



Security Products

SSG 500M Series Hardware Installation and Configuration Guide

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-017259-01, Revision 02

Copyright Notice

Copyright © 2007 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 Network's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

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

Table of Contents

About This Guide	5
Organization	5
Document Conventions.....	6
Command Line Interface Conventions.....	6
Naming Conventions and Character Types.....	7
Web User Interface Conventions	8
Juniper Networks Documentation	8
Chapter 1 Hardware Overview	9
Port and Power Connectors	10
Front Panel	11
Device Status LEDs	11
Port Descriptions	12
Built-in Gigabit Ethernet Ports	12
Console Port	13
AUX Port	13
Power Button.....	13
Reset Config Button	13
USB Ports	13
Physical Interface Modules	14
PIM Summary	15
Gigabit Ethernet	16
Dual-Port Serial	17
Dual-Port T1 or E1	18
Dual-Port T3.....	19
Four-Port Fast Ethernet	19
Back Panel	20
Power Supply Units	20
AC Power Supply Unit.....	21
DC Power Supply Unit.....	22
Grounding Lug.....	22
Chapter 2 Installing and Connecting a Device	23
Before You Begin	24
Installing Equipment	24
Connecting Interface Cables to a Device	26
Chassis Grounding	26
Connecting the Power.....	26
AC Power	26
DC Power	27
Powering a Device On and Off.....	29
Connecting a Device to a Network	30
Connecting a Device to an Untrusted Network	30

	Connecting a Device Using Ethernet Ports	31
	Connecting a Device Using Serial (AUX) Ports	31
	Connecting PIMs to an Untrusted Network	31
	Connecting an Internal Network or a Workstation	32
Chapter 3	Configuring a Device	33
	Default Device Settings	34
	Accessing a Device	35
	Using a Console Connection	35
	Using the WebUI	36
	Using Telnet	37
	Basic Device Configuration	37
	Admin Name and Password	38
	Administrative Access	38
	Interface IP Address	38
	Management Services	39
	Hostname and Domain Name	39
	Domain Name System Server	39
	Date and Time	40
	Default Route	40
	High Availability Configuration	41
	WAN PIM Configuration	43
	Serial Interface	43
	T1 Interface	44
	E1 Interface	44
	T3 Interface	45
	Basic Firewall Protections	46
	Verifying External Connectivity	47
	Resetting a Device to Factory Defaults	47
Chapter 4	Servicing a Device	49
	Required Tools and Parts	49
	Physical Interface Modules	50
	Removing a Blank Faceplate	50
	Removing a PIM	50
	Installing a PIM	51
	Device Power Components (SSG 550M Only)	52
	Removing a Power Supply Unit	52
	Installing a Power Supply Unit	54
	Replacing a Power-Supply Cord	55
	Upgrading Memory	55
	Replacing an Air Filter	57
Appendix A	Specifications	61
	Physical	61
	Electrical	62
	Environmental Tolerance	62
	Certifications	62
	Connectors	64
	Index	67

About This Guide

A Juniper Networks Secure Services Gateway (SSG) 500M Series device is a multiple operating system (multiOS) integrated router and firewall platform designed for enterprise-edge environments. Juniper Networks offers two models of the SSG 500M Series device:

- SSG 520M
- SSG 550M

Both SSG 500M Series devices support six physical interfaces module (PIM) slots. The devices provide 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 5.4.0r2 or later. 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 chapters and appendix:

- Chapter 1, “Hardware Overview,” describes the chassis and components of an SSG 500M Series device.
- Chapter 2, “Installing and Connecting a Device,” describes how to mount an SSG 500M Series device and how to connect cables and power to it.
- Chapter 3, “Configuring a Device,” describes how to configure and manage an SSG 500M Series device and how to perform some basic configuration tasks.
- Chapter 4, “Servicing a Device,” describes service and maintenance procedures for an SSG 500M Series device.
- Appendix A, “Specifications,” provides general system specifications for an SSG 500M Series device.

Document Conventions

This document uses several types of conventions, which are introduced in the following sections:

- “Command Line Interface Conventions” on this page
- “Naming Conventions and Character Types” on page 7
- “Web User Interface Conventions” on page 8

Command Line Interface Conventions

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

Naming Conventions and Character Types

ScreenOS employs the following conventions regarding the names of objects—such as addresses, admin users, auth servers, IKE gateways, virtual systems, VPN tunnels, and zones—defined in ScreenOS configurations:

- If a name string includes one or more spaces, the entire string must be enclosed within double quotes; for example:

set address trust "local LAN" 10.1.1.0/24

- Any leading spaces or trailing text within a set of double quotes are trimmed; for example, " local LAN " becomes "local LAN".
- Multiple consecutive spaces are treated as a single space.
- Name strings are case-sensitive, although many CLI keywords are case-insensitive. For example, "local LAN" is different from "local lan".

ScreenOS supports the following character types:

- Single-byte character sets (SBCS) and multiple-byte character sets (MBCS). Examples of SBCS are ASCII, European, and Hebrew. Examples of MBCS—also referred to as double-byte character sets (DBCS)—are Chinese, Korean, and Japanese.
- ASCII characters from 32 (0x20 in hexadecimal) to 255 (0xff), except double quotes ("), which have special significance as an indicator of the beginning or end of a name string that includes spaces.

NOTE: A console connection only supports SBCS. The WebUI supports both SBCS and MBCS, depending on the character sets that your browser supports.

Web User Interface Conventions

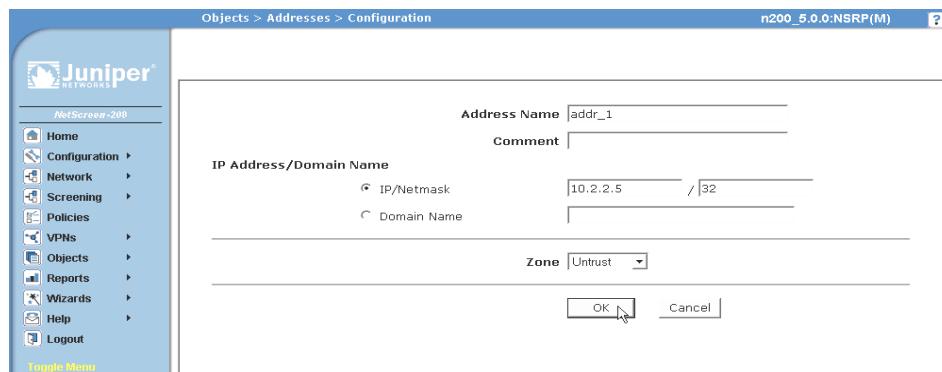
To perform a task with the WebUI, you first navigate to the appropriate dialog box, where you then define objects and set parameters. A chevron (>) shows the navigational sequence through the WebUI, which you follow by clicking menu options and links. The set of instructions for each task is divided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



Juniper Networks Documentation

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 email address below:

techpubs-comments@juniper.net

Chapter 1

Hardware Overview

This chapter provides detailed descriptions of the Secure Services Gateway (SSG) 500M Series security devices, namely the SSG 520M and SSG 550M chassis and components. It includes the following sections:

- “Port and Power Connectors” on page 10
- “Front Panel” on page 11
- “Back Panel” on page 20

Port and Power Connectors

This section displays and describes the location of the built-in ports, PIM slots, and cable connectors.

Figure 2: Built-in Ports and PIM Slot Locations

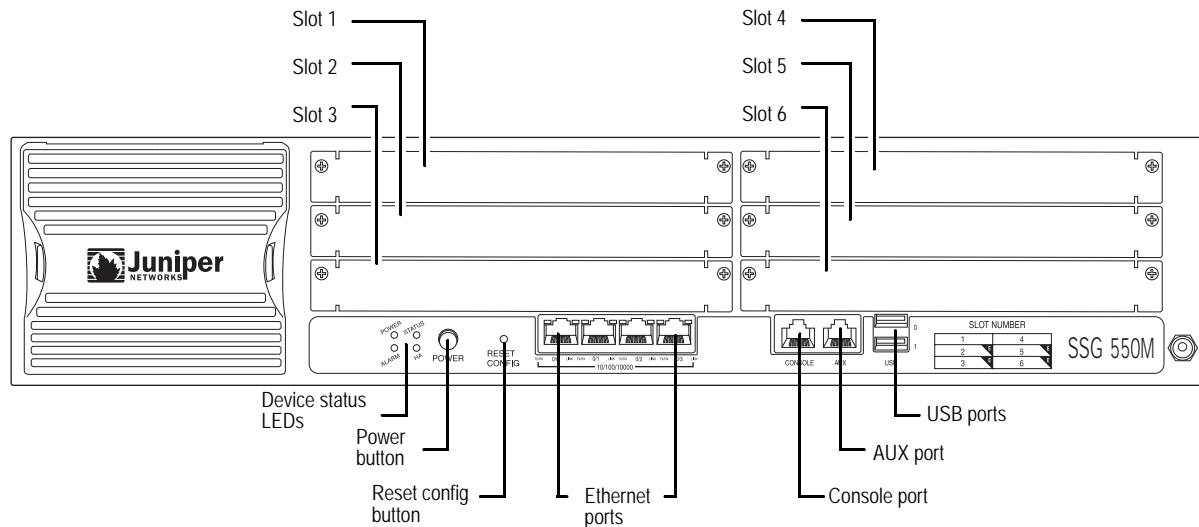


Table 1: SSG 500M Series Port and Cable Connector Descriptions

Port Labels	Description	Connector	Speed/Protocol
0/0-0/3	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	Functionality not supported in this release.	N/A	N/A
Console	Enables a serial connection with the device. 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
PIMs			
GB SFP	Enables direct connections to workstations or a LAN connection through a switch or hub.	LC	10/100/1000 Mbps
10/100/1000	Enables direct connections to workstations or a LAN connection through a switch or hub.	RJ-45	10/100/1000 Mbps 1000Base-TX SFP
4x10/100	Enables direct connections to workstations or a LAN connection through a switch or hub.	RJ-45	10/100 Mbps Ethernet Autosensing duplex and auto MDI/MDIX
SYNC Serial	Enables a connection from serial network media types to the untrusted network.	DTE	N/A
T1	Enables a connection from the T1 line to the untrusted network.	RJ-45	1.544 Mbps (full-time slots)

Port Labels	Description	Connector	Speed/Protocol
T3	Enables a connection from the T3 line to the untrusted network.	N/A	N/A
E1	Enables a connection from the E1 line to the untrusted network.	RJ-45	2.048 Mbps (full-time slots)

Front Panel

This section describes the following elements on the front panel of an SSG 500M Series device:

- Device Status LEDs
- Port Descriptions
- Power Button
- Reset Config Button
- USB Ports
- Physical Interface Modules

Device Status LEDs

The SSG 500M Series device status LEDs display information about critical device functions. When the device powers up, the STATUS LED changes from off to blinking green. Startup takes approximately 90 seconds. If you want to turn the device off and on again, we recommend you wait a few seconds between shutting it down and restarting it. Table 2 shows the name, color, status, and description of each device status LED.

Table 2: Device Status LED Descriptions

Name	Color	Status	Description
POWER	Green	On steadily	Device is receiving power
	Red	On steadily	Power Supply Unit (PSU) failure
		Off	Device is operating normally or that the device is not receiving power
STATUS	Green	On steadily	Device is starting or performing diagnostics
		Blinking	Device is operating normally
	Red	Blinking	Error is detected

Name	Color	Status	Description
ALARM	Red	On steadily	Critical alarm: <ul style="list-style-type: none"> ■ Failure of hardware component or software module ■ Firewall attacks detected
	Amber	On steadily	Major alarm: <ul style="list-style-type: none"> ■ Low memory (less than 10% remaining) ■ High CPU utilization (more than 90% in use) ■ Session full ■ Maximum number of VPN tunnels reached ■ HA status changed or redundant group member not found
		Off	No alarms
HA	Green	On steadily	Unit is the primary (master) device
	Amber	On steadily	Unit is the secondary (backup) device
		Off	High availability not enabled

Port Descriptions

This section explains the purpose and function of the following components:

- Built-in Gigabit Ethernet Ports
- Console Port
- AUX Port

Built-in Gigabit Ethernet Ports

Four built-in 10/100/1000 Gigabit Ethernet ports provide LAN connections to hubs, switches, local servers, and workstations. You can also designate an Ethernet port for management traffic.

When configuring one of these ports, you 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 **ethernet0/3**.

Each port has two LEDs located on the top of the port. Figure 3 displays the location of the LEDs on each Ethernet port, and Table 3 shows the name, function, color, state, and description of the Ethernet port LEDs.

Figure 3: Activity Link LEDs

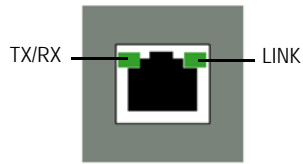


Table 3: LAN Port LEDs

Name	Function	Color	State	Description
LINK	Link	Green	On steadily	Port is online
TX/RX	Activity	Green	Blinking	Port is receiving data
			Off	Port might be on, but it is not receiving data

Console Port

The console port is an RJ-45 serial data terminal equipment (DTE) port that can be used for either local or remote administration. For local administration, connect the port to a terminal with an RJ-45-to-DB-9 (female-to-male) straight-through serial cable. For remote administration, connect the port to a workstation with an RJ-45-to-DB-9 (female-to-male) serial cable with a null modem adapter.

See “Connectors” on page 64 for the RJ-45 connector pinouts.

AUX Port

The auxiliary (AUX) port is an RJ-45 serial port wired as a DTE that you can connect 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.

See “Connectors” on page 64 for the RJ-45 connector pinouts.

Power Button

The power button is located on the left side of the front panel. You can use the power button to power the device on and off. When you power on the device, ScreenOS starts as the power supply completes its startup sequence.

Reset Config Button

The Reset Config button restarts the device and resets it to the default configuration.

USB Ports

Universal serial bus (USB) ports are not supported in this release.

Physical Interface Modules

Physical interface modules (PIMs) are removable and can be inserted into a slot when the device is powered off. If a slot is unoccupied, a PIM blank panel must be installed to shield the empty slot and to allow cooling air to circulate properly through the chassis.

The SSG 500M Series devices support the following PIMs:

- Gigabit Ethernet
- Dual-Port Serial
- Dual-Port T1 or E1
- Dual-Port T3
- Four-Port Fast Ethernet



PIM Summary

Figure 4 shows the slot numbering on an SSG 520M device. Table 4 shows the PIM types you can install in the slots of an SSG 520M device. The E located on some of the slots identifies where the enhanced PIMs (EPIMs) can be installed.



CAUTION: PIMs are *not* hot-swappable. PIMs must be installed in the front panel slots before the device is started.

Figure 4: SSG 520M Slot Location

SLOT NUMBER	
1	4
2	5
3 	6 






SSG 520M

Table 4: PIM Slots, SSG 520M

Slot	PIM Types	Slot	PIM Types
1	WAN Connectivity (PIM only) Serial, T1/E1, DS3	4	WAN Connectivity (PIM only) Serial, T1/E1, DS3
2	WAN Connectivity (PIM only) Serial, T1/E1, DS3	5	WAN Connectivity (PIM only) Serial, T1/E1, DS3
3	LAN or WAN Connectivity (PIM or EPIM) 10/100/1000, SFP, FE Serial, T1/E1, DS3	6	LAN or WAN Connectivity (PIM or EPIM) 10/100/1000, SFP, FE Serial, T1/E1, DS3

Figure 5 shows the slot numbering on an SSG 550M device. Table 5 shows the PIM types you can install in the slots of an SSG 550M device. The E located on some of the slots identifies where the enhanced PIMs (EPIMs) can be installed.

Figure 5: SSG 550M Slot Location

SLOT NUMBER	
1	4 
2 	5 
3 	6 

SSG 550M

Table 5: PIM Slots, SSG 550M

Slot	PIM Types	Slot	PIM Types
1	WAN Connectivity (PIM only) Serial, T1/E1, DS3	4	WAN Connectivity (PIM only) Serial, T1/E1, DS3
2	LAN or WAN Connectivity (PIM or EPIM) 10/100/1000, SFP, FE Serial, T1/E1, DS3	5	LAN or WAN Connectivity (PIM or EPIM) 10/100/1000, SFP, FE Serial, T1/E1, DS3
3	LAN or WAN Connectivity (PIM or EPIM) 10/100/1000, SFP, FE Serial, T1/E1, DS3	6	LAN or WAN Connectivity (PIM or EPIM) 10/100/1000, SFP, FE Serial, T1/E1, DS3

Table 6: Physical Interface Module Status LED

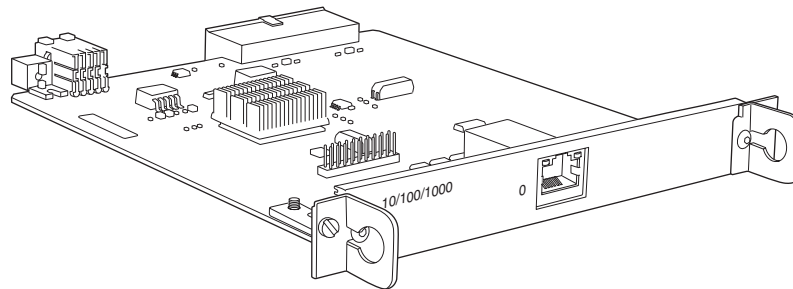
Color	State	Description
Green	On steadily	Online with no alarms or failures
Red	On steadily	Active with a local alarm; device has detected a failure

Gigabit Ethernet

In addition to the four built-in Gigabit Ethernet ports, the SSG 500M Series devices also supports the field-replaceable Gigabit Ethernet PIM, which provides a physical connection to Gigabit Ethernet network media types. The field-replaceable Gigabit Ethernet PIM is available in two versions, copper and optical, and each version has one port.

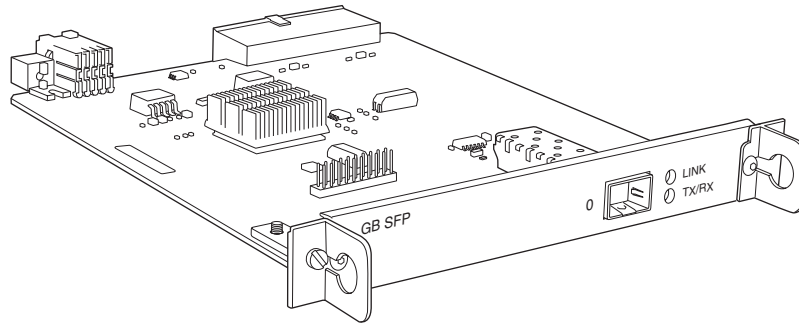
You can manually configure the copper Gigabit Ethernet PIM (shown in Figure 6) to link speeds of 10, 100, or 1000 Mbps, and you can configure the mode to half-duplex or full-duplex. The optical Gigabit Ethernet PIM cannot be manually configured; it is set at 1000 Mbps and full duplex.

NOTE: The Gigabit Ethernet PIMs do not support Simple Network Management Protocol (SNMP).

Figure 6: Copper Gigabit Ethernet PIM

The optical Gigabit Ethernet PIM (shown in Figure 7) uses small form-factor pluggable (SFP) transceivers that allow different interfaces to be used on the PIM. The optical Gigabit Ethernet PIM supports 1000Base-LX and 1000Base-SX SFPs only. Connect the module with a single-mode or multimode optical cable.

Figure 7: Optical Gigabit Ethernet PIM



NOTE: Configure Gigabit Ethernet interfaces up to a Maximum Transmission Unit (MTU) size of 1518 bytes. The CLI allows you to configure an MTU of up to 9192 bytes; however, packets greater than 1518 bytes will be dropped.

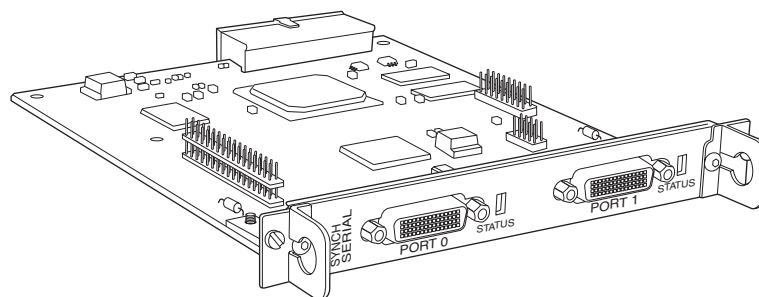
Dual-Port Serial

The dual-port serial PIM (shown in Figure 8) provides a physical connection to serial network media types through two serial interface ports. This PIM provides the following key features:

- Onboard network processor
- Autoselection of operation modes based on DTE or data circuit-terminating equipment (DCE) cables
- Local and remote loopback diagnostics
- Configurable clock rate for the transmit (Tx) clock and receive (Rx) clock

See “Connectors” on page 64 for the serial connector pinouts.

Figure 8: Dual-Port Serial PIM



Dual-Port T1 or E1

The dual-port T1 PIM (shown in Figure 9) and dual-port E1 PIM (shown in Figure 10) provide a physical connection to T1 or E1 network media types. Each PIM has two physical T1 or E1 ports with an integrated channel service unit (CSU) or data service unit (DSU).

Figure 9: Dual-Port T1 PIM

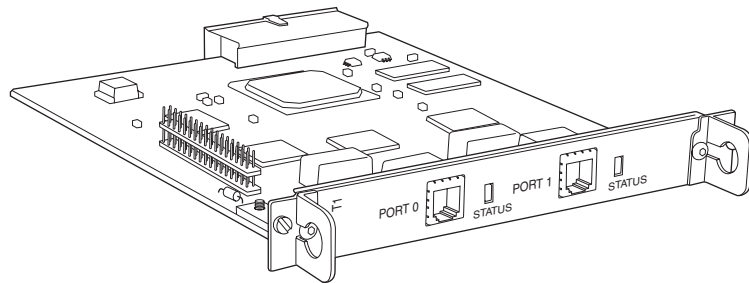
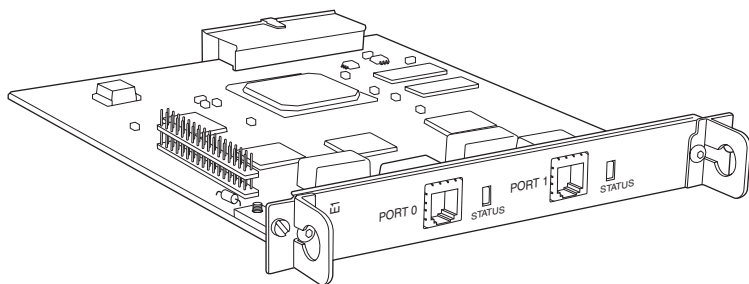


Figure 10: Dual-Port E1 PIM



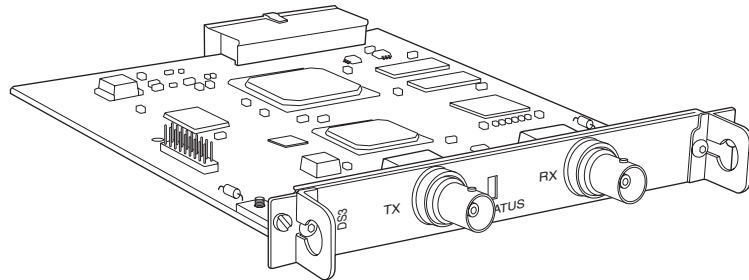
These PIMs provide the following key features:

- Onboard network processor
- Integrated CSU/DSU—eliminates the need for a separate external device
- 56-Kbps and 64-Kbps modes
- Independent internal and external clocking system
- Loopback, bit error rate test (BERT), T1 facilities data link (FDL), and long buildout diagnostics

Dual-Port T3

The dual-port T3 (also known as DS3) PIM (shown in Figure 11) provides a physical connection to T3 network media types. The T3 PIM includes two physical T3 ports with integrated data service unit (DSU).

Figure 11: T3 PIM



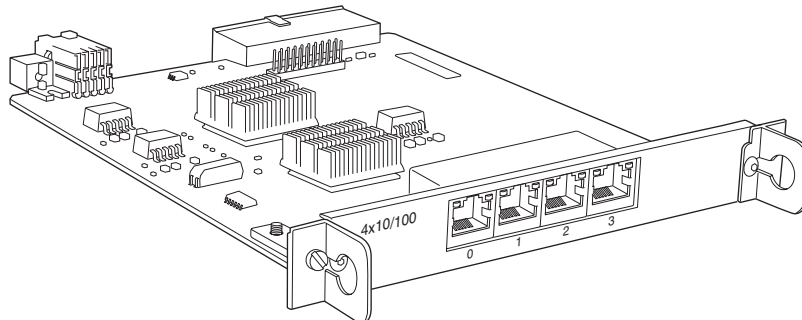
The T3 PIM provides the following key features:

- Onboard network processor
- Integrated DSU—eliminates the need for a separate external device
- Subrate and scrambling options with support for major DSU vendors
- Independent internal and external clocking system
- Loopback, BERT, and T3 far-end alarm and control (FEAC) diagnostics

Four-Port Fast Ethernet

The four-port 10/100-Mbps Fast Ethernet PIM (shown in Figure 12) has four physical Fast Ethernet ports.

Figure 12: Four-Port Fast Ethernet PIM



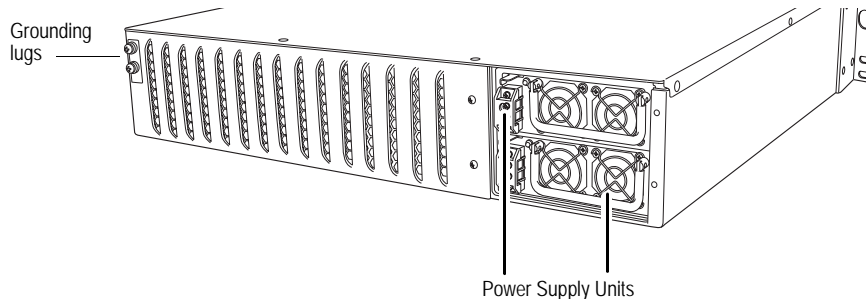
The four-port Fast Ethernet PIM provides the following features:

- Full-duplex and half-duplex modes
- Autonegotiation through medium-dependent interface (MDI) and MDI crossover (MDI-X) support
- Maximum frame size of 1518 bytes

Back Panel

The back panel of an SSG 500M Series device contains the fan tray and power supply unit(s) and a two-hole grounding lug.

Figure 13: Back Panel of an SSG 500M Series Device



Power Supply Units

The power supply units (PSUs) are located at the right side of the back panel:

- The SSG 520M device is equipped with a single permanently installed AC or DC power supply unit (PSU).
- The SSG 550M device has slots for two field-installable PSUs and is supplied with a single AC or DC PSU. You can add a second AC or DC PSU for increased reliability.

For PSU servicing instructions, see “Device Power Components (SSG 550M Only)” on page 52.

NOTE: Do not mix SSG 550M PSU types. The only supported combinations are AC + AC and DC + DC.

The POWER LED on the front panel of an SSG 500M Series device glows either green or red. Green indicates correct function and red indicates PSU failure.

Table 7 describes the LED states on the field-installable AC and DC PSUs.

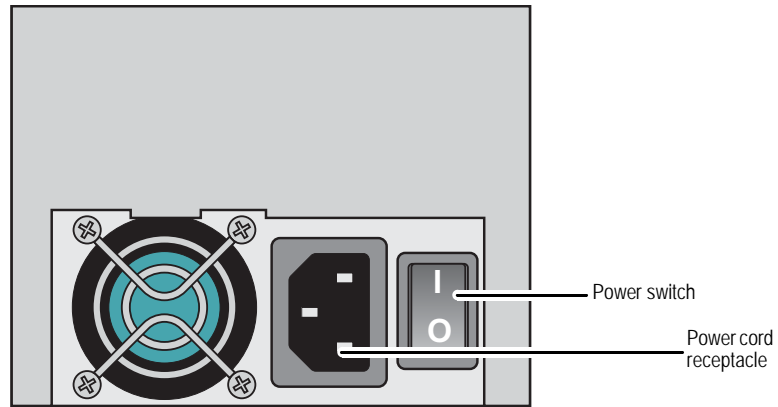
Table 7: Input Power LED Descriptions

Color	Status	Description
Green	On steadily	Input power is on and device is on
Yellow	On steadily	Input power is on but device is off
Amber	On steadily	Input power is on and device is off
	Off	Input power is off

AC Power Supply Unit

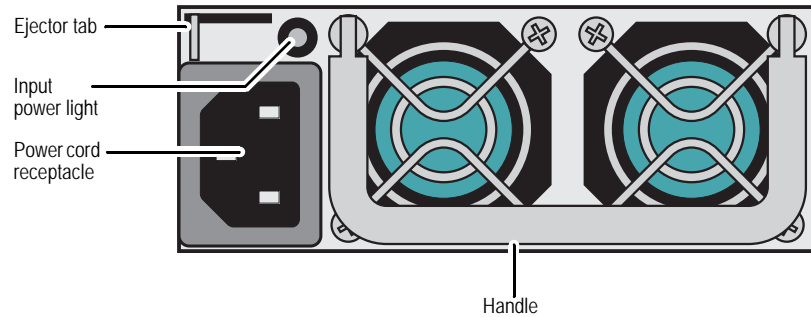
The fixed AC PSU faceplate for an SSG 520M device contains a power switch and a male power-cord receptacle. The fixed AC PSU does not have a power LED on the PSU.

Figure 14: SSG 520M Device Fixed AC PSU Faceplate



The field-replaceable AC PSU faceplate for an SSG 550M device contains an ejector tab handle, an input power light, and a power cord receptacle.

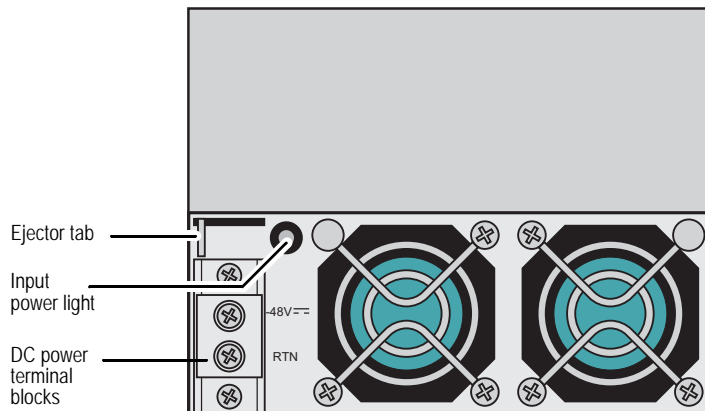
Figure 15: SSG 550M Device Replaceable AC PSU Faceplate



DC Power Supply Unit

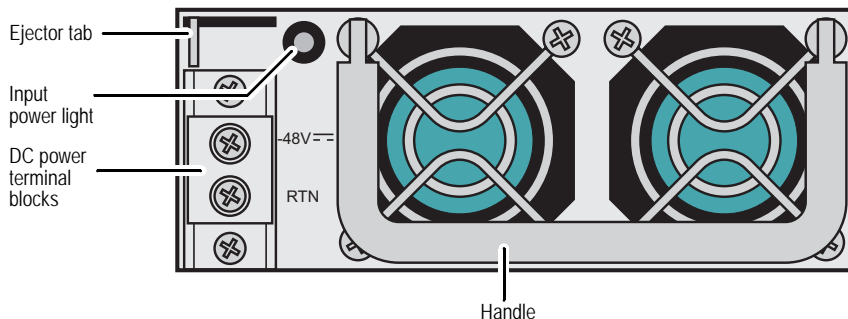
The fixed DC PSU faceplate for an SSG 520M device contains an ejector tab, an input power light, and two DC power terminal blocks that connect to power cables.

Figure 16: SSG 520M Device Fixed DC PSU Faceplate



The field-replaceable DC PSU faceplate contains an ejector tab, a handle, an input power light, and two DC power terminal blocks that connect to power cables.

Figure 17: SSG 550M Device Replaceable DC PSU Faceplate



Grounding Lug

A two-hole grounding lug is provided on the left rear of the chassis to connect the device to earth ground (see Figure 13 on page 20).

To ground the device before connecting power, you connect a grounding cable to earth ground and then attach the cable to the lug on the rear of the chassis. For more information, see “Chassis Grounding” on page 26.

Chapter 2

Installing and Connecting a Device

This chapter describes how to install an SSG 500M Series device in a standard 19-inch equipment rack and how to connect cables and power to the device. This chapter includes the following sections:

- “Before You Begin” on page 24
- “Installing Equipment” on page 24
- “Connecting Interface Cables to a Device” on page 26
- “Chassis Grounding” on page 26
- “Connecting the Power” on page 26
- “Powering a Device On and Off” on page 29
- “Connecting a Device to a Network” on page 30

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 you should be familiar with standard practices for preventing accidents.

Before You Begin

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



CAUTION: To prevent abuse and intrusion by unauthorized personnel, install the 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).
- Allow three feet (one meter) of clear space to the front and back of the device.
- 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.
- This device exceeds 18 pounds (8.2 kilograms). Take precautions when lifting and stabilizing the device.
- 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 rack-mount a device into a standard 19-inch equipment rack. The device is shipped with mounting brackets.

You can mid- or front-mount a SSG 500M Series device in a rack. In general, a center-mount rack is preferable to a front-mount rack because the more even distribution of weight in the center-mount rack provides greater stability.

NOTE: If you are installing multiple devices in one rack, install the lowest one first and proceed upward in the rack.



CAUTION: The chassis weighs between 18 lb. (8.2 kg) and 24 lb. (10.9 kg). Installing it into the rack requires at least one person to lift the device and a second person to secure the mounting screws.

To mount a device, you need a number-2 phillips screwdriver (not provided) and four screws that are compatible with the equipment rack (not provided).

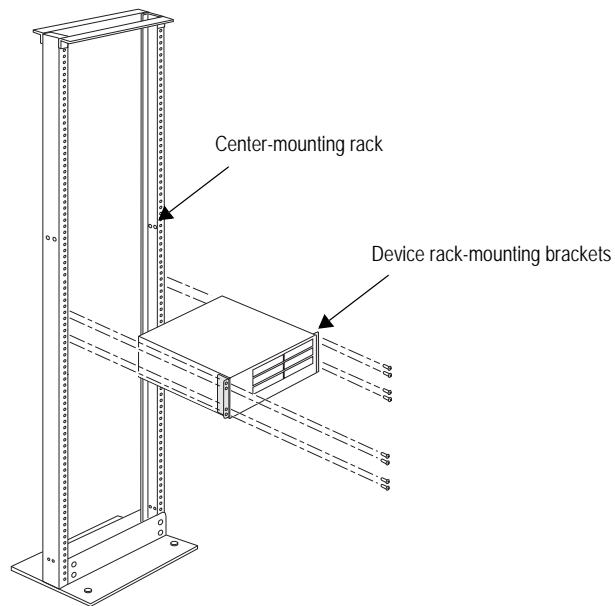
There are two ways to rack-mount an SSG 500M Series device:

- Mid-mount: attach the left and right mounting brackets to the middle of each side of the chassis.
- Front-mount: attach the left and right mounting brackets to the front of each side of the chassis.

To install an SSG 500M Series device into a rack, perform the following steps:

1. Have one person grasp the sides of the device, lift the device, and position it in the rack.
2. Align the bottom hole in each mounting bracket with a hole in each rack rail, making sure the chassis is level.
3. Have a second person install a mounting screw into each of the two aligned holes. Use a number-2 phillips screwdriver to tighten the screws.
4. Install the remaining screws in each mounting bracket.
5. Verify that the mounting screws on one side of the rack are aligned with the mounting screws on the opposite side and that the device is level.

Figure 18: Rack-Mount Installation



When correctly installed, the device sits level in the equipment rack.

Connecting Interface Cables to a Device

To connect interface cables 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 excess cable out of the way in a neatly coiled loop.
 - c. Use fasteners to maintain the shape of cable loops.

Chassis Grounding

To meet safety and electromagnetic interference (EMI) requirements, and to ensure proper operation, the device must be adequately grounded before power is connected. A two-hole grounding lug is provided on the rear of the chassis to connect the device to earth ground (see Figure 13 on page 20).



CAUTION: Before device installation begins, a licensed electrician must attach a cable lug to the grounding cable that you supply. A cable with an incorrectly attached lug can damage the device (for example, by causing a short circuit).

The grounding cable must be American Wire Gauge (AWG) number-14 single-strand wire cable and must be able to handle up to 6 ampere (A).

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

Connecting the Power

This section provides instructions for connecting AC and DC power to a device.

AC Power

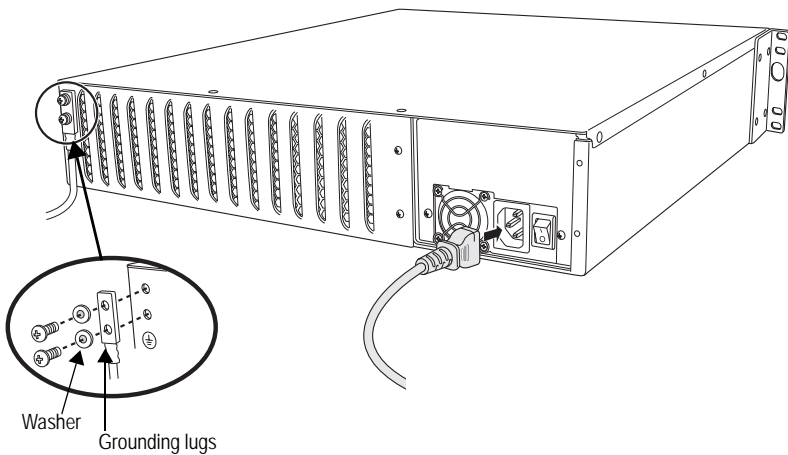
The AC power cord shipped with the device connects the device to earth ground when plugged into an AC grounding-type power outlet. The device must be connected to earth ground during normal operation.

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

1. Locate the power cord or cords shipped with the device, which has a plug appropriate for your geographical location.

2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strip to the ESD point on the chassis.
3. Use a grounding cable to connect the device to earth ground, and do the following:
 - a. Verify that a licensed electrician has attached an appropriate grounding-cable lug to the grounding cable.
 - b. Connect one end of the grounding cable to a proper earth ground, such as the rack in which the device is installed.
 - c. Connect the other end of the grounding cable to the two-hole grounding lug at the rear of an SSG 500M Series device.

Figure 19: AC Grounding



4. For each power supply unit (PSU), do the following:
 - a. Insert the appliance-coupler end of a power cord into the appliance inlet on the power-supply faceplate.
 - b. Insert the plug into an AC power-source receptacle.
5. Verify that the power cord does not block access to device components or drape where people can trip on it.

DC Power

Each DC PSU has a single DC input (–48 VDC and return) that requires a dedicated 15 A (–48 VDC) circuit breaker.



CAUTION: If your device includes an optional redundant DC PSU, connect each of the two power supplies to different input-power sources. Failure to do so makes the device susceptible to total power failure if one of the power supplies fails.

Most sites distribute DC power through a main conduit that leads to frame-mounted DC power distribution panels, one of which might be located at the top of the rack that houses the router. A pair of cables (one input and one return) connects each set of terminal studs to the power distribution panel.



CAUTION: There is no standard color coding for DC power cables. The color coding used by the external DC power source at your site determines the color coding for the leads on the power cables that attach to the terminal studs on each power supply. You must ensure that power connections maintain the proper polarity. The power source cables might be labeled (+) and (-) to indicate their polarity.

The device must be connected to earth ground during normal operation. The protective grounding terminal on the rear of the chassis is provided to connect the device to ground.



WARNING: Power-plant ground and chassis ground must be connected to the same building ground.

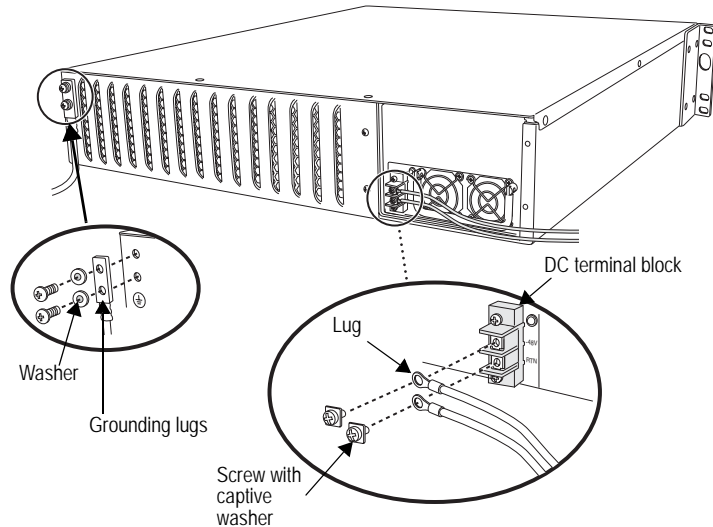
The DC return terminal must be connected to the central office (CO) ground. This common DC return connection (DC-C) and the -48 VDC connection must both be 14 AWG single-strand wire cable (minimum). Each lug attached to the power cables must be U-type.

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

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strip to the ESD point on the chassis.
2. Use a grounding cable to connect the device to earth ground, and do the following:
 - a. Verify that a licensed electrician has attached an appropriate grounding-cable lug to the grounding cable.
 - b. Connect one end of the grounding cable to a proper earth ground, such as the rack in which the device is installed.
 - c. Connect the other end of the grounding cable to the two-hole grounding lug at the rear of the device (Figure 20).
3. For each power supply, do the following:
 - a. Ensure that the voltage across the DC power source cable leads is 0 V and that there is no chance that the cable leads might become active during installation.
 - b. Verify that a licensed electrician has attached the appropriate power-cable lugs to the negative and positive DC source power cables.
 - c. Within the terminal block, loosen the two center screws next to the labels **-48 VDC** and **RTN**.

Each screw contains a washer used to secure a DC source power-cable lug to the terminal block.

Figure 20: Connecting DC Power-Cable Lugs



- d. Secure the positive (+) DC source power cable lug to the RTN terminal.
- e. Secure the negative (-) DC source power cable lug to the -48 VDC terminal.
- f. Dress the power cables appropriately.



CAUTION: Ensure that the DC cables do not touch the two screws on the chassis that are adjacent to the terminal block. Contact between the DC cables and the chassis screws will cause a circuit failure.

4. Verify that the power cord does not block access to device components or drape where people can trip on them.

Powering a Device On and Off

To power on a device, press the power button. ScreenOS starts as the power supply completes its startup sequence. The POWER LED illuminates during startup and remains on steadily when the device is operating normally.

NOTE: The PSU in the rear panel of the device could include a power switch. If such a switch is included, make sure the switch is in the ON position.

To power off a device, press the power button and hold it for more than 5 seconds.

To remove power completely from the device, unplug the power cord. The power button on the device is a standby power switch.



CAUTION: If the device is connected to an AC power-source receptacle when you press the power button to power off, the device remains in standby mode, and a small amount (5 V and 3.3 V) of standby voltage is still available in the chassis.

Connecting a Device to a Network

An SSG 500M Series 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 PIMs to an Untrusted Network
- Connecting an Internal Network or a Workstation

Connecting a Device to an Untrusted Network

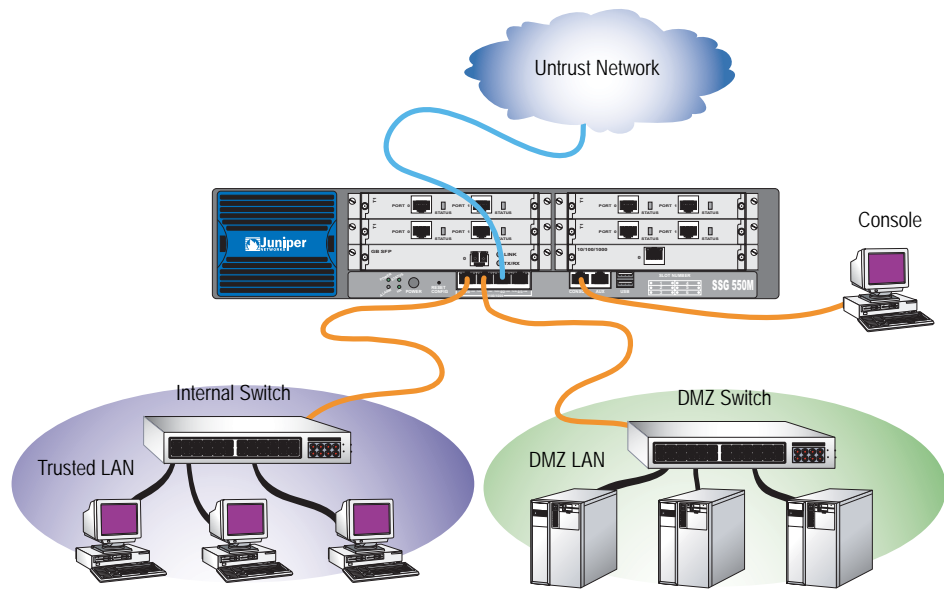
You can connect a device to the untrusted network using one of the following ways:

- Connecting a Device Using Ethernet Ports
- Connecting a Device Using Serial (AUX) Ports

To add an SSG 550M device to a network (Figure 21), perform the following steps:

1. Connect an RJ-45 crossover cable from the port labeled 0/0 (ethernet0/0 interface) to the internal switch. The ethernet0/0 interface is prebound to the Trust security zone.
2. Connect an RJ-45 crossover cable from the port labeled 0/1 (ethernet0/1 interface) to the DMZ switch. The ethernet0/1 interface is prebound to the DMZ security zone.
3. Connect an RJ-45 crossover cable from the port labeled 0/2 (ethernet0/2 interface) to the external switch or router. The ethernet0/2 interface is prebound to the Untrust security zone.
4. Connect an RJ-45 straight-through cable from the Console port using the instructions provided in “Using a Console Connection” on page 35 for management access.

Figure 21: Basic Cabling Example



Connecting a Device Using Ethernet Ports

To establish a high-speed connection, connect the provided Ethernet cable from the Ethernet port marked 0/2 (ethernet0/2, which is in the Untrust security zone) on an SSG 500M Series device to the external router. The device auto-senses the correct speed, duplex, and MDI/MDIX settings.

Connecting a Device Using Serial (AUX) Ports

You can connect to the untrusted network with an RJ-45 straight through serial cable and 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 PIMs to an Untrusted Network

You can connect Ethernet and WAN PIMs to an untrusted network. To connect the PIMs to a network, 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 an Internal Network or a Workstation

You can connect your local area network (LAN) or workstation with the Ethernet interfaces. An SSG 500M Series device contains four built-in 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 34 for the default zone-to-interface bindings.

Chapter 3

Configuring a Device

ScreenOS software is preinstalled on SSG 500M Series devices. When the device is started, 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 includes the following sections:

- “Default Device Settings” on page 34
- “Accessing a Device” on page 35
- “Basic Device Configuration” on page 37
- “High Availability Configuration” on page 41
- “WAN PIM Configuration” on page 43
- “Basic Firewall Protections” on page 46
- “Verifying External Connectivity” on page 47
- “Resetting a Device to Factory Defaults” on page 47

NOTE: After you configure an SSG 500M Series device and verify connectivity through the remote network, you must register your product at www.juniper.net/support/ so that certain ScreenOS services, such as Deep Inspection (DI) Signature Service and Antivirus (AV), can be activated on the device. After registering your product, use the WebUI to obtain the subscription for the service. For more information about registering your product and obtaining subscriptions for specific services, see the *Fundamentals* volume of the *Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.4.0.

Default Device Settings

This section describes the default settings and operation of the SSG 500M Series devices.

Table 8 describes the default interface-to-zone bindings on an SSG 500M Series device.

Table 8: Default Interface-to-Zone Bindings

Port Label	Interface	Zone
AUX	serial0/0	Null
0/0	ethernet0/0 (default IP address is 192.168.1.1/24)	Trust
0/1	ethernet0/1	DMZ
0/2	ethernet0/2	Untrust
0/3	ethernet0/3	Null
PIM ports		Untrust
EPIM ports		Null

Note that the ethernet0/0 interface has the default IP address 192.168.1.1/24 and is configured for management services. If you connect the ethernet0/0 port 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 ethernet0/0 interface to match the addresses on your LAN. There are no other default IP addresses configured on other ports on the device; you need to assign IP addresses to other interfaces.

Accessing a Device

You can access, configure, and manage an SSG 500M Series 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 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) using secure HTTP (S-HTTP).
- **Telnet/SSH:** Telnet and Secure Shell (SSH) are applications that allow 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 (NSM):** NSM is Juniper Networks' enterprise-level management application, which enables you to control and manage Juniper Networks firewall/IPSec VPN devices. For more information, refer to the *NetScreen-Security Manager Administrator's Guide*.

Using a Console Connection

NOTE: Use an 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 22: DB-9 Adapter



2. Plug the male RJ-45 end of the serial cable into the console port on the device. Be sure that the RJ-45 connector is properly seated in the port.

3. Launch a serial terminal-emulation program on your workstation. The required settings to launch a console session with the device 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 username 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**.
6. Once the command prompt is displayed, the device is ready to be configured. See “Basic Device Configuration” on page 37 to complete the initial device configuration.

Using the WebUI

To use the WebUI, you must be on the same subnet as the device. To access the device with the WebUI browser interface, perform the following steps:

1. Connect your workstation to the port labeled 0/0 (ethernet0/0 interface), which is prebound to the Trust security zone.
2. Launch your browser, enter the IP address for the ethernet0/0 interface (the default IP address is 192.168.1.1), then press **Enter**.

The WebUI application displays the login prompt.

3. If you have not yet changed the default username and password, enter **netscreen** at both the login and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive.)
4. Once the WebUI home page is displayed, the device is ready to be configured. See “Basic Device Configuration” on page 37 to complete the initial device configuration.

Using Telnet

To use a Telnet connection, the workstation must be in the same subnetwork as the security device. To access the device with a Telnet connection, perform the following steps:

1. Connect your workstation to the port labeled 0/0 (ethernet0/0 interface), which is prebound to the Trust security zone.
2. Start a Telnet client application to the IP address for the ethernet0/0 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.

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

Basic Device Configuration

This section describes the following basic configurations:

- Admin Name and Password
- Administrative Access
- Interface IP Address
- Management Services
- Hostname and Domain Name
- Domain Name System Server
- Date and Time
- Default Route

The examples provided in this section are used to establish initial network connectivity. For advanced configuration information, refer to the *Concepts & Examples ScreenOS Reference Guide*.

Admin Name and Password

The administrative user has complete privileges to configure a device. We recommend that you change the default admin name (netscreen) and password (netscreen) immediately.

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

WebUI

Configuration > Admin > Administrators > Edit (for the NetScreen Administrator Name): Enter the following, then click **OK**:

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

CLI

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

Administrative Access

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

To configure a 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
```

Interface IP Address

The ethernet0/0 interface has the default IP address 192.168.1.1/24 and is preconfigured for management services. If you connect the ethernet0/0 interface on a 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. To change the default interface IP address on the device, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > Edit (for ethernet0/0): Enter the following, then click **OK**:

IP Address/Netmask: *ip_addr/mask*

CLI

```
set interface ethernet0/0 ip ip_addr/mask  
save
```

Management Services

ScreenOS provides services for configuring and managing a device, such as SNMP, SSL, and SSH, which you can enable on a per-interface basis. WAN interfaces cannot be configured for management services.

To configure the management services for the ethernet0/0 interface, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > 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 eth0/0 manage web  
unset interface eth0/0 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 a device in the network. To configure the hostname and domain name on the device, use the WebUI or CLI as follows:

WebUI

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

Host Name: *hostname*
Domain Name: *domain-name*

CLI

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

Domain Name System Server

The Domain Name System (DNS) server on the network maintains a database for resolving hostnames and IP addresses. A device accesses the configured DNS servers to resolve hostnames. In ScreenOS, you configure the IP addresses for the primary and secondary DNS servers and the time of the day at which the device performs a DNS refresh.

To configure the DNS server IP address, use the WebUI or CLI as follows:

WebUI

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

Primary DNS Server: *ip_addr*
 Secondary DNS Server: *ip_addr*
 DNS Refresh: (select)
 Every Day at: *time*

CLI

```
set dns host name ip_addr
set dns host name ip_addr
set dns host schedule time
save
```

Date and Time

The time settings on a device affect events such as the setup of virtual private network (VPN) tunnels. The easiest way to set the date and time on the device is to use the WebUI to synchronize the device clock with the clock on your workstation.

To configure the date and time on the 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 device clock and adjust it according to daylight saving time, or click **No** to synchronize the device clock without adjusting for daylight saving time.

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

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**:

Network Address/Netmask: 0.0.0.0/0.0.0.0
 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
```

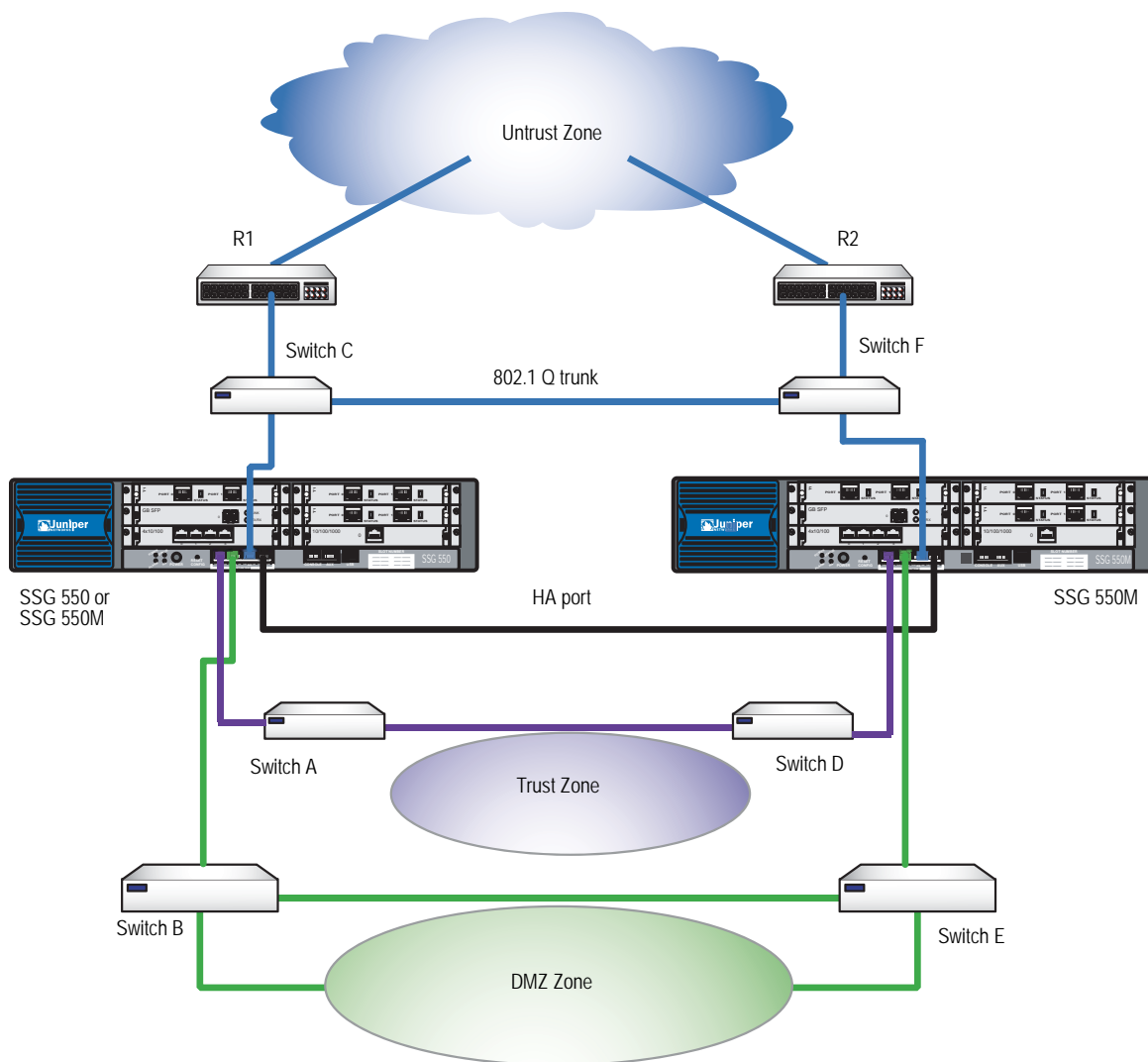

High Availability Configuration

An HA port allows you to cable two devices together and configure them to work as a *redundant group*. A redundant group consists of one primary device and one backup device. If the primary device fails, the backup device takes over as the new primary, thus avoiding interruption of services.

This section describes how to connect your device for high availability.

NOTE: Do not mix port interface types. HA configuration is not supported on WAN interfaces. You must have the same hardware configuration for both devices for HA to work correctly. For more information about HA configuration, refer to the *Concepts & Examples ScreenOS Reference Guide*.

Figure 23: HA Cabling Connections



NOTE: The provided cabling instructions reproduce the configuration shown in Figure 23; however, this is not the only possible HA configuration. In addition, the instructions assume that all physical ports and interfaces are still at their defaults. If you have changed the port and interface settings, the instructions might not work properly.

To cable SSG 550 and SSG 550M security devices together for HA and connect them to the network, perform the following steps:

Configuring HA Ports

1. Set the HA interface by executing the **set interface ethernet0/3 zone ha** CLI command on both devices.

Primary Unit

2. Connect a crossover cable from **ethernet0/0** to **Switch A**.
3. Connect a crossover cable from **ethernet0/1** to **Switch B**.
4. Connect a crossover cable from **ethernet0/2** to **Switch C**.

Backup Unit

5. Connect a crossover cable from **ethernet0/0** to **Switch D**.
6. Connect a crossover cable from **ethernet0/1** to **Switch E**.
7. Connect a crossover cable from **ethernet0/2** to **Switch F**.

Switches

8. Cable together **Switch A** and **Switch D**.
9. Cable together **Switch B** and **Switch E**.
10. Cable together **Switch C** and **Switch F**.
11. Cable **Switch C** to **R1**.
12. Cable **Switch F** to **R2**.

NOTE: The switch ports must be defined as 802.1Q trunk ports, and the external routers must be able to use either Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP). For the best configuration method, refer to the documentation for your switch or router.

13. Press the power switch to the ON position for both devices.

WAN PIM Configuration

This section explains how to configure the wide area network (WAN) physical interface modules (PIMs):

- “Serial Interface” on this page
- “T1 Interface” on page 44
- “T3 Interface” on page 45
- “E1 Interface” on page 44

Interfaces on PIMs are bound to the Untrust zone by default. The examples provided in this section are only used to establish initial WAN interface connectivity. For detailed information about configuring WAN interfaces, refer to the *Concepts & Examples ScreenOS Reference Guide*.

Serial Interface

Serial links provide bidirectional links that require very few control signals. In a basic serial setup, the data communications equipment (DCE) is responsible for establishing, maintaining, and terminating a connection. A modem is a typical DCE device. A serial cable connects the DCE to a telephony network where, ultimately, a link is established with data circuit-terminating equipment (DTE). DTE is typically where a link terminates.

The SYNC Serial PIM supports the following standards:

- TIA/EIA 530
- V.35
- X.21
- RS-232
- RS-449

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

WebUI

Network > Interfaces > List > Edit (*interface*) > WAN: Select the following, then click **Apply**:

DTE Options
Select your options

CLI

```
set interface interface serial-options dte-options { ... }  
save
```

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 and can support 24 DS0 channels.

The T1 PIM supports the following 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 interface, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > List > Edit (*interface*): Enter or select the applicable option value, 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
save
```

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 E1 PIM supports the following standards:

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

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

WebUI

Network > Interfaces > List > Edit (*interface*): Enter or select the applicable option value, then click **OK**.

WAN Configure: main link
WAN Encapsulation: PPP

Click **Apply**.

Binding a PPP Profile: junipertest
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"
save
```

T3 Interface

T3, also known as data signal 3 (DS3), is a high-speed data-transmission medium formed by multiplexing 28 DS1 signals into seven separate DS2 signals and combining the DS2 signals into a single DS3 signal. T3 links operate at 43.736 Mbps.

The DS3 PIM supports the following standards:

- ANSI T1.107, T1.102
- Telcordia GR 499-CORE, GR 253-CORE
- Telcordia TR-TSY-000009
- AT&T Technical Reference 54014
- ITU G.751, G.823

To configure the T3 interface, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > List > Edit (*interface*): Enter or select the applicable option value, 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
save
```

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*.

SSG 500M Series devices provide 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, see the *Attack Detection and Defense Mechanisms* volume in 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, see the Administration chapter in the *Administration* volume of the *Concepts & Examples ScreenOS Reference Guide*.
- Using the device serial number.

To reset the device to factory defaults using the serial number, perform the following steps:

1. At the Login prompt, enter the serial number of the device.
2. At the Password prompt, enter the serial number again. The following message appears:

```
!!! Lost Password Reset !!! You have initiated a command to reset the device to
factory defaults, clearing all current configuration and settings. Would you like to
continue? y/[n]
```

3. Press the **y** key. The following message appears:

```
!! Reconfirm Lost Password Reset !! If you continue, the entire configuration of the
device will be erased. In addition, a permanent counter will be incremented to
signify that this device has been reset. This is your last chance to cancel this
command. If you proceed, the device will return to factory default configuration,
which is: device IP: 192.168.1.1; username: netscreen; password: netscreen.
Would you like to continue? y/[n]
```

4. Press the **y** key to reset the device.

You can now log in using **netscreen** as the default admin name and password.

- Using the reset config button on the front panel of the device.

You can reset the device and restore the factory default settings by pressing the reset config button. 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 35.

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

1. Locate the reset config button on the front panel. Push the config button 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 device 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 config button 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 restart messages. The device generates SNMP and SYSLOG alerts to configured SYSLOG or SNMP trap hosts.

After the device has restarted, the Console displays the login prompt for the device. The STATUS LED blinks green. The login for username and password is **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 a Device

This chapter describes service and maintenance procedures for SSG 500M Series devices. It includes the following sections:

- “Required Tools and Parts” on this page
- “Physical Interface Modules” on page 50
- “Device Power Components (SSG 550M Only)” on page 52
- “Upgrading Memory” on page 55
- “Replacing an Air Filter” on page 57

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 should be familiar with standard practices for preventing accidents.

Required Tools and Parts

To replace a component on an SSG 500M Series device, you need the following tools and parts:

- Electrostatic bag or antistatic mat
- Electrostatic discharge (ESD) grounding wrist strap
- Flat-tip screwdriver, 1/8-inch
- Number-2 phillips screwdriver

Physical Interface Modules

Both SSG 500M Series devices have six slots in the front panel for Ethernet or WAN physical interface modules (PIMs). PIMs are field installable and replaceable.



WARNING: Make sure the device is powered off before removing PIMs. PIMs are not hot-swappable.

Removing a Blank Faceplate

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

To remove a blank faceplate, perform the following steps:

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to the ESD point on the device chassis or to an outside ESD point if the device is disconnected from earth ground.
2. Press and release the power button to power off the device. Verify that the POWER LED blinks and then turns off.
3. Loosen and remove the screws on each side of the faceplate using a 1/8-inch flat-tip screwdriver.
4. Remove the faceplate by grasping the handles on each side of the faceplate.

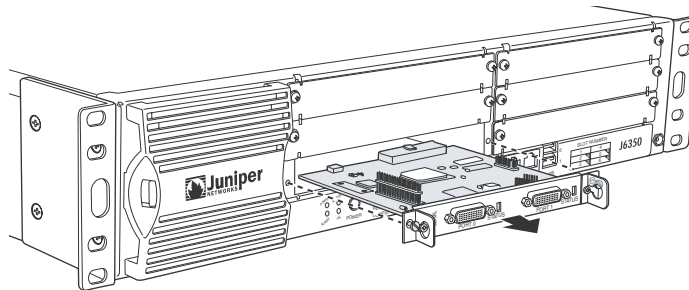
Removing a PIM

To remove a PIM, perform the following steps:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface to receive the 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 device is disconnected from earth ground.
3. Press and release the power button to power off the device. Verify that the POWER LED blinks and then turns off.
4. Label the cables connected to the PIM so that you can later reconnect each cable to the correct PIM.
5. Disconnect the cables from the PIM.

6. If necessary, arrange the cables to prevent them from dislodging or developing stress points:
 - Secure the cable so that it is not supporting its own weight as it hangs to the floor.
 - Place excess cable out of the way in a neatly coiled loop.
 - Use fasteners to maintain the shape of cable loops.
7. Loosen and remove the screws on each side of the PIM faceplate using a 1/8-inch flat-tip screwdriver.
8. Grasp the handles on each side of the PIM faceplate, and slide the PIM out of the device (Figure 24). Place it in the electrostatic bag or on the antistatic mat.

Figure 24: Removing/Installing a Physical Interface Module



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

Installing a PIM

To install a 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 device is disconnected from earth ground.
2. Press and release the power button to power off the device. Verify that the POWER LED blinks and then turns off.
3. Grasp the handles on each side of the PIM faceplate, and align the notches in the connector at the rear of the PIM with the notches in the PIM slot in the device. Then slide in the PIM until it lodges firmly in the device.



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

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

6. If necessary, arrange the cables to prevent them from dislodging or developing stress points:
 - Secure the cable so that it is not supporting its own weight as it hangs to the floor.
 - Place excess cable out of the way in a neatly coiled loop.
 - Use fasteners to maintain the shape of cable loops.
7. Press and release the power button to power on the device. Verify that the POWER LED lights steadily after you press the power button.
8. Verify that the PIM status LED glows steadily green to confirm that the PIM is online.

Device Power Components (SSG 550M Only)

The SSG 550M device has two load-sharing AC or DC power supplies located at the rear of the chassis. Each power supply provides power to all components in the device. The power supplies are fully redundant. If one power supply fails or is removed, the remaining power supply instantly assumes the entire electrical load. One power supply can provide full power for as long as the device is operational.

A power supply weighs 2.4 pounds. (1.1 kilogram.). Each power supply is hot-swappable. To replace a power-supply unit, use the procedures described in this section.



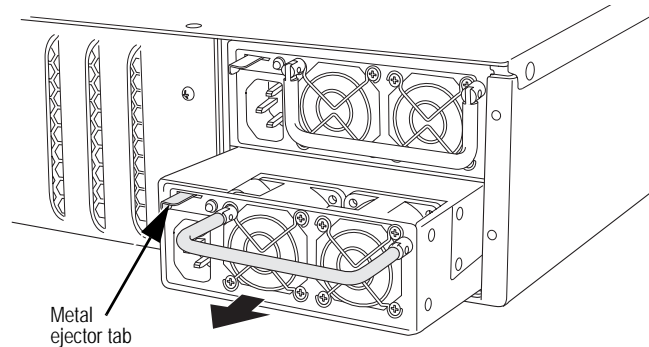
CAUTION: Do not leave a power supply slot empty while the device is operational. The power supply or a blank power-supply faceplate must remain in the chassis for proper airflow.

Removing a Power Supply Unit

To remove an AC power-supply unit (PSU) from a 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 power cord from the power-source receptacle.
3. Unplug the power cord from the appliance inlet on the power-supply faceplate.
4. With your thumb, slide the metal ejector tab on the power-supply faceplate to the right, and hold it in place to unlock the PSU.

Figure 25: Sliding AC/DC Power Supply Ejector Tab



5. Grasp the handle on the power supply faceplate, and pull firmly to start removing the power supply. Slide it halfway out of the chassis as shown in Figure 25.
6. Place one hand underneath the power supply to support it, then slide it completely out of the chassis.

NOTE: If you are not reinstalling a power supply into the emptied slot, install a blank power-supply faceplate over the slot.

To remove a DC PSU, 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.



WARNING: Before removing a DC PSU, you must shut off current to the DC feed wires that lead to the PSU.

2. Loosen the retaining screws on the terminal block.
3. Remove the feed wires.



CAUTION: Ensure that the DC cables do not touch the two screws on the chassis that are adjacent to the terminal block. Contact between the DC cables and the chassis screws will cause a circuit failure.

4. With your thumb, slide the ejector tab on the power supply faceplate to the right, and hold it in place to unlock the power supply.
5. Grasp the handle on the power supply faceplate, and pull firmly to start removing the power supply. Slide it halfway out of the chassis as shown in Figure 25.
6. Place one hand underneath the power supply to support it, then slide it completely out of the chassis.

NOTE: If you are not reinstalling a power supply into the emptied slot, install a blank power-supply faceplate over the slot.

Installing a Power Supply Unit

To install an AC PSU, 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. Using both hands, slide the PSU into the chassis until you feel resistance.
3. Firmly push the power supply into the chassis until it comes to a stop. Make sure that the PSU is flush with any other adjacent PSU.
4. Insert the appliance-coupler end of a power cord into the appliance inlet on the power-supply faceplate.
5. Insert the power-cord plug into an AC power-source receptacle.

NOTE: Each power supply must be connected to a dedicated AC power feed.

6. Verify that the power cord does not block access to device components or drape where people might trip on it.

To install a DC PSU, 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 device is disconnected from earth ground.



WARNING: Before installing a DC power supply, you must shut off current to the DC feed wires that lead to the power supply.

2. Using both hands, slide the PSU into the chassis until you feel resistance.
3. Firmly push the power supply into the chassis until it comes to a stop. Make sure that the PSU is flush with any other adjacent PSU.
4. Attach the feed wires to the terminal block.



CAUTION: Ensure that the DC cables do not touch the two screws on the chassis that are adjacent to the terminal block. Contact between the DC cables and the chassis screws will cause a circuit failure.

5. Tighten the retaining screws on the terminal block.
6. See “DC Power” on page 27 before turning on the current to the DC PSU.

Replacing a Power-Supply Cord

To replace the AC power cord for a redundant power supply, perform the following steps:

1. Locate a replacement power cord with the type of plug appropriate for your geographical location.
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 device is disconnected from earth ground.
3. Unplug the power cord from the power-source receptacle.
4. Unplug the power cord from the appliance inlet on the power-supply faceplate.
5. Insert the appliance-coupler end of the replacement power cord into the appliance inlet on the power-supply faceplate.
6. Insert the power-cord plug into an AC power-source receptacle.

NOTE: Each power supply must be connected to a dedicated AC power feed.

7. Verify that the power cord does not block access to device components or drape where people might trip on it.

Upgrading Memory

You can upgrade a device that has a single 256 MB single in-line memory module (SIMM) dynamic random access memory (DRAM) module to two 512 MB modules (1 GB of memory).

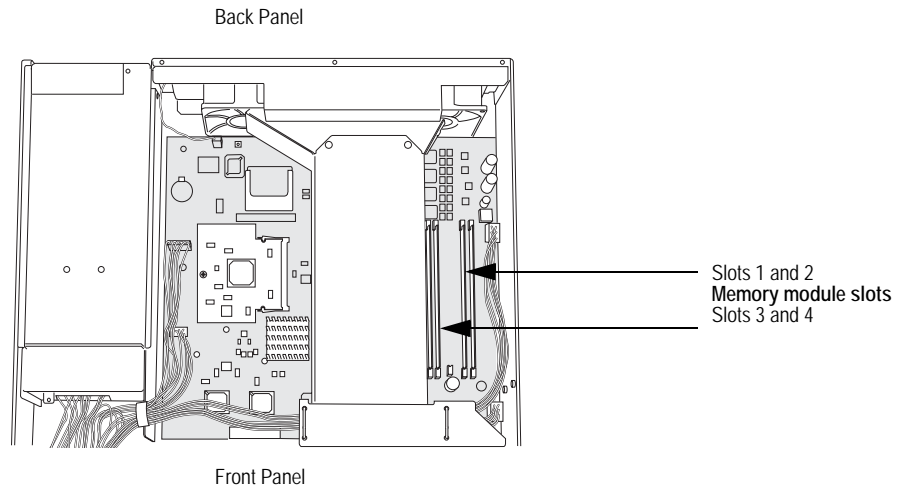
NOTE: The device must have 1 GB of memory installed to run ScreenOS content security features:

- Web filtering
 - Antivirus
 - Anti-spam
 - Intrusion protection system (deep inspection)
-

To upgrade the memory on a device, perform the following steps:

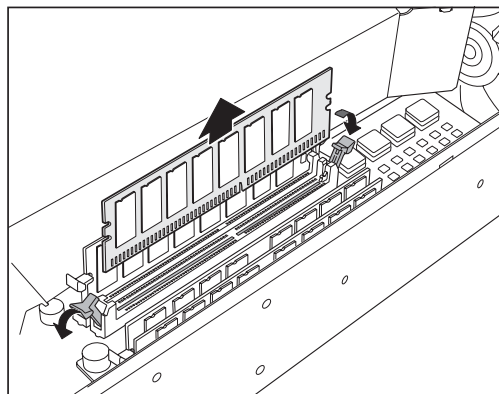
1. Attach an ESD grounding strap to your bare wrist, and connect the strap to the ESD point on the chassis or to an outside ESD point if the device is disconnected from earth ground.
2. Press and release the power button to power off the device. Verify that the POWER LED blinks and then turns off.

3. Use a phillips screwdriver to remove the screws from the top panel of the chassis. The screws are located at the rear and sides of the panel. Keep the screws nearby for use when closing the chassis later.
4. Grip the rear edge of the top panel, lift it up, and then remove it.
5. Locate the memory module slots (Figure 26).

Figure 26: Memory Module Slots

NOTE: Install 512 MB memory modules either in slots 1 and 3 or in slots 2 and 4. Do not install memory modules in adjacent slots.

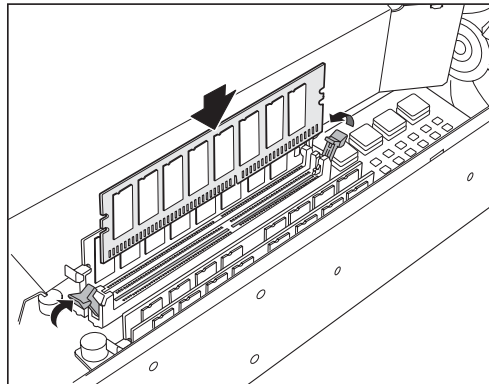
6. Release the 256 MB SIMM DRAM module by pressing your thumbs downward on the locking tabs on each side of the module so that the tabs swivel away from the module (Figure 27).

Figure 27: Removing a Memory Module

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

8. Insert one of the 512 MB SIMM DRAM modules into the slot from which you just removed the 256 MB SIMM DRAM module. 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 28).

Figure 28: Installing a Memory Module



9. Locate the appropriate slot for the second 512 MB SIMM DRAM module. Repeat step 8 to install the second memory module in the slot.
10. To replace the top panel on the chassis, set the front edge of the top panel into the groove that runs along the top front edge of the chassis. Then lower the top panel onto the chassis.
11. Use the phillips screwdriver to tighten the screws you removed earlier, securing the top panel to the chassis.

Replacing an Air Filter

The front panel of the device includes a cooling air vent. To prevent foreign particles from entering the device, the air vent includes a protective cover and, in some cases, a filter.

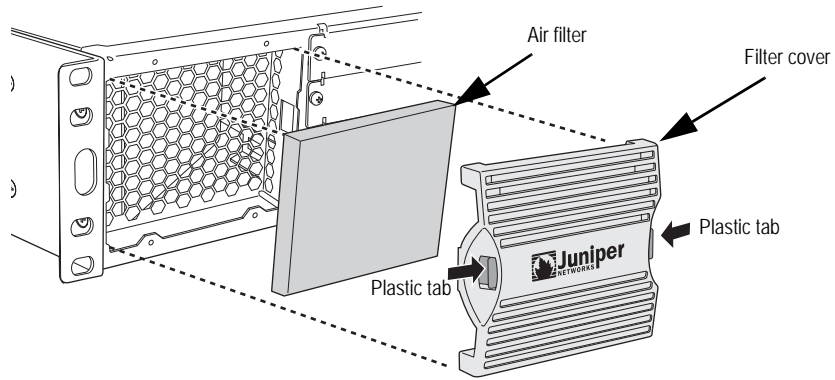
If the temperature alarm continues to appear, we recommend inspecting the fan filter. To remove a filter cover and replace a filter, use the procedures described in this section.

NOTE: Depending on the working environment where the device is located, we recommend changing the fan filter every six months. The fan filter SKU number is SSG-500-FLTR.

To remove an air filter, perform the following steps:

1. Remove the filter cover by squeezing the plastic tabs on each side of the filter cover.

Figure 29: Air Filter Components



2. Pull the filter cover away from the chassis.
3. Remove the old filter.
4. Place the new filter in the opening.
5. With your thumbs, push the front of the filter cover adjacent to each plastic tab until you hear each side click into place as shown in Figure 30.

Figure 30: Securing the Filter Cover



Appendix A

Specifications

This appendix provides general system specifications for an SSG 500M Series device. It includes the following sections:

- “Physical” on this page
- “Electrical” on page 62
- “Environmental Tolerance” on page 62
- “Certifications” on page 62
- “Connectors” on page 64

Physical

Table 9 provides the physical specifications for an SSG 500M Series device.

Table 9: SSG 500M Series Physical Specifications

Description	Value
Chassis dimensions	3.44 in. (8.74 cm) high
	17.44 in. (44.3 cm) wide—19.44 in. (49.38 cm) wide with mounting brackets attached
	21.13 in. (53.66 cm) deep—plus 0.5 in. (1.27 cm) of hardware that protrudes from the chassis front
Device weight	SSG 520M device:
	Minimum (no PIMs): 23 lb (10.4 kg)
	Maximum (six PIMs): 25.3 lb (11.5 kg)
	SSG 550M device:
Minimum (no PIMs and one power supply): 25.5 lb (11.6 kg)	
Maximum (six PIMs and two power supplies): 30.7 lb (13.9 kg)	

Electrical

Table 10 provides the electrical specifications for an SSG 500M Series device.

Table 10: SSG 500M Series Electrical Specifications

Item	Specification
AC input voltage	Operating range: 100 to 240 VAC
AC input line frequency	50 or 60 Hz
AC system current rating (SSG 520M)	6 A
AC system current rating (SSG 550M)	8 A
DC input voltage	Operating range: -48 to -60 VDC
DC system current rating	20 A

Environmental Tolerance

Table 11 provides the environmental tolerance for an SSG 500M Series device.

Table 11: SSG 500M Series Environmental Tolerance

Description	Value
Altitude	No performance degradation to 10,000 ft (3048 m)
Relative humidity	Normal operation ensured in relative humidity range of 5% to 90%, noncondensing
Temperature	Normal operation ensured in temperature range of 32°F (0°C) to 104°F (40°C) Non-operating storage temperature in shipping carton: -40°F (-40°C) to 158°F (70°C)
Seismic	Designed to meet Telcordia Technologies Zone 4 earthquake requirements
Maximum thermal output	SSG 520M chassis: 1092 BTU/hour (320W) SSG 550M chassis: 1126 BTU/hour (330W)

Certifications

Table 12 provides the device certifications for an SSG 500M Series device.

Table 12: SSG 500M Series Device Certifications

Certification Type	Certification Name
NEBS	GR-63-CORE Issue 2, GR-1089-CORE Issue 3
Safety	CAN/CSA-C22.2 No. 60950-1-03/UL 60950-1 EN 60950-1 EN 60825-1 Safety of Laser Products - Part 1
EMC Emissions	FCC Part 15 Class B (USA) EN 55022 Class B (Europe, Australia, New Zealand) VCCI Class B (Japan)

Certification Type	Certification Name
EMC Immunity	EN 55024 EN-61000-3-2 Power Line Harmonics EN-61000-3-3 Voltage Fluctuations and Flicker 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-300386-2: 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

Table 13 lists the RJ-45 connector pinouts.

Table 13: 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

Table 14 provides the DB-9 connector pinouts.

Table 14: DB-9 Connector Pinouts

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

Table 15 provides the RJ-45 connector pinouts for the Gigabit Ethernet ports.

Table 15: Gigabit Ethernet RJ-45 Connector Pinout

Pin	Signal
1	MDI0 +
2	MDI0-
3	MDI1 +
4	MDI2 +
5	MDI2-
6	MDI1-
7	MDI3 +
8	MDI3-

Table 16 lists the cables that you can order from Juniper Networks to connect to a port on the serial PIM. The device to which you are connecting and the serial interface type determine which cable you need.

Table 16: Juniper Serial Cables

Product Number	Interface Type	Length (in feet)	Connector Type
JX-CBL-EIA530-DCE	EIA 530 (DCE)	10 feet	Female
JX-CBL-EIA530-DTE	EIA 530 (DTE)	10 feet	Male
JX-CBL-RS232-DCE	RS-232 (DCE)	10 feet	Female
JX-CBL-RS232-DTE	RS-232 (DTE)	10 feet	Male
JX-CBL-RS449-DCE	RS-449 (DCE)	10 feet	Female
JX-CBL-RS449-DTE	RS-449 (DTE)	10 feet	Male
JX-CBL-V35-DCE	V.35 (DCE)	10 feet	Female
JX-CBL-V35-DTE	V.35 (DTE)	10 feet	Male
JX-CBL-X21-DCE	X.21 (DCE)	10 feet	Female
JX-CBL-X21-DTE	X.21 (DTE)	10 feet	Male

The E1 and T1 PIMs use an RJ-48 cable, which is not supplied with the PIM.



CAUTION: To maintain agency approvals, use only a properly constructed, shielded cable.

Table 17 describe the RJ-48 connector pinouts.

Table 17: RJ-48 Connector to RJ-48 Connector (Straight) Pinout

RJ-48 Pin (on T1/E1 PIM) (Data Numbering Form)	RJ-48 Pin (Data Numbering Form)	Signal
1	1	RX, Ring, -
2	2	RX, Tip, +
4	4	TX, Ring, -
5	5	TX, Tip, +

Index

A

AC grounding	27
AC power supply	21, 22
installing	54
replacing cord	55
admin name and password	38
administrative access	38
alarm LED	11, 20

B

back panel components	20
-----------------------------	----

C

Cable connectors	10
cable connectors	
AUX	10
Console	10
Ethernet	10
PIMs	10
chassis grounding	22, 26
configuration	
admin name and password	38
administrative access	38
date and time	40
default route	40
DNS server	39
high availability	41
host and domain name	39
management services	39
Console port, using	35

D

date and time	40
DC grounding	28
DC power supply	22
installing	54
removing	53
default interface-to-zone bindings	34
default IP address	34
default route	40
device dimensions	61
device weight	24, 61
DNS server	39

E

E1 PIM	20
electrical specifications	62
environmental specifications	62
Ethernet ports, built-in	12

F

front panel components	11
------------------------------	----

G

gigabit Ethernet ports	12
grounding	22, 26

H

HA LED	11, 20
high availability, configuring	41 to 42
hostname and domain name	39

I

installation	
before you begin	24
chassis grounding	22, 26
connecting power	26
equipment rack	24

L

LEDs	
device status descriptions	11, 20
LAN ports	13
PIMs	15, 16

M

management services	39
managing	
through console	35
through Telnet	37
through WebUI	36
memory, upgrading	55

P

PIMs	
Copper Gigabit Ethernet	16
E1	20
Four-Port Fast Ethernet	19

installing.....	51
Optical Gigabit Ethernet.....	17
Serial.....	17
status LEDs.....	15, 16
T1.....	18
T3.....	19
power LED.....	11, 20
power supplies	
AC.....	21, 22
AC, removing.....	52
connecting.....	26
DC.....	22
DC, removing.....	53
installing.....	54
replacing.....	52
R	
rack mount.....	25
reset	
config button, using.....	48
S	
shutting down a device.....	29
slot numbering.....	15
status LED.....	11, 20
T	
T1 PIM.....	18
T3 PIM.....	19
Telnet, using.....	37
W	
WAN slots.....	15
WebUI, using.....	36
weight of device.....	61
Z	
zones, default bindings.....	34