレーズを設定します。PSK の HEX 値か ASCII 値の入力を選択できます。HEX PSK は、256 ビット (64 テキスト文字) HEX 値とします。ASCII パスフレーズはテキスト文字 8 文字から 63 文字とします。このオプションの暗号化タイプには、Temporal Key Integrity Protocol (TKIP) または Advanced Encryption Standard (AES) を選択するか、Auto を選択して両方のオプションを有効にしてください。 ■ WPA2 事前共有鍵 ■ WPA オート事前共有鍵
Interface IP	WLAN インターフェースの IP アドレスを設定します。
Netmask	WLAN インターフェースネットマスクを設定します。

14. Interface Summary ウィンドウ

WAN インターフェースを構成すると、Interface Summary ウィンドウが表示されます。

図 43: Interface Summary ウィンドウ

Initial Configuration Wizard

Before proceeding further, review the following interface settings.

ISDN Configuration:			
Switch Type:	etsi		
SPID1:	32546564565	SPID2:	23488458235
TEI Negotiation:	first call	Calling Number:	01023456789
T310 Value:	10	Sending Complete:	enabled
Leased Line Mode:	disabled	Dialer Enable:	disabled
PPP Profile:	myprofile	Authentication:	any
Local User:	myuser	Password:	mypwd
PPP Static IP:	enabled	Interface IP:	122.122.122.122

```

set interface bril/0 isdn switch-type etsi
set interface bril/0 isdn spid1 "32546564565"
set interface bril/0 isdn spid2 "23488458235"
set interface bril/0 isdn tei-negotiation first-call
set interface bril/0 isdn calling-number "01023456789"
set interface bril/0 isdn t310-value "10"
  
```

Click Next to enter other configuration

<< Previous Next >> Cancel

インターフェース構成を確認し、問題がなければ **Next** をクリックします。Physical Ethernet DHCP ウィンドウが表示されます。

15. Physical Ethernet DHCP Interface ウィンドウ

Yes を選択します。これで、SSG 20 から DHCP 経由で有線ネットワークに IP アドレスを設定できます。ネットワークを使用するクライアントに SSG 20 で割り当てる IP アドレスの範囲を入力し、**Next** をクリックします。

図 44: Physical Ethernet DHCP Interface ウィンドウ

Initial Configuration Wizard

Do you want the Juniper device to dynamically assign IP addresses to your local **wired** hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses.

☐ Yes

IP Address Range Start: 192.168.1.33

End: 192.168.1.126

DNS Server 1 (optional):

DNS Server 2 (optional):

☒ No

<< Previous Next >> Cancel

16. Wireless DHCP Interface ウィンドウ

Yes を選択します。これで、SSG 20 から DHCP 経由でワイヤレスネットワークに IP アドレスを設定できます。ネットワークを使用するクライアントに SSG 20 で割り当てる IP アドレスの範囲を入力し、**Next** をクリックします。

図 45: Wireless DHCP Interface ウィンドウ

Initial Configuration Wizard

Do you want the Juniper device to dynamically assign IP addresses to your local **wireless** hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses.

☐ Yes

IP Address Range Start: 192.168.2.33

End: 192.168.2.126

DNS Server 1 (optional):

DNS Server 2 (optional):

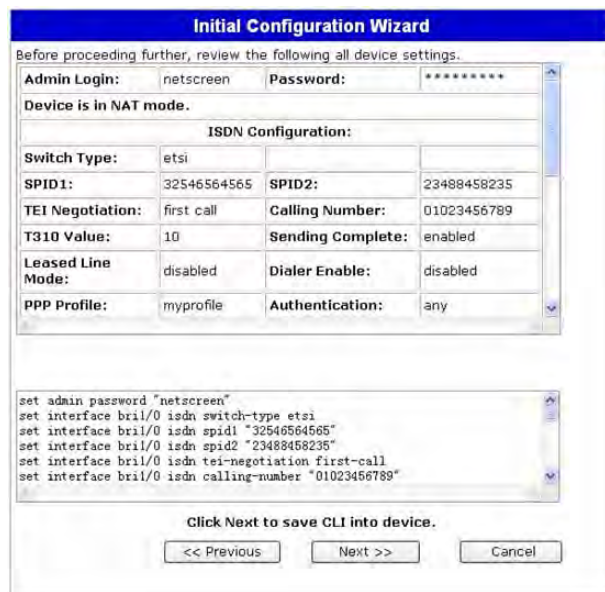
☒ No

<< Previous Next >> Cancel

17. Confirmation ウィンドウ

必要に応じて、SSG 20 の構成と変更結果を確認します。**Next** をクリックして構成や変更結果を保存し、SSG 20 をリブートして構成を実行します。

図 46: Confirmation ウィンドウ



The image shows a screenshot of the 'Initial Configuration Wizard' window. At the top, it says 'Before proceeding further, review the following all device settings.' Below this, there are fields for 'Admin Login: netscreen' and 'Password: *****'. A message states 'Device is in NAT mode.' The main section is titled 'ISDN Configuration:' and contains a table with the following settings:

Switch Type:	etsi		
SPID1:	32546564565	SPID2:	23488458235
TEI Negotiation:	first call	Calling Number:	01023456789
T310 Value:	10	Sending Complete:	enabled
Leased Line Mode:	disabled	Dialer Enable:	disabled
PPP Profile:	myprofile	Authentication:	any

Below the table, there is a text area showing the CLI commands that will be executed:

```
set admin password "netscreen"
set interface bri1/0 isdn switch-type etsi
set interface bri1/0 isdn spid1 "32546564565"
set interface bri1/0 isdn spid2 "23488458235"
set interface bri1/0 isdn tei-negotiation first-call
set interface bri1/0 isdn calling-number "01023456789"
```

At the bottom, there is a message 'Click Next to save CLI into device.' and three buttons: '<< Previous', 'Next >>', and 'Cancel'.

保存したシステム構成で SSG 20 がリブートすると、WebUI ログインプロンプトが表示されます。WebUI による SSG 20 のアクセス方法については、「27 ページの「WebUI の使用」」を参照してください。

索引

ADSL	
インターフェースの構成	39
ケーブルの接続	21
ポートの接続	21
Mini-PIM	
取り外し	50
Point-to-Point Protocol over ATM	
PPPoA を参照	
Point-to-Point Protocol over Ethernet	
PPPoE を参照	
VPI/VCI	
値	39
構成	40
ケーブル	
基本ネットワーク接続	20
ワイヤレス	
デフォルトインターフェースの使用	23

A	
AAL5 多重化	39
Annex A	21
Annex B	21
ATM Adaptation Layer 5	39

I	
ISP IP アドレスとネットマスク	42

L	
LED	
PIM 1	11
PIM 2	11
POWER	11
STATUS	11
イーサネットポートのアクティビティリンク	12

M	
Mini-PIM	
ブランク面板	50
取り付け	51

P	
PPPoA	39
PPPoE	39

U	
Untrust ゾーンにバックアップインターフェース	34
Untrust ゾーン、バックアップインターフェースの構成	34

W	
WLAN LED	
802.11a	11
b/g	11

あ	
アンテナ	23

か	
仮想パス識別子 / 仮想チャネル識別子	
VPI/VCI 参照	
管理	
WebUI で	27
Telnet 接続による	28
コンソールによる	26

け	
ケーブル	
ADSL	21
シリアル	21

こ	
構成	
ADSL 2/2 + Mini-PIM	39
E1 Mini-PIM	44
ISDN Mini-PIM	43
T1 Mini-PIM	44
USB	16
V.92 モデム Mini-PIM	45
VPI/VCI ペア	40
デフォルトルート	34
ブリッジグループ (bgroup)	32
仮想回路	39
管理アクセス	33
管理アドレス	34
管理サービス	33
管理者名とパスワード	31
バックアップ Untrust インターフェース	34
日付と時刻	31
ホストとドメイン名	33
ワイヤレスとイーサネットの組み合わせ	38
ワイヤレス認証と暗号化	36

せ	
静的 IP アドレス	39
接続、基本ネットワーク	20

た	
多重化、構成	40

て

デフォルト ip アドレス	30
---------------------	----

ほ

保証

EMC (イミューティ)	56
EMC (エミッション)	56
T1 インターフェース	57
安全性	56
欧州電気通信標準化機構 (ETSI)	57

む

無線トランシーバ

WLAN 0	15
WLAN 1	15

め

メモリのアップグレード手順	52
---------------------	----

り

リセットスイッチ、使用	47
-------------------	----

わ

ワイヤレス

アンテナ	23
------------	----

目录

关于本指南	5
组织结构	6
WebUI 约定	6
CLI 约定	7
获取文档和技术支持	7
第 1 章 硬件概述	9
端口和电源连接器	10
前面板	11
系统状态 LED	11
端口说明	12
以太网端口	12
控制台端口	13
AUX 端口	13
小型物理接口模块端口说明	14
后面板	16
电源适配器	16
无线电收发器	16
接地片	17
天线类型	17
USB 端口	17
第 2 章 安装和连接设备	19
准备工作	20
安装设备	20
将接口电缆连接到设备	22
连接电源	22
将设备连接到网络	22
将设备连接到不可信网络	22
以太网端口	23
串行 (AUX/ 控制台) 端口	23
将小型 PIM 连接到不可信网络	24
ADSL2/2+ 小型 PIM	24
ISDN、T1、E1 和 V.92 小型 PIM	25
将设备连接到内部网络或工作站	25
以太网端口	25
无线天线	25
第 3 章 配置设备	27
访问设备	28
使用控制台连接	28
使用 WebUI	29

使用 Telnet	30
缺省设备设置	30
基本设备配置	32
根 Admin 名称和密码	32
日期和时间	33
桥接组接口	33
管理存取	34
管理服务	34
主机名和域名	34
缺省路由	35
管理接口地址	35
备份 Untrust 接口配置	35
基本无线配置	36
小型 PIM 配置	39
ADSL2/2 + 接口	39
虚拟电路	40
VPI/VCI 和多路传输方法	41
PPPoE 或 PPPoA	41
静态 IP 地址和网络掩码	42
ISDN 接口	43
T1 接口	44
E1 接口	44
V.92 调制解调器接口	45
基本防火墙保护	46
验证外部连通性	46
将设备重置为出厂缺省值	47
第 4 章 维护设备	49
需要的工具和部件	49
更换小型物理接口模块	49
移除空面板	50
移除小型 PIM	50
安装小型 PIM	51
升级内存	52
附录 A 规格	55
物理	56
电气	56
环境忍耐力	56
证书	57
安全	57
EMC 辐射	57
EMC 抗扰度	57
ETSI	57
T1 接口	58
连接器	58
附录 B 初始配置向导	61
索引	83

关于本指南

Juniper Networks 安全服务网关 (SSG) 20 设备是一种集成路由器和防火墙平台，可为分公司或零售渠道提供“互联网协议安全”(IPSec)、“虚拟专用网”(VPN) 和防火墙服务。

Juniper Networks 提供两种型号的 SSG 20 设备：

- 支持辅助 (AUX) 连通性的 SSG 20
- 支持集成式 802.11a/b/g 无线标准的 SSG 20-WLAN

两种型号的 SSG 20 设备都支持通用串行总线 (USB) 存储功能，并且都带有两个小型物理接口模块 (PIM) 插槽，可支持任何小型 PIM。此外，设备还提供局域网 (LAN) 与广域网 (WAN) 之间的协议转换。

注意： 本文档中的配置说明和范例均指运行 ScreenOS 5.4 的设备所具有的功能。根据运行的 ScreenOS 版本的不同，设备的功能也可能有所不同。有关最新设备文档的信息，请参阅 Juniper Networks 技术出版物网站 <http://www.juniper.net/techpubs/hardware>。要查看设备当前可用的 ScreenOS 版本，请访问 Juniper Networks 支持网站 <http://www.juniper.net/customers/support/>。

组织结构

本指南包含以下部分：

- 第 1 章，“硬件概述”介绍 SSG 20 设备的机箱和组件。
- 第 2 章，“安装和连接设备”介绍如何安装 SSG 20 设备以及如何将电缆和电源连接到设备。
- 第 3 章，“配置设备”介绍如何配置和管理 SSG 20 设备以及如何执行某些基本配置任务。
- 第 4 章，“维护设备”介绍 SSG 20 设备的保养和维护过程。
- 附录 A，“规格”提供 SSG 20 设备的通用系统规格。
- 附录 B，“初始配置向导”提供有关 SSG 20 设备的初始配置向导 (ICW) 的详细信息。

WebUI 约定

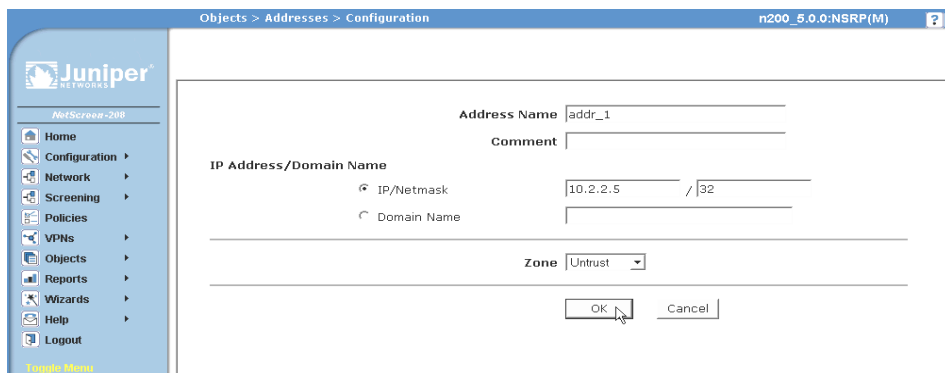
要用 WebUI 执行任务，首先导航到相应的对话框，然后在该对话框中定义对象和设置参数。V 形符号 (>) 指示在 WebUI 中导航的顺序，使用时单击菜单选项和链接即可。每个任务的指令集都分为导航路径和配置设置：

下图列出进入地址配置对话框的路径，采用的是下面的示例配置设置：

Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**：

Address Name: addr_1
 IP Address/Domain Name:
 IP/Netmask: (选择), 10.2.2.5/32
 Zone: Untrust

图 1: 导航路径和配置设置



CLI 约定

在范例和文本中出现 CLI 命令的语法时，使用下列约定。

在范例中：

- 在中括号 [] 中的任何内容都是可选的。
- 大括号 { } 中的任何内容都是必需项。
- 如果有多个选项，则使用竖线 (|) 分隔每个选项。例如：

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

意思就是“设置 ethernet1、ethernet2 或 ethernet3 接口的管理选项”。

- 变量为斜体形式：

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

在文本中：

- 命令为**粗体**形式。
- 变量为斜体形式。

注意： 输入关键字时，只需键入足以唯一标识相关单词的字母即可。例如，要输入命令 **set admin user kathleen j12fmt54**，只需输入 **set adm u kath j12fmt54**。尽管输入命令时可以使用此捷径，但本文所述的所有命令都以完整的方式提供。

获取文档和技术支持

要获取任何 Juniper Networks 产品的技术文档，请访问 www.juniper.net/techpubs/。

要获取技术支持，请使用 <http://www.juniper.net/support/> 中的 Case Manager 链接打开支持案例，还可拨打电话 1-888-314-JTAC (美国国内) 或 1-408-745-9500 (美国以外)。

如果在本文档中发现任何错误或遗漏，请通过下面的电子邮件地址与我们联系：

techpubs-comments@juniper.net

第 1 章

硬件概述

本章提供了有关 SSG 20 机箱及其组件的详细说明。其中包括以下部分：

- 第 10 页上的“端口和电源连接器”
- 第 11 页上的“前面板”
- 第 16 页上的“后面板”

端口和电源连接器

本节介绍和显示内置端口和电源连接器的位置。请参阅下图以了解内置端口的位
置和参阅表 1 以了解有关电源连接器的说明。

图 2: 内置端口和小型 PIM 的位置

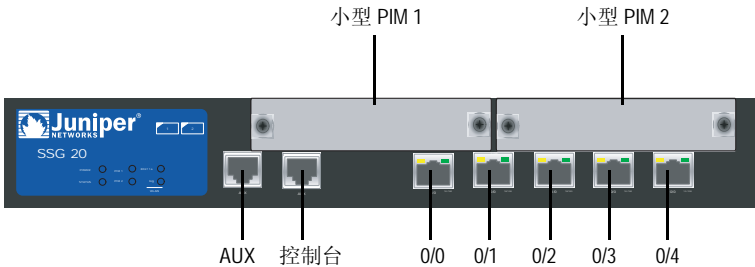


表 1: SSG 20 端口和电源连接器

端口	说明	连接器	速度 / 协议
0/0-0/4	通过交换机或集线器实现至工作站的直接连接或 LAN 连接。此连接也可通过 Telnet 会话或 WebUI 来管理设备。	RJ-45	10/100 Mbps 以太网 自动检测双工和自动 MDI/MDIX
USB	实现与系统之间的 1.1 USB 连接。	不适用	12M (全速) 或 1.5M (低速)
控制台	实现与系统之间的串行连接。用于终端仿真连接以启动 CLI 会话。	RJ-45	9600 bps/RS-232C 串行
AUX	通过外部调制解调器实现备份 RS-232 异步串行互联网连接。	RJ-45	9600 bps - 115 Kbps/RS-232C 串行
小型 PIM			
ADSL 2/2 +	通过 ADSL 数据链路实现互联网连接。	RJ-11 (Annex A) RJ-45 (Annex B)	ANSI T1.413 Issue 2 (仅 Annex A) ITU G.992.1 (G.dmt) ITU G.992.3 (ADSL2) ITU G.992.5 (ADSL2 +)
V.92 调制解调器	实现到服务提供商的主要互联网连接或备份互联网连接，或者主要不可信网络连接或备份不可信网络连接。	RJ-11	9600 bps - 115 Kbps/RS-232 串行自动检测双工和极性
T1	实现到不可信网络的 T1 线路的连接。	RJ-45	1.544 Mbps (全时槽)
E1	实现到不可信网络的 E1 线路的连接。	RJ-45	2.048 Mbps (全时槽)
ISDN	可将 ISDN 线路用作不可信或备份接口。(S/T)	RJ-45	B 信道为 64 Kbps 租用线路为 128 Kbps
天线 A 和天线 B (SSG 20-WLAN)	在无线电连接附近实现到工作站的直接连接。	RPSMA	802.11a (无线电波段为 5 GHz 时传输速度为 54 Mbps) 802.11b (无线电波段为 2.4 GHz 时传输速度为 11 Mbps) 802.11g (无线电波段为 2.4 GHz 时传输速度为 54 Mbps) 802.11 superG (无线电波段为 2.4 GHz 和 5 GHz 时传输速度为 108 Mbps)

前面板

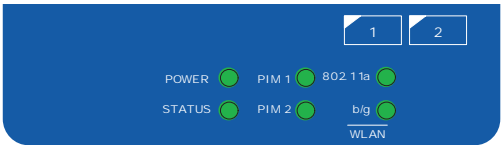
本节介绍 SSG 20 设备前面板上的以下元素：

- 系统状态 LED
- 端口说明
- 小型物理接口模块端口说明

系统状态 LED

系统状态 LED 显示有关主要设备功能的信息。图 3 说明了 SSG 20-WLAN 设备前面板上各状态 LED 的位置。WLAN LED 仅出现在 SSG 20-WLAN 设备上。

图 3: 状态 LED



启动系统后，POWER LED 从关闭状态变为闪烁绿色状态，而 STATUS LED 则按以下顺序发生变化：红色、绿色、闪烁绿色。完成启动这一过程大约需要两分钟时间。如果要在关闭系统后重新启动系统，建议在关闭之后和重新启动之前稍候几秒。表 2 提供了各系统状态 LED 的名称、颜色、状态和说明。

表 2: 状态 LED 说明

名称	颜色	状态	说明
POWER	绿色	始终为开	表示系统已通电。
		关	表示系统没有通电。
	红色	始终为开	表示设备未正常运行。
		关	表示设备正常运行。
STATUS	绿色	始终为开	表示系统正在启动或正在执行诊断。
		闪烁	表示设备正常运行。
	红色	闪烁	表示检测到错误。
PIM 1	绿色	始终为开	表示此小型 PIM 正在起作用。
		闪烁	表示此小型 PIM 正在传输信息流。
		关	表示此小型 PIM 未起作用。

名称	颜色	状态	说明
PIM 2	绿色	始终为开	表示此小型 PIM 正在起作用。
		闪烁	表示此小型 PIM 正在传输信息流。
		关	表示此小型 PIM 未起作用。
WLAN (仅在 WLAN 设备上)			
802.11a	绿色	始终为开	表示已建立无线连接，但无链接活动。
		慢速闪烁	表示已建立无线连接。波特率与链接活动成比例。
		关	表示未建立无线连接。
b/g	绿色	始终为开	表示已建立无线连接，但无链接活动。
		慢速闪烁	表示已建立无线连接。波特率与链接活动成比例。
		关	表示未建立无线连接。

端口说明

本节介绍以下端口的目的和功能：

- 以太网端口
- 控制台端口
- AUX 端口

以太网端口

五个 10/100 以太网端口提供了到集线器、交换机、本地服务器和工作站的 LAN 连接。也可指定一个以太网端口来管理信息流。各端口被标记为 0/0 到 0/4。有关各以太网端口缺省区段绑定的信息，请参阅第 30 页上的“缺省设备设置”。

配置各端口时，请参考与端口位置相对应的接口名称。前面板上从左至右，端口的接口名称依次为 ethernet0/0 到 ethernet0/4。

图 4 显示了各以太网端口上 LED 的位置。

图 4: 活动链接 LED 位置

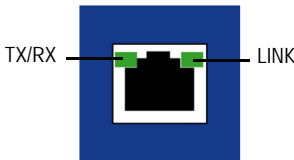


表 3 介绍以太网端口 LED。

表 3: LAN 端口 LED

名称	颜色	状态	说明
LINK	绿色	始终为开 关	端口在线。 端口离线。
TX/RX	绿色	闪烁 关	信息流正在通过。波特率与链接活动成比例。 端口可能正在使用中，但并未接收数据。

控制台端口

控制台端口为 RJ-45 串行端口，将充当数据电路终端设备 (DCE)，用于进行本地管理。进行终端连接时，请使用直通电缆；连接到另一 DCE 设备时，请使用交叉电缆。提供了 RJ-45 到 DB-9 适配器。

有关 RJ-45 连接器插脚引线的信息，请参阅第 58 页上的“连接器”。

AUX 端口

辅助 (AUX) 端口为 RJ-45 串行端口，将充当数据终端设备 (DTE)，通过将其连接到调制解调器可实现远程管理。建议不要将此端口用于进行日常远程管理。通常将 AUX 端口指定为备份串行接口。可以调节波特率，范围从 9600 bps 到 115200 bps，并且需要使用硬件流程控制。连接到调制解调器时，请使用直通电缆；连接到另一 DTE 设备时，请使用交叉电缆。

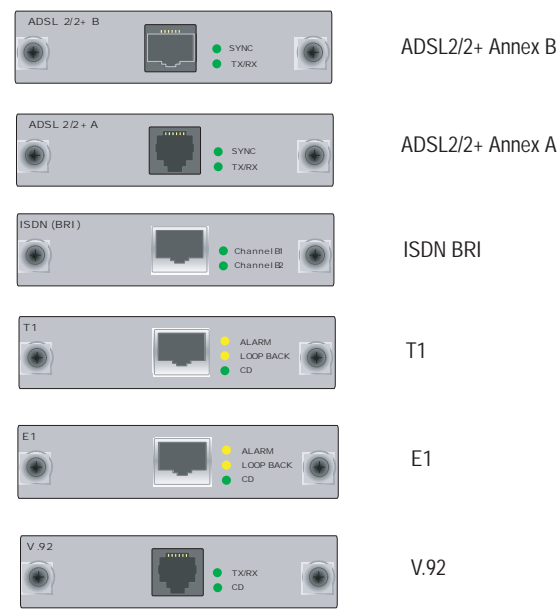
有关 RJ-45 连接器插脚引线的信息，请参阅第 58 页上的“连接器”。

小型物理接口模块端口说明

设备上支持的各小型物理接口模块 (PIM) 都具有以下组件：

- 一个电缆连接器端口 - 接受网络媒体连接器。图 5 显示了可用的小型 PIM。最多可在一个设备上安装两个小型 PIM。

图 5: SSG 20 的小型 PIM



- 两个到三个状态 LED - 指示端口状态。表 4 介绍 LED 状态的含义。

表 4: SSG 20 上的小型 PIM LED 状态

类型	名称	颜色	状态	说明
ADSL 2/2 + (Annex A 和 B)	SYNC	绿色	始终为开	表示 ADSL 接口已就绪
			闪烁	表示正在进行通信
			关	表示接口闲置
	TX/RX	绿色	闪烁	表示正在交换信息流
			关	表示没有交换信息流
ISDN (BRI)	CH B1	绿色	始终为开	表示 B 信道 1 处于活动状态
			关	表示 B 信道 1 处于非活动状态
	CH B2	绿色	始终为开	表示 B 信道 2 处于活动状态
			关	表示 B 信道 2 处于非活动状态
T1/E1	ALARM	黄色	始终为开	表示存在本地警告或远程警告；设备已检测到故障
			关	表示没有警告或故障
	LOOP BACK	黄色	始终为开	表示检测到回传或链路状态
			关	表示回传处于非活动状态
	CD	绿色	始终为开	表示检测到载波器，并且小型 PIM 中的内部 DSU/CSU 正在与另一 DSU/CSU 通信
			关	表示载波检测处于非活动状态
V.92	CD	绿色	始终为开	表示链接处于活动状态
			关	表示串行接口处于非服务状态
	TX/RX	绿色	闪烁	表示正在交换信息流
			关	表示没有交换信息流



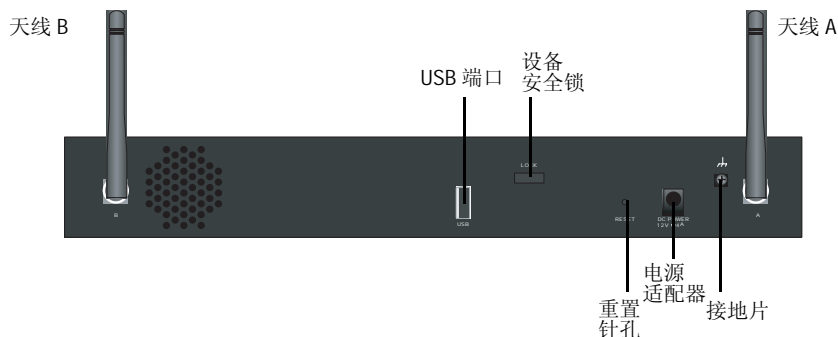
小心：小型 PIM 不具有热插拔功能。必须将其安装在前面板插槽中，然后再打开设备电源。

后面板

本节介绍 SSG 20 设备后面板上的以下元素：

- 电源适配器
- 无线电收发器
- 接地片
- 天线类型
- USB 端口

图 6: SSG 20-WLAN 设备的后面板



电源适配器

设备前面板上的 POWER LED 呈绿色或为关闭状态。绿色表示运行正常，关闭表示电源适配器故障或设备处于关闭状态。

无线电收发器

SSG 20-WLAN 包含两个具有无线连通性的无线电收发器，这些收发器支持 802.11a/b/g 标准。第一个收发器 (WLAN 0) 使用 2.4 GHz 无线电波段，它在传输速度为 11 Mbps 时支持 802.11b 标准，在传输速度为 54 Mbps 时支持 802.11g 标准，在传输速度为 108 Mbps 时支持 802.11 SuperG 标准。第二个无线电收发器 (WLAN 1) 使用 5GHz 无线电波段，它在传输速度为 54 Mbps 时支持 802.11a 标准。有关配置无线电波段的信息，请参阅第 36 页上的“基本无线配置”。

接地片

机箱后部提供一个单孔接地片，可使用此接地片将设备接地（请参阅图 6）。

要在连接电源前将设备接地，请将接地电缆连接到地面，然后将电缆连接到机箱后部的接地片上。

天线类型

SSG 20-WLAN 设备支持三种类型的定制无线电天线：

- **分集天线** - 分集天线可提供 2dBi 定向覆盖，并且覆盖区域内的信号强度电平相当均衡，适合大部分安装。设备随带有此类天线。
- **外部全向天线** - 外部天线可提供 2dBi 全向覆盖。与成对运行的分集天线不同，外部天线用于消除某些时候在使用两个天线时由信号的些微延迟特性所产生的回波效应。
- **外部定向天线** - 外部定向天线可提供 2dBi 单向覆盖，适合安装在诸如走廊和外墙之类的位置（天线朝内）。

USB 端口

SSG 20 设备后面板上的 USB 端口接受安装有袖珍闪存盘的通用串行总线 (USB) 存储设备或 USB 存储设备适配器（如 CompactFlash 协会发布的 *CompactFlash Specification* 中所定义）。安装和配置 USB 存储设备后，它会在主袖珍闪存盘无法启动时自动充当第二启动设备。

USB 端口允许文件在外部 USB 存储设备与安全设备中的内部闪存之间传输各种数据，如设备配置、用户证书和更新版本映像等信息。USB 端口在低速 (1.5M) 或全速 (12M) 文件传输时均支持 USB 1.1 规格。

要在 USB 存储设备和 SSG 20 之间传输文件，请执行以下步骤：

1. 将 USB 存储设备插入安全设备上的 USB 端口中。
2. 使用 **save {software | config | image-key} from usb 文件名 to flash** CLI 命令将文件从 USB 存储设备保存到设备的内部闪存中。
3. 取出 USB 存储设备前，使用 **exec usb-device stop** CLI 命令停止 USB 端口。
4. 现在可安全取出 USB 存储设备。

如果要从 USB 存储设备删除文件，请使用 **delete file usb:/ 文件名** CLI 命令。

如果要查看 USB 存储设备或内部闪存上保存的文件信息，请使用 **get file** CLI 命令。

第 2 章

安装和连接设备

本章介绍如何安装 SSG 20 设备以及如何将电缆和电源连接到本设备。其中包括以下部分：

- 第 20 页上的“准备工作”
- 第 20 页上的“安装设备”
- 第 22 页上的“将接口电缆连接到设备”
- 第 22 页上的“连接电源”
- 第 22 页上的“将设备连接到网络”

注意： 有关安全警告和说明，请参阅 *Juniper Networks Security Products Safety Guide*。在使用任何设备之前，应注意由电路引发的危险以及熟悉标准操作以防止意外事故的发生。

准备工作

机箱位置、安装设备的布局以及布线间的安全对于系统的正常运行而言均至关重要。



警告：为防止未经授权人员的误用和侵入，应将 SSG 20 设备安装在安全的环境中。

遵守以下预防措施可防止出现关机、设备故障以及人身伤害：

- 安装前，请务必确定此设备电源与任何电源断开连接。
- 确保运行设备的房间保持良好的通风状况，并且室温不超过 104°F (40°C)。
- 请勿将设备放置在会阻塞设备进气口或排气口的设备机架中。确保封闭式机架具有风扇且各面装有百叶窗板。
- 执行任何安装前，请改善并消除以下危险状况：地面潮湿、存在渗漏、电缆未接地或已磨损，或者未进行安全接地。

安装设备

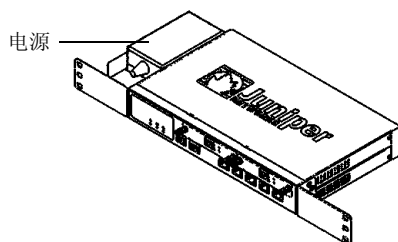
可以前置安装、壁式安装或桌面安装的方式安装 SSG 20 设备。可单独购买安装套件。

要安装 SSG 20 设备，您需要一个 2 号十字螺丝起子（未提供）和若干与设备机架相匹配的螺丝（已包括在套件中）。

注意： 安装设备时，请确保可将此设备连接到电源插座。

要将 SSG 20 设备以前置安装的方式安装到一个标准的 19 英寸设备机架上，请执行以下步骤：

图 7: SSG 20 前置安装

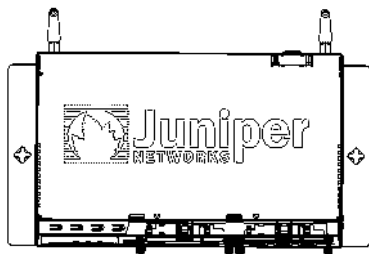


1. 将电源机架安装耳对准设备的左前边缘处。
2. 将螺丝放入孔中并使用十字螺丝起子将其固定。
3. 将其它机架安装耳对准设备的右前边缘处。

4. 将螺丝放入孔中并使用十字螺丝起子将其固定。
5. 使用提供的螺丝将设备安装到机架上。
6. 将电源插入电源插座。

要以壁式安装的方式安装 SSG 20 设备，请执行以下步骤：

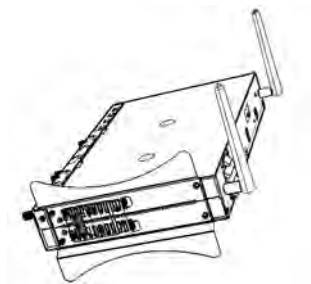
图 8: SSG 20 壁式安装



1. 将墙壁安装耳对准设备。
2. 将螺丝放入孔中并使用十字螺丝起子将其固定。
3. 确保要使用的墙壁表面光滑、平整、干燥且坚固。
4. 使用提供的螺丝将设备安装到墙壁上。
5. 将电源插入电源插座。

要以桌面安装的方式安装 SSG 20 设备，请执行以下步骤：

图 9: SSG 20 桌面安装



1. 将桌面支架安装到设备一侧。建议使用靠近电源适配器的一侧。
2. 将装有桌面支架的设备放置在桌面上。
3. 插入电源适配器，并将电源连接到电源插座。

将接口电缆连接到设备

要将接口电缆连接到设备，请执行以下步骤：

1. 准备一段适用于接口的电缆。
2. 将电缆连接器插入接口面板上的电缆连接器端口中。
3. 按以下方式排列电缆以防止其移动或成为受力点：
 - a. 固定电缆，使其在悬挂到地板时不用承受其自身的重量。
 - b. 将所有多余电缆整齐地盘绕成圆环状。
 - c. 使用紧固件以保持电缆线圈的形状。

连接电源

要将电源连接到设备，请执行以下步骤：

1. 将电缆的 DC 连接器端插入设备后面的 DC 电源插座。
2. 将电缆的 AC 适配器端插入 AC 电源。



警告：建议将电涌保护器用于电源连接。

将设备连接到网络

当将 SSG 20 设备放置在内部网络和不可信网络之间时，它可为网络提供防火墙和通用安全保障。本节介绍以下内容：

- 将设备连接到不可信网络
- 将设备连接到内部网络或工作站

将设备连接到不可信网络

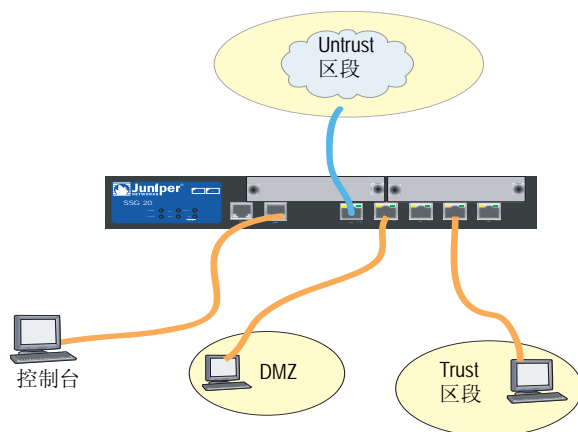
可通过以下方法中的一种将 SSG 20 设备连接到不可信网络：

- 以太网端口
- 串行 (AUX/ 控制台) 端口
- 将小型 PIM 连接到不可信网络

图 10 显示了带有基本网络电缆连接的 SSG 20，其中两个空白小型 PIM 和 10/100 以太网端口的电缆连接方式如下：

- 将标记为 0/0 的端口 (ethernet0/0 接口) 连接到不可信网络。
- 将标记为 0/1 的端口 (ethernet0/1 接口) 连接到 DMZ 安全区段中的工作站。
- 将标记为 0/3 的端口 (bgroup0 接口) 连接到 Trust 安全区段中的工作站。
- 将控制台端口连接到串行终端以进行管理访问。

图 10: 基本网络连接范例



以太网端口

要建立高速连接，请将提供的以太网电缆从 SSG 20 设备上标记为 0/0 的以太网端口连接到外部路由器。设备将自动检测正确的速度、双工和 MDI/MDIX 设置。

串行 (AUX/ 控制台) 端口

可通过 RJ-45 直通串行电缆和外部调制解调器连接到不可信网络。



警告：请勿因疏忽而将设备上的“控制台”、“AUX”或“以太网”端口连接到电话接口。

将小型 PIM 连接到不可信网络

本节介绍如何将小型 PIM 设备连接到不可信网络。

ADSL2/2+ 小型 PIM

将提供的 ADSL 电缆从 ADSL2/2+ 小型 PIM 连接到电话接口。Annex A 版设备上的 ADSL 端口使用 RJ-11 连接器，而 Annex B 版上的 ADSL 端口则使用 RJ-45 连接器。使用 Annex B 型号时，从 ADSL 端口连接到电话接口的电缆与直通 10 Base-T 以太网电缆的外观和布线方式完全相同。

连接分离器 and 微型过滤器

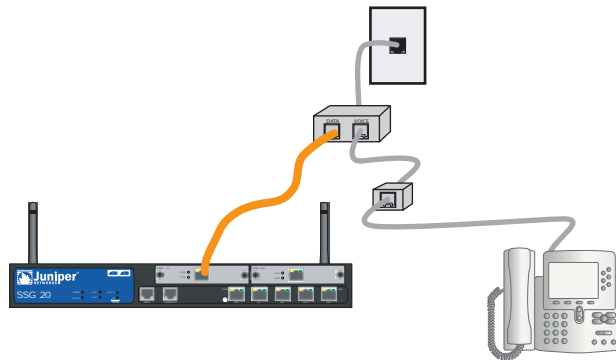
信号分离器将电话信号分为用于语音呼叫的低频语音信号和用于数据信息流的高频数据信号。服务提供商通常将分离器作为设备的一部分来安装，用以连接站点电话线路和提供商网络。

也可自行安装的分离器，具体情况视服务提供商的设备而定。如果要自行安装此类分离器，则需从设备将 ADSL 电缆和电话线连接到分离器上相应的连接器（例如，“数据”或“语音”）。将分离器的另一端连接到电话接口。

可能需要在连接到 ADSL 线路的各部电话、传真机、电话答录机或模拟调制解调器上安装 *微型过滤器*。微型过滤器将过滤掉电话线路上的高频噪音。在电话、传真机、电话答录机或模拟调制解调器与分离器上的语音连接器间的电话线上安装微型过滤器。

图 11 显示了安装在站点上的微型过滤器和分离器的一个范例。（必须从服务提供商处获取合适的微型过滤器或分离器。）

图 11: 网络连接上的微型过滤器和分离器



ISDN、T1、E1 和 V.92 小型 PIM

要将小型 PIM 连接到设备，请执行以下步骤：

1. 准备一段适用于接口的电缆。
2. 将电缆连接器插入接口面板上的电缆连接器端口中。
3. 按以下方式排列电缆以防止其移动或成为受力点：
 - a. 固定电缆，使其在悬挂到地板时不用承受其自身的重量。
 - b. 将所有多余电缆整齐地盘绕成圆环状。
 - c. 使用紧固件以保持电缆线圈的形状。

要配置 ISDN、E1、T1 或 V.92 小型 PIM，请参阅第 39 页上的“小型 PIM 配置”。

将设备连接到内部网络或工作站

可将局域网 (LAN) 或工作站与以太网和 / 或无线接口相连。

以太网端口

SSG 20 设备包含五个以太网端口。可使用这些端口中的一个或多个通过交换机或集线器连接到 LAN。也可以直接将一个或所有的端口连接到工作站，排除集线器或交换机的需求。可使用交叉电缆或直通电缆将以太网端口连接到其它设备。有关缺省区段到接口绑定的信息，请参阅第 30 页上的“缺省设备设置”。

无线天线

如果要使用无线接口，需连接所提供的设备上的天线。如果有标准 2dB 分集天线，请使用螺丝将它们安装到设备背面标记为 A 和 B 的接头上。在各天线弯曲处顺势弯曲，以免使隔板连接器受压。

图 12: SSG 20-WLAN 天线位置



如果要使用可选的外部天线，请遵循此天线附带的连接说明。

第 3 章

配置设备

SSG 20 设备上已经预先安装了 ScreenOS 软件。打开设备电源后，即可对其进行配置。尽管设备有缺省的出厂配置，可以先连接到设备，但需要进行进一步配置以满足特定的网络需求。

本章包括以下各节：

- 第 28 页上的“访问设备”
- 第 30 页上的“缺省设备设置”
- 第 32 页上的“基本设备配置”
- 第 36 页上的“基本无线配置”
- 第 39 页上的“小型 PIM 配置”
- 第 46 页上的“基本防火墙保护”
- 第 46 页上的“验证外部连通性”
- 第 47 页上的“将设备重置为出厂缺省值”

注意： 在配置设备并通过远程网络验证连通性后，必须在 www.juniper.net/support/ 上注册产品，以便能在设备中激活某些 ScreenOS 服务，如深入检查签名服务和防病毒（单独购买）。在注册完产品之后，使用 WebUI 获得对服务的预订。有关注册产品和获得对特定服务的预订的详细信息，请参阅设备上运行的 ScreenOS 版本的概念与范例 ScreenOS 参考指南中的基本原理卷。

访问设备

可以用几种方法配置和管理设备：

- 控制台：设备上的“控制台”端口用于通过连接到工作站或终端的串行电缆来访问设备。要配置设备，请在终端或工作站上的终端仿真程序中输入 ScreenOS 命令行界面 (CLI) 命令。
- WebUI: ScreenOS Web 用户界面 (WebUI) 是一个可以通过浏览器使用的图形接口。最初使用 WebUI 时，运行浏览器的工作站必须与设备处于同一子网中。还可使用带有安全 HTTP (S-HTTP) 的安全套接字层 (SSL)，通过安全服务器访问 WebUI。
- Telnet/SSH: Telnet 和 SSH 是可以通过 IP 网络访问设备的应用程序。要配置设备，请在工作站的 Telnet 会话中输入 ScreenOS CLI 命令。有关详细信息，请参阅 *概念与范例 ScreenOS 参考指南* 中的 *管理* 卷。
- NetScreen-Security Manager: NetScreen-Security Manager 是 Juniper Networks 的企业级管理应用程序，用于控制和管理 Juniper Networks 防火墙 /IPSec VPN 设备。有关如何使用 NetScreen-Security Manager 管理设备的说明，请参阅 *NetScreen-Security Manager Administrator's Guide*。

使用控制台连接

注意： 将带有阳性 RJ-45 连接器的直通 RJ-45 CAT5 串行电缆插入设备的控制台端口。

要建立控制台连接，请执行以下步骤：

1. 将提供的 DB-9 适配器的凹端插入工作站的串行端口。(确保 DB-9 正确插入并固定。) 图 13 显示了所需的 DB-9 连接器类型。

图 13: DB-9 适配器



2. 将 RJ-45 CAT5 串行电缆的凸端插入 SSG 20 的控制台端口。(确保将 CAT5 电缆的另一端正确插入并固定在 DB-9 适配器中。)

3. 在工作站上启动串行终端仿真程序。启动控制台会话需要如下设置：

- 波特率：9600
- 奇偶：无
- 数据位：8
- 停止位：1
- 流量控制：无

4. 如果尚未更改 admin 名称和密码的缺省登录，请在登录名和密码提示中都输入 **netscreen**。（仅使用小写字母。登录名和密码字段都区分大小写。）

有关如何使用 CLI 命令配置设备的信息，请参阅 *概念与范例 ScreenOS 参考指南*。

5. （可选）在缺省情况下，空闲时间超过 10 分钟后控制台将超时并自动终止。要清除超时，请输入 **set console timeout 0**。

使用 WebUI

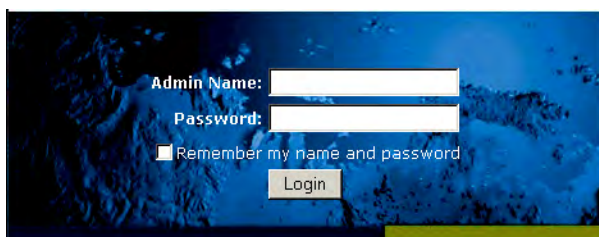
要使用 WebUI，用于管理设备的工作站最初必须与设备处于同一子网中。要使用 WebUI 访问设备，请执行以下步骤：

1. 将工作站连接到设备上的 0/2 - 0/4 端口 (Trust 区段中的 bgroup0 接口)。
2. 确保工作站配置为“动态主机配置协议” (DHCP) 或静态配置为 192.168.1.0/24 子网中的 IP 地址。
3. 启动浏览器，为 bgroup0 接口输入 IP 地址（缺省 IP 地址为 192.168.1.1/24），然后按 **Enter**。

注意： 第一次通过 WebUI 访问设备时，会出现初始配置向导 (ICW)。如果决定使用 ICW 配置设备，请参阅第 61 页上的“初始配置向导”。

WebUI 应用程序将显示如图 14 所示的登录提示。

图 14: WebUI 登录提示



4. 如果尚未更改 admin 名称和密码的缺省登录，请在 admin 名称和密码提示中都输入 **netscreen**。（仅使用小写字母。登录名和密码字段都区分大小写。）

使用 Telnet

要建立 Telnet 连接，请执行以下步骤：

- 1. 将工作站连接到设备上的 0/2 - 0/4 端口 (Trust 区段中的 bgroup0 接口)。
- 2. 确保工作站配置为 DHCP 或静态配置为 192.168.1.0/24 子网中的 IP 地址。
- 3. 启动 Telnet 客户端应用程序至 bgroup0 接口的 IP 地址 (缺省 IP 地址为 192.168.1.1)。例如，输入 **telnet 192.168.1.1**。

Telnet 应用程序显示登录提示。

- 4. 如果尚未更改登录名和密码的缺省登录，请在登录名和密码提示中都输入 **netScreen**。(仅使用小写字母。登录名和密码字段都区分大小写。)
- 5. (可选) 在缺省情况下，空闲时间超过 10 分钟后控制台将超时并自动终止。要清除超时，请输入 **set console timeout 0**。

缺省设备设置

本节介绍 SSG 20 设备的缺省设置和操作。

表 5 显示了设备端口的缺省区段绑定。

表 5: 缺省物理接口到区段的绑定

端口标签	接口	区段
10/100 以太网端口：		
0/0	ethernet0/0	Untrust
0/1	ethernet0/1	DMZ
0/2	bgroup0 (ethernet0/2)	Trust
0/3	bgroup0 (ethernet0/3)	Trust
0/4	bgroup0 (ethernet0/4)	Trust
AUX	serial0/0	Null
WAN 小型 PIM 端口 (x = 小型 PIM 插槽 1 或 2):		
ADSL2/2 + (Annex A)	adsl(x/0)	Untrust
ADSL2/2 + (Annex B)	adsl(x/0)	Untrust
T1	serial(x/0)	Untrust
E1	serial(x/0)	Untrust
ISDN	bri(x/0)	Untrust
V.92	serial(x/0)	Null

桥接组 (bgroup) 旨在让网络用户可以在有线和无线信息流间进行切换，而不必重新配置或重新启动设备。在缺省情况下，ethernet0/2 - ethernet0/4 接口 (在设备上标记为端口 0/2 - 0/4) 被组合为 bgroup0 接口，其 IP 地址为 192.168.1.1/24，且被绑定到 Trust 安全区段。最多可配置四个 bgroup。

如果要将以以太网或无线接口设置在 bgroup 中，必须先确保以太网或无线接口处于 Null 安全区段。取消设置 bgroup 中的以太网或无线接口会将接口置于 Null 安全区段中。将以以太网接口分配到 Null 安全区段后，即可将其绑定到某一安全区段并分配不同的 IP 地址。

要取消设置 bgroup0 中的 ethernet0/3，并将其分配到静态 IP 地址为 192.168.3.1/24 的 Trust 区段，请按以下所述使用 WebUI 或 CLI:

WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port: 取消选择 **ethernet0/3**，然后单击 **Apply**。

List > Edit (ethernet0/3): 输入以下内容，然后单击 **Apply**:

Zone Name: Trust (选择)
IP Address/Netmask: 192.168.3.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
set interface ethernet0/3 zone trust
set interface ethernet0/3 ip 192.168.3.1/24
save
```

表 6: 无线和逻辑接口绑定

SSG 20-WLAN	接口	区段
无线接口		
指定一个可配置使用 2.4G 和 / 或 5G 无线电的无线接口	wireless0/0 (缺省 IP 地址为 192.168.2.1/24)。	Trust
	wireless0/1-0/3。	Null
逻辑接口		
第 2 层接口	在设备处于透明模式时，vlan1 指定用于管理和 VPN 信息流终止的逻辑接口。	N/A
通道接口	tunnel.n 指定一个逻辑通道接口。此接口用于 VPN 信息流。	N/A

可以更改 bgroup0 接口的缺省 IP 地址，以匹配 LAN 和 WLAN 上的地址。有关将无线接口配置到 bgroup 的信息，请参阅第 36 页上的“基本无线配置”。

注意： 在 bgroup 接口包含无线接口时，在透明模式下将不起作用。

有关 bgroup 的其它信息和范例，请参阅 *概念与范例 ScreenOS 参考指南*。

设备上的其它以太网或无线接口没有配置其它缺省 IP 地址；需要为其它接口 (包括 WAN 接口) 分配 IP 地址。

基本设备配置

本节介绍以下基本配置设置：

- 根 Admin 名称和密码
- 日期和时间
- 桥接组接口
- 管理存取
- 管理服务
- 主机名和域名
- 缺省路由
- 管理接口地址
- 备份 Untrust 接口配置

根 Admin 名称和密码

根 admin 用户拥有配置 SSG 20 设备的全部权限。我们建议立即更改缺省根 admin 名称和密码 (均为 **netscreen**)。

要更改根 admin 名称和密码，请按以下所述使用 WebUI 或 CLI:

WebUI

Configuration > Admin > Administrators > Edit (对于 netscreen 管理员名称值): 输入以下内容，然后单击 **OK**:

Administrator Name:
Old Password: netscreen
New Password:
Confirm New Password:

注意： WebUI 中不会显示密码。

CLI

```
set admin name 名称
set admin password 密码字符串
save
```

日期和时间

SSG 20 设备上设置的时间会影响事件，如 VPN 通道的设置。设置设备的日期和时间的最简单的方法，就是利用 WebUI 同步设备系统时钟和工作站时钟。

要配置设备的日期和时间，请按以下所述使用 WebUI 或 CLI:

WebUI

1. Configuration > Date/Time: 单击 Sync Clock with Client 按钮。
会弹出一条消息，提示您指定是否已在工作站时钟上启用了夏令时选项。
2. 单击 **Yes** 将同步系统时钟，并根据夏令时调整时钟；或单击 **No** 只同步系统时钟，不根据夏令时对其进行调整。

还可使用 Telnet 或控制台会话中的 **set clock** CLI 命令，手动输入设备的日期和时间。

桥接组接口

在缺省情况下，SSG 20 设备将以太网接口 ethernet0/2 - ethernet0/4 一起组合在 Trust 安全区段中。组合接口会将接口设置在一个子网内。可以对组中的接口取消设置，并将其分配到不同的安全区段。将接口分配到某个组之前，它们必须已在 Null 安全区段中。要将已分组的接口置于 Null 安全区段中，请使用 **unset interface 接口 port 接口** CLI 命令。

SSG 20-WLAN 设备可将以太网和无线接口组合在一个子网中。

注意： 在 bgroup 组内只能设置无线和以太网接口。

要为某个组配置以太网和无线接口，请按以下所述使用 WebUI 或 CLI:

WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port: 取消选择 **ethernet0/3** 和 **ethernet0/4**，然后单击 **Apply**。

Edit (bgroup1) > Bind Port: 选择 **ethernet0/3**、**ethernet0/4** 和 **wireless0/2**，然后单击 **Apply**。

> Basic: 输入以下内容，然后单击 **Apply**:

Zone Name: DMZ (选择)
IP Address/Netmask: 10.0.0.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
unset interface bgroup0 port ethernet0/4
set interface bgroup1 port ethernet0/3
set interface bgroup1 port ethernet0/4
set interface bgroup1 port wireless0/2
set interface bgroup1 zone DMZ
set interface bgroup1 ip 10.0.0.1/24
save
```


管理存取

在缺省情况下，如果知道登录名和密码，网络中的任何用户都可以管理设备。

要将设备配置为仅通过网络上的指定主机进行管理，请按以下所述使用 WebUI 或 CLI:

WebUI

Configuration > Admin > Permitted Ips: 输入以下内容，然后单击 **Add**:

IP Address/Netmask: *ip 地址 / 掩码*

CLI

```
set admin manager-ip ip 地址 / 掩码
save
```

管理服务

ScreenOS 提供了配置和管理设备的服务，如 SNMP、SSL 和 SSH，可以根据接口启用相应的服务。

要配置设备的管理服务，请按以下所述使用 WebUI 或 CLI:

WebUI

Network > Interfaces > List > Edit (对于 ethernet0/0): 在 **Management Services** 下，选择或清除要在接口上使用的管理服务，然后单击 **Apply**。

CLI

```
set interface ethernet0/0 manage web
unset interface ethernet0/0 manage snmp
save
```

主机名和域名

域名定义设备所属的网络或子网，而主机名则表示特定的设备。主机名和域名一起，唯一标识网络中的设备。

要配置设备的主机名和域名，请按以下所述使用 WebUI 或 CLI:

WebUI

Network > DNS > Host: 输入以下内容，然后单击 **Apply**:

Host Name: *名称*
Domain Name: *名称*

CLI

```
set hostname 名称
set domain 名称
save
```

缺省路由

缺省路由是一个静态路由，用于将数据包引至未在路由表中明确列出的网络。数据包到达设备时，如果设备未包含该设备地址的路由信息，设备会将数据包发送到缺省路由指定的目标。

要配置设备的缺省路由，请按以下所述使用 WebUI 或 CLI:

WebUI

Network > Routing > Destination > New (trust-vr): 输入以下内容，然后单击 OK:

IP Address/Netmask: 0.0.0.0/0.0.0.0
 Next Hop
 Gateway: (选择)
 Interface: ethernet0/2 (选择)
 Gateway IP Address: *ip 地址*

CLI

```
set route 0.0.0.0/0 interface ethernet0/2 gateway ip 地址
save
```

管理接口地址

Trust 接口的缺省 IP 地址为 192.168.1.1/24，且配置用于管理服务。如果将设备的 0/2 - 0/4 端口连接到工作站，则可使用管理服务（如 Telnet），通过 192.168.1.1/24 子网中的工作站配置设备。

可更改 Trust 接口的缺省 IP 地址。例如，您可能要更改接口以匹配 LAN 中现有的 IP 地址。

备份 Untrust 接口配置

SSG 20 设备可以为不可信的故障切换配置备份接口。要为不可信的故障切换设置备份接口，请执行以下步骤：

1. 使用 **unset interface 接口 [port 接口]** CLI 命令，在 Null 安全区段中设置备份接口。
2. 使用 **set interface 接口 zone 区段名称** CLI 命令，将备份接口绑定到与主接口相同的安全区段。

注意： 主接口和备份接口必须在相同的安全区段中。一个主接口只能有一个备份接口，同样，一个备份接口也只能有一个主接口。

要将 ethernet0/4 接口设置为 ethernet0/0 接口的备份接口，请按以下所述使用 WebUI 或 CLI:

WebUI

Network > Interfaces > Backup > 输入以下内容，然后单击 **Apply**。

Primary: ethernet0/0
Backup: ethernet0/4
Type: track-ip (选择)

CLI

```
unset interface bgroup0 port ethernet0/4
set interface ethernet0/4 zone untrust
set interface ethernet0/0 backup interface ethernet0/4 type track-ip
save
```

基本无线配置

本节提供有关在 SSG 20-WLAN 设备上配置无线接口的信息。无线网络由称为服务集标识符 (SSID) 的名称组成。指定 SSID 可将多个无线网络驻留在同一位置，而不会互相干扰。SSID 名称最多可包含 32 个字符。如果 SSID 名称字符串包含有空格，则必须将该字符串用引号括起来。设置 SSID 名称后，即可配置更多的 SSID 属性。要使用设备的无线局域网 (WLAN) 功能，至少必须配置一个 SSID 并将其绑定到无线接口。

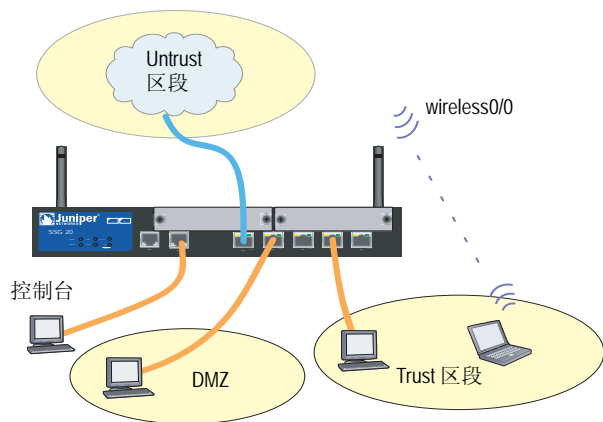
SSG 20-WLAN 设备最多可创建 16 个 SSID，但只能同时使用其中 4 个。可配置设备以使用任一收发器上的 4 个 SSID，或在两个收发器上使用 (例如，分配给 WLAN 0 的 3 个 SSID 和分配给 WLAN 1 的 1 个 SSID)。使用 **set interface 无线接口 wlan {0 | 1 | both}** CLI 命令设置 SSG 20-WLAN 设备的无线电收发器。

设置 wireless0/0 接口的 SSID 后，即可按照第 28 页上的“访问设备”中介绍的步骤，使用缺省的 wireless0/0 接口 IP 地址访问设备。图 15 显示了 SSG 20-WLAN 设备的缺省配置。

注意： 如果您在美国、日本、加拿大、中国、中国台湾、韩国、以色列或新加坡以外的国家 / 地区使用 SSG 20-WLAN 设备，则必须使用 **set wlan country-code** CLI 命令或在 Wireless > General Settings WebUI 页面上对其进行设置，然后才能建立 WLAN 连接。此命令设置可选的通道范围和传输功率电平。

如果您的区段代码为 ETSI，则必须设置满足本地无线电频谱规定的正确的国家 / 地区代码。

图 15: 缺省的 SSG 20-WLAN 配置



在缺省情况下，wireless0/0 接口的 IP 地址配置为 192.168.2.1/24。所有需要连接到 Trust 区段的无线客户端的 IP 地址都必须都在无线子网内。也可将设备配置为使用 DHCP，以便将 192.168.2.1/24 子网内的 IP 地址自动分配给设备。

在缺省情况下，wireless0/1 - wireless0/3 接口定义为 Null，且未分配 IP 地址。如果要使用其它无线接口，则必须为其配置 IP 地址、分配 SSID 并将其绑定到安全区段。表 7 显示了无线认证和加密方法。

表 7: 无线认证和加密选项

认证	加密
开放式	允许任何无线客户端访问设备
共享密钥	WEP 共享密钥
WPA-PSK	使用预共享密钥的 AES/TKIP
WPA	使用 RADIUS 服务器密钥的 AES/TKIP
WPA2-PSK	使用预共享密钥的 802.11i
WPA2	使用 RADIUS 服务器的 802.11i
WPA-Auto-PSK	允许使用预共享密钥的 WPA 和 WPA2 加密
WPA-Auto	允许使用 RADIUS 服务器的 WPA 和 WPA2 加密
802.1x	使用 RADIUS 服务器密钥的 WEP

有关与无线安全配置有关的配置范例、SSID 属性和 CLI 命令的信息，请参阅 *概念与范例 ScreenOS 参考指南*。

要配置无线接口以实现基本连通性，请按以下所述使用 WebUI 或 CLI:

WebUI

1. 设置 WLAN 国家 / 地区代码和 IP 地址。

Wireless > General Settings > 选择以下内容，然后单击 **Apply**:

Country code: 选择您的代码
IP Address/Netmask: *ip 地址 / 网络掩码*

2. 设置 SSID。

Wireless > SSID > New: 输入以下内容，然后单击 **OK**:

SSID:
Authentication:
Encryption:
Wireless Interface Binding:

3. (可选) 设置 WEP 密钥。

SSID > WEP Keys: 选择 keyID，然后单击 **Apply**。

4. 设置 WLAN 模式。

Network > Interfaces > List > Edit (无线接口): 对于 WLAN 模式，选择 **Both**，然后单击 **Apply**。

5. 激活无线更改。

Wireless > General Settings > 单击 **Activate Changes**。

CLI

1. 设置 WLAN 国家 / 地区代码和 IP 地址。

```
set wlan country-code {code_id}
set interface 无线接口 ip ip 地址 / 网络掩码
```

2. 设置 SSID。

```
set ssid name 名称字符串
set ssid 名称字符串 authentication 认证类型 encryption 加密类型
set ssid 名称字符串 interface 接口
(可选) set ssid 名称字符串 key-id 编号
```

3. 设置 WLAN 模式。

```
set interface 无线接口 wlan both
```

4. 激活无线更改。

```
save
exec wlan reactivate
```

可以设置 SSID，以便与有线子网在同一子网中使用。此操作让客户端可使用任一接口，而不必重新连接另一子网。

要将以太网和无线接口设置到同一桥接组接口，请按以下所述使用 WebUI 或 CLI:

WebUI

Network > Interfaces > List > Edit (桥接组名称) > Bind Port: 选择无线接口和以太网接口，然后单击 **Apply**。

CLI

```
set interface 桥接组名称 port 无线接口
set interface 桥接组名称 port 以太网接口
```

注意： 桥接组名称可以是 bgroup0-bgroup3。

以太网接口可以是 ethernet0/0-ethernet0/4。

无线接口可以是 wireless0/0-wireless0/3。

如果配置了无线接口，则需要使用 **exec wlan reactivate** CLI 命令或单击 Wireless > General Settings WebUI 页面上的 **Activate Changes** 来重新激活 WLAN。

小型 PIM 配置

本节介绍如何配置小型物理接口模块 (PIM):

- ADSL2/2+ 接口
- ISDN 接口
- T1 接口
- E1 接口
- V.92 调制解调器接口

ADSL2/2+ 接口

网络使用设备上的 ADSL2/2+ 接口 **adslx/0** (其中 x 代表小型 PIM 插槽 (1 或 2))，通过异步传输模式 (ATM) 虚拟电路连接到服务提供商的网络。可以通过创建 ADSL2/2+ 子接口来配置其它虚拟电路。有关详细信息，请参阅第 40 页上的“虚拟电路”。

在 WebUI 中，导航至 Network > Interfaces > List 页面以查看设备当前接口的列表。如果使用 Telnet 或控制台会话，请输入 **get interface** CLI 命令。应该可以看到 adslx/0 接口绑定在 Untrust 区段。

如果使用 ADSL2/2+ 接口连接到提供商的服务网络，则必须配置 adsl(x/0) 接口。为此，必须从您的服务提供商处获取以下信息：

- “虚拟路径标识符”和“虚拟通道标识符”(VPI/VCI) 值
- ATM 适配层 5 (AAL5) 多路传输方法，可以是以下任何一项：
 - 基于虚拟电路的多路传输，分别通过单独的 ATM 虚拟电路来传输每个协议
 - 逻辑链路控制 (LLC) 封装，它允许在同一 ATM 虚拟电路上传输多个协议（缺省的多路传输方法）
- 服务提供商分配的用户名和密码，用于通过“以太网点对点传输协议”(PPPoE) 或“ATM 点对点传输协议”(PPPoA) 连接到服务提供商的网络
- 为 PPPoE 或 PPPoA 连接提供的认证方法（如果有）
- 网络的静态 IP 地址和网络掩码值（可选）

虚拟电路

要添加虚拟电路，可创建 ADSL2/2+ 接口的子接口。最多可创建 10 个 ADSL2/2+ 子接口。例如，要创建名为 **adsl1/0.1** 的新子接口，并将其绑定到名为 **Untrust** 的预定义区段，请按以下所述使用 WebUI 或 CLI:

WebUI

Network > Interfaces > List > New ADSL Sub-IF: 输入以下内容，然后单击 **Apply**:

Interface Name: adsl1/0.1
VPI/VCI: 0/35
Zone Name: Untrust (选择)

CLI

```
set interface adsl 1/0.1 pvc 0 35 zone Untrust
save
```

需要按照配置 ADSL 2/2+ 主接口的相同方式配置 ADSL2/2+ 子接口，包括设置 VPI/VCI 值，如第 39 页上的“ADSL2/2+ 接口”中所述。可以独立地配置 ADSL2/2+ 主接口的 ADSL2/2+ 子接口；也就是说可以在 ADSL2/2+ 子接口上，而非主接口上配置不同的多路传输方法、VPI/VCI 和 PPP 客户端。即使 ADSL2/2+ 主接口没有静态 IP 地址，也可在子接口上配置静态 IP 地址。

VPI/VCI 和多路传输方法

服务提供商将为每个虚拟电路连接分配一个 VPI/VCI 对。例如，可能会接收到 VPI/VCI 对 1/32，它表示 VPI 值为 1，VCI 值为 32。这些值必须与服务提供商在“数字用户线接入多路复用器” (DSLAM) 的用户侧配置的值相匹配。

要在 adsl1/0 接口上配置 VPI/VCI 对 1/32，请按以下所述使用 WebUI 或 CLI:

WebUI

Network > Interfaces > List > Edit (对于 adsl1/0 接口): 在 VPI/VCI 字段中输入 1/32，然后单击 **Apply**。

CLI

```
set interface adsl1/0 pvc 1 32
save
```

在缺省情况下，设备对每个虚拟电路使用基于逻辑链路控制 (LLC) 的多路传输。

要在 adslx/0 接口上配置 VPI/VCI 1/32，并在虚拟电路上使用 LLC 封装，请按以下所述使用 WebUI 或 CLI:

WebUI

Network > Interfaces > List > Edit (对于 adsl1/0 接口): 输入以下内容，然后单击 **Apply**:

VPI/VCI: 1 / 32
Multiplexing Method: LLC (选定)

CLI

```
set interface adsl1/0 pvc 1 32 mux llc
save
```

PPPoE 或 PPPoA

SSG 20 设备包括 PPPoE 客户端和 PPPoA 客户端，可通过 ADSL 链路连接到服务提供商的网络。PPPoE 是最常用的 ADSL 封装形式，适用于网络上每个主机的终止。PPPoA 主要用于商业级服务，因为 PPP 会话可在设备上终止。要将设备连接到服务提供商的网络，必须配置服务提供商分配的用户名和密码。PPPoA 的配置方法与 PPPoE 相似。

注意： 设备在每个虚拟电路上仅支持一个 PPPoE 会话。

要为 PPPoE 配置用户名 **roswell** 和密码 **area51**，并将 PPPoE 配置绑定到 adsl1/0 接口，请按以下所述使用 WebUI 或 CLI:

WebUI

Network > PPP > PPPoE Profile > New: 输入以下内容，然后单击 **OK**:

```
PPPoE Instance: poe1
Bound to Interface: adsl1/0 ( 选择 )
Username: roswell
Password: area51
```

CLI

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1/0
save
```

可在设备上配置其它 PPPoE 或 PPPoA 参数，包括认证方法（在缺省情况下，设备支持“质询握手认证协议”或“密码认证协议”）和空闲超时（缺省值为 30 分钟）等。请咨询您的服务提供商是否需要配置其它 PPPoE 或 PPPoA 参数，以便能够与服务提供商的服务器正确通信。

静态 IP 地址和网络掩码

如果服务给定了网络的特定、固定的 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设备的路由器端口的 IP 地址。还需要将设备指定为使用静态 IP 地址。（设备通常充当 PPPoE 或 PPPoA 客户端，并通过与 PPPoE 或 PPPoA 服务器的协商接收 ADSL 接口的 IP 地址。）

必须配置 PPPoE 或 PPPoA 实例，并将其绑定到 adsl1/0 接口，如第 41 页上的“PPPoE 或 PPPoA”中所述。确保选择 **Obtain IP using PPPoE** 或 **Obtain IP using PPPoA** 以及 PPPoE 或 PPPoA 实例的名称。

要为网络配置静态 IP 地址 1.1.1.1/24，请按以下所述使用 WebUI 或 CLI:

WebUI

Network > Interfaces > List > Edit (对于 adsl1/0 接口): 输入以下内容，然后单击 **Apply**:

```
IP Address/Netmask: 1.1.1.1/24
Static IP: ( 选择 )
```

CLI

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

或

```
set interface adsl1/0 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,网络中的计算机至少必须有一个 DNS 服务器的 IP 地址。如果设备通过 PPPoE 或 PPPoA 接收 ADSL2/2+ 接口的 IP 地址,则可自动接收 DNS 服务器的 IP 地址。如果网络中的计算机通过设备上的 DHCP 服务器获取其 IP 地址,则还将获取这些 DNS 服务器地址。

如果将静态 IP 地址分配给 ADSL2/2+ 接口,则服务提供商必须为您提供 DNS 服务器的 IP 地址。可在网络中的每台计算机上配置 DNS 服务器地址,也可在 Trust 区段接口上配置 DHCP 服务器,以便它能为每台计算机提供 DNS 服务器地址。

要在 bgroup0 接口上配置 DHCP 服务器,以便为网络中的计算机提供 DNS 服务器地址 1.1.1.152,请按以下所述使用 WebUI 或 CLI:

WebUI

Network > DHCP > Edit (对于 bgroup0 接口) > DHCP Server: 输入 DNS1 地址 1.1.1.152,然后单击 **Apply**。

CLI

```
set interface bgroup0 dhcp server option dns1 1.1.1.152
save
```

有关配置 ADSL 和 ADSL2/2+ 接口的详细信息,请参阅 *概念与范例 ScreenOS 参考指南*。

ISDN 接口

“集成服务数字网络”(ISDN)是在“国际电报电话咨询委员会”(CCITT)和“国际电信联盟”(ITU)创建的不同媒体上进行数字传输的一组标准。作为一项按需拨号服务,它具有快速呼叫设置和低延迟时间,以及传输高质量语音、数据和视频的能力。ISDN 还有一种电路交换服务,可用于多点和点对点连接。ISDN 为服务路由器的网络接口提供了一种多链路点对点协议 (PPP) 连接。ISDN 接口通常被配置为以太网接口的备份接口以访问外部网络。

要配置 ISDN 接口,请按以下所述使用 WebUI 或 CLI:

WebUI

Network > Interfaces > List > Edit (bri1/0): 输入或选择以下内容,然后单击 **OK**:

```
BRI Mode: Dial Using BRI
Primary Number: 123456
WAN Encapsulation: PPP
PPP Profile: isdnprofile
```

CLI

```
set interface bri1/0 dialer-enable
set interface bri1/0 primary-number "123456"
set interface bri1/0 encap ppp
set interface bri1/0 ppp profile isdnprofile
save
```

要将 ISDN 接口配置为备份接口,请参阅第 35 页上的“备份 Untrust 接口配置”。

有关如何配置 ISDN 接口的详细信息,请参阅 *概念与范例 ScreenOS 参考指南*。

T1 接口

T1 接口是北美地区“数字信号电平 1 (DS-1) 多路传输方法”所使用的一个基本物理层协议。T1 接口运行时的位速率为 1.544 Mbps 或最多 24 个 DS0 通道的速率。

设备支持以下 T1 DS-1 标准：

- ANSI T1.107、T1.102
- GR 499-core、GR 253-core
- AT&T Pub 54014
- ITU G.751、G.703

要配置 T1 小型 PIM，请按以下所述使用 WebUI 或 CLI:

WebUI

Network > Interfaces > List > Edit (serial1/0): 输入或选择以下内容，然后单击 **OK**:

WAN Configure: main link
 WAN Encapsulation: cisco-hdlc
 单击 **Apply**
 Fixed IP: (选择)
 IP Address/Netmask: 172.18.1.1/24

CLI

```
set interface serial1/0 encap cisco-hdlc
set interface serial1/0 ip 172.18.1.1/24
```

有关如何配置 T1 接口的信息，请参阅 *概念与范例 ScreenOS 参考指南*。

E1 接口

E1 接口是标准的广域网 (WAN) 数字通信格式，以 2.048 Mbps 的速率在铜质设施上使用。E1 在北美以外地区得到广泛使用，是一种基本的分时多路传输方案，用于传送数字电路。

设备支持以下 E1 标准：

- ITU-T G.703
- ITU-T G.751
- ITU-T G.775

要配置 E1 小型 PIM，请按以下所述使用 WebUI 或 CLI:

WebUI

Network > Interfaces > List > Edit (serial1/0): 输入或选择以下内容，然后单击 **OK**:

WAN Configure: main link
 WAN Encapsulation: PPP
 Binding a PPP Profile: junipertest
 单击 **Apply**
 Fixed IP: (选择)
 IP Address/Netmask: 172.18.1.1/24

CLI

```
set interface serial1/0 encapsulation ppp
set ppp profile "junipertest" static-ip
set ppp profile "junipertest" auth type chap
set ppp profile "junipertest" auth local-name "juniper"
set ppp profile "junipertest" auth secret "password"
set interface serial1/0 ppp profile "junipertest"
set interface serial1/0 ip 172.18.1.1/24
set user "server" type wan
set user "server" password "server"
```

有关如何配置 E1 接口的信息，请参阅 *概念与范例 ScreenOS 参考指南*。

V.92 调制解调器接口

V.92 接口提供了一个内部模拟调制解调器，可以与服务提供商建立 PPP 连接。可将串行接口配置为主接口或备份接口，备份接口在接口出现故障切换时使用。

注意： V.92 接口在透明模式下不起作用。

要配置 V.92 接口，请按以下所述使用 WebUI 或 CLI:

WebUI

Network > Interfaces > List > Edit (对于 serial1/0): 输入以下内容，然后单击 **OK**:

Zone Name: Untrust (选择)

ISP: 输入以下内容，然后单击 **OK**:

ISP Name: isp_juniper
 Primary Number: 1234567
 Login Name: juniper
 Login Password: juniper

Modem: 输入以下内容，然后单击 **OK**:

Modem Name: mod1
 Init String: AT&FS7=255S32=6
 Active Modem setting
 Inactivity Timeout: 20

CLI

```
set interface serial1/0 zone untrust
set interface serial1/0 modem isp isp_juniper account login juniper password
juniper
set interface serial1/0 modem isp isp_juniper primary-number 1234567
set interface serial1/0 modem idle-time 20
set interface serial1/0 modem settings mod1 init-strings AT&FS7=255S32=6
set interface serial1/0 modem settings mod1 active
```

有关如何配置 V.92 调制解调器接口的信息，请参阅 *概念与范例 ScreenOS 参考指南*。

基本防火墙保护

设备配置的缺省策略允许网络中 Trust 区段的工作站访问 Untrust 安全区段的所有资源，但不允许外部计算机访问或启动工作站的会话。可以配置指导设备的策略，允许外部计算机启动其与您的计算机之间的特定种类的会话。有关创建或修改策略的信息，请参阅 *概念与范例 ScreenOS 参考指南*。

SSG 20 设备提供了各种检测方法和防御机制，以对抗旨在破坏或损害网络或网络资源的探查和攻击：

- ScreenOS SCREEN 选项用于保护区段的安全，具体做法是先检查要求经过该区段的某一接口的所有连接尝试，然后予以准许或拒绝。例如，可以将端口扫描保护应用于 Untrust 区段，以阻止远程网络源识别服务，从而进一步发起攻击的企图。
- 设备对从一个区段到另一个区段传递 SCREEN 过滤器的信息流应用防火墙策略（这些策略可能包含内容过滤和入侵检测及防护 (IDP) 组件）。在缺省情况下，不允许通过设备从一个区段到另一个区段传递信息流。要允许通过设备从一个区段到另一个区段传递信息流，必须创建一个覆盖缺省行为的策略。

要设置区段的 ScreenOS SCREEN 选项，请按以下所述使用 WebUI 或 CLI:

WebUI

Screening > Screen: 选择要应用选项的区段。选择所需的 SCREEN 选项，然后单击 **Apply**。

CLI

```
set zone 区段 screen 选项
save
```

有关配置 ScreenOS 中可用的网络安全选项的详细信息，请参阅 *概念与范例 ScreenOS 参考指南*。

验证外部连通性

要验证网络中的工作站能否访问互联网中的资源，请从网络中的任何工作站启动浏览器并输入以下的 URL: www.juniper.net。

将设备重置为出厂缺省值

如果丢失了 admin 密码，可以将设备重置为其缺省设置。此操作会破坏现有的所有配置，但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设置并关闭现有的所有防火墙和 VPN 服务。

可以使用以下任一方式将设备恢复为其缺省设置：

- 使用控制台连接。有关详细信息，请参阅 *概念与范例 ScreenOS 参考指南*。
- 使用设备后面板上的重置针孔，如下一节所述。

按压重置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，如第 28 页上的“使用控制台连接”中所述。

要使用重置针孔来重置和恢复缺省设置，请执行以下步骤：

1. 找到后面板上的重置针孔。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。

STATUS LED 闪烁红色。控制台上的消息表明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；设备正等待第二次重置。控制台消息现在表明设备正等待第二次确认。

3. 再次推压重置针孔四至六秒。

控制台消息验证第二次重置。STATUS LED 亮红色半秒钟时间，然后返回到闪烁绿色状态。

然后，设备重置为其原始的出厂设置。设备重置后，STATUS LED 亮红色半秒钟时间，然后亮绿色。控制台显示设备启动信息。系统产生 SNMP 和 SYSLOG 警示，发给已配置的 SYSLOG 或 SNMP 陷阱主机。

设备重新启动后，控制台显示设备的登录提示。STATUS LED 闪烁绿色。登录名和密码为 **netscreen**。

如果不遵循完整的程序，重置过程会取消且不更改任何配置，同时控制台消息表明已中止删除配置。STATUS LED 返回到闪烁绿色状态。如果设备没有重置，则会发送 SNMP 警示以确认失败。

第 4 章 维护设备

本章介绍 SSG 20 设备的保养和维护过程。其中包括以下部分：

- 本页上的“需要的工具和部件”
- 本页上的“更换小型物理接口模块”
- 第 52 页上的“升级内存”

注意： 有关安全警告和说明，请参阅 *Juniper Networks Security Products 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，应注意由电路引发的危险以及熟悉标准操作以防止意外事故的发生。

需要的工具和部件

要更换 SSG 20 设备上的组件，需要使用以下工具和部件：

- 防静电袋或防静电垫
- 静电放电 (ESD) 接地腕带
- 1/8 英寸的十字螺丝起子

更换小型物理接口模块

两种 SSG 20 型号设备的前面板上都具有两个插槽，适用于广域网小型物理接口模块 (WAN 小型 PIM)。可以安装和更换 SSG 20 设备中的小型 PIM。移除或安装小型 PIM 前，必须关闭设备电源。



小心： 确保在移除小型 PIM 时关闭设备电源。它们不具有热插拔功能。

移除空面板

为保持 SSG 20 设备良好的通风状况，应在未装有小型 PIM 的插槽上保留空面板。除非要在空插槽中安装小型 PIM，否则请勿移除空面板。

要移除空面板，请执行以下步骤：

1. 将防静电袋或抗静电垫放在要放置小型 PIM 的平整、稳固的表面上。
2. 如果 SSG 20 设备未接地，请将 ESD 接地腕带绑到露出的手腕上，然后将此腕带与机箱上的 ESD 点或外部 ESD 点相连。
3. 从设备上拔下电源适配器。验证 POWER LED 是否已关闭。
4. 使用螺丝起子拧松并移除面板各侧面上的螺丝。
5. 移除面板，然后将面板放入防静电袋或将其放在抗静电垫上。

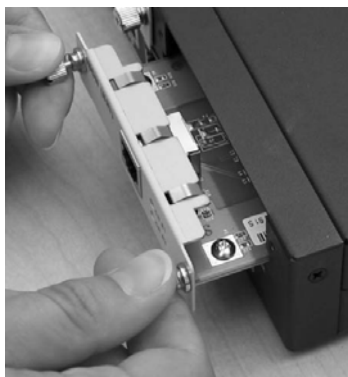
移除小型 PIM

小型 PIM 被安装在 SSG 20 设备的前面板中。小型 PIM 的重量不足 0.2 磅 (106g)。

要移除小型 PIM，请执行以下步骤：

1. 将防静电袋或抗静电垫放在要放置小型 PIM 的平整、稳固的表面上。
2. 如果 SSG 20 设备未接地，请将 ESD 接地腕带绑到露出的手腕上，然后将此腕带与机箱上的 ESD 点或外部 ESD 点相连。
3. 从设备上拔下电源适配器。验证 POWER LED 是否已关闭。
4. 标记连接到小型 PIM 的电缆，以便稍后能够将各电缆重新连接到正确的小型 PIM。
5. 将电缆与小型 PIM 的连接断开。
6. 如有必要，排列电缆以防止其移动或成为受力点：
 - a. 固定电缆，使其在悬挂到地板时不用承受其自身的重量。
 - b. 将所有多余电缆整齐地盘绕成圆环状。
 - c. 使用紧固件以保持电缆线圈的形状。
7. 使用螺丝起子拧松并移除小型 PIM 面板各侧面上的螺丝。
8. 抓住小型 PIM 面板各侧面上的螺丝，然后将小型 PIM 平缓滑出设备。将小型 PIM 放入防静电袋或将其放在抗静电垫上。

图 16: 移除小型 PIM



9. 如果未将小型 PIM 重新安装到空的插槽中，请将空面板安装到插槽上以保持良好的通风状况。

安装小型 PIM

要安装小型 PIM，请执行以下步骤：

1. 如果 SSG 20 设备未接地，请将 ESD 接地腕带绑到露出的手腕上，然后将此腕带与机箱上的 ESD 点或外部 ESD 点相连。
2. 从设备上拔下电源适配器。验证 POWER LED 是否已关闭。
3. 抓住小型 PIM 面板各侧面上的螺丝，然后将小型 PIM 后部连接器中的槽口对准 SSG 20 设备中小型 PIM 插槽的槽口。然后平缓滑动小型 PIM 直至其牢固地卡在设备内。

图 17: 安装小型 PIM



小心：将小型 PIM 径直滑向插槽，以避免损坏小型 PIM 上的组件。

4. 使用 1/8 英寸的一字螺丝起子拧紧小型 PIM 面板各侧面上的螺丝。
5. 将相应的电缆插入小型 PIM 上的电缆连接器中。

6. 如有必要，排列电缆以防止其移动或成为受力点：
 - a. 固定电缆，使其在悬挂到地板时不用承受其自身的重量。
 - b. 将所有多余电缆整齐地盘绕成圆环状。
 - c. 使用紧固件以保持电缆线圈的形状。
7. 从设备上拔下电源适配器。按下电源按钮后，验证 POWER LED 是否始终显示绿色。
8. 验证系统面板上的 PIM 状态 LED 是否始终显示绿色，以此来确认小型 PIM 是否在线。

升级内存

可将 SSG 20 设备从单个 128 MB 的双列直插式内存模块 (DIMM) 动态随机存取内存 (DRAM) 升级为 256 MB DIMM DRAM。

要升级 SSG 20 设备的内存，请执行以下步骤：

1. 如果设备未接地，请将 ESD 接地腕带绑到露出的手腕上，然后将此腕带与机箱上的 ESD 点或外部 ESD 点相连。
2. 从电源插座上拔下交流电源线。
3. 翻转设备，以便将其顶部放置在平整表面上。
4. 使用十字螺丝起子移除内存卡盖上的螺丝。将螺丝放在手边，以便稍后固定盖子时取用。
5. 移除内存卡盖。

图 18: 设备底部



- 用拇指按住模块两边的锁定装置向外轻推，使这些锁定装置与模块分离，从而取下 128 MB DIMM DRAM。

图 19: 解除内存模块锁定



- 抓住内存模块的较长边将其滑出。并把它放在一边。

图 20: 取下模块插槽



- 将 256 MB DIMM DRAM 插入插槽。用两个拇指对模块上边缘均匀施力，然后向下按压模块直到锁定装置发出“咔”的一声入位。

图 21: 插入内存模块



9. 将内存卡盖放置在插槽上。
10. 使用十字螺丝起子拧紧螺丝，从而固定设备盖。

附录 A 规格

本附录提供 SSG 20 设备的通用系统规格。其中包括以下部分：

- 第 56 页上的“物理”
- 第 56 页上的“电气”
- 第 56 页上的“环境忍耐力”
- 第 57 页上的“证书”
- 第 58 页上的“连接器”

物理

表 8: SSG 20 物理规格

说明	值
机箱尺寸	294 mm x 194.8 mm x 44 mm (11.5 英寸 x 7.7 英寸 x 2 英寸)
设备重量	1.53 kg (3.3 磅)，不含安装的 PIM 的重量
ISDN PIM	70g
ADSL Annex A PIM	106g
ADSL Annex B PIM	106g
T1 PIM	75g
E1 PIM	75g
V.92 PIM	79g

电气

表 9: SSG 20 电气规格

项目	规格
DC 输入电压	12V
DC 系统额定电流	3 - 4.16 A

环境忍耐力

表 10: SSG 20 环境忍耐力

说明	值
高度	6,600 英尺 (2,000 m) 以下性能稳定
相对湿度	相对湿度为 10% - 90% (非冷凝) 时可确保正常运行
温度	温度为 32°F (0°C) - 104°F (40°C) 时可确保正常运行 集装箱中非工作存储温度: -4°F (-20°C) - 158°F (70°C)

证书

安全

- CAN/CSA-C22.2 No. 60950-1-03/UL 60950-1 信息技术设备的安全性
- EN 60950-1 (2000) 第三版, 信息技术设备的安全性
- IEC 60950-1 (1999) 第三版, 信息技术设备的安全性

EMC 辐射

- FCC Part 15 Class B (美国)
- EN 55022 Class B (欧洲)
- AS 3548 Class B (澳大利亚)
- VCCI Class B (日本)

EMC 抗扰度

- EN 55024
- EN-61000-3-2 电源线谐波
- EN-61000-3-3 电源线谐波
- EN-61000-4-2 ESD
- EN-61000-4-3 辐射抗扰度
- EN-61000-4-4 EFT
- EN-61000-4-5 电涌
- EN-61000-4-6 低频通用抗扰度
- EN-61000-4-11 电压骤降与凹陷

ETSI

欧洲电信标准机构 (ETSI) EN-3000386-2: 电信网络设备。电磁兼容性要求;
(设备类别 - 电信中心除外)

T1 接口

- FCC Part 68 - TIA 968
- Industry Canada CS-03
- UL 60950-1 关于具有外部设备引线连接的 TNV 电路的相关要求

连接器

图 22 显示了 RJ-45 连接器引脚的位置。

图 22: RJ-45 插脚引线

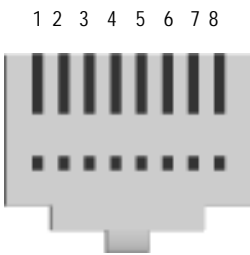


表 11 列出了 RJ-45 连接器插脚引线。

表 11: RJ-45 连接器插脚引线

引脚	名称	I/O	说明
1	RTS 输出	O	请求发送
2	DTR 输出	O	数据终端就绪
3	TxD	O	传输数据
4	GND	不适用	机箱接地
5	GND	不适用	机箱接地
6	RxD	I	接收数据
7	DSR	I	数据设备就绪
8	CTS	I	清除发送

图 23 显示了 DB-9 凹连接器引脚的位置。

图 23: DB-9 凹连接器

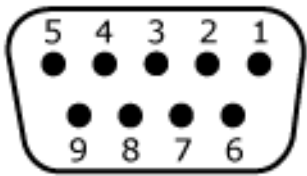


表 12 提供 DB-9 连接器插脚引线。

表 12: DB-9 连接器插脚引线

引脚	名称	I/O	说明
1	DCD	I	载波检测
2	RxD	I	接收数据
3	TxD	O	传输数据
4	DTR	O	数据终端就绪
5	GND	不适用	信号接地
6	DSR	I	数据设备就绪
7	RTS	O	请求发送
8	CTS	I	清除发送
9	RING	I	振铃指示器

附录 B

初始配置向导

本附录提供 SSG 20 设备初始配置向导 (ICW) 的详细信息。

将设备实际连接到网络后，便可使用 ICW 来配置已安装在本设备上的接口。

本节介绍以下 ICW 窗口：

- 第 62 页上的快速部署窗口
- 第 62 页上的管理员登录窗口
- 第 63 页上的 WLAN 接入点窗口
- 第 63 页上的物理接口窗口
- 第 64 页上的 ADSL2/2+ 接口窗口
- 第 66 页上的 T1 接口窗口
- 第 71 页上的 E1 接口窗口
- 第 73 页上的 ISDN 接口窗口
- 第 76 页上的 V.92 调制解调器接口窗口
- 第 77 页上的 Eth0/0 接口 (Untrust 区段) 窗口
- 第 78 页上的 Eth0/1 接口 (DMZ 区段) 窗口
- 第 78 页上的 Bgroup0 接口 (Trust 区段) 窗口
- 第 79 页上的 Wireless0/0 接口 (Trust 区段) 窗口
- 第 80 页上的接口汇总窗口
- 第 81 页上的物理以太网 DHCP 接口窗口
- 第 81 页上的无线 DHCP 接口窗口
- 第 82 页上的确认窗口

1. 快速部署窗口

图 24: 快速部署窗口



Rapid Deployment Wizard

Welcome to the Rapid Deployment Wizard.

Do you have a Rapid Deployment Configlet file?

☒ No, use the Initial Configuration Wizard instead.

☐ Yes, use the following Rapid Deployment Configlet file:

Load Configlet from:

☐ No, skip the Wizard and go straight to the WebUI management session instead.

如果网络使用 NetScreen-Security Manager (NSM)，则可使用快速部署 configlet 以自动配置设备。从 NSM 管理员处获得 configlet，选择 **Yes**，选择 **Load Configlet from:**，浏览文件位置，然后单击 **Next**。configlet 会为您设置设备，因此无需执行以下步骤来配置设备。

如果要绕过 ICW 直接转到 WebUI，请选择最后一个选项，然后单击 **Next**。

如果不使用 configlet 而要使用 ICW 来配置设备，请选择第一个选项，然后单击 **Next**。出现 ICW 欢迎屏幕。单击 **Next**。出现管理员登录窗口。

2. 管理员登录窗口

输入新的管理员登录名和密码，然后单击 **Next**。

图 25: 管理员登录窗口



Initial Configuration Wizard

Enter the administrator's login name and password:

Administrator Login Name:

Password:

Confirm Password:

Note: You cannot retrieve the login name and password if you lose it. Please make sure you have a copy of this information in a secure location.

HTTP Redirect: ☐

Note: HTTP Redirect will redirect all HTTP traffic to HTTPS, ie, HTTPS is only way to manage the device through Web browsers.

3. WLAN 接入点窗口

如果使用 WORLD 或 ETSI 调节域中的设备，则必须选择一个国家 / 地区代码。选择相应选项，然后单击 **Next**。

图 26: 无线接入点国家 / 地区代码窗口



4. 物理接口窗口

在接口到区段绑定屏幕中，设置要绑定到 Untrust 安全区段的接口。将 Bgroup0 预绑定到 Trust 安全区段。Eth0/1 已被绑定到 DMZ 安全区段，但还可选择绑定其它接口。

图 27: 物理接口窗口



将接口绑定到区段后，便可配置此接口。完成此操作后显示的配置窗口将因安全设备上安装的小型 PIM 的不同而有所不同。要使用 ICW 继续配置设备，请单击 **Next**。

5. ADSL2/2+ 接口窗口

如果设备中已安装 ADSL2/2 + 小型 P1M，则可使用以下窗口配置 adslx/0 接口。

注意： 如果设备上安装有两个 ADSL2/2 + 小型 P1M，则无法使用 ICW 配置“多重链接”功能。要配置 ML ADSL，请参阅 *概念与范例 ScreenOS 参考指南*。

图 28: ADSL 接口配置窗口

The image shows the 'Initial Configuration Wizard' for a Juniper SSG 20 device. The wizard is titled 'Initial Configuration Wizard' and features the Juniper logo and 'SSG 20' text. Below the title bar, there is a navigation bar with icons for various configuration steps. The main content area is titled 'Please click the following links or the above figure to configure interfaces.' and lists three links: 'adsl1/0(Untrust Zone)', 'bgroup0(Trust Zone)', and 'eth0/1(DMZ Zone)'. The wizard then asks 'How does the Juniper device connect to the outside via adsl1/0 interface?'. It provides fields for 'VPI/VCI' (8 / 35) and 'Multiplexing Method' (LLC). Below these, there are radio buttons for 'RFC1483 Protocol Mode' (Bridged, Routed) and 'Operating Mode' (Auto, ANSI DMT, ITU DMT, Adsl2, Adsl2+). The wizard then presents four options for IP configuration: 'Dynamic IP via DHCP', 'Dynamic IP via PPPoA' (with Username, Password, and Confirm fields), 'Dynamic IP via PPPoE' (with Username, Password, and Confirm fields), and 'Static IP' (with Interface IP, Netmask, and Gateway fields). The 'Static IP' option is selected. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

表 13: ADSL 接口配置窗口中的字段

字段	说明
来自服务提供商的信息：	
VPI/VCI	用于识别永久虚拟电路的 VPI/VCI 值。
Multiplexing Method	ATM 多路传输方法 (缺省为 LLC)。
RFC1483 Protocol Mode	协议模式设置 (缺省为 Bridged)。
Operating Mode	物理线路的操作模式 (缺省为 Auto)。
IP 配置设置	<ul style="list-style-type: none"> ■ 选择 Dynamic IP via DHCP 启动设备以接收来自服务提供商的 ADSL 接口的 IP 地址。 ■ 选择 Dynamic IP via PPPoA 启动设备，使其充当 PPPoA 客户端。输入服务提供商所分配的用户名和密码。 ■ 选择 Dynamic IP via PPPoE 启动设备，使其充当 PPPoE 客户端。输入服务提供商所分配的用户名和密码。 ■ 选择 Static IP 为 ADSL 接口分配唯一且固定的 IP 地址。输入接口 IP 地址、网络掩码和网关 (网关地址是指连接到设备的路由器端口的 IP 地址)。

如果对这些设置仍有不明之处，请参阅随服务提供商设备而提供的 *Common Settings for Service Providers* 文档。

6. T1 接口窗口

如果设备中已安装 T1 小型 PIM 并已选择 Frame Relay 选项，则将显示以下窗口：

- T1 Physical Layer 选项卡窗口
- T1 Frame Relay 选项卡窗口

注意： 如果设备上安装有两个 T1 小型 PIM 并选择 Multi-link 选项，则将显示两个 Physical Layer 选项卡。

图 29: T1 Physical Layer 选项卡窗口

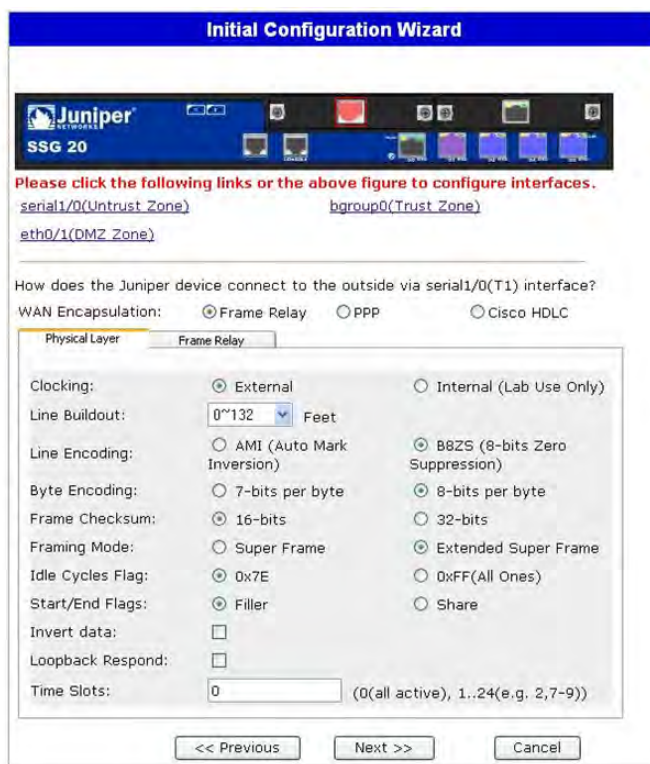


表 14: T1 Physical Layer 选项卡窗口中的字段

字段	说明
Clocking	设置接口上的传输时钟。
Line Buildout	设置接口在线路上的有效距离。缺省设置为 0 - 132 英尺。
Line Encoding	设置接口上的线路编码格式： <ul style="list-style-type: none"> ■ Auto Mark Inversion ■ 8-bits zero suppression
Byte Encoding	将 T1 接口上的字节编码设置为使用 7 位 / 字节或 8 位 / 字节。缺省设置为 8 位 / 字节。
Frame Checksum	设置校验和的尺寸。缺省设置为 16。
Framing Mode	设置帧格式。缺省设置为 Extended mode 。
Idle Cycles Flag	设置接口在空闲周期中传输的值。缺省设置为 0x7E ： <ul style="list-style-type: none"> ■ 0x7E (flags) ■ 0xFF (ones)
Start/End Flags	将开始标志和结束标志的传输设置为填充符或共享。缺省设置为 filler 。
Invert Data 复选框	启动未使用数据位的反向传输。
Loopback Respond 复选框	从远程信道服务设备 (CSU) 启用 T1 接口上的回传。
Time Slots	设置 T1 接口上时槽的使用。缺省设置为 0 ，使用全部 24 个时槽。

图 30: T1 Frame Relay 选项卡窗口

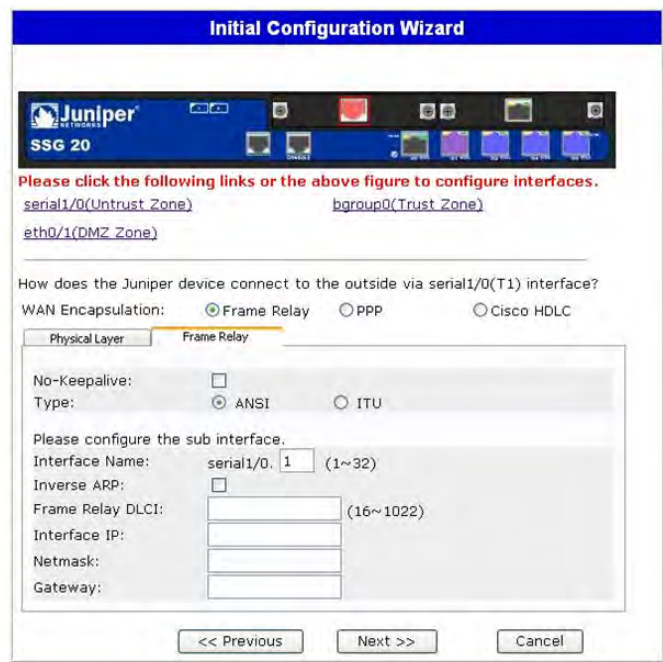


表 15: T1 Frame Relay 选项卡窗口中的字段

字段	说明
No-Keepalive 复选框	启用非激活。
Type	设置帧中继 LMI 类型： <ul style="list-style-type: none">■ ANSI: “美国国家标准学会”支持高达 8Mbps 的下行数据速率和 1Mbps 的上行数据速率。■ ITU: “国际电信同盟”支持 6.144 Mbps 的下行数据速率和 640 kbps 的上行数据速率。
Interface Name	设置子接口名称。
Inverse ARP	启用子接口的反向“地址解析协议”。
Frame Relay DLCI	向子接口分配数据链路连接标识符 (DLCI)。
Interface IP	设置子接口的 IP 地址。
Netmask	设置子接口的网络掩码。
Gateway	设置子接口的网关地址。

如果设备中已安装 T1 小型 PIM 并已选择 PPP 选项，则将显示以下窗口：

- PPP 选项的 PPP 选项卡窗口
- PPP 选项的 Peer User 选项卡窗口

图 31: PPP 选项的 PPP 选项卡窗口

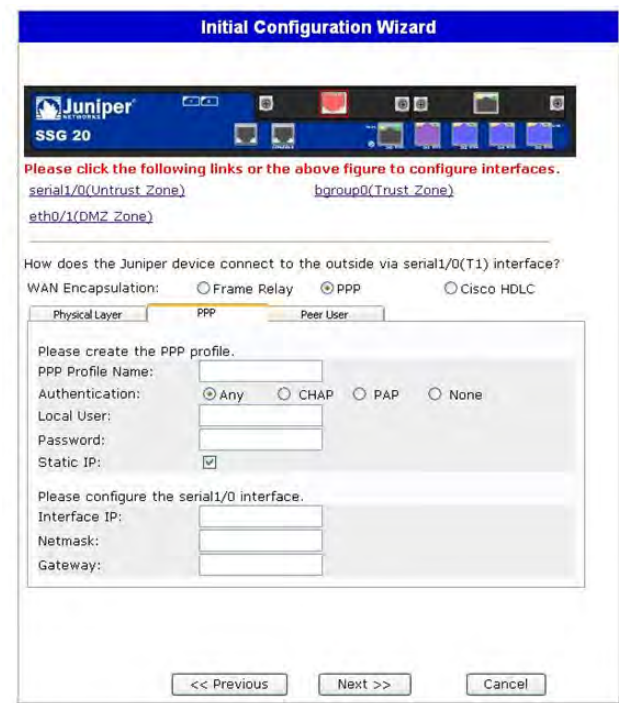


表 16: PPP 选项的 PPP 选项卡窗口中的字段

字段	说明
PPP Profile Name	设置 PPP 配置文件的文件名
Authentication	设置认证类型
Local User	设置本地用户的名称
Password	设置本地用户的密码
Static IP 复选框	启用静态 IP 地址
Interface IP	设置 serialx/0 接口 IP 地址
Netmask	设置 serialx/0 网络掩码
Gateway	设置 serialx/0 网关地址

图 32: PPP 选项的 Peer User 选项卡窗口

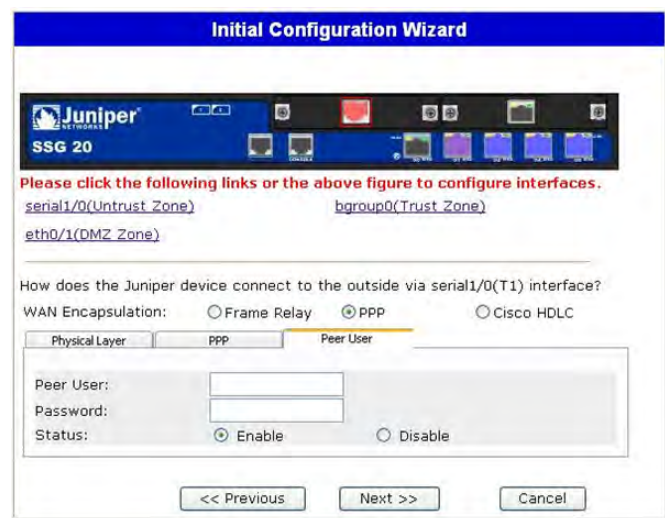


表 17: PPP 选项的 Peer User 选项卡窗口中的字段

字段	说明
Peer User	设置对等用户的名称
Password	为 Peer User 文本字段中指定的对等用户设置密码
Status	启用或禁用 PPP

如果设备已安装 T1 小型 PIM 并已选择 Cisco HDLC 选项，则将显示以下窗口：

图 33: Cisco HDLC 选项的 Cisco HDLC 选项卡窗口



表 18: Cisco HDLC 选项的 Cisco HDLC 选项卡窗口中的字段

字段	说明
Interface IP	设置 T1 Cisco HDLC 接口的 IP 地址
Netmask	设置 T1 Cisco HDLC 接口的网络掩码
Gateway	设置 T1 Cisco HDLC 接口的网关地址

7. E1 接口窗口

如果设备中已安装 E1 小型 PIM 并已选择 Frame Relay 选项，则将显示以下窗口：

- E1 Physical Layer 选项卡窗口
- E1 Frame Relay 选项卡窗口

注意： 如果设备上安装有两个 E1 小型 PIM 并选择 Multi-link 选项，则将显示两个 Physical Layer 选项卡。

图 34: E1 Physical Layer 选项卡窗口



表 19: E1 Physical Layer 选项卡窗口中的字段

字段	说明
Clocking	设置接口上的传输时钟。
Frame Checksum	设置校验和的尺寸。缺省设置为 16。
Framing Mode	设置帧格式。缺省设置为 without CRC4 。
Idle Cycles Flag	设置接口在空闲周期中传输的值。缺省设置为 0x7E : ■ 0x7E (flags) ■ 0xFF (ones)
Start/End Flags	将开始标志和结束标志的传输设置为填充符或共享。缺省设置为 filler。
Invert Data 复选框	启动未使用数据位的反向传输。
Time Slots	设置 T1 接口上时槽的使用。缺省设置为 0，使用全部 32 个时槽。

图 35: E1 Frame Relay 选项卡窗口



表 20: E1 Frame Relay 选项卡窗口中的字段

字段	说明
No-Keepalive 复选框	启用非激活。
Type	设置帧中继 LMI 类型： ■ ANSI: “美国国家标准学会”支持高达 8Mbps 的下行数据速率和 1Mbps 的上行数据速率。 ■ ITU: “国际电信同盟”支持 6.144 Mbps 的下行数据速率和 640 kbps 的上行数据速率。
Interface Name	设置子接口名称。
Inverse ARP 复选框	启用子接口的反向“地址解析协议”(ARP)。
Frame Relay DLCI	将 DLCI 分配给子接口。
Interface IP	设置子接口的 IP 地址。

字段	说明
Netmask	设置子接口的网络掩码。
Gateway	设置子接口的网关地址。

要使用 PPP 选项配置 E1 接口，请参阅第 69 页上的“PPP 选项的 PPP 选项卡窗口”。

要使用 Cisco HDLC 选项配置 E1 接口，请参阅第 70 页上的“Cisco HDLC 选项的 Cisco HDLC 选项卡窗口”。

8. ISDN 接口窗口

如果设备中已安装 ISDN 小型 PIM，则可使用以下窗口配置 bri1/0 (Untrust)。

注意： 如果设备中安装有两个 ISDN 小型 PIM 并已选择 Multi-link 选项，则将显示两个 Physical Layer 选项卡。

图 36: ISDN Physical Layer 选项卡窗口



表 21: ISDN Physical Layer 选项卡窗口中的字段

字段	说明
Switch Type	设置服务提供商的交换机类型： <ul style="list-style-type: none"> ■ att5e: At&T 5ESS ■ ntdms100: Nortel DMS 100 ■ ins-net: NTT INS-Net ■ etsi: European variants ■ ni1: National ISDN-1
SPID1	服务提供商 ID，通常是带有若干可选数字的七位电话号码。只有 DMS-100 和 NI1 交换机类型要求输入 SPID。DMS-100 交换机类型有两个分配的 SPID，每个 B 信道分别对应一个 SPID。
SPID2	服务提供商备份 ID。
TEI Negotiation	指定何时协商 TEI，或在启动时进行协商或在第一次呼叫时进行协商。通常在欧洲提供 ISDN 服务和连接到用于发起 TEI 协商的 DMS-100 交换机时使用此类设置。
Calling Number	ISDN 网络帐号。
Sending Complete 复选框	启用将完整信息发送到外向设置消息。通常仅在中国香港特别行政区和中国台湾地区使用。

可选择 bri1/0 接口使用拨号器、多重链接拨号器、租用线路或通过 BRI 拨号的方式进行连接。不选择任何选项、选择一个选项或选择两个选项，将显示与以下窗口相类似的窗口。

图 37: ISDN 连接选项卡窗口

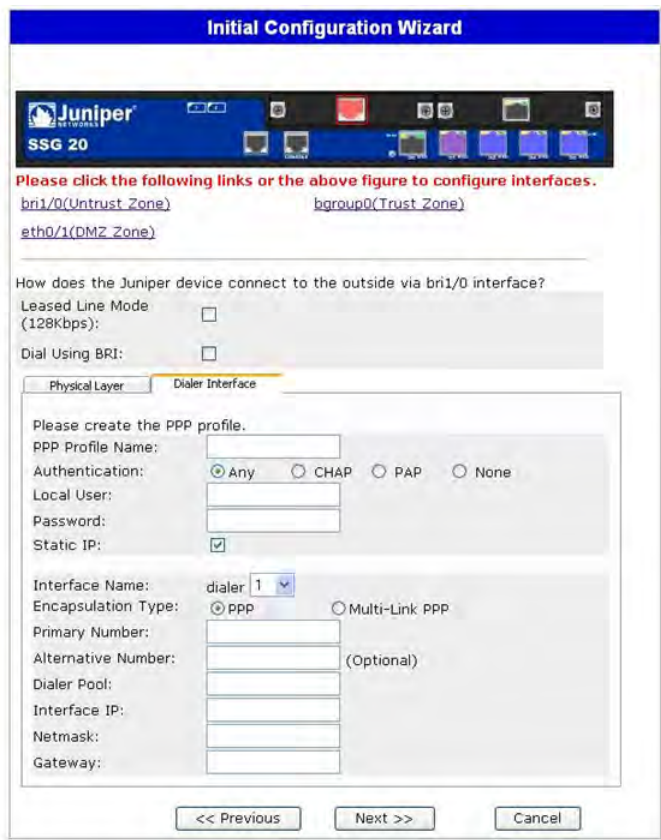


表 22: ISDN 连接选项卡窗口中的字段

字段	说明
PPP Profile Name	设置 ISDN 接口的 PPP 配置文件的文件名。
Authentication	设置 PPP 认证类型： <ul style="list-style-type: none"> ■ Any ■ CHAP: 质询握手认证协议 ■ PAP: 密码认证协议 ■ None
Local User	设置本地用户。
Password	设置本地用户的密码。
Static IP 复选框	启用接口的静态 IP 地址。
Interface IP	设置接口的 IP 地址。
Interface Name (仅 Dialer)	设置拨号器接口名称。缺省设置为 dialer.1 。
Encapsulation Type	设置拨号器和使用 BRI 接口的拨号器的封装类型。缺省设置为 PPP 。
Primary Number	为拨号器和使用 BRI 接口的拨号器设置主号。
Alternative Number	设置无法使用主号进行连接时的备选 (第二) 号码以实现连接。
Dialer Pool (仅 Dialer)	设置拨号器接口拨号器池的名称。

字段	说明
Netmask	设置网络掩码。
Gateway	设置网关地址。

9. V.92 调制解调器接口窗口

如果设备中已安装 V.92 小型 PIM，则可使用以下窗口配置 serialx/0 (Modem) 接口：

图 38: 调制解调器接口窗口



表 23: 调制解调器接口窗口中的字段

字段	说明
Modem Name	设置调制解调器接口的名称
Init String	设置调制解调器的初始化字符串
ISP Name	为服务提供商分配名称
Primary Number	指定用于访问服务提供商的电话号码
Alternative Number (可选)	指定主号无法接通时的备选电话号码以访问服务提供商
Login Name	设置服务提供商帐户的登录名
Password	设置登录名的密码
Confirm	确认在 Password 字段中输入的密码

10. Eth0/0 接口 (Untrust 区段) 窗口

eth0/0 接口可具有通过 DHCP 或 PPPoE 分配的静态或动态 IP 地址。

图 39: Eth0/0 接口窗口

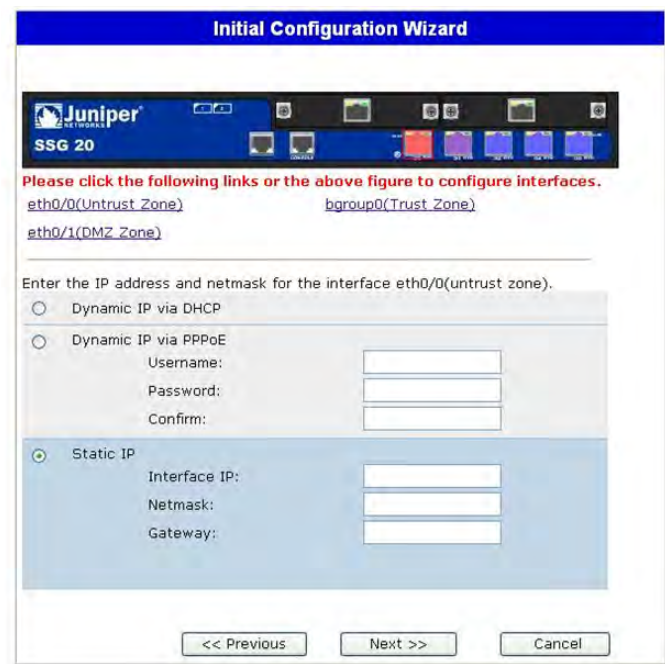


表 24: Eth0/0 接口窗口中的字段

字段	说明
Dynamic IP via DHCP	使设备可以从服务提供商处获取 Untrust 区段接口的 IP 地址。
Dynamic IP via PPPoE	使设备可以充当 PPPoE 客户端，以便从服务提供商处获取 Untrust 区段的 IP 地址。输入服务提供商所分配的用户名和密码。
Static IP	为 Untrust 区段接口分配唯一且固定的 IP 地址。输入 Untrust 区段接口 IP 地址、网络掩码和网关地址。

11. Eth0/1 接口 (DMZ 区段) 窗口

eth0/1 接口可具有通过 DHCP 分配的静态或动态 IP 地址。

图 40: Eth0/1 接口窗口



表 25: Eth0/1 接口窗口中的字段

字段	说明
Dynamic IP via DHCP	使设备可以从服务提供商处获取 DMZ 接口的 IP 地址。
Static IP	为 DMZ 接口分配唯一且固定的 IP 地址。输入 DMZ 接口 IP 和网络掩码。

12. Bgroup0 接口 (Trust 区段) 窗口

bgroup0 接口可具有通过 DHCP 分配的静态或动态的 IP 地址。

缺省接口 IP 地址为 192.168.1.1，网络掩码为 255.255.255.0 或 24。

图 41: Bgroup0 接口窗口

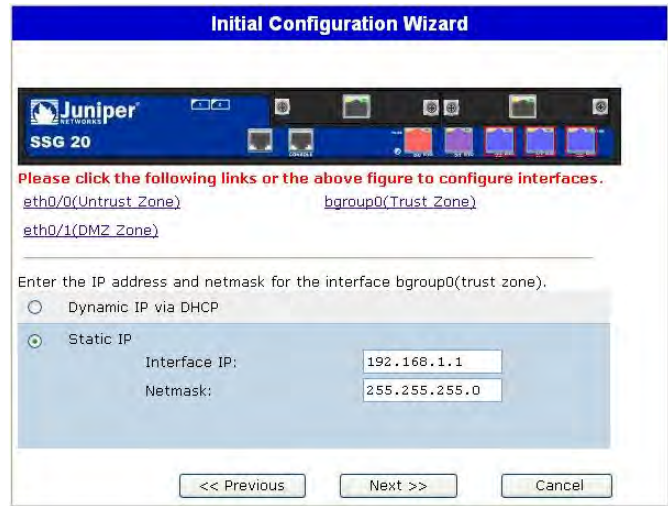


表 26: Bgroup0 接口窗口中的字段

字段	说明
Dynamic IP via DHCP	使设备可以从服务提供商处获取 Trust 区段接口的 IP 地址。
Static IP	为 Trust 区段接口分配唯一且固定的 IP 地址。输入 Trust 区段接口 IP 地址和网络掩码。

13. Wireless0/0 接口 (Trust 区段) 窗口

如果配置 SSG 20-WLAN 设备，则必须先设置服务集标识符 (SSID)，否则将无法激活 wireless0/0 接口。有关配置无线接口的详细说明，请参阅 *概念与范例 ScreenOS 参考指南*。

图 42: Wireless0/0 接口窗口

Initial Configuration Wizard

Please click this wlan radio to configure wireless.

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.

[eth0/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#) [wireless0/0\(Trust Zone\)](#)

How do you want to configure wireless0/0 interface(trust zone)?

Wlan Mode: 2.4G(802.11b/g)

SSID:

☒ Open No Encryption

☐ WPA-PSK

☒ Passphrase(8~63 ASCII):
Confirm:

☐ PSK(64 hexadecimal):
Confirm:

Encryption Type: ☒ Auto ☐ TKIP ☐ AES

Interface IP: 192.168.2.1
Netmask: 255.255.255.0

<< Previous Next >> Cancel

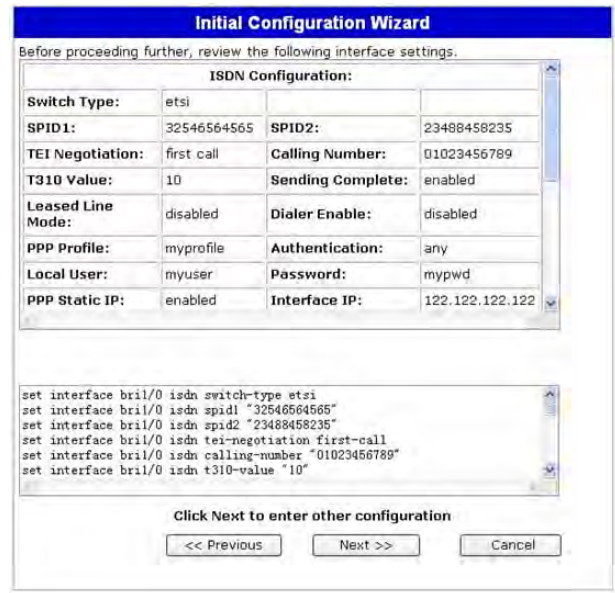
表 27: Wireless0/0 接口窗口中的字段

字段	说明
Wlan Mode	设置 WLAN 无线模式： <ul style="list-style-type: none">■ 5G (802.11a)。■ 2.4G (802.11b/g)。■ Both (802.11a/b/g)。
SSID	设置 SSID 名称。
Authentication and Encryption	设置 WLAN 接口认证和加密： <ul style="list-style-type: none">■ Open 认证为缺省设置，在这种情况下允许任何人访问设备。对此认证选项无需进行加密处理。■ WPA Pre-Shared Key 认证设置访问无线连接时必须输入的预共享密钥 (PSK) 或密码短语。可以选择输入 HEX 或 PSK 的 ASCII 值。HEX PSK 必须是一个 256 位 (64 个文本字符) 的 HEX 值。ASCII 密码短语必须是 8 到 63 个文本字符。必须选择“临时密钥完整性协议”(TKIP) 或“高级加密标准”(AES) 作为此选项的加密类型，或者选择 Auto 以允许使用任一选项。■ WPA2 预共享密钥。■ WPA 自动预共享密钥。
Interface IP	设置 WLAN 接口 IP 地址。
Netmask	设置 WLAN 接口网络掩码。

14. 接口汇总窗口

配置 WAN 接口以后，将显示接口汇总窗口。

图 43: 接口汇总窗口



检查接口配置，准备好继续后，单击 **Next**。出现物理以太网 DHCP 接口窗口。

15. 物理以太网 DHCP 接口窗口

选择 **Yes** 启动设备以通过 DHCP 为有线网络分配 IP 地址。输入 IP 地址范围 (设备会将这些 IP 地址分配给正在使用您的网络的客户端), 然后单击 **Next**。

图 44: 物理以太网 DHCP 接口窗口

16. 无线 DHCP 接口窗口

选择 **Yes** 启动设备以通过 DHCP 为无线网络分配 IP 地址。输入 IP 地址范围 (设备会将这些 IP 地址分配给正在使用您的网络的客户端), 然后单击 **Next**。

图 45: 无线 DHCP 接口窗口

17. 确认窗口

根据需要确认设备配置和更改。单击 **Next** 保存、重新启动设备和运行配置。

图 46: 确认窗口

Initial Configuration Wizard

Before proceeding further, review the following all device settings.

Admin Login:	netscreen		Password:	*****
Device is in NAT mode.				
ISDN Configuration:				
Switch Type:	etsi			
SPID1:	32546564565		SPID2:	23488458235
TEI Negotiation:	first call		Calling Number:	01023456789
T310 Value:	10		Sending Complete:	enabled
Leased Line Mode:	disabled		Dialer Enable:	disabled
PPP Profile:	myprofile		Authentication:	any

```

set admin password "netscreen"
set interface bril/0 isdn switch-type etsi
set interface bril/0 isdn spid1 "32546564565"
set interface bril/0 isdn spid2 "23488458235"
set interface bril/0 isdn tei-negotiation first-call
set interface bril/0 isdn calling-number "01023456789"
  
```

Click Next to save CLI into device.

<< Previous Next >> Cancel

以保存的系统配置重新启动设备后，将出现 WebUI 登录提示。有关如何使用 WebUI 访问设备的信息，请参阅第 29 页上的“使用 WebUI”。

索引

A

AAL5 多路传输	40
ADSL	
连接电缆	23
连接端口	23
配置接口	39
Annex A	23
Annex B	23
ATM 点对点传输协议	
请参阅 PPPoA	
ATM 适配层 5	40

C

重置针孔，使用	47
---------------	----

D

电缆	
ADSL	24
串行	23
基本网络连接	23
多路传输，配置	41

G

管理	
通过 Telnet 连接	30
通过 WebUI	29
通过控制台	28

I

ISP IP 地址和网络掩码	42
----------------------	----

J

将接口备份到 Untrust 区段	35
静态 IP 地址	40

L

LED	
PIM 1	11
PIM 2	12
POWER	11
STATUS	11
以太网端口上的活动链接	13
连接，基本网络	23

N

内存升级步骤	52
--------------	----

P

PPPoA	40
PPPoE	40
配置	
admin 名称和密码	32
ADSL 2/2 + 小型 PIM	39
备份不可信接口	35
E1 小型 PIM	45
管理存取	34
管理地址	35
管理服务	34
ISDN 小型 PIM	43
桥接组 (bgroup)	33
缺省路由	35
日期和时间	33
T1 小型 PIM	44
V.92 调制解调器小型 PIM	45
VPI/VCI 对	41
USB	17
无线接口和以太网组合	39
无线认证和加密	37
虚拟电路	40
主机名和域名	34

Q

缺省 ip 地址	31
----------------	----

T

天线	25
----------	----

U

Untrust 区段，配置备份接口	35
-------------------------	----

V

VPI/VCI	
配置	41
值	40

W

WLAN LED

- 802.11a..... 12
- b/g..... 12

无线

- 使用缺省接口..... 25
- 天线..... 25

无线电收发器

- WLAN 0..... 16
- WLAN 1..... 16

X

小型 PIM

- 安装..... 51
- 空面板..... 50
- 移除..... 50

虚拟路径标识符 / 虚拟通道标识符

- 请参阅 VPI/VCI

Y

以太网点对点传输协议

- 请参阅 PPPoE

Z

证书

- 安全..... 57
- EMC (辐射)..... 57
- EMC 抗扰度..... 57
- 欧洲电信标准机构 (ETSI)..... 57
- T1 接口..... 58

目錄

關於本指南	5
組織	6
WebUI 慣例	6
CLI 慣例	7
獲取文件和技術支援	7
第 1 章 硬體綜述	9
連接埠和電源連接器	10
前面板	11
系統狀態 LED	11
連接埠說明	12
乙太網路連接埠	12
主控台連接埠	12
AUX 連接埠	13
迷你實體介面模組連接埠說明	13
後面板	15
電源配接卡	15
無線電收發機	15
接地插孔	15
天線類型	16
USB 連接埠	16
第 2 章 安裝及連接裝置	17
開始之前	18
安裝設備	18
將介面纜線連接到裝置	20
連接電源	20
將裝置連接到網路	21
將裝置連接到不信任的網路	21
乙太網路連接埠	21
序列 (AUX/ 主控台) 連接埠	22
將迷你 PIM 連接到不信任的網路	22
ADSL2/2 + 迷你 PIM	22
ISDN、T1、E1 及 V.92 迷你 PIM	23
將裝置連接到內部網路或工作站	23
乙太網路連接埠	23
無線天線	23
第 3 章 組態裝置	25
存取裝置	26
使用主控台連接	26
使用 WebUI	27

使用 Telnet	28
預設裝置設定	28
基本裝置組態	30
根管理名稱及密碼	30
日期與時間	31
橋接群組介面	31
管理式存取	32
管理服務	32
主機名稱及網域名稱	32
預設路由	33
管理介面位址	33
備份 Untrust 介面組態	33
基本無線組態	34
迷你 PIM 組態	37
ADSL2/2 + 介面	37
虛擬電路	38
VPI/VCI 及多工法	38
PPPoE 或 PPPoA	39
靜態 IP 位址及網路遮罩	39
ISDN 介面	41
T1 介面	41
E1 介面	42
V.92 數據機介面	43
基本防火牆保護	44
驗證外部連接性	44
將裝置重設為出廠預設設定	45
第 4 章 維修裝置	47
必要工具及零件	47
更換迷你實體介面模組	47
移除空白面板	48
移除迷你 PIM	48
安裝迷你 PIM	49
升級記憶體	50
附錄 A 規格	53
實體	54
電器設備	54
環境容忍度	54
憑證	55
安全	55
EMC 輻射	55
EMC 耐受性	55
ETSI	55
T1 介面	56
連接器	56
附錄 B 初始組態精靈	59
索引	81

關於本指南

Juniper Networks Secure Services Gateway (SSG) 20 裝置是一個整合的路由器及防火牆平台，能夠為分支機構或零售商店提供「網際網路通訊協定安全性」(IPSec) 虛擬私人網路 (VPN) 及防火牆服務。

Juniper Networks 提供兩種機型的 SSG 20 裝置：

- SSG 20，支援附屬 (AUX) 連接
- SSG 20-WLAN，支援整合的 802.11a/b/g 無線標準

兩種 SSG 20 裝置都支援「通用序列匯流排」(USB) 儲存裝置和兩個迷你實體介面模組 (PIM) 插槽（用於固定迷你 PIM）。裝置也提供「區域網路」(LAN) 與「廣域網路」(WAN) 之間的通訊協定對話。

注意： 文件中的組態說明和範例是根據執行 ScreenOS 5.4 之裝置的功能。您的裝置的功能可能與文件中所描述的不同，這視您所執行的 ScreenOS 版本而定。如需最新的裝置文件，請造訪 Juniper Networks Technical Publications 網站：
<http://www.juniper.net/techpubs/hardware>。若要了解目前適用於您裝置的 ScreenOS 版本，請造訪 Juniper Networks Support 網站：
<http://www.juniper.net/customers/support/>。

組織

本指南包括下列各節：

- 第 1 章，「硬體綜述」說明 SSG 20 裝置的機架和元件。
- 第 2 章，「安裝及連接裝置」說明安裝 SSG 20 裝置的方法及對裝置進行纜線與電源連接的方法。
- 第 3 章，「組態裝置」說明組態並管理 SSG 20 裝置的方法及執行某些基本組態工作的方法。
- 第 4 章，「維修裝置」說明 SSG 20 裝置的維修和維護程序。
- 附錄 A，「規格」提供 SSG 20 裝置的通用系統規格。
- 附錄 B，「初始組態精靈」提供有關使用 SSG 20 裝置的 Initial Configuration Wizard (初始組態精靈，ICW) 的詳細資訊。

WebUI 慣例

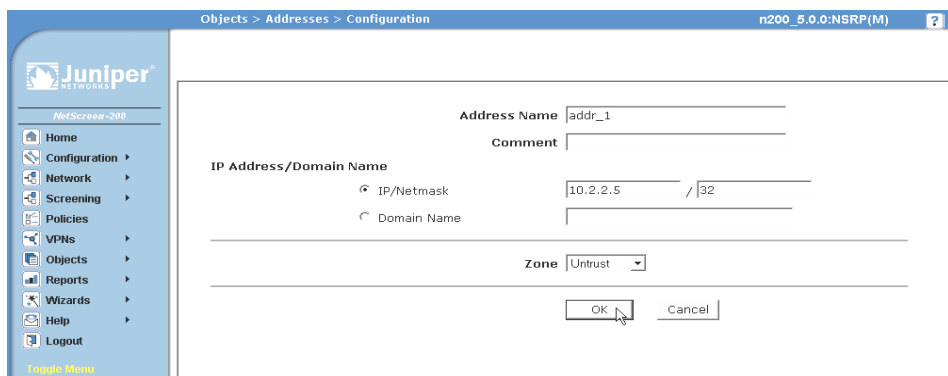
如要用 WebUI 執行任務，必須先瀏覽到相應的對話方塊，然後在該對話方塊中定義物件和設定參數。尖角符號 (>) 表示 WebUI 中的瀏覽順序，您可按一下功能表選項及連結來依循該順序。每個任務的說明集分為瀏覽路徑及組態設定兩個部分。

下圖列出了前往具有以下範例組態設定之位址組態對話方塊的路徑：

Objects > Addresses > List > New: 輸入以下內容，然後按一下 **OK**:

Address Name: addr_1
 IP Address/Domain Name:
 IP/Netmask: (選擇), 10.2.2.5/32
 Zone: Untrust

圖 1: 瀏覽路徑與組態設定



CLI 慣例

下列慣例用於在範例及文字中呈現 CLI 指令語法。

在範例中：

- 在中括弧 [] 中的任何內容都是選擇性的。
- 在大括弧 { } 中的任何內容都是必需的。
- 如果選項不止一個，則使用導線 (|) 分隔每個選項。例如：

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

意味著「設定 ethernet1、ethernet2 或 ethernet3 介面的管理選項」。

- 變數以斜體方式顯示：

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

在文字中：

- 指令以粗體方式顯示。
- 變數以斜體方式顯示。

注意： 輸入關鍵字時，您需鍵入足以唯一識別單詞的字母。例如，若要輸入指令 **set admin user kathleen j12fmt54**，只要鍵入 **set adm u kath j12fmt54** 即可。儘管輸入指令時可以使用此捷徑，本文所述的所有指令都以其完整形式呈現。

獲取文件 and 技術支援

要獲得任何 Juniper Networks 產品的技術文件，請造訪 www.juniper.net/techpubs/。

如需技術支援，請使用 <http://www.juniper.net/support/> 的 Case Manager 連結來開啓一個支援案例，或電洽 1-888-314-JTAC (美國境內) 或 1-408-745-9500 (美國境外)。

如果在本文中發現任何錯誤或遺漏，請用下面的電子郵件位址與我們連絡：

techpubs-comments@juniper.net

第 1 章

硬體綜述

本章提供 SSG 20 機架及其元件的詳細說明。本章包含下列各節：

- 第 10 頁上的「連接埠和電源連接器」
- 第 11 頁上的「前面板」
- 第 15 頁上的「後面板」

連接埠和電源連接器

本節說明並顯示內建連接埠及電源連接器的位置。請參閱下圖，以取得內建連接埠位置，並參閱表 1，以取得電源連接器說明。

圖 2: 內建連接埠及迷你 PIM 位置

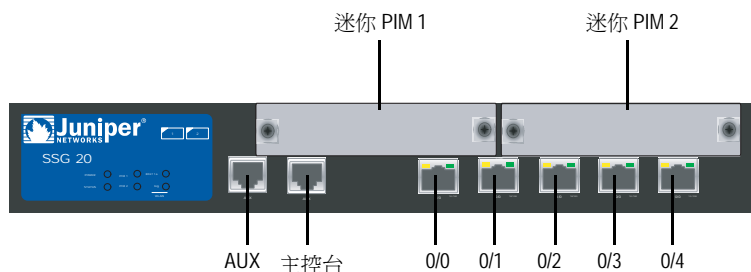


表 1: SSG 20 連接埠和電源連接器

連接埠	說明	連接器	速度 / 通訊協定
0/0-0/4	透過交換機或集線器啓用至工作站的直接連接或 LAN 連接。此連接也可讓您透過 Telnet 會話或 WebUI 來管理裝置。	RJ-45	10/100 Mbps 乙太網路 自動感應雙工及自動 MDI/MDIX
USB	啓用與系統的 1.1 USB 連接。	N/A	12M (全速) 或 1.5M (低速)
主控台	啓用與系統之間的系列連接。用於終端模擬連接，以啓動 CLI 會話。	RJ-45	9600 bps/RS-232C 序列
AUX	透過外部數據機啓用備份 RS-232 非同步序列網際網路連接。	RJ-45	9600 bps - 115 Kbps/RS-232C 序列
迷你 PIM			
ADSL 2/2 +	透過 ADSL 資料連結啓用網際網路連接。	RJ-11 (附件 A) RJ-45 (附件 B)	ANSI T1.413 問題 2 (只限附件 A) ITU G.992.1 (G.dmt) ITU G.992.3 (ADSL2) ITU G.992.5 (ADSL2 +)
V.92 數據機	啓用與服務提供者的主要或備份網際網路或不受信任的網路連接。	RJ-11	9600 bps - 115 Kbps/RS-232 序列自動感應雙工及極性
T1	啓用與不受信任網路的 T1 線路的連接。	RJ-45	1.544 Mbps (全時插槽)
E1	啓用與不受信任網路的 E1 線路的連接。	RJ-45	2.048 Mbps (全時插槽)
ISDN	啓用 ISDN 線路作為 Untrust 或備份介面。(S/T)	RJ-45	速度為 64 Kbps 的 B 通道 速度為 128 Kbps 的租借線路
天線 A 與 B (SSG 20-WLAN)	允許直接連接到無線電連接的鄰近的工作站。	RPSMA	802.11a (54 Mbps, 無線電頻為 5 GHz) 802.11b (11 Mbps, 無線電頻為 2.4 GHz) 802.11g (54 Mbps, 無線電頻為 2.4 GHz) 802.11 superG (108 Mbps, 無線電頻為 2.4 GHz 及 5 GHz)

前面板

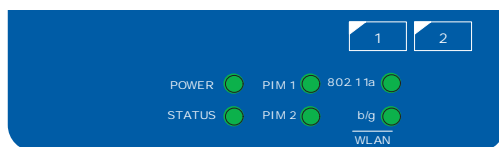
本節說明 SSG 20 裝置前面板上的下列元素：

- 系統狀態 LED
- 連接埠說明
- 迷你實體介面模組連接埠說明

系統狀態 LED

系統狀態 LED 顯示重要裝置功能的相關資訊。圖 3 顯示了 SSG 20-WLAN 裝置前面的每一個狀態 LED 的位置。WLAN LED 只出現在 SSG 20-WLAN 裝置上。

圖 3: 狀態 LED



當系統電源開啓時，POWER LED 會從熄滅變更為閃爍綠色，而且 STATUS LED 會依下列順序變更：紅色、綠色、閃爍綠色。完成啓動工作大約需要兩分鐘。如果您想要關閉系統後重新開啓，我們建議您在關閉後等待數秒，然後再開啓電源。表 2 提供了每一個系統狀態 LED 的名稱、顏色、狀態及說明。

表 2: 狀態 LED 說明

名稱	顏色	狀態	說明
POWER	綠色	穩定亮起	指出系統已經通電。
		關閉	指出系統沒有通電。
	紅色	穩定亮起	指出裝置操作不正常。
		關閉	指出裝置操作正常。
STATUS	綠色	穩定亮起	指出系統正在啓動或執行診斷。
		閃爍	指出裝置操作正常。
	紅色	閃爍	指出偵測到錯誤。
PIM 1	綠色	穩定亮起	指出迷你 PIM 正在運作中。
		閃爍	指出迷你 PIM 正在傳遞流量。
		關閉	指出迷你 PIM 不在操作中。
PIM 2	綠色	穩定亮起	指出迷你 PIM 正在運作中。
		閃爍	指出迷你 PIM 正在傳遞流量。
		關閉	指出迷你 PIM 不在操作中。
WLAN (只限 WLAN 裝置)			
802.11a	綠色	穩定亮起	指出已建立無線連接，但沒有連結活動。
		緩慢閃爍	指出已建立無線連接。 序列傳輸速率和連結活動成比例。
		關閉	指出未建立無線連接。

名稱	顏色	狀態	說明
b/g	綠色	穩定亮起	指出已建立無線連接，但沒有連結活動。
		緩慢閃爍	指出已建立無線連接。序列傳輸速率和連結活動成比例。
		關閉	指出未建立無線連接。

連接埠說明

本節說明下列連接埠的用途及功能：

- 乙太網路連接埠
- 主控台連接埠
- AUX 連接埠

乙太網路連接埠

五個 10/100 乙太網路連接埠提供與集線器、交換機、本機伺服器及工作站的 LAN 連接。您也可以指定一個乙太網路連接埠來管理流量。這些連接埠標示為 0/0 到 0/4。有關每一個乙太網路連接埠的預設區域繫結，請參閱第 28 頁上的「預設裝置設定」。

當組態其中一個連接埠時，請參考對應於連接埠位置的介面名稱。前面板上由左至右，連接埠的介面名稱為 ethernet0/0 到 ethernet0/4。

圖 4 顯示每一個乙太網路連接埠上的 LED 位置。

圖 4: 活動連結 LED 位置

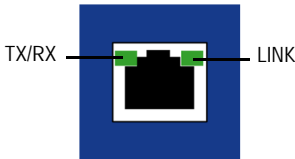


表 3 說明乙太網路連接埠 LED。

表 3: LAN 連接埠 LED

名稱	顏色	狀態	說明
LINK	綠色	穩定亮起	連接埠連線中。
		關閉	連接埠已離線。
TX/RX	綠色	閃爍	有流量正在通過。序列傳輸速率和連結活動成比例。
		關閉	連接埠可能開啓，但是未接收資料。

主控台連接埠

「主控台」連接埠是一種作為資料電路終止設備 (DCE) 的有線 RJ-45 序列連接埠，可用於本機管理。使用終端連接時，請使用直通電纜，但連接到另一個 DCE 裝置時，請使用交叉電纜。裝置隨附有 RJ-45 到 DB-9 的配接卡。

請參閱第 56 頁上的「連接器」，以取得 RJ-45 連接器接腳配置資訊。

AUX 連接埠

附屬 (AUX) 連接埠是一種作為資料終止設備 (DTE) 的有線 RJ-45 序列連接埠，可連接到數據機以允許遠端管理。我們不建議使用此連接埠進行一般遠端管理。通常，是將 AUX 連接埠指派為備份序列介面。序列傳輸速率是可調的，範圍為 9600 bps 至 115200 bps，而且需要由硬體進行流量控制。連接到數據機時，請使用直通電纜，但連接到另一個 DTE 裝置時，請使用交叉電纜。

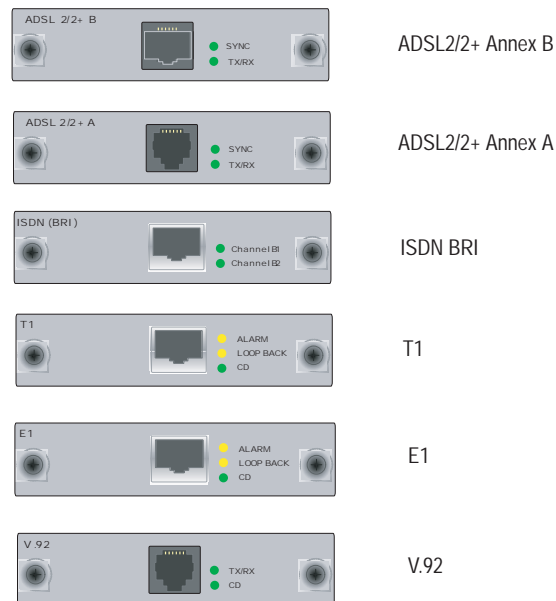
請參閱第 56 頁上的「連接器」，以取得 RJ-45 連接器接腳配置資訊。

迷你實體介面模組連接埠說明

裝置上支援的每一個迷你實體介面模組 (PIM) 都有下列元件：

- 一個纜線連接器連接埠 - 接受網路媒體連接器。圖 5 顯示了可用的迷你 PIM。
- 您最多可在一個裝置中安裝兩個迷你 PIM。

圖 5: SSG 20 的迷你 PIM



- 兩個到三個狀態 LED - 指出連接埠狀態。表 4 說明了 LED 狀態的意義。

表 4: SSG 20 上的迷你 PIM LED 狀態

類型	名稱	顏色	狀態	說明
ADSL 2/2 + (附件 A 及 B)	SYNC	綠色	穩定亮起	指出已連接 ADSL 介面
			閃爍	指出正在連接
			關閉	指出介面目前為閒置
	TX/RX	綠色	閃爍	指出有流量正在通過
			關閉	指出沒有流量正在通過
ISDN (BRI)	CH B1	綠色	穩定亮起	指出 B 通道 1 正在作用中
			關閉	指出 B 通道 1 不在作用中
	CH B2	綠色	穩定亮起	指出 B 通道 2 正在作用中
			關閉	指出 B 通道 2 不在作用中
T1/E1	ALARM	黃色	穩定亮起	指出有本機或遠端警示；裝置偵測到失敗
			關閉	指出沒有警示或失敗
	LOOP BACK	黃色	穩定亮起	指出偵測到回傳或線路狀態
			關閉	指出回傳不在作用中
	CD	綠色	穩定亮起	指出偵測到載波訊號，而且迷你 PIM 中的內部 DSU/CSU 正在與另一個 DSU/CSU 通訊
			關閉	指出載波偵測不在作用中
V.92	CD	綠色	穩定亮起	指出連結正在作用中
			關閉	指出序列介面不在服務中
	TX/RX	綠色	閃爍	指出有流量正在通過
			關閉	指出沒有流量正在通過



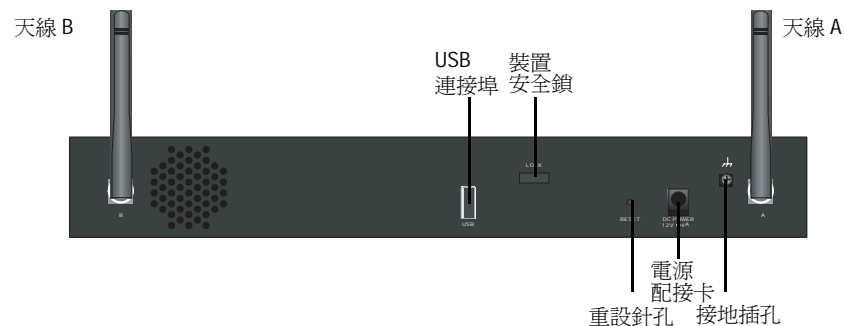
小心：迷你 PIM 不可熱抽換。您必須先將它們安裝在前面板插槽中，然後才能開啓裝置電源。

後面板

本節說明 SSG 20 裝置後面板上的下列元素：

- 電源配接卡
- 無線電收發機
- 接地插孔
- 天線類型
- USB 連接埠

圖 6: SSG 20-WLAN 裝置的後面板



電源配接卡

裝置前面板上的 POWER LED 不是發出綠光，就是熄滅。綠光指出運作正常，而熄滅則指出電源配接卡失敗或裝置關閉。

無線電收發機

SSG 20-WLAN 包含兩個支援 802.11a/b/g 標準的無線連接無線電收發機。第一個無線電收發機 (WLAN 0) 使用 2.4 GHz 無線電頻，支援速度為 11 Mbps 的 802.11b 標準、速度為 54 Mbps 的 802.11g 標準，以及速度為 108 Mbps 的 802.11 SuperG 標準。第二個無線電收發機 (WLAN 1) 使用 5GHz 無線電頻，支援速度為 54 Mbps 的 802.11a。有關組態無線電頻的資訊，請參閱第 34 頁上的「基本無線組態」。

接地插孔

單孔接地插孔在機架後面，用來將裝置接地（請參閱圖 6）。

若要在連接電源之前將裝置接地，請將接地纜線接地，然後將纜線連接到機架後面的插孔。

天線類型

SSG 20-WLAN 裝置支援三種類型的自建無線天線：

- **分集天線** - 分集天線具有 2dBi 方向覆蓋範圍，並在覆蓋區域內提供相當一致的訊號強度，因此適用於大部份安裝。裝置出廠時隨附有此類型的天線。
- **外部全向天線** - 外部天線提供 2dBi 全向覆蓋範圍。不同於成對運作的分集天線，外部天線的目的是消除使用兩個天線時，因訊號接收中輕微延遲的特性而偶爾發生的回音效果。
- **外部方向天線** - 外部方向天線提供 2dBi 單向覆蓋範圍，因此適用於如走廊及外牆的位置（天線面向內）。

USB 連接埠

SSG 20 裝置後面板上的 USB 連接埠接受安裝有 Compact-Flash 磁碟的通用序列匯流排 (USB) 儲存裝置或 USB 儲存裝置配接卡，CompactFlash Association 發佈的 *CompactFlash Specification* 中對其有詳細定義。安裝並組態 USB 儲存裝置後，如果主要的 Compact-Flash 磁碟無法啟動，它會自動充當次要啟動裝置。

USB 連接埠允許在外部 USB 儲存裝置與位於安全裝置內部的快閃儲存區之間傳送檔案，例如裝置組態、使用者憑證及更新版本影像。USB 連接埠支援 USB 1.1 規格，其檔案傳送速度可以是低速 (1.5M) 或全速 (12M)。

若要在 USB 儲存裝置與 SSG 20 之間傳送檔案，請執行下列步驟：

1. 將 USB 儲存裝置插入安全裝置上的 USB 連接埠。
2. 利用 **save {software | config | image-key} from usb 檔案名稱 to flash** CLI 指令，將檔案從 USB 儲存裝置儲存到裝置上的內部快閃儲存區。
3. 移除 USB 儲存裝置之前，請利用 **exec usb-device stop** CLI 指令，停止 USB 連接埠。
4. 現在可以安全移除 USB 儲存裝置。

如果想要從 USB 儲存裝置刪除檔案，請使用 **delete file usb:/ 檔案名稱** CLI 指令。

如果想要檢視 USB 儲存裝置或內部快閃儲存區上儲存的檔案資訊，請使用 **get file** CLI 指令。

第 2 章

安裝及連接裝置

本章說明如何安裝 SSG 20 裝置，並將纜線及電源連接到裝置。本章包括下列各節：

- 第 18 頁上的「開始之前」
- 第 18 頁上的「安裝設備」
- 第 20 頁上的「將介面纜線連接到裝置」
- 第 20 頁上的「連接電源」
- 第 21 頁上的「將裝置連接到網路」

注意： 有關安全警告和說明，請參閱 *Juniper Networks Security Products Safety Guide*。在使用任何設備之前，請注意由電路引發的危險以及熟悉標準操作以防止意外事故的發生。

開始之前

機架的位置、安裝設備的配置，以及有線空間的安全性對於能否適當操作系統有決定性的影響。



警告：若要防止未授權人員的濫用及侵入，請在安全環境中安裝 SSG 20 裝置。

遵守下列預防措施可以防止關機、設備故障及傷害：

- 安裝之前，一定要檢查電源供應器是否與任何電源中斷連接。
- 確定您操作裝置的空間有足夠的空氣流通，而且室溫不超過 104°F (40°C)。
- 不要將裝置放在阻塞通風口或排氣管的設備安裝框架中。確定安裝的機櫃有風扇，而且兩側設有百葉窗。
- 開始安裝之前，請改善這些危險狀況：潮濕地板、漏電、未接地或磨損的電纜，或遺失安全接地線。

安裝設備

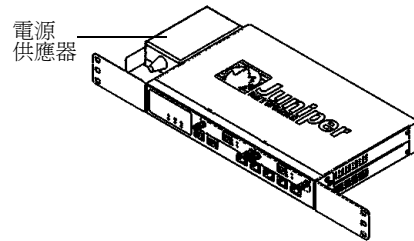
您可以對 SSG 20 裝置採用正面安裝、牆上安裝或桌上安裝。安裝套件可以另外購買。

若要安裝 SSG 20 裝置，您需要 2 號十字螺絲起子（未提供）及與設備機櫃相容的螺絲（附在套件中）。

注意： 安裝裝置時，請確定它在電源插座的範圍內。

若要在標準 19 吋設備機櫃上正面安裝 SSG 20 裝置，請執行下列步驟：

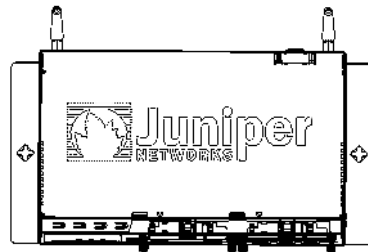
圖 7: SSG 20 正面安裝



1. 使電源供應器機櫃安裝耳與裝置的左邊正面邊緣對齊。
2. 將螺絲置於孔中，然後使用十字螺絲起子來鎖緊它們。
3. 使另一個機櫃安裝耳與裝置的右邊正面邊緣對齊。
4. 將螺絲置於孔中，然後使用十字螺絲起子來鎖緊它們。
5. 利用所提供的螺絲，在機櫃上安裝裝置。
6. 將電源供應器插入電源插座。

若要在牆上安裝 SSG 20 裝置，請執行下列步驟：

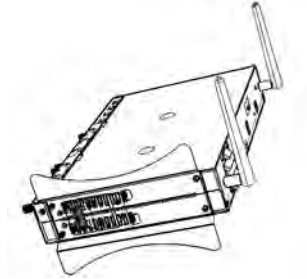
圖 8: SSG 20 牆上安裝



1. 使牆上安裝耳與裝置對齊。
2. 將螺絲置於孔中，然後使用十字螺絲起子來鎖緊它們。
3. 確定要安裝的牆面滑順、平坦、乾燥及結實。
4. 利用所提供的螺絲，在牆上安裝裝置。
5. 將電源供應器插入電源插座。

若要桌上安裝 SSG 20 裝置，請執行下列步驟：

圖 9: SSG 20 桌上安裝



1. 將桌上支架連接到裝置的一側。我們建議使用最接近電源轉接器的那一側。
2. 將已安裝的裝置放在桌上。
3. 插入電源轉接器，然後將電源供應器連接到電源插座。

將介面纜線連接到裝置

若要將介面纜線連接到裝置，請執行下列步驟：

1. 準備好介面所使用之纜線類型的長度。
2. 將纜線連接器插入介面面板上的纜線連接器連接埠。
3. 依如下方式排列纜線，以防止它移動或遭受壓力：
 - a. 固定住纜線，以便它垂下到地板時不會承受自身的重量。
 - b. 將任何多餘的纜線整齊地捲成圈收好。
 - c. 使用固定器來維持纜線圓圈的形狀。

連接電源

若要將電源連接到裝置，請執行下列步驟：

1. 將電源線的 DC 連接器端插入設備背面的 DC 電源插座。
2. 將電源線的 AC 轉接器端插入 AC 電源。



警告：我們建議將電湧保護器用於電源連接。

將裝置連接到網路

當 SSG 20 裝置放在內部網路與不信任的網路之間時，它會對網路提供防火牆及一般安全性。本節介紹下列內容：

- 將裝置連接到不信任的網路
- 將裝置連接到內部網路或工作站

將裝置連接到不信任的網路

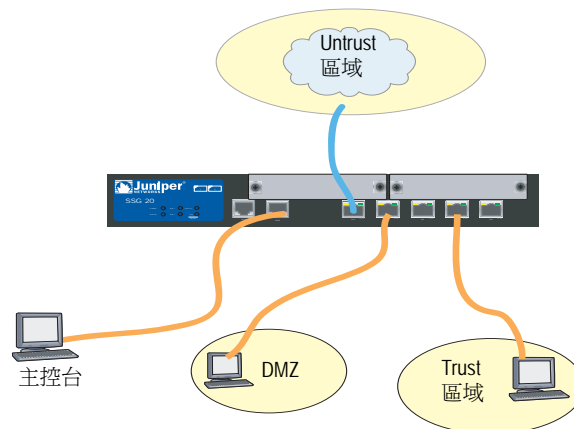
您可以利用以下任何一種方法，將 SSG 20 裝置連接到不信任的網路：

- 乙太網路連接埠
- 序列 (AUX/ 主控台) 連接埠
- 將迷你 PIM 連接到不信任的網路

圖 10 顯示 SSG 20，其基本網路佈線連接具有兩個空白迷你 PIM 及 10/100 乙太網路連接埠，佈線如下所示：

- 標示為 0/0 (ethernet0/0 介面) 的連接埠連接到不信任的網路。
- 標示為 0/1 (ethernet0/1 介面) 的連接埠連接到 DMZ 安全區中的工作站。
- 標示為 0/3 (bgroup0 介面) 的連接埠連接到 Trust 安全區中的工作站。
- 「主控台」連接埠連接到序列終端機以管理存取。

圖 10: 基本網路範例



乙太網路連接埠

若要建立高速連接，請將所提供的乙太網路纜線從 SSG 20 裝置上標示為 0/0 的乙太網路連接埠連接到外部路由器。裝置會自動感應正確的速度、雙工及 MDI/MDIX 設定。

序列 (AUX/ 主控台) 連接埠

您可以利用 RJ-45 直通序列纜線及外部數據機，連接到不信任的網路。



警告：確定您未不慎地將裝置上的主控台、AUX 或乙太網路連接埠連接到電話插座。

將迷你 PIM 連接到不信任的網路

本節將介紹如何將裝置迷你 PIM 連接到不信任的網路。

ADSL2/2+ 迷你 PIM

將所提供的 ADSL 纜線從 ADSL2/2+ 迷你 PIM 連接到電話插座。裝置的附件 A 版本上的 ADSL 連接埠使用 RJ-11 連接器，而附件 B 版本則使用 RJ-45 連接器。在附件 B 機型的情況下，您從 ADSL 連接埠連接到電話插座的纜線在外觀上與直通 10 Base-T 乙太網路纜線相同，而且與其相連。

連接分離器與微濾波器

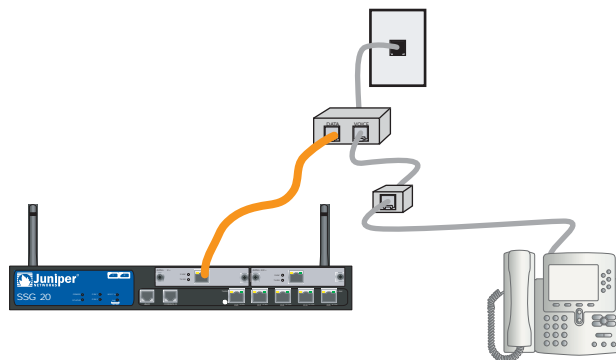
訊號分離器會將電話訊號分成低頻的語音訊號以進行語音呼叫，及高頻的資料訊號進行資料傳送。您的服務供應商通常會將分離器安裝成設備的一部份，將您站台的電話線連接到供應商網路。

也有可供您自行安裝的分離器，視您的服務供應商設備而定。如果您是自行安裝這類分離器，請將 ADSL 纜線從裝置及電話線連接到分離器上的適當連接器（例如，「資料」或「語音」）。將分離器的另一端連接到電話插座。

您可能需要在每一個連接到 ADSL 線的電話、傳真機、答錄機或類比數據機上安裝微濾波器。微濾波器會篩選電話線上的高頻噪音。您可以在電話、傳真機、答錄機或類比數據機與分離器上的語音連接器之間的電話線上安裝微濾波器。

圖 11 顯示在您的站台上安裝的微濾波器及分離器的範例。（您必須從服務供應商處取得適當的微濾波器或分離器。）

圖 11: 您的網路連接上的微濾波器及分離器



ISDN、T1、E1 及 V.92 迷你 PIM

若要將迷你 PIM 連接到裝置，請執行下列步驟：

1. 準備好介面所使用之纜線類型的長度。
2. 將纜線連接器插入介面面板上的纜線連接器連接埠。
3. 依如下方式排列纜線，以防止它移動或遭受壓力：
 - a. 固定住纜線，以便它垂下到地板時不會承受自身的重量。
 - b. 將任何多餘的纜線整齊地捲成圈收好。
 - c. 使用固定器來維持纜線圓圈的形狀。

若要組態 ISDN、E1、T1 或 V.92 迷你 PIM，請參閱第 37 頁上的「迷你 PIM 組態」。

將裝置連接到內部網路或工作站

您可以利用乙太網路及 / 或無線介面，連接區域網路 (LAN) 或工作站。

乙太網路連接埠

SSG 20 裝置包含五個乙太網路連接埠。您可以使用其中一個或多個連接埠，透過交換機或集線器來連接到 LAN。也可以直接將一個或所有的連接埠連接到工作站，排除集線器或切換機的需求。您可以使用交叉電纜或直通電纜，將乙太網路連接埠連接到其他裝置。請參閱第 28 頁上的「預設裝置設定」，以取得預設區域到介面繫結的相關資訊。

無線天線

如果您是使用無線介面，您需要連接裝置上所提供的天線。如果您有標準 2dB 分集天線，請使用螺絲將它們連接到裝置背面標示為 A 及 B 的柱子。使每一個天線在其彎頭處轉彎，如此可確定不會對隔板連接器加壓。

圖 12: SSG 20-WLAN 天線位置



如果您是使用選購的外部天線，請遵循天線所附的连接指示。

第 3 章

組態裝置

ScreenOS 軟體會預先安裝在 SSG 20 裝置上。當開啓裝置電源時，它已準備好進行組態。裝置具有預設出廠組態，可讓您最初連接到裝置，您需要針對特定的網路需求執行進一步的組態。

本章包括下列各節：

- 第 26 頁上的「存取裝置」
- 第 28 頁上的「預設裝置設定」
- 第 30 頁上的「基本裝置組態」
- 第 34 頁上的「基本無線組態」
- 第 37 頁上的「迷你 PIM 組態」
- 第 44 頁上的「基本防火牆保護」
- 第 44 頁上的「驗證外部連接性」
- 第 45 頁上的「將裝置重設為出廠預設設定」

注意： 在組態裝置並透過遠端網路來驗證連接之後，您必須在 www.juniper.net/support/ 註冊您的產品，以便可以在裝置上啓動某些 ScreenOS 服務，例如深入檢查簽名服務及防病毒（另外購買）。在註冊完產品之後，請使用 WebUI 獲得對服務的訂閱。如需註冊您的產品及取得特定服務之訂閱的相關資訊，請參閱「*概念與範例/ScreenOS 參考指南*」（適用於裝置上執行的 ScreenOS 版本）的「*基本原理*」一卷。

存取裝置

您可以利用數種方法來組態和管理裝置：

- 主控台：裝置上的「主控台」連接埠用於透過連接到工作站或終端機的序列電纜來存取裝置。若要組態裝置，請在終端機或工作站上的終端模擬程式中輸入 ScreenOS 指令行介面 (CLI) 指令。
- WebUI: 「ScreenOS Web 使用者介面」(WebUI) 是一種可透過瀏覽器使用的圖形式介面。若要開始使用 WebUI，您執行瀏覽器的工作站必須與裝置位於同一個子網路上。您也可以使用「安全通訊端階層」(SSL) 與安全 HTTP (S-HTTP) 搭配，透過安全伺服器來存取 WebUI。
- Telnet/SSH: Telnet 及 SSH 是可讓您透過 IP 網路存取裝置的應用程式。若要組態裝置，您可以從工作站在 Telnet 會話中輸入 ScreenOS CLI 指令。如需詳細資訊，請參閱「[概念與範例/ScreenOS 參考指南](#)」的「[管理](#)」一卷。
- NetScreen-Security Manager: NetScreen-Security Manager 是 Juniper Networks 企業級管理應用程式，可讓您控制及管理 Juniper Networks 防火牆 /IPSec VPN 裝置。如需如何利用 NetScreen-Security Manager 管理裝置的說明，請參閱 *NetScreen-Security Manager Administrator's Guide*。

使用主控台連接

注意： 使用帶有公 RJ-45 連接器的直通 RJ-45 CAT5 序列纜線，插入裝置上的「主控台」連接埠。

若要建立主控台連接，請執行下列步驟：

1. 將所提供的 DB-9 配接卡的母端插入工作站的序列連接埠。(確定 DB-9 已適當地插入並固定住。)圖 13 顯示所需的 DB-9 連接器類型。

圖 13: DB-9 配接卡



2. 將 RJ-45 CAT5 序列纜線的公端插入 SSG 20 上的「主控台」連接埠。(確定 CAT5 纜線的另一端已適當地插入並固定在 DB-9 配接卡)。

3. 在工作站上啟動序列終端模擬程式。啟動主控台會話所需的設定如下：
 - 序列傳輸速率：9600
 - 同位元：無
 - 資料位元：8
 - 停止位元：1
 - 流量控制：無
4. 如果您尚未變更管理名稱及密碼的預設登入，請在登入及密碼提示中同時輸入 **netscreen**。（僅使用小寫字母。登入和密碼欄位都會區分大小寫。）
如需如何利用 CLI 指令來組態裝置的相關資訊，請參閱「[概念與範例 ScreenOS 參考指南](#)」。
5. （選擇性）依預設，主控台會在閒置 10 分鐘之後逾時並自動終止。若要移除逾時，請輸入 **set console timeout 0**。

使用 WebUI

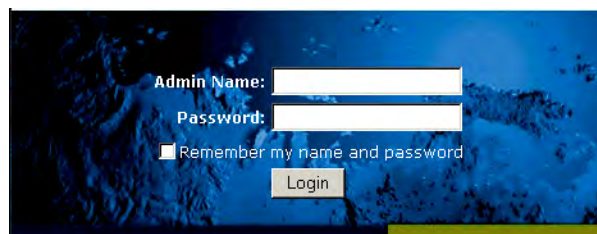
若要使用 WebUI，您從中管理裝置的工作站最初必須與裝置位於同一個子網路上。若要利用 WebUI 存取裝置，請執行下列步驟：

1. 將工作站連接到裝置上的 0/2 - 0/4 連接埠 (Trust 區域中的 bgroup0 介面)。
2. 確定工作站是針對「動態主機組態通訊」(DHCP) 而組態的，或利用 192.168.1.0/24 子網路中的 IP 位址，以靜態方式組態的。
3. 啟動瀏覽器、輸入 bgroup0 介面的 IP 位址（預設 IP 位址為 192.168.1.1/24），然後按 **Enter**。

注意： 第一次透過 WebUI 存取裝置時，初始組態精靈 (ICW) 就會出現。如果決定要使用 ICW 來組態裝置，請參閱第 59 頁上的「初始組態精靈」。

WebUI 應用程式會顯示登入提示，如圖 14 中所示。

圖 14: WebUI 登入提示



4. 如果您尚未變更管理名稱及密碼的預設登入，請在管理名稱及密碼提示中同時輸入 **netscreen**。（僅使用小寫字母。登入和密碼欄位都會區分大小寫。）

使用 Telnet

若要建立 Telnet 連接，請執行下列步驟：

1. 將工作站連接到裝置上的 0/2 - 0/4 連接埠 (Trust 區域中的 bgroup0 介面)。
2. 確定工作站是針對 DHCP 而組態的，或利用 192.168.1.0/24 子網路中的 IP 位址，以靜態方式組態的。
3. 將 Telnet 用戶端應用程式啟動到 bgroup0 介面的 IP 位址 (預設 IP 位址為 192.168.1.1)。

Telnet 應用程式會顯示登入提示。

4. 如果您尚未變更登入及密碼的預設登入，請在登入及密碼提示中同時輸入 **netscreen**。(僅使用小寫字母。登入和密碼欄位都會區分大小寫。)
5. (選擇性) 依預設，主控台會在閒置 10 分鐘之後逾時並自動終止。若要移除逾時，請輸入 **set console timeout 0**。

預設裝置設定

本節介紹 SSG 20 裝置的預設設定及操作。

表 5 顯示裝置上連接埠的預設區域繫結。

表 5: 預設實體介面到區域繫結

連接埠標籤	介面	區域
10/100 乙太網路連接埠：		
0/0	ethernet0/0	Untrust
0/1	ethernet0/1	DMZ
0/2	bgroup0 (ethernet0/2)	Trust
0/3	bgroup0 (ethernet0/3)	Trust
0/4	bgroup0 (ethernet0/4)	Trust
AUX	serial0/0	Null
WAN 迷你 PIM 連接埠 (x = 迷你 PIM 插槽 1 或 2):		
ADSL2/2 + (附件 A)	adsl(x/0)	Untrust
ADSL2/2 + (附件 B)	adsl(x/0)	Untrust
T1	serial(x/0)	Untrust
E1	serial(x/0)	Untrust
ISDN	bri(x/0)	Untrust
V.92	serial(x/0)	Null

橋接群組 (bgroup) 是設計來允許網路使用者不需重新組態或重新啟動裝置，便可在有線及無線流量之間切換。依預設，ethernet0/2 - ethernet0/4 介面 (裝置上標示為 0/2 - 0/4 的連接埠) 會一起群組成 bgroup0 介面，IP 位址為 192.168.1.1/24，並且會繫結到 Trust 安全區。您最多可以組態四個 bgroup。

如果您想要將乙太網路或無線介面設定為 bgroup，首先您必須確定乙太網路或無線介面位於 Null 安全區中。取消設定位於 bgroup 的乙太網路或無線介面會將介面置於 Null 安全區。一旦指派給 Null 安全區，乙太網路介面便可以繫結到安全區並指派其他 IP 位址。

若要從 bgroup0 取消設定 ethernet0/3，並將它指派給靜態 IP 位址為 192.168.3.1/24 的 Trust 區域，請使用 WebUI 或 CLI，如下所示：

WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port: 取消選擇 **ethernet0/3**，然後按一下 **Apply**。

List > Edit (ethernet0/3): 輸入下面的內容，然後按一下 **Apply**:

Zone Name: Trust (選擇)
IP Address/Netmask: 192.168.3.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
set interface ethernet0/3 zone trust
set interface ethernet0/3 ip 192.168.3.1/24
save
```

表 6: 無線及邏輯介面繫結

SSG 20-WLAN	介面	區域
無線介面 指定可以組態為以 2.4 G 及 / 或 5 G 無線電運作的無線介面	wireless0/0 (預設 IP 位址為 192.168.2.1/24)。	Trust
	wireless0/1-0/3。	Null
邏輯介面		
第 2 層介面	vlan1 指定當裝置處於「透通」模式時用於管理及終止 VPN 通訊流量的邏輯介面。	N/A
通道介面	tunnel.n 指定邏輯通道介面。此介面用於 VPN 通訊流量。	N/A

您可以變更 bgroup0 介面上的預設 IP 位址，以符合 LAN 與 WLAN 上的位址。如需有關組態 bgroup 的無線介面的相關資訊，請參閱第 34 頁上的「基本無線組態」。

注意： 當 bgroup 介面包含無線介面時，它無法在「透通」模式中運作。

如需其他 bgroup 資訊及範例，請參閱「[概念與範例 ScreenOS 參考指南](#)」。

在裝置上的其他乙太網路或無線介面上未組態任何其他預設 IP 位址；您需要指派 IP 位址給其他介面，包括 WAN 介面。

基本裝置組態

本節說明下列基本組態設定：

- 根管理名稱及密碼
- 日期與時間
- 橋接群組介面
- 管理式存取
- 管理服務
- 主機名稱及網域名稱
- 預設路由
- 管理介面位址
- 備份 Untrust 介面組態

根管理名稱及密碼

根管理使用者具有組態 SSG 20 裝置的完整權限。我們建議您立即變更預設根管理名稱及密碼（兩者皆為 **netscreen**）。

若要變更根管理名稱及密碼，請使用 WebUI 或 CLI，如下所示：

WebUI

Configuration > Admin > Administrators > Edit (針對 netscreen 管理員名稱值): 輸入以下內容，然後按一下 **OK**:

Administrator Name:
Old Password: netscreen
New Password:
Confirm New Password:

注意： 密碼不會顯示在 WebUI 中。

CLI

```
set admin name 名稱
set admin password 密碼字串
save
```

日期與時間

SSG 20 裝置上設定的時間會影響如設定 VPN 通道之類的事件。在裝置上設定日期及時間的最簡單方式，就是使用 WebUI 將裝置系統時鐘與工作站時鐘同步。

若要組態裝置上的日期與時間，請使用 WebUI 或 CLI，如下所示：

WebUI

1. Configuration > Date/Time: 按一下 Sync Clock with Client 按鈕。

彈出的訊息會提示您指定是否已在工作站時鐘上啓用了夏令時間選項。

2. 按一下 **Yes** 以同步化系統時鐘並根據夏令時間調整，或是按 **No** 以同步化系統時鐘而不根據夏令時間調整。

您也可以在 Telnet 或「主控台」會話中使用 **set clock** CLI 指令來手動輸入裝置的日期及時間。

橋接群組介面

依預設，SSG 20 裝置的乙太網路介面 ethernet0/2 - ethernet0/4 會在 Trust 安全區中群組在一起。群組介面可設定某個子網路的介面。您可以從群組取消設定介面，然後將它指派給不同的安全區。介面必須位於 Null 安全區，然後才能指派給群組。若要將群組的介面置於 Null 安全區，請使用 **unset interface 介面 port 介面** CLI 指令。

SSG 20-WLAN 裝置可讓乙太網路與無線介面群組在某個子網路之下。

注意： 只有無線及乙太網路介面才能在 bgroup 中設定。

若要利用乙太網路及無線介面來組態群組，請使用 WebUI 或 CLI，如下所示：

WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port: 取消選擇 **ethernet0/3** 及 **ethernet0/4**，然後按一下 **Apply**。

Edit (bgroup1) > Bind Port: 選擇 **ethernet0/3**、**ethernet0/4** 及 **wireless0/2**，然後按一下 **Apply**。

> 基本：輸入下面的內容，然後按一下 **Apply**：

Zone Name: DMZ (選擇)
IP Address/Netmask: 10.0.0.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
unset interface bgroup0 port ethernet0/4
set interface bgroup1 port ethernet0/3
set interface bgroup1 port ethernet0/4
set interface bgroup1 port wireless0/2
set interface bgroup1 zone DMZ
set interface bgroup1 ip 10.0.0.1/24
save
```


管理式存取

依預設，如果知道登入和密碼，網路中的任何使用者都可以管理裝置。

若要將裝置組態為只能從您網路上特定主機進行管理，請使用 WebUI 或 CLI，如下所示：

WebUI

Configuration > Admin > Permitted IPs: 輸入下面的內容，然後按一下 **Add**:

IP Address/Netmask: *ip 位址 / 遮罩*

CLI

```
set admin manager-ip ip 位址 / 遮罩
save
```

管理服務

ScreenOS 提供用於組態及管理裝置的服務，例如 SNMP、SSL 及 SSH，您可以個別介面為基礎來啟用這些服務。

若要組態裝置上的管理服務，請使用 WebUI 或 CLI，如下所示：

WebUI

Network > Interfaces > List > Edit (針對 ethernet0/0): 在 **Management Services** 下，選擇或取消選擇您要在介面上使用的管理服務，然後按一下 **Apply**。

CLI

```
set interface ethernet0/0 manage web
unset interface ethernet0/0 manage snmp
save
```

主機名稱及網域名稱

網域名稱定義裝置所屬的網路或子網路，而主機名稱則代表特定裝置。主機名稱及網域名稱合起來可唯一識別網路中的裝置。

若要組態裝置上的主機名稱及網域名稱，請使用 WebUI 或 CLI，如下所示：

WebUI

Network > DNS > Host: 輸入下面的內容，然後按一下 **Apply**:

Host Name: *名稱*
Domain Name: *名稱*

CLI

```
set hostname 名稱
set domain 名稱
save
```

預設路由

預設路由是一種靜態路由，用來引導定址到未在路由設定表中明確列出之網路的封包。如果封包抵達之裝置不具有該裝置路由設定資訊的位址，則裝置會將封包傳送到預設路由指定的目的地。

若要組態裝置上的預設路由，請使用 WebUI 或 CLI，如下所示：

WebUI

Network > Routing > Destination > New (trust-vr): 輸入以下內容，然後按一下 OK:

IP Address/Netmask: 0.0.0.0/0.0.0.0
 Next Hop
 Gateway: (選擇)
 Interface: ethernet0/2 (選擇)
 Gateway IP Address: ip 位址

CLI

```
set route 0.0.0.0/0 interface ethernet0/2 gateway ip 位址
save
```

管理介面位址

Trust 介面具有預設 IP 位址 192.168.1.1/24，而且是針對管理服務而組態的。如果將裝置上的 0/2 - 0/4 連接埠連接到工作站，您可以使用如 Telnet 的管理服務，從 192.168.1.1/24 子網路中的工作站組態裝置。

您可以變更 Trust 介面上的預設 IP 位址。例如，您可能想要變更介面，以符合已存在於 LAN 上的 IP 位址。

備份 Untrust 介面組態

SSG 20 device 可讓您組態不信任故障後移轉的備份介面。若要設定不信任故障後移轉的備份介面，請執行下列步驟：

1. 利用 **unset interface 介面 [port 介面]** CLI 指令，在 Null 安全區中設定備份介面。
2. 利用 **set interface 介面 zone 區域名稱** CLI 指令，將備份介面繫結到與主要介面相同的安全區。

注意： 主要與備份介面必須位於相同的安全區。一個主要介面只能有一個備份介面，而一個備份介面也只能有一個主要介面。

若要將 ethernet0/4 介面設定為 ethernet0/0 介面的備份介面，請使用 WebUI 或 CLI，如下所示：

WebUI

Network > Interfaces > Backup > 請輸入下列的內容，然後按一下 **Apply**。

Primary: ethernet0/0
Backup: ethernet0/4
Type: track-ip (選擇)

CLI

```
unset interface bgroup0 port ethernet0/4
set interface ethernet0/4 zone untrust
set interface ethernet0/0 backup interface ethernet0/4 type track-ip
save
```

基本無線組態

本節提供在 SSG 20-WLAN 裝置上組態無線介面的資訊。無線網路由所稱的「服務集識別碼」(SSID) 組成。指定 SSID 可讓您具有多個位於相同位址且彼此不會干擾的無線網路。SSID 名稱最多可有 32 個字元。如果 SSID 名稱字串包含空格，則字串必須以引號括住。一旦設定了 SSID 名稱，便可組態更多的 SSID 屬性。若要在裝置上使用無線區域網路 (WLAN) 功能，您必須至少組態一個 SSID，然後將它繫結到無線介面。

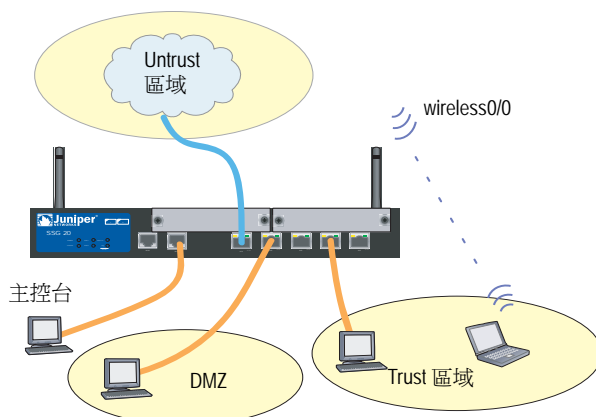
SSG 20-WLAN 裝置可讓您最多建立 16 個 SSID，但是只能同時使用其中 4 個。您可以組態裝置，從而使任意一個收發機使用 4 個 SSID，或分開在兩個收發機上使用（例如，3 個 SSID 指派給 WLAN 0，而 1 個 SSID 指派給 WLAN 1）。使用 **set interface 無線介面 wlan {0 | 1 | both}** CLI 指令，在 SSG 20-WLAN 裝置上設定無線電收發機。

一旦您對 wireless0/0 介面設定了 SSID，您可以利用第 26 頁上的「存取裝置」中說明的步驟使用預設 wireless0/0 介面 IP 位址存取裝置。圖 15 顯示了 SSG 20-WLAN 裝置的預設組態。

注意： 如果是在美國、日本、加拿大、中國大陸、台灣地區、韓國、以色列或新加坡以外的國家操作 SSG 20-WLAN 裝置，則您必須使用 **set wlan country-code** CLI 指令，或在 Wireless > General Settings WebUI 頁面上設定它，然後才能建立 WLAN 連接。此指令會設定可選擇的通道範圍及傳輸電源層級。

如果您的地區碼為 ETSI，則您必須設定正確的國碼以符合當地的無線電頻譜規定。

圖 15: 預設 SSG 20-WLAN 組態



依預設，wireless0/0 介面是利用 IP 位址 192.168.2.1/24 來組態。所有需要連接到 Trust 區域的無線用戶端都必須具有該無線子網路中的 IP 位址。您也可以組態裝置，使用 DHCP 將 192.168.2.1/24 子網路中的 IP 位址自動指派給裝置。

依預設，wireless0/1 - wireless0/3 介面會定義為 Null，而且不會指派 IP 位址給它們。如果想要使用任何其他的無線介面，您必須為它組態 IP 位址、指派 SSID，然後將它繫結到安全區。表 7 顯示了無線驗證及加密方法。

表 7: 無線驗證和加密選項

驗證	加密
Open	允許任何無線用戶端存取裝置
Shared-key	WEP 共享金鑰
WPA-PSK	AES/TKIP (具有預先共享的金鑰)
WPA	AES/TKIP (具有來自 RADIUS 伺服器的金鑰)
WPA2-PSK	802.11i (符合預先共享的金鑰)
WPA2	802.11i (符合 RADIUS 伺服器)
WPA-Auto-PSK	允許具有預先共享之金鑰的 WPA 及 WPA2 類型
WPA-Auto	允許具有 RADIUS 伺服器的 WPA 及 WPA2 類型
802.1x	WEP (具有來自 RADIUS 伺服器的金鑰)

請參閱「[概念與範例 ScreenOS 參考指南](#)」，以取得與無線安全性組態相關的組態範例、SSID 屬性及 CLI 指令。

若要組態基本連接的無線介面，請使用 WebUI 或 CLI，如下所示：

WebUI

1. 設定 WLAN 國碼及 IP 位址。

Wireless > General Settings > 選擇以下內容，然後按一下 **Apply**：

Country code: 選擇您的國碼
IP Address/Netmask: *ip 位址 / 網絡遮罩*

2. 設定 SSID。

Wireless > SSID > New: 輸入以下內容，然後按一下 **OK**：

SSID:
Authentication:
Encryption:
Wireless Interface Binding:

3. (選擇性) 設定 WEP 金鑰。

SSID > WEP Keys: 選擇 KeyID，然後按一下 **Apply**。

4. 設定 WLAN 模式。

Network > Interfaces > List > Edit (無線介面): 選擇 **Both** 作為 WLAN 模式，然後按一下 **Apply**。

5. 啟動無線變更。

Wireless > General Settings > 按一下 **Activate Changes**。

CLI

1. 設定 WLAN 國碼及 IP 位址。

```
set wlan country-code {code_id}
set interface 無線介面 ip ip 位址 / 網絡遮罩
```

2. 設定 SSID。

```
set ssid name 名稱字串
set ssid 名稱字串 authentication 驗證類型 encryption 加密類型
set ssid 名稱字串 interface 介面
(選擇性) set ssid 名稱字串 key-id 編號
```

3. 設定 WLAN 模式。

```
set interface 無線介面 wlan both
```

4. 啟動無線變更。

```
save
exec wlan reactivate
```

您可以設定一個 SSID，以便在與有線子網路相同的子網路中進行操作。此動作允許用戶端在任一介面中運作，不需在另一個子網路中重新連接。

若要將乙太網路及無線介面設定為相同的橋接群組介面，請使用 WebUI 或 CLI，如下所示：

WebUI

Network > Interfaces > List > Edit (橋接群組名稱) > Bind Port: 選擇無線及乙太網路介面，然後按一下 **Apply**。

CLI

```
set interface 橋接群組名稱 port 無線介面
set interface 橋接群組名稱 port 乙太網路介面
```

注意： 橋接群組名稱可以是 bgroup0-bgroup3。

乙太網路介面可以是 ethernet0/0-ethernet0/4。

無線介面可以是 wireless0/0-wireless0/3。

如果組態了無線介面，則您需要利用 **exec wlan reactivate** CLI 指令，或在 Wireless > General Settings WebUI 頁面上按一下 **Activate Changes** 來重新啟動 WLAN。

迷你 PIM 組態

本節說明如何組態迷你實體介面模組 (PIM)：

- ADSL2/2+ 介面
- ISDN 介面
- T1 介面
- E1 介面
- V.92 數據機介面

ADSL2/2+ 介面

您的網路會在裝置上使用 ADSL2/2+ 介面 **adslx/0** (其中 x 代表迷你 PIM 插槽 (1 或 2))，透過「非同步傳送模式」(ATM) 虛擬電路連接到服務供應商的網路。您可以透過建立 ADSL2/2+ 子介面來組態其他虛擬電路。如需詳細資訊，請參閱第 38 頁上的「虛擬電路」。

在 WebUI 中，瀏覽到 Network > Interfaces > List 頁面，以查看裝置上目前介面的清單。如果您是使用 Telnet 或「主控台」會話，請輸入 **get interface** CLI 指令。您應該看到 adslx/0 介面已繫結到 Untrust 區域。

如果是使用 ADSL2/2+ 介面連接到供應商的服務網路，您必須組態 adsl(x/0) 介面。要這樣做，您必須向服務供應商取得下列資訊：

- 「虛擬路徑識別碼及虛擬通道識別碼 (VPI/VCI) 值

- ATM Adaptation Layer 5 (AAL5) 多工法可以是下列其中一個：
 - 以虛擬電路為基礎的多工法，其中每一個通訊協定均由個別的 ATM 虛擬電路支援。
 - 「邏輯連結控制」(LLC) 封裝，其可在同一 ATM 虛擬電路上支援數個通訊協定（預設的多工法）
- 服務供應商指派的使用者名稱及密碼，用於透過「乙太網路上的點對點通訊協定」(PPPoE) 或「ATM 上的點對點通訊協定」(PPPoA) 連接到服務供應商的網路
- 針對 PPPoE 或 PPPoA 連接提供的驗證方法，如果有的話
- 您網路的靜態 IP 位址及網路遮罩值（選擇性）

虛擬電路

若要新增虛擬電路，您可以建立 ADSL2/2+ 介面的子介面。您最多可以建立 10 個 ADSL2/2+ 子介面。例如，若要建立名為 **adsl1/0.1** 的新子介面（繫結到預先定義的名為 **Untrust** 的區域），請使用 WebUI 或 CLI，如下所示：

WebUI

Network > Interfaces > List > New ADSL Sub-IF: 輸入下面的內容，然後按一下 **Apply**:

Interface Name: adsl1/0.1
VPI/VCI: 0/35
Zone Name: Untrust (選擇)

CLI

```
set interface adsl 1/0.1 pvc 0 35 zone Untrust
save
```

您需要依第 37 頁上的「ADSL2/2+ 介面」所述，利用與組態主要 ADSL2/2+ 介面相同的方式，來組態 ADSL 2/2+ 子介面，包括設定 VPI/VCI 值。您可以組態與主要 ADSL2/2+ 介面無關的 ADSL2/2+ 子介面；亦即，您可以在子介面上組態與主要 ADSL2/2+ 介面不同的多工法、VPI/VCI 及 PPP 用戶端。即使主要 ADSL2/2+ 介面沒有靜態 IP 位址，您也可以在此子介面上組態靜態 IP 位址。

VPI/VCI 及多工法

您的服務供應商會為每一個虛擬電路連接指派一個 VPI/VCI 配對。例如，您收到的 VPI/VCI 配對可能是 1/32，表示 VPI 值為 1，而 VCI 值為 32。這些值必須符合服務供應商在「數位用戶線路接取多工器」(DSLAM) 的用戶端上組態的值。

若要在 adsl1/0 介面上組態 VPI/VCI 配對 1/32，請使用 WebUI 或 CLI，如下所示：

WebUI

Network > Interfaces > List > Edit (針對 adsl1/0 介面): 在 VPI/VCI 欄位中輸入 **1/32**，然後按一下 **Apply**。

CLI

```
set interface adsl1/0 pvc 1 32
save
```

依預設，裝置會對每一個虛擬電路使用基於「邏輯連結控制」(LLC) 的多工法。

若要在 adslx/0 介面上組態 VPI/VCI 配對 1/32，並在虛擬電路上使用 LLC 封裝，請使用 WebUI 或 CLI，如下所示：

WebUI

Network > Interfaces > List > Edit (針對 adsl1/0 介面): 輸入下面的內容，然後按一下 **Apply**:

VPI/VCI: 1 / 32
Multiplexing Method: LLC (選擇)

CLI

```
set interface adsl1/0 pvc 1 32 mux llc
save
```

PPPoE 或 PPPoA

SSG 20 裝置同時包括 PPPoE 及 PPPoA 用戶端，可以透過 ADSL 連結連接到服務供應商網路。PPPoE 是 ADSL 封裝的最常用形式，而且主要用於終止您網路上的每一個主機。PPPoA 主要用於商業類別服務，因為可在裝置上終止 PPP 會話。若要允許裝置連接到服務供應商的網路，您需要組態服務供應商所指派的使用者名稱及密碼。PPPoA 的組態類似於 PPPoE 的組態。

注意： 在每一個虛擬電路上，裝置只支援一個 PPPoE 會話。

若要對 PPPoE 組態使用者名稱 **roswell** 及密碼 **area51**，並將 PPPoE 組態繫結到 adsl1/0 介面，請使用 WebUI 或 CLI，如下所示：

WebUI

Network > PPP > PPPoE Profile > New: 輸入以下內容，然後按一下 **OK**:

PPPoE Instance: poe1
Bound to Interface: adsl1/0 (選擇)
Username: roswell
Password: area51

CLI

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1/0
save
```

您還可以在裝置上組態其他 PPPoE 或 PPPoA 參數，包括驗證方法（依預設，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。詢問您的服務供應商，是否需要組態其他的 PPPoE 或 PPPoA 參數，才能與服務供應商的伺服器正確通訊。

靜態 IP 位址及網路遮罩

如果您的服務給您網路指派了固定的特定 IP 位址及網路遮罩，請組態網路的 IP 位址及網路遮罩，以及連接到裝置的路由器連接埠的 IP 位址。您也需要指定裝置將使用靜態 IP 位址。（通常，裝置會充當 PPPoE 或 PPPoA 用戶端，並透過與 PPPoE 或 PPPoA 伺服器交涉，接收 ADSL 介面的 IP 位址。）

您需要依第 39 頁上的「PPPoE 或 PPPoA」所述來組態 PPPoE 或 PPPoA 實例，並將它繫結到 adsl1/0 介面。確定您選擇 **Obtain IP using PPPoE** 或 **Obtain IP using PPPoA**，以及 PPPoE 或 PPPoA 實例的名稱。

若要組態網路的靜態 IP 位址 1.1.1.1/24，請使用 WebUI 或 CLI，如下所示：

WebUI

Network > Interfaces > List > Edit (針對 adsl1/0 介面): 輸入下面的內容，然後按一下 **Apply**:

IP Address/Netmask: 1.1.1.1/24
Static IP: (選擇)

CLI

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

或者

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoa name poa1 static-ip
save
```

若要使用「網域名稱系統」(DNS) 進行網域名稱及位址解析，您網路中的電腦需要至少具有一個 DNS 伺服器的 IP 位址。如果裝置透過 PPPoE 或 PPPoA 接收 ADSL2/2+ 介面的 IP 位址，則它也會自動接收 DNS 伺服器的 IP 位址。如果您網路中的電腦從裝置上的 DHCP 伺服器取得其 IP 位址，則電腦也會取得這些 DNS 伺服器位址。

如果您指派靜態 IP 位址給 ADSL2/2+ 介面，則服務供應商必須提供給您 DNS 伺服器的 IP 位址。您可以在您網路中的每一部電腦上組態 DNS 伺服器位址，或您可以在 Trust 區域介面上組態 DHCP 伺服器，這樣它就會提供 DNS 伺服器位址給每一部電腦。

若要在 bgroup0 介面上組態 DHCP 伺服器，以提供 DNS 伺服器位址 1.1.1.152 給您網路中的電腦，請使用 WebUI 或 CLI，如下所示：

WebUI

Network > DHCP > Edit (針對 bgroup0 介面) > DHCP Server: 為 DNS1 輸入 1.1.1.152，然後按一下 **Apply**。

CLI

```
set interface bgroup0 dhcp server option dns1 1.1.1.152
save
```

如需組態 ADSL 及 ADSL2/2+ 介面的相關資訊，請參閱「*概念與範例 ScreenOS 參考指南*」。

ISDN 介面

「整合服務數位網路」(ISDN) 是由「國際電報電話諮詢委員會」(CCITT) 及「國際電信聯盟」(ITU) 建立的在不同媒體間進行數位傳輸的一組標準。作為隨選撥接服務，它具有快速呼叫設定及低延遲的特點，並且能夠支援高品質語音、資料及視訊傳輸。ISDN 也是電路交換服務，可以用於多點及點對點連接。ISDN 提供具有多連結「點對點通訊協定」(PPP) 連接的服務路由器給網路介面。ISDN 介面通常會組態為乙太網路介面的備份介面，以存取外部網路。

若要組態 ISDN 介面，請使用 WebUI 或 CLI，如下所示：

WebUI

Network > Interfaces > List > Edit (bri1/0): 輸入或選擇下面的內容，然後按一下 **OK**:

BRI Mode: Dial Using BRI
Primary Number: 123456
WAN Encapsulation: PPP
PPP Profile: isdnprofile

CLI

```
set interface bri1/0 dialer-enable
set interface bri1/0 primary-number "123456"
set interface bri1/0 encaps ppp
set interface bri1/0 ppp profile isdnprofile
save
```

若要將 ISDN 介面組態為備份介面，請參閱第 33 頁上的「備份 Untrust 介面組態」。

如需如何組態 ISDN 介面的相關資訊，請參閱「[概念與範例 ScreenOS 參考指南](#)」。

T1 介面

T1 介面是北美「數位訊號第 1 層」(DS-1) 多工法所使用的基本「實體層」通訊協定。T1 介面以 1.544 Mbps 的位元率運作，或可使用最多 24 DS0 個通道。

裝置支援下列 T1 DS-1 標準：

- ANSI T1.107、T1.102
- GR 499-core、GR 253-core
- AT&T Pub 54014
- ITU G.751、G.703

若要組態 T1 迷你 PIM，請使用 WebUI 或 CLI，如下所示：

WebUI

Network > Interfaces > List > Edit (serial1/0): 輸入或選擇下面的內容，然後按一下 **OK**:

WAN Configure: main link
 WAN Encapsulation: cisco-hdlc
 按一下 **Apply**。
 Fixed IP: (選擇)
 IP Address/Netmask: 172.18.1.1/24

CLI

```
set interface serial1/0 encap cisco-hdlc
set interface serial1/0 ip 172.18.1.1/24
```

如需如何組態 T1 介面的相關資訊，請參閱「[概念與範例 ScreenOS 參考指南](#)」。

E1 介面

E1 介面是標準寬域網路 (WAN) 數位通訊格式，是設計來透過銅製設備以 2.048 Mbps 的速率來運作。E1 是用來支援數位電路的基本分時多工法配置，廣泛地在北美以外的地區使用。

裝置支援下列 E1 標準：

- ITU-T G.703
- ITU-T G.751
- ITU-T G.775

若要組態 E1 迷你 PIM，請使用 WebUI 或 CLI，如下所示：

WebUI

Network > Interfaces > List > Edit (serial1/0): 輸入或選擇下面的內容，然後按一下 **OK**:

WAN Configure: main link
 WAN Encapsulation: PPP
 Binding a PPP Profile: junipertest
 按一下 **Apply**。
 Fixed IP: (選擇)
 IP Address/Netmask: 172.18.1.1/24

CLI

```
set interface serial1/0 encapsulation ppp
set ppp profile "junipertest" static-ip
set ppp profile "junipertest" auth type chap
set ppp profile "junipertest" auth local-name "juniper"
set ppp profile "junipertest" auth secret "password"
set interface serial1/0 ppp profile "junipertest"
set interface serial1/0 ip 172.18.1.1/24
set user "server" type wan
set user "server" password "server"
```

如需如何組態 E1 介面的相關資訊，請參閱「[概念與範例 ScreenOS 參考指南](#)」。

V.92 數據機介面

V.92 介面提供內部類比數據機，用於建立與服務提供者的 PPP 連接。您可以將序列介面組態為在發生介面故障後移轉時使用的主要或備份介面。

注意： V.92 介面不會在「透通」模式中運作。

若要組態 V.92 介面，請使用 WebUI 或 CLI，如下所示：

WebUI

Network > Interfaces > List > Edit (針對 serial1/0): 輸入以下內容，然後按一下 **OK**:

Zone Name: untrust (選擇)

ISP: 輸入以下內容，然後按一下 **OK**:

ISP Name: isp_juniper
Primary Number: 1234567
Login Name: juniper
Login Password: juniper

Modem: 輸入以下內容，然後按一下 **OK**:

Modem Name: mod1
Init String: AT&FS7=255S32=6
Active Modem setting
Inactivity Timeout: 20

CLI

```
set interface serial1/0 zone untrust
set interface serial1/0 modem isp isp_juniper account login juniper password
juniper
set interface serial1/0 modem isp isp_juniper primary-number 1234567
set interface serial1/0 modem idle-time 20
set interface serial1/0 modem settings mod1 init-strings AT&FS7=255S32=6
set interface serial1/0 modem settings mod1 active
```

如需如何組態 V.92 數據機介面的相關資訊，請參閱「[概念與範例 ScreenOS 參考指南](#)」。

基本防火牆保護

裝置是以預設政策來組態的，此政策許可您網路的 Trust 區域中的工作站存取 Untrust 安全區中的任何資源，但不允許外面的電腦利用您的工作站來存取或啟動會話。可以組態政策指導裝置允許外部電腦啟動網路中電腦具有的特定種類的階段作業。如需建立或修改政策的相關資訊，請參閱「[概念與範例 ScreenOS 參考指南](#)」。

SSG 20 裝置提供各種偵測方法及防禦機制，以對抗意圖危及或傷害網路或網路資源的探查及攻擊：

- ScreenOS SCREEN 選項用於保護區域的安全，做法是先檢查要求跨越該區域之介面的所有連接嘗試，然後予以允許或拒絕。例如，您可以在 Untrust 區域應用連接埠掃描保護，阻止來自遠端網路的來源識別作為未來攻擊目標的服務。
- 裝置會將防火牆政策（可以包含內容篩選及「侵入偵測與預防」(IDP) 元件）應用到將 SCREEN 篩選器從某個區域傳遞到另一個區域的流量。依預設，不許可任何流量通過裝置從某個區域傳遞到另一個區域。若要許可流量跨越裝置從某個區域到另一個區域，您必須建立一個政策來覆寫預設行為。

若要設定區域的 ScreenOS SCREEN 選項，請使用 WebUI 或 CLI，如下所示：

WebUI

Screening > Screen: 選擇選項應用的區域。選擇您想要的 SCREEN 選項，然後按一下 **Apply**。

CLI

```
set zone 區域 screen 選項
save
```

如需組態 ScreenOS 中可用之網路安全性選項的相關資訊，請參閱「[概念與範例 ScreenOS 參考指南](#)」。

驗證外部連接性

若要驗證網路中的工作站能否存取網際網路上的資源，請從網路中的任何工作站啟動瀏覽器並輸入以下的 URL: www.juniper.net。

將裝置重設為出廠預設設定

如果遺失了管理密碼，可以將裝置重設為預設設定。這會破壞任何現有的組態，但可復原對裝置的存取。



警告：重設裝置會刪除所有現有的組態設定，並且會停用所有現有的防火牆及 VPN 服務。

可以使用以下方式中的一種復原裝置到預設設定：

- 使用主控台連接。如需進一步資訊，請參閱「[概念與範例/ScreenOS 參考指南](#)」。
- 使用裝置後面板上的重設針孔，如以下一節所述。

按壓重設針孔可以重設裝置並復原出廠預設設定。若要執行此操作，需要檢視前面板上的裝置狀態 LED，或依第 26 頁上的「使用主控台連接」所述來啟動「主控台」會話。

若要使用重設針孔來重設及還原預設設定，請執行下列步驟：

1. 找到後面板上的重設針孔。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。

STATUS LED 閃爍紅色。「主控台」上的訊息聲明已經開始刪除組態，而且系統發出一個 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；裝置現在正等待第二次重設。「主控台」訊息現在聲明裝置正等待第二次確認。

3. 再次推壓重設針孔四至六秒。

「主控台」訊息會驗證第二次重設。STATUS LED 發出紅光半秒，然後返回到閃爍綠色狀態。

然後，裝置重設為原始的出廠設定。當裝置重設時，STATUS LED 會發出紅光半秒，然後發出綠光。主控台會顯示裝置啟動訊息。系統產生 SNMP 和 SYSLOG 警示，發給已組態的 SYSLOG 或 SNMP 回報主機。

在裝置重新啟動之後，主控台會顯示裝置的登入提示。STATUS LED 閃爍綠色。登入及密碼皆是 **netscreen**。

如果不遵循完整的順序，重設過程會取消且不變更任何組態，同時主控台訊息聲明已中止刪除組態。STATUS LED 返回到閃爍綠色狀態。如果裝置沒有重設，則會傳送 SNMP 警示以確認失敗。

第 4 章

維修裝置

本章說明 SSG 20 裝置的維修及維護程序。本章包含下列各節：

- 本頁上的「必要工具及零件」
- 本頁上的「更換迷你實體介面模組」
- 第 50 頁上的「升級記憶體」

注意： 有關安全警告及指示，請參閱 *Juniper Networks Security Products 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，請注意由電路引發的危險以及熟悉標準操作以防止意外事故的發生。

必要工具及零件

若要更換 SSG 20 裝置上的元件，您需要下列工具及零件：

- 靜電袋或防靜電墊
- 消除靜電 (ESD) 的接地腕帶
- 十字螺絲起子 (1/8 吋)

更換迷你實體介面模組

這兩個 SSG 20 機型在前面板中都有兩個插槽，供寬域網路迷你實體介面模組 (WAN 迷你 PIM) 使用。您可以安裝及更換 SSG 20 裝置中的迷你 PIM。必須關閉裝置電源，然後才能移除或安裝迷你 PIM。



小心： 移除迷你 PIM 時，確定已關閉電源。它們不是可熱抽換的。

移除空白面板

若要維持適當氣流流過 SSG 20 裝置，空白面板應該留在沒有插入迷你 PIM 的插槽上面。除非您是在空白插槽中安裝迷你 PIM，否則請不要移除空白面板。

若要移除空白面板，請執行下列步驟：

1. 將靜電袋或防靜電墊放在您打算放置迷你 PIM 的平坦且穩定的表面上。
2. 將 ESD 接地腕帶戴到手腕上，然後將腕帶連接到機架上的 ESD 點，或連接到外面的 ESD 點（如果 SSG 20 裝置沒有接地）。
3. 從裝置拔下電源配接卡。確認 POWER LED 已熄滅。
4. 使用螺絲起子鬆開並移除面板每一側的螺絲。
5. 移除面板，然後將面板放入靜電袋或放在防靜電墊上。

移除迷你 PIM

迷你 PIM 安裝在 SSG 20 裝置的前面板中。迷你 PIM 的重量不到 0.2 磅 (106 公克)。

若要移除迷你 PIM，請執行下列步驟：

1. 將靜電袋或防靜電墊放在您打算放置迷你 PIM 的平坦且穩定的表面上。
2. 將 ESD 接地腕帶戴到手腕上，然後將腕帶連接到機架上的 ESD 點，或連接到外面的 ESD 點（如果 SSG 20 裝置沒有接地）。
3. 從裝置拔下電源配接卡。確認 POWER LED 已熄滅。
4. 標示已連接到迷你 PIM 的纜線，以便稍後可以將每一條纜線重新連接到正確的迷你 PIM。
5. 中斷纜線與迷你 PIM 的連接。
6. 需要的話，請將纜線排好，以防止它們移動或遭受壓力：
 - a. 固定住纜線，以便它們垂下到地板時，不用支持自己的重量。
 - b. 將任何多餘的纜線整齊地捲成圈收好。
 - c. 使用固定器來維持纜線圓圈的形狀。
7. 使用螺絲起子鬆開並移除迷你 PIM 面板每一側的螺絲。

8. 抓住迷你 PIM 面板每一側的螺絲，然後將迷你 PIM 滑出裝置。將迷你 PIM 放入靜電袋或放在防靜電墊上。

圖 16: 移除迷你 PIM



9. 如果您不是將迷你 PIM 重新安裝到空白插槽，請將空白面板安裝在插槽上面，以維持適當的氣流。

安裝迷你 PIM

若要安裝迷你 PIM，請執行下列步驟：

1. 將 ESD 接地腕帶戴到手腕上，然後將腕帶連接到機架上的 ESD 點，或連接到外面的 ESD 點（如果 SSG 20 裝置沒有接地）。
2. 從裝置拔下電源配接卡。確認 POWER LED 已熄滅。
3. 抓住迷你 PIM 面板每一側的螺絲，再將迷你 PIM 後面的連接器中的凹口對齊 SSG 20 裝置的迷你 PIM 插槽中的凹口。然後，滑進迷你 PIM，直到它穩定地嵌入裝置中。

圖 17: 安裝迷你 PIM



小心：將迷你 PIM 滑入插槽，以避免損害迷你 PIM 上的元件。

4. 使用 1/8 吋的十字螺絲起子鎖緊迷你 PIM 面板每一側的螺絲。
5. 將適當的纜線插入迷你 PIM 上的纜線連接器。

6. 需要的話，請將纜線排好，以防止它們移動或遭受壓力：
 - a. 固定住纜線，以便它們垂下到地板時，不用支持自己的重量。
 - b. 將任何多餘的纜線整齊地捲成圈收好。
 - c. 使用固定器來維持纜線圓圈的形狀。
7. 從裝置拔下電源配接卡。確認在按下電源按鈕之後，POWER LED 穩定地發出綠光。
8. 驗證系統儀表板上的 PIM 狀態 LED 是否穩定地發出綠光，以確認迷你 PIM 已連線。

升級記憶體

您可以將 SSG 20 裝置從單一 128 MB 雙直列記憶體模組 (DIMM) 動態隨機存取記憶體 (DRAM) 升級到 256 MB DIMM DRAM。

若要升級 SSG 20 裝置上的記憶體，請執行下列步驟：

1. 將 ESD 接地腕帶戴到手腕上，然後將腕帶連接到機架上的 ESD 點，或連接到外面的 ESD 點（如果裝置沒有接地）。
2. 從電源插座拔下 AC 電源線。
3. 將裝置倒置，將其頂部放在平坦的表面上。
4. 使用十字螺絲起子移除記憶體卡蓋的螺絲。將螺絲放在旁邊，以供稍後鎖緊蓋子時使用。
5. 移除記憶體卡蓋。

圖 18: 裝置底部



- 在模組每一側的鎖片上以拇指向外壓，讓鎖片移出模組，以便拆除 128 MB DIMM DRAM。

圖 19: 解除鎖定記憶體模組



- 抓住記憶體模組的長邊，然後將它滑出。將它放在一旁。

圖 20: 移除模組插槽



- 將 256 MB DIMM DRAM 插入插槽。在模組的上緣以兩根拇指均勻向下施壓，直到鎖片卡嗒一聲卡入位置。

圖 21: 插入記憶體模組



9. 將記憶體卡蓋放在插槽上面。
10. 使用十字螺絲起子鎖緊螺絲，從而將裝置的蓋子固定。

附錄 A 規格

本附錄提供 SSG 20 裝置的通用系統規格。本章包含下列各節：

- 第 54 頁上的「實體」
- 第 54 頁上的「電器設備」
- 第 54 頁上的「環境容忍度」
- 第 55 頁上的「憑證」
- 第 56 頁上的「連接器」

實體

表 8: SSG 20 實體規格

說明	值
機架尺寸	294 公釐 x 194.8 公釐 x 44 公釐 (11.5 英吋 x 7.7 英吋 x 2 英吋)
裝置重量	1.53 公斤 (3.3 磅) (未安裝 PIM)
ISDN PIM	70 公克
ADSL 附件 A PIM	106 公克
ADSL 附件 B PIM	106 公克
T1 PIM	75 公克
E1 PIM	75 公克
V.92 PIM	79 公克

電器設備

表 9: SSG 20 電器設備規格

項目	規格
DC 輸入電壓	12 伏特
DC 系統電流	3 - 4.16 安培

環境容忍度

表 10: SSG 20 環境容忍度

說明	值
高度	6,600 英尺 (2,000 公尺) 以下無效能損失
相對濕度	確保正常操作的相對濕度範圍是 10 % 到 90 %，無凝結
溫度	確保正常操作的溫度範圍是 32°F (0°C) 到 104°F (40°C) 出貨紙箱中非操作儲存溫度：-4°F (-20°C) 到 158°F (70°C)

憑證

安全

- CAN/CSA-C22.2 No. 60950-1-03/UL 60950-1 Safety of Information Technology Equipment
- EN 60950-1 (2000) Third Edition Safety of Information Technology Equipment
- IEC 60950-1 (1999) Third Edition Safety of Information Technology Equipment

EMC 輻射

- FCC 第 15 部分 B 類 (美國)
- EN 55022 B 類 (歐洲)
- AS 3548 B 類 (澳洲)
- VCCI B 類 (日本)

EMC 耐受性

- EN 55024
- EN-61000-3-2 Power Line Harmonics
- EN-61000-3-3 Power Line Harmonics
- EN-61000-4-2 ESD
- EN-61000-4-3 Radiated Immunity
- EN-61000-4-4 EFT
- EN-61000-4-5 Surge
- EN-61000-4-6 Low Frequency Common Immunity
- EN-61000-4-11 Voltage Dips and Sags

ETSI

歐洲電信標準協會 (ETSI) EN-3000386-2: Telecommunication Network Equipment (電信網路設備)。電磁相容性要求；(設備類別 - 非電信中心)

T1 介面

- FCC 第 68 部分 - TIA 968
- Industry Canada CS-03
- UL 60950-1 具外部設備引導連接之 TNV 電路的適用要求

連接器

圖 22 顯示 RJ-45 連接器上接腳的位置。

圖 22: RJ-45 接腳配置

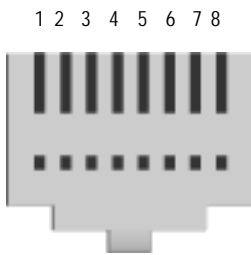


表 11 列出 RJ-45 連接器接腳配置。

表 11: RJ-45 連接器接腳配置

接腳	名稱	I/O	說明
1	RTS Out	O	要求傳送
2	DTR Out	O	資料終端備妥
3	TxD	O	傳輸資料
4	GND	不適用	機架接地
5	GND	不適用	機架接地
6	RxD	I	接收資料
7	DSR	I	資料備妥
8	CTS	I	允許傳送

圖 23 顯示 DB-9 母連接器上接腳的位置。

圖 23: DB-9 母連接器

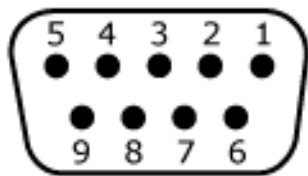


表 12 提供 DB-9 連接器接腳配置。

表 12: DB-9 連接器接腳配置

接腳	名稱	I/O	說明
1	DCD	I	載波偵測
2	RxD	I	接收資料
3	TxD	O	傳輸資料
4	DTR	O	資料終端備妥
5	GND	不適用	訊號電路接地
6	DSR	I	資料備妥
7	RTS	O	要求傳送
8	CTS	I	允許傳送
9	RING	I	響鈴偵測

附錄 B

初始組態精靈

本附錄提供有關使用 SSG 20 裝置的 Initial Configuration Wizard (初始組態精靈，ICW) 的詳細資訊。

當您的裝置實際連接至網路後，您可使用 ICW 來組態已安裝於您裝置上的介面。

本節說明下列 ICW 視窗：

- 第 60 頁上的「Rapid Deployment 視窗」
- 第 60 頁上的「Administrator Login 視窗」
- 第 61 頁上的「WLAN Access Point 視窗」
- 第 61 頁上的「Physical Interface 視窗」
- 第 62 頁上的「ADSL2/2 + Interface 視窗」
- 第 63 頁上的「T1 Interface 視窗」
- 第 68 頁上的「E1 Interface 視窗」
- 第 70 頁上的「ISDN Interface 視窗」
- 第 73 頁上的「V.92 Modem Interface 視窗」
- 第 74 頁上的「Eth0/0 介面 (Untrust 區域) 視窗」
- 第 75 頁上的「Eth0/1 介面 (DMZ 區域) 視窗」
- 第 75 頁上的「Bgroup0 介面 (Trust 區域) 視窗」
- 第 76 頁上的「Wireless0/0 介面 (Trust 區域) 視窗」
- 第 77 頁上的「Interface Summary 視窗」
- 第 78 頁上的「Physical Ethernet DHCP Interface 視窗」
- 第 78 頁上的「Wireless DHCP Interface 視窗」
- 第 79 頁上的「Confirmation 視窗」

1. Rapid Deployment 視窗

圖 24: Rapid Deployment 視窗



Rapid Deployment Wizard

Welcome to the Rapid Deployment Wizard.

Do you have a Rapid Deployment Configlet file?

☒ No, use the Initial Configuration Wizard instead.

☐ Yes, use the following Rapid Deployment Configlet file:

Load Configlet from:

☐ No, skip the Wizard and go straight to the WebUI management session instead.

您的網路若使用 NetScreen-Security Manager (NSM)，則您可使用 Rapid Deployment configlet 自動組態裝置。若要從 NSM 管理員處取得一個 configlet，請選取 **Yes**，再選取 **Load Configlet from:**，瀏覽至檔案位置，然後按一下 **Next**。configlet 會為您設定裝置，因此您不需要使用下列步驟組態裝置。

若您要略過 ICW，直接轉至 WebUI，請選取最後一個選項，然後按一下 **Next**。

若您沒有使用 configlet 來組態裝置，而是要使用 ICW，請選取第一個選項，然後按一下 **Next**。ICW Welcome 畫面隨即出現。按一下 **Next**。Administrator Login 視窗隨即出現。

2. Administrator Login 視窗

輸入新的管理員登入名稱和密碼，然後按一下 **Next**。

圖 25: Administrator Login 視窗



Initial Configuration Wizard

Enter the administrator's login name and password:

Administrator Login Name:

Password:

Confirm Password:

Note: You cannot retrieve the login name and password if you lose it. Please make sure you have a copy of this information in a secure location.

HTTP Redirect: ☐

Note: HTTP Redirect will redirect all HTTP traffic to HTTPS, ie, HTTPS is only way to manage the device through Web browsers.

3. WLAN Access Point 視窗

若您於 WORLD 或 ETSI 管制網域中使用裝置，您必須選擇一個國家 / 地區代碼。選取適當的選項，然後按一下 **Next**。

圖 26: Wireless Access Point Country Code 視窗

The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with white text. The main area has a white background. The text 'How do you want to configure the wireless access point?' is at the top. Below it, there are four dropdown menus: 'Regulatory Domain' (set to 'WORLD'), 'Country Code' (set to 'NO_COUNTRY_SET'), '2.4G Mode' (set to '802.11b/g'), and '5G Mode' (set to '802.11a'). At the bottom, there is a checkbox labeled 'Configure wireless0/0 interface in trust zone.' which is checked. Below the checkbox are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

4. Physical Interface 視窗

在介面至區域繫結畫面上，設定您要繫結 Untrust 安全區的介面。Bgroup0 已預先繫結至 Trust 安全區。Eth0/1 是繫結到 DMZ 安全區，但這是可選的。

圖 27: Physical Interface 視窗

The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with white text. The main area has a white background. The text 'Please choose one interface for untrust, dmz and trust zone respectively.' is at the top. Below it, there are three dropdown menus: 'Untrust Zone' (set to 'eth0/0'), 'DMZ Zone' (set to 'eth0/1'), and 'Trust Zone' (set to 'bgroup0'). At the bottom are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

將介面繫結至一個區域後，您可組態介面。於此點之後顯示的組態視窗將取決於安裝於您安全性裝置中的迷你 PIM。若要繼續以 ICW 組態您的裝置，請按一下 **Next**。

5. ADSL2/2+ Interface 視窗

若您在裝置上安裝了 ADSL2/2 + 迷你 PIM，您可使用下列視窗組態 adslx/0 介面。

注意： 若您在裝置上安裝了兩個 ADSL2/2 + 迷你 PIM，您無法以 ICW 組態多連結功能。若要組態 ML ADSL，請參閱「[概念與範例 ScreenOS 參考指南](#)」。

圖 28: ADSL Interface Configuration 視窗

Initial Configuration Wizard

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.
[adsl1/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

How does the Juniper device connect to the outside via adsl1/0 interface?

VPI/VCI: 8 / 35

Multiplexing Method: LLC

RFC1483 Protocol Mode: ☒ Bridged ☐ Routed

Operating Mode: ☒ Auto ☐ ANSI DMT ☐ ITU DMT ☐ Adsl2 ☐ Adsl2+

☐ Dynamic IP via DHCP

☐ Dynamic IP via PPPoA

Username:

Password:

Confirm:

☐ Dynamic IP via PPPoE

Username:

Password:

Confirm:

☒ Static IP

Interface IP:

Netmask:

Gateway:

<< Previous Next >> Cancel

表 13: ADSL Interface Configuration 視窗中的欄位

欄位	說明
來自服務供應商的資訊：	
VPI/VCI	識別永久虛擬電路的 VPI/VCI 值。
Multiplexing Method	ATM 多工方法 (LLC 為預設值)。
RFC1483 Protocol Mode	通訊協定模式設定 (Bridged 為預設值)。
Operating Mode	實體線路的操作模式 (Auto 為預設值)。
IP 組態設定	
	<ul style="list-style-type: none"> ■ 選取 Dynamic IP via DHCP 使裝置接收來自服務供應商之 ADSL 介面的 IP 位址。 ■ 選取 Dynamic IP via PPPoA 使裝置作為 PPPoA 用戶端。輸入服務供應商指派的使用者名稱和密碼。 ■ 選取 Dynamic IP via PPPoE 使裝置作為 PPPoE 用戶端。輸入服務供應商指派的使用者名稱和密碼。 ■ 選取 Static IP，為 ADSL 介面指派一個唯一且固定的 IP 位址。輸入介面 IP 位址、網路遮罩和閘道 (閘道位址是連接至裝置的路由器連接埠的 IP 位址)。

若您不知道這些設定，請參閱服務供應商裝置隨附的*服務供應商一般設定文件*。

6. T1 Interface 視窗

若您在裝置上安裝了 T1 迷你 PIM，且您選取了 Frame Relay 選項，則將顯示下列視窗：

- T1 Physical Layer 標籤視窗
- T1 Frame Relay 標籤視窗

注意： 若您在裝置上安裝了兩個 T1 迷你 PIM，且您選取了 Multi-link 選項，則您將看到兩個 Physical Layer 標籤。

圖 29: T1 Physical Layer 標籤視窗

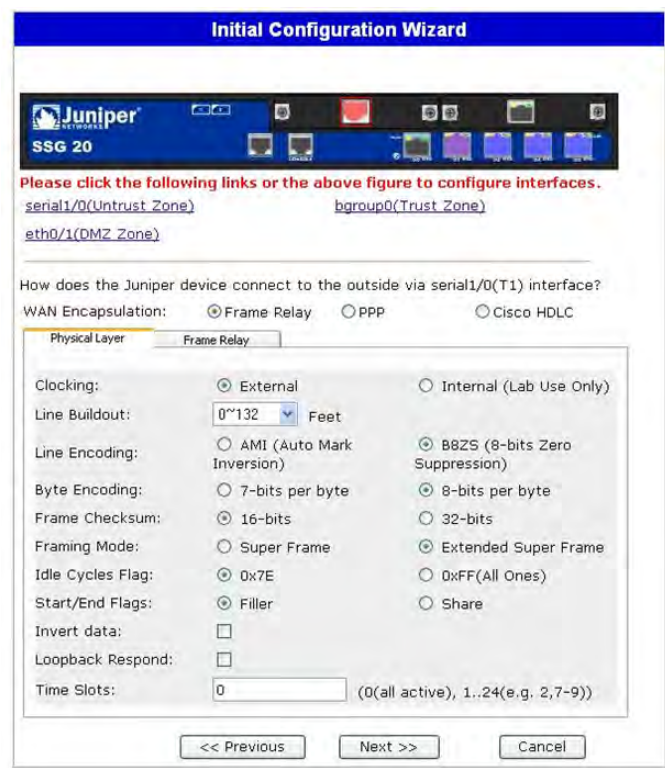


表 14: T1 Physical Layer 標籤視窗中的欄位

欄位	說明
Clocking	設定介面上的傳輸時鐘。
Line Buildout	設定介面驅動線路的距離。預設設定為 0 - 132 呎。
Line Encoding	設定介面上的線路編碼格式： <ul style="list-style-type: none">■ Auto Mark Inversion■ 8-bits zero suppression
Byte Encoding	在 T1 介面上設定位元組編碼，以使用每個位元組中的 7 個位元或每個位元組中的 8 個位元。預設值為每個位元組 8 個位元。
Frame Checksum	設定總和檢查碼的大小。預設值為 16。
Framing Mode	設定框架格式。預設值為 Extended mode 。
Idle Cycles Flag	設定閒置循環期間介面傳輸的值。預設設定為 0x7E : <ul style="list-style-type: none">■ 0x7E (旗標)■ 0xFF (ones)
Start/End Flags	將傳輸的開始和結束旗標設定為 filler 或 shared。預設值為 filler 。
Invert Data 核取方塊	啟用未使用資料位元的反向傳輸。
Loopback Respond 核取方塊	啟用從遠端通道服務單位 (CSU) 到 T1 介面的回傳。
Time Slots	在 T1 介面上設定時間插槽的使用。預設值為 0，所有的 24 個時間插槽皆已使用。

圖 30: T1 Frame Relay 標籤視窗

Initial Configuration Wizard

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.
[serial1/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

How does the Juniper device connect to the outside via serial1/0(T1) interface?
 WAN Encapsulation: ☒ Frame Relay ☐ PPP ☐ Cisco HDLC

Physical Layer **Frame Relay**

No-Keepalive: ☐
 Type: ☒ ANSI ☐ ITU

Please configure the sub interface.
 Interface Name: serial1/0. (1~32)
 Inverse ARP: ☐
 Frame Relay DLCI: (16~1022)
 Interface IP:
 Netmask:
 Gateway:

<< Previous Next >> Cancel

表 15: T1 Frame Relay 標籤視窗中的欄位

欄位	說明
No-Keepalive 核取方塊	啟用非 keepalive。
Type	設定訊框傳送 LMI 類型： <ul style="list-style-type: none"> ■ ANSI: 美國國家標準局 (ANSI) 支援高達 8 Mbps 的下游資料速率及 1 Mbps 的上游資料速率。 ■ ITU: 國際電信聯盟支援高達 6.144 Mbps 的下游資料速率及 640 kbps 的上游資料速率。
Interface Name	設定子介面名稱。
Inverse ARP	啓用子介面的反向位址解析通訊協定 (Address Resolution Protocol)。
Frame Relay DLCI	對子介面指派一個資料，連結連接識別字 (DLCI)。
Interface IP	設定子介面的 IP 位址。
Netmask	設定子介面的網路遮罩。
Gateway	設定子介面的閘道位址。

若您在裝置上安裝了 T1 迷你 PIM，且您選取了 PPP 選項，則將顯示下列附加的視窗：

- PPP 選項的 PPP 標籤視窗
- PPP 選項的 Peer User 標籤視窗

圖 31: PPP 選項的 PPP 標籤視窗

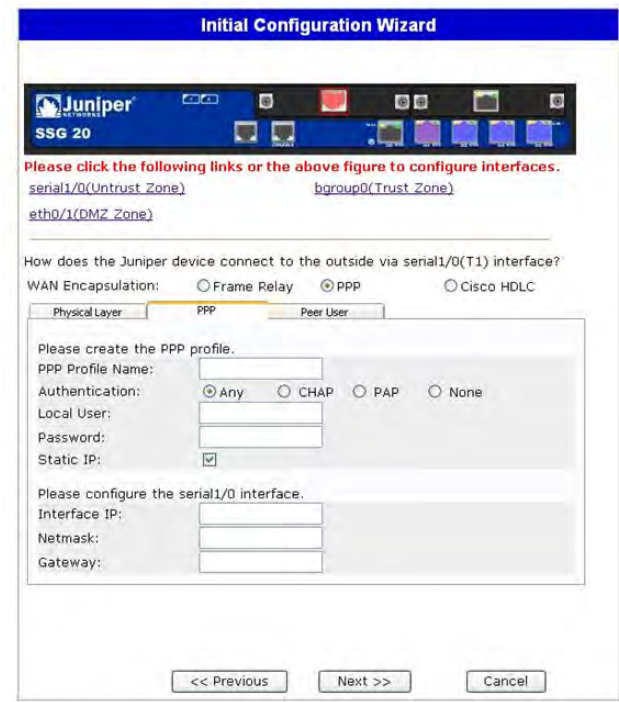


表 16: PPP 選項之 PPP 標籤視窗中的欄位

欄位	說明
PPP Profile Name	設定 PPP 設定檔的名稱
Authentication	設定驗證類型
Local User	設定本機使用者的名稱
Password	設定本機使用者的密碼
Static IP 核取方塊	啟用靜態 IP 位址
Interface IP	設定 serialx/0 介面 IP 位址
Netmask	設定 serialx/0 網路遮罩
Gateway	設定 serialx/0 閘道位址

圖 32: PPP 選項的 Peer User 標籤視窗



表 17: PPP 選項之 Peer User 標籤視窗中的欄位

欄位	說明
Peer User	設定對等使用者名稱
Password	設定於 Peer User 文字欄位中指定之對等使用者的密碼
Status	啟用或停用 PPP

若您在裝置上安裝了 T1 迷你 PIM，且您選取了 Cisco HDLC 選項，則將顯示下列視窗：

圖 33: Cisco HDLC 選項的 Cisco HDLC 標籤視窗

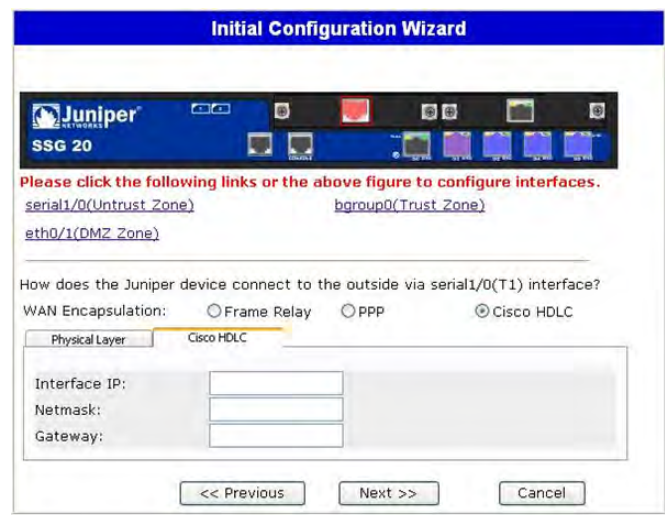


表 18: Cisco HDLC 選項之 Cisco HDLC 標籤視窗中的欄位

欄位	說明
Interface IP	設定 T1 Cisco HDLC 介面的 IP 位址
Netmask	設定 T1 Cisco HDLC 介面的網路遮罩
Gateway	設定 T1 Cisco HDLC 介面的閘道位址

7. E1 Interface 視窗

若您在裝置上安裝了 E1 迷你 PIM，且您選取了 Frame Relay 選項，則將顯示下列視窗：

- E1 Physical Layer 標籤視窗
- E1 Frame Relay 標籤視窗

注意： 若您在裝置上安裝了兩個 E1 迷你 PIM，且您選取了 Multi-link 選項，則您將看到兩個 Physical Layer 標籤。

圖 34: E1 Physical Layer 標籤視窗

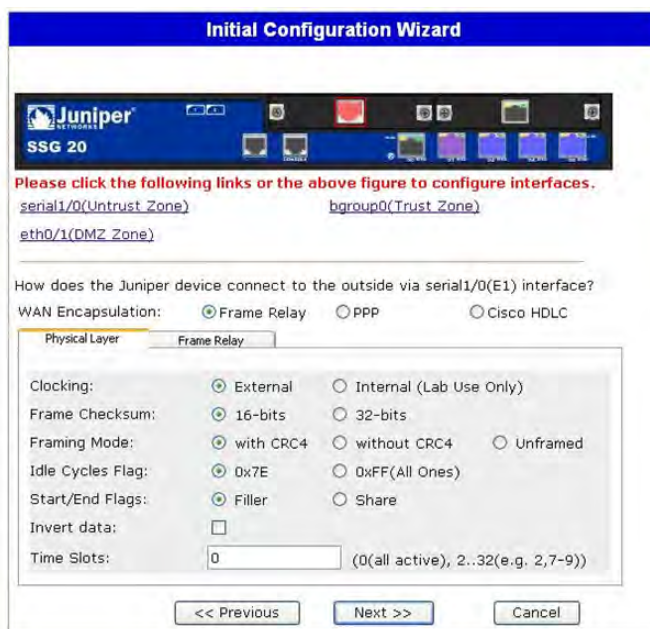


表 19: E1 Physical Layer 標籤視窗中的欄位

欄位	說明
Clocking	設定介面上的傳輸時鐘。
Frame Checksum	設定總和檢查碼的大小。預設值為 16 。
Framing Mode	設定框架格式。預設值為 without CRC4 。
Idle Cycles Flag	設定閒置循環期間介面傳輸的值。預設設定為 0x7E : <ul style="list-style-type: none"> ■ 0x7E (旗標) ■ 0xFF (ones)
Start/End Flags	將傳輸的開始和結束旗標設定為 filler 或 shared 。預設值為 filler 。
Invert Data 核取方塊	啟用未使用資料位元的反向傳輸。
Time Slots	在 T1 介面上設定時間插槽的使用。預設值為 0 ，所有的 32 個時間插槽皆已使用。

圖 35: E1 Frame Relay 標籤視窗



表 20: E1 Frame Relay 標籤視窗中的欄位

欄位	說明
No-Keepalive 核取方塊	啟用非 keepalive。
Type	設定訊框傳送 LMI 類型： <ul style="list-style-type: none">■ ANSI: 美國國家標準局 (ANSI) 支援高達 8 Mbps 的下游資料速率及 1 Mbps 的上游資料速率。■ ITU: 國際電信聯盟支援高達 6.144 Mbps 的下游資料速率及 640 kbps 的上游資料速率。
Interface Name	設定子介面名稱。
Inverse ARP 核取方塊	啓用子介面的反向位址解析通訊協定 (Address Resolution Protocol, ARP)。
Frame Relay DLCI	對子介面指派一個 DLCI。
Interface IP	設定子介面的 IP 位址
Netmask	設定子介面的網路遮罩
Gateway	設定子介面的閘道位址

若要以 PPP 選項組態 E1 介面，請參閱第 66 頁上的「PPP 選項的 PPP 標籤視窗」。

若要以 Cisco HDLC 組態 E1 介面，請參閱第 68 頁上的「Cisco HDLC 選項的 Cisco HDLC 標籤視窗」。

8. ISDN Interface 視窗

若您在裝置上安裝了 ISDN 迷你 PIM，您可使用下列視窗組態 brix/0 (Untrust) 介面。

注意： 若您在裝置上安裝了兩個 ISDN 迷你 PIM，且您選取了 Multi-link 選項，則您將看到兩個 Physical Layer 標籤。

圖 36: ISDN Physical Layer 標籤視窗



表 21: ISDN Physical Layer 標籤視窗中的欄位

欄位	說明
Switch Type	設定服務供應商交換機類型： <ul style="list-style-type: none"> ■ att5e: At&T 5ESS ■ ntdms100: Nortel DMS 100 ■ ins-net: NTT INS-Net ■ etsi: European variants ■ ni1: National ISDN-1
SPID1	服務供應商 ID，通常是一個含選用數字的 7 位數電話號碼。只有 DMS-100 和 NI1 交換機類型需要 SPID。DMS-100 交換機類型指派了兩個 SPID，每個 B 通道都有一個。
SPID2	備份服務供應商 ID。
TEI Negotiation	指定交涉 TEI 的時間，是在啟動時還是在第一次呼叫時。此設定通常用於歐洲的 ISDN 服務產品，以及設計來初始化 TEI 交涉的 DMS-100 交換機連接。
Calling Number	ISDN 網路請款號碼。
Sending Complete 核取方塊	啟用傳送完整資訊至向外設定訊息。通常僅使用於香港和台灣地區。

您可使用撥接器、多連結撥接器、租借線路或利用 BRI 撥接，選取 bri1/0 介面來連接。不選取或選取一或兩個選項會顯示類似於如下的視窗。

圖 37: ISDN Connection 標籤視窗

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20 device. The 'Dialer Interface' tab is selected. The configuration options include:

- Physical Layer: Leased Line Mode (128Kbps) and Dial Using BRI (both unchecked).
- Dialer Interface: PPP Profile Name, Authentication (Any selected), Local User, Password, Static IP (checked), Interface Name (dialer 1), Encapsulation Type (PPP selected), Primary Number, Alternative Number, Dialer Pool, Interface IP, Netmask, and Gateway.

表 22: ISDN Connection 標籤視窗中的欄位

欄位	說明
PPP Profile Name	對 ISDN 介面設定 PPP 設定檔的名稱。
Authentication	設定 PPP 驗證類型： <ul style="list-style-type: none">■ Any■ CHAP: 詢問交握式驗證通訊協定■ PAP: 密碼驗證通訊協定■ None
Local User	設定本機使用者。
Password	設定本機使用者的密碼。
Static IP 核取方塊	啟用介面的靜態 IP 位址。
Interface IP	設定介面 IP 位址。
Interface Name (僅限撥接器)	設定撥接器介面名稱。預設值為 dialer.1 。
Encapsulation Type	在撥接器上及使用 BRI 介面的撥接器上設定封裝類型。預設值為 PPP 。
Primary Number	設定撥接器及使用 BRI 介面之撥接器的主號碼。

欄位	說明
Alternative Number	當主號碼無法用於連接時，設定要使用的替代（次要）號碼。
Dialer Pool (僅限撥接器)	設定撥接器介面的撥接器集區名稱。
Netmask	設定網路遮罩。
Gateway	設定閘道位址。

9. V.92 Modem Interface 視窗

若您在裝置上安裝了 V.92 迷你 PIM，您可使用下列視窗組態 serialx/0（數據機）介面。

圖 38: Modem Interface 視窗

Initial Configuration Wizard

Juniper
SSG 20

Please click the following links or the above figure to configure interfaces.
[serial0/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

How does the Juniper device connect to the outside via serial0/0(Modem) interface?

Modem Name:

Init Strings:

ISP Name:

Primary Number:

Alternative Number: (Optional)

Login Name:

Password:

Confirm:

<< Previous Next >> Cancel

表 23: Modem Interface 視窗中的欄位

欄位	說明
Modem Name	設定數據機介面的名稱
Init String	設定數據機的初始化字串
ISP Name	對服務供應商指派一個名稱
Primary Number	指定電話號碼以存取服務供應商
Alternative Number (選用)	若主號碼沒有連接，請指定替代的電話號碼以存取服務供應商
Login Name	設定服務供應商帳戶的登入名稱
Password	設定登入名稱的密碼
Confirm	確認 Password 欄位中鍵入的密碼

10. Eth0/0 介面 (Untrust 區域) 視窗

可經由 DHCP 或 PPPoE 為 eth0/0 介面指派一個靜態或一個動態 IP 位址。

圖 39: Eth0/0 Interface 視窗

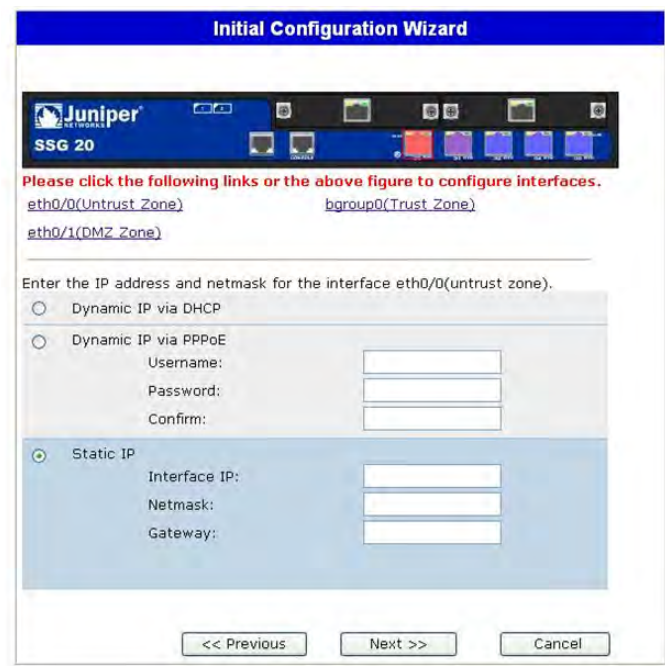


表 24: Eth0/0 Interface 視窗中的欄位

欄位	說明
Dynamic IP via DHCP	允許裝置從服務供應商處接收 Untrust 區域介面的 IP 位址。
Dynamic IP via PPPoE	允許裝置做為 PPPoE 用戶端，從服務供應商處接收 Untrust 區域介面的 IP 位址。輸入服務供應商指派的使用者名稱和密碼。
Static IP	對 Untrust 區域介面指派一個唯一且固定的 IP 位址。輸入 Untrust 區域介面 IP 位址、網路遮罩和閘道位址。

11. Eth0/1 介面 (DMZ 區域) 視窗

可經由 DHCP 為 eth0/1 介面指派一個靜態或一個動態 IP 位址。

圖 40: Eth0/1 Interface 視窗

Initial Configuration Wizard

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.
[eth0/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

Enter the IP address and netmask for the interface eth0/1(dmz zone).

☐ Dynamic IP via DHCP

☒ Static IP

Interface IP:

Netmask:

<< Previous Next >> Cancel

表 25: Eth0/1 Interface 視窗中的欄位

欄位	說明
Dynamic IP via DHCP	允許裝置從服務供應商處接收 DMZ 介面的 IP 位址。
Static IP	對 DMZ 介面指派一個唯一且固定的 IP 位址。輸入 DMZ 介面 IP 和網路遮罩。

12. Bgroup0 介面 (Trust 區域) 視窗

可經由 DHCP 為 bgroup0 介面指派一個靜態或一個動態 IP 位址。

預設介面 IP 位址為 192.168.1.1，網路遮罩為 255.255.255.0 或 24。

圖 41: Bgroup0 Interface 視窗

Initial Configuration Wizard

Juniper SSG 20

Please click the following links or the above figure to configure interfaces.
[eth0/0\(Untrust Zone\)](#) [bgroup0\(Trust Zone\)](#)
[eth0/1\(DMZ Zone\)](#)

Enter the IP address and netmask for the interface bgroup0(trust zone).

☐ Dynamic IP via DHCP

☒ Static IP

Interface IP:

Netmask:

<< Previous Next >> Cancel

表 26: Bgroup0 Interface 視窗中的欄位

欄位	說明
Dynamic IP via DHCP	允許裝置從服務供應商處接收 Trust 區域介面的 IP 位址。
Static IP	對 Trust 區域介面指派一個唯一且固定的 IP 位址。輸入 Trust 區域介面 IP 位址和網路遮罩。

13. Wireless0/0 介面 (Trust 區域) 視窗

若您正在組態 SSG 20-WLAN 裝置，您必須先設定服務集識別碼 (SSID)，才可啟動 wireless0/0 介面。如需有關組態無線介面的詳細說明，請參閱「[概念與範例 ScreenOS 參考指南](#)」。

圖 42: Wireless0/0 Interface 視窗

The image shows the 'Initial Configuration Wizard' for the Wireless0/0 interface on a Juniper SSG 20 device. The wizard is titled 'Initial Configuration Wizard' and has a blue header. Below the header, there is a message: 'Please click this wlan radio to configure wireless.' with a small icon of a radio. Below this, there is a navigation bar with icons for various configuration steps. The main content area has a message: 'Please click the following links or the above figure to configure interfaces.' followed by four links: [eth0/0\(Untrust Zone\)](#), [bgroup0\(Trust Zone\)](#), [eth0/1\(DMZ Zone\)](#), and [wireless0/0\(Trust Zone\)](#). Below the links, there is a question: 'How do you want to configure wireless0/0 interface(trust zone)?'. The 'Wlan Mode' is set to '2.4G(802.11b/g)'. The 'SSID' field is empty. The 'Encryption' section has three options: 'Open' (selected), 'WPA-PSK', and 'No Encryption'. The 'WPA-PSK' option is expanded, showing 'Passphrase(8~63 ASCII):', 'Confirm:', and 'PSK(64 hexadecimal):' fields. The 'Encryption Type' is set to 'Auto'. The 'Interface IP' is set to '192.168.2.1' and the 'Netmask' is set to '255.255.255.0'. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

表 27: Wireless0/0 Interface 視窗中的欄位

欄位	說明
Wlan Mode	設定 WLAN 無線電模式： <ul style="list-style-type: none"> ■ 5 G (802.11a)。 ■ 2.4 G (802.11b/g)。 ■ Both (802.11a/b/g)。
SSID	設定 SSID 名稱。
Authentication 和 Encryption	設定 WLAN 介面驗證和加密： <ul style="list-style-type: none"> ■ Open 驗證 (預設值)，可讓每個人存取裝置。此驗證選項並無加密。 ■ WPA Pre-Shared Key 驗證設定預先共享的金鑰 (PSK) 或存取無線連接時必須輸入的 passphrase。您可選擇為 PSK 輸入一個 HEX 或一個 ASCII 值。HEX PSK 必須是一個 256 位元 (64 文字字元) 的 HEX 值。ASCII passphrase 必須是 8 至 63 個文字字元。您必須選取「臨時金鑰完整性通訊協定」(TKIP) 或「進階加密標準」(AES) 作為此選項的加密類型，或選取 Auto 以使用其他選項。 ■ WPA2 Pre-Shared Key。 ■ WPA Auto Pre-Shared Key。
Interface IP	設定 WLAN 介面 IP 位址。
Netmask	設定 WLAN 介面網路遮罩。

14. Interface Summary 視窗

組態 WAN 介面之後，您將看到 Interface Summary 視窗。

圖 43: Interface Summary 視窗

The screenshot shows the 'Initial Configuration Wizard' window. At the top, it says 'Before proceeding further, review the following interface settings.' Below this is a section titled 'ISDN Configuration:' containing a table of settings:

Switch Type:	etsi	SPID1:	32546564565	SPID2:	23488458235
TEI Negotiation:	first call	Calling Number:	01023456789	T310 Value:	10
Sending Complete:	enabled	Leased Line Mode:	disabled	Dialer Enable:	disabled
PPP Profile:	myprofile	Authentication:	any	Local User:	myuser
Password:	mypwd	PPP Static IP:	enabled	Interface IP:	122.122.122.122

Below the table, there is a text area showing the configuration commands:

```
set interface bri1/0 isdn switch-type etsi
set interface bri1/0 isdn spid1 "32546564565"
set interface bri1/0 isdn spid2 "23488458235"
set interface bri1/0 isdn tei-negotiation first-call
set interface bri1/0 isdn calling-number "01023456789"
set interface bri1/0 isdn t310-value "10"
```

At the bottom, there are buttons for '<< Previous', 'Next >>', and 'Cancel'.

檢查您的介面組態，然後當準備好繼續時，按一下 **Next**。Physical Ethernet DHCP Interface 視窗隨即出現。

15. Physical Ethernet DHCP Interface 視窗

選取 **Yes** 以允許裝置透過 DHCP 對有線網路指派 IP 位址。輸入您要裝置指派給使用您網路之用戶端的 IP 位址範圍，然後按一下 **Next**。

圖 44: Physical Ethernet DHCP Interface 視窗

The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. The main content area has a light gray background. At the top, it asks: 'Do you want the Juniper device to dynamically assign IP addresses to your local **wired** hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses.' Below this, there are two radio buttons: 'Yes' and 'No'. The 'No' button is selected. To the right of the 'Yes' button, there are four input fields: 'IP Address Range Start' (192.168.1.33), 'End' (192.168.1.126), 'DNS Server 1 (optional)', and 'DNS Server 2 (optional)'. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

16. Wireless DHCP Interface 視窗

選取 **Yes** 以允許裝置透過 DHCP 對無線網路指派 IP 位址。輸入您要裝置指派給使用您網路之用戶端的 IP 位址範圍，然後按一下 **Next**。

圖 45: Wireless DHCP Interface 視窗

The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. The main content area has a light gray background. At the top, it asks: 'Do you want the Juniper device to dynamically assign IP addresses to your local **wireless** hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses.' Below this, there are two radio buttons: 'Yes' and 'No'. The 'No' button is selected. To the right of the 'Yes' button, there are four input fields: 'IP Address Range Start' (192.168.2.33), 'End' (192.168.2.126), 'DNS Server 1 (optional)', and 'DNS Server 2 (optional)'. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

17. Confirmation 視窗

確認您的裝置組態，並依需要進行變更。按一下 **Next** 進行儲存、重新啟動裝置並執行組態。

圖 46: Confirmation 視窗



Initial Configuration Wizard

Before proceeding further, review the following all device settings.

Admin Login: netscreen Password: *****

Device is in NAT mode.

ISDN Configuration:

Switch Type:	etsi	SPID2:	23488458235
SPID1:	32546564565	TEI Negotiation:	first call
TEI Negotiation:	first call	Calling Number:	01023456789
T310 Value:	10	Sending Complete:	enabled
Leased Line Mode:	disabled	Dialer Enable:	disabled
PPP Profile:	myprofile	Authentication:	any

```

set admin password "netscreen"
set interface bri1/0 isdn switch-type etsi
set interface bri1/0 isdn spid1 "32546564565"
set interface bri1/0 isdn spid2 "23488458235"
set interface bri1/0 isdn tei-negotiation first-call
set interface bri1/0 isdn calling-number "01023456789"
  
```

Click Next to save CLI into device.

<< Previous Next >> Cancel

裝置使用儲存的系統組態重新開機後，WebUI 登入提示隨即出現。如需有關使用 WebUI 來存取裝置之方法的資訊，請參閱第 27 頁上的「使用 WebUI」。

索引

A

AAL5 多工法	38
ADSL	
組態介面	37
連接連接埠	22
連接纜線	22
ATM Adaptation Layer 5	38
ATM 上的點對點通訊協定	
請參閱 PPPoA	

I

ISP IP 位址及網路遮罩	39
----------------------	----

L

LED	
PIM 1	11
PIM 2	11
POWER	11
STATUS	11
乙太網路連接埠上的活動連結	12

P

PPPoA	38
PPPoE	38

U

Untrust 區域，組態備份介面	33
-------------------------	----

V

VPI/VCI	
值	37
組態	38

W

WLAN LED	
802.11a	11
b/g	12

一畫

乙太網路上的點對點通訊協定	
請參閱 PPPoE	

四畫

天線	23
----------	----

六畫

多工法，組態	38
--------------	----

八畫

附件 A	22
附件 B	22

九畫

重設針孔，使用	45
---------------	----

十畫

記憶體升級程序	50
迷你 PIM	
安裝	49
空白面板	48
移除	48

十一畫

組態	
ADSL 2/2 + 迷你 PIM	37
E1 迷你 PIM	42
ISDN 迷你 PIM	41
T1 迷你 PIM	41
USB	16
V.92 數據機迷你 PIM	43
VPI/VCI 配對	38
日期與時間	31
主機及網域名稱	32
備份 Untrust 介面	33
無線驗證和加密	35
結合的無線及乙太網路	37
虛擬電路	38
預設路由	33
管理名稱及密碼	30
管理式存取	32
管理位址	33
管理服務	32
橋接群組 (bgroup)	31
連接，基本網路	21

十二畫

備份介面到 Untrust 區域.....	33
無線	
天線.....	23
使用預設介面.....	23
無線電收發機	
WLAN 0.....	15
WLAN 1.....	15
虛擬路徑識別碼 / 虛擬通道識別碼	
請參閱 VPI/VCI	

十三畫

預設 IP 位址.....	29
---------------	----

十四畫

管理	
透過 Telnet 連接.....	28
透過 WebUI.....	27
透過主控台.....	26

十六畫

憑證	
EMC (輻射).....	55
EMC 耐受性.....	55
T1 介面.....	56
安全.....	55
歐洲電信標準協會 (ETSI).....	55
靜態 IP 位址.....	38

二十五畫以上

纜線	
ADSL.....	22
序列.....	22
基本網路連接.....	21