**Security Products**

# Secure Services Gateway (SSG) 500 Series Hardware Installation and Configuration Guide

*ScreenOS Version 5.4.0*

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Part Number: 530-015646-01, Revision A

### 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

A Juniper Networks Secure Services Gateway (SSG) 500 series device is an integrated router and firewall platform designed for enterprise edge environments. Juniper Networks offers two models of the SSG 500 series device:

- SSG 520
- SSG 550

Both of the SSG 500 series devices support universal storage bus (USB) storage and six physical interfaces modules (PIM) slots that can hold any of the PIMs. The devices also provide conversions between local area networks (LANs) and wide area networks (WANs).

## Organization

This guide contains the following chapters and appendix:

Chapter 1, “Hardware Overview,” describes the chassis and components of an SSG 500 series device.

Chapter 2, “Installing and Connecting the Device,” describes how to install an SSG 500 series device in a standard 19-inch equipment rack and connect the cables and power supplies.

Chapter 3, “Configuring the Device,” describes how to configure and manage an SSG 500 series device and how to perform some basic configuration tasks.

Chapter 4, “Servicing the Device,” describes service and maintenance procedures for an SSG 500 series device.

Appendix A, “Specifications,” provides general system specifications for both of the SSG 500 series devices.

## Document Conventions

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



### *CLI 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.

---

### *WebUI Conventions*

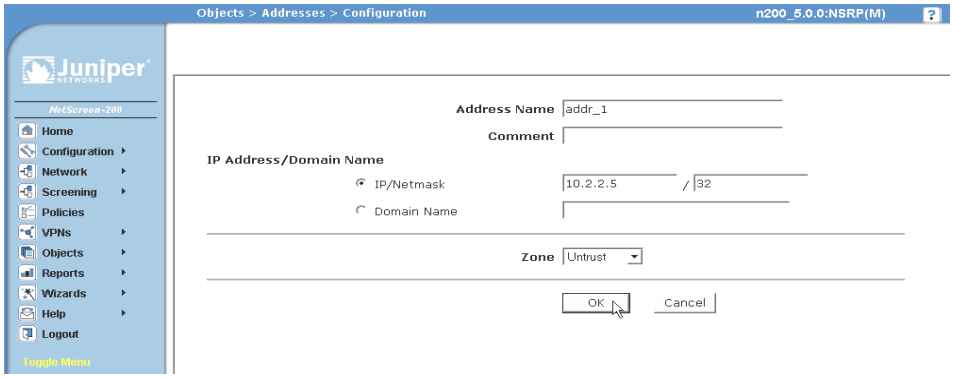
To perform a task with the WebUI, you first navigate to the appropriate dialog box, where you then define objects and set parameters. A chevron ( > ) shows the navigational sequence through the WebUI, which you follow by clicking menu options and links. The set of instructions for each task is divided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




## 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) 500 series security devices, namely the SSG 520 and SSG 550 chassis and components. It includes the following topics:

## Front Panel

The front panel of an SSG 500 series device contains the following components:

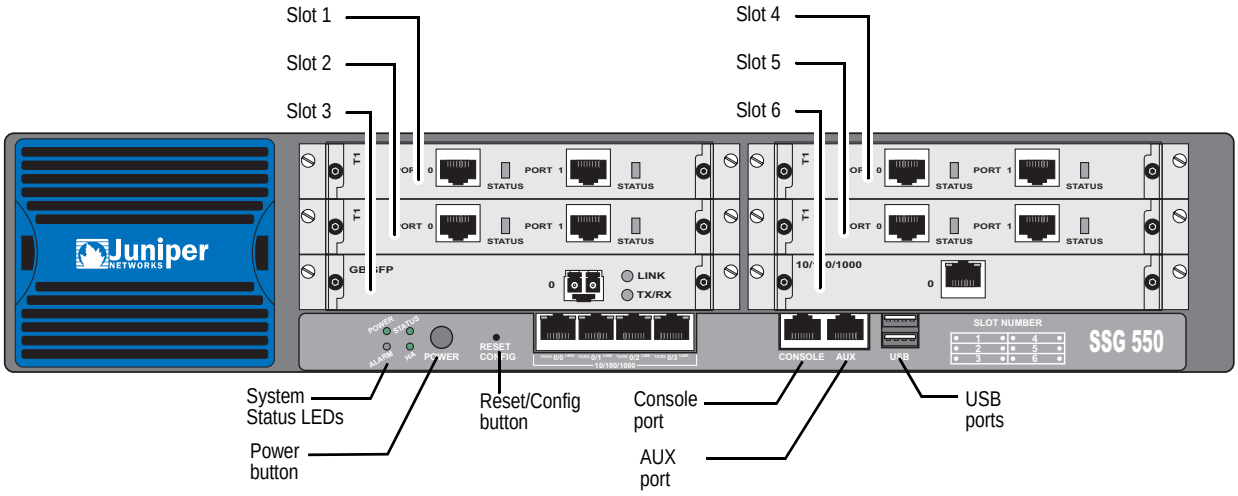
- System status LEDs
- Power button
- Reset configuration pinhole

**NOTE:** The reset configuration is currently not supported.

- Four built-in 10/100 Gigabit Ethernet ports for local area network (LAN) connections
- A console port
- An auxiliary (AUX) port
- A Universal Serial Bus (USB) 1.1 host module for storage
- Six front panel slots for user-installable Physical Interface Modules (PIMs)

**NOTE:** GBE and 4FE PIMs can only be installed in LAN connectivity slots. See Table 4 and Table 5 on page 7 for applicable slot and PIM types.

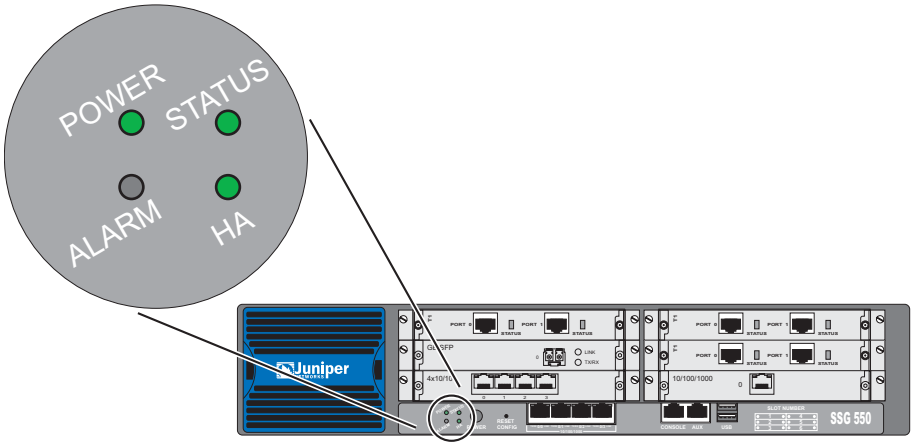
**Figure 2: Front Panel of a Secure Services Gateway Device**



## *System Status LEDs*

The system status LEDs display information about critical device functions. Figure 3 illustrates the position of each system status LED.

**Figure 3: System Status LEDs**




When the system powers up, the STATUS LED changes from off to blinking green. Startup takes approximately 90 seconds to complete. If you want to turn the system off and on again, we recommend waiting a few seconds between shutting it down and powering it back up.

Table 1 shows the name, color, status, and description for each LED.

**Table 1: LED Descriptions**

| Name | Color | Status | Description |
|---|---|---|---|
| POWER | Green | On steadily | Indicates that the system is receiving power |
| | Red | On steadily | Indicates Power Supply Unit (PSU) failure |
| | | Off | System is not receiving power |
| STATUS | Green | On steadily | Startup or performing diagnostics. |
| | | Blinking | Normal operation |
| | Red | Blinking | Error detected |

| Name | Color | Status | Description |
|---|---|---|---|
| ALARM | Red | On steadily | Critical alarm:<br>■ Failure of hardware component or software module<br>■ Firewall attacks detected |
| | Amber | On steadily | Major alarm:<br>■ Low memory (less than 10 % remaining)<br>■ High CPU utilization (more than 90 % in use)<br>■ Session full<br>■ Maximum number of VPN tunnels reached<br>■ HA status changed or redundant group member not found |
| | | Off | No alarms |
| HA (High Availability) | Green | On steadily | Unit is the primary (master) device |
| | Amber | On steadily | Unit is the secondary (backup) device |
| | | Off | High availability not enabled |

### *Power Button*

The power button is located on the left side of the front panel. You can use the power button to power an SSG 500 series device on and off. When you power on the device, ScreenOS boots up as the power supply completes its startup sequence.

### *Reset Config Button*

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

### *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, ethernet0/1, ethernet0/2, and ethernet0/3.

The built-in Gigabit Ethernet ports are bound by default to specific zones, as shown in Table 2.

**Table 2: Ethernet Ports Bound to Zones**

| Ethernet Port | Zone |
|---|---|
| ethernet0/0 | Trust (default IP address 192.168.1.1/24) |
| ethernet0/1 | DMZ |
| ethernet0/2 | Untrust |
| ethernet0/3 | HA |

Each port has two LEDs located on the bottom of the port.

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

**Figure 4: Activity Link LEDs**

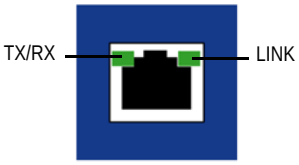



Table 3 describes the Ethernet port LEDs.

**Table 3: LAN Port LEDs**

| Function | Color | State | Description |
|---|---|---|---|
| Link | Green | On steadily | Port is online |
| 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 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 3 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 3 for the RJ-45 connector pinouts.

### *Universal Serial Bus (USB) Host Modules*

The slots labeled USB on the front panel of an SSG 500 series device implements a host-only USB 1.1 host module for a USB device adapter or USB flash key, as defined in the *CompactFlash Specification* published by the CompactFlash Association. When the USB storage device, or flash key, is installed and configured, it automatically acts as a secondary storage device.

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

To use a USB flash key to transfer files between the device, perform the following steps:

1. Insert the USB flash key into the USB host module on the security device.
2. Save the files from the USB flash key 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 flash key, stop the host module with the **exec usb-device stop** CLI command.
4. It is now safe to remove the USB flash key.

To save files from a USB flash key to the device, use the save { software | config | image-key } from usb *filename* to flash CLI command.

If you want to delete a file from the USB flash key, use the **delete file** *path:/filename* CLI command.

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

### *Physical Interface Modules*

All SSG 500 series devices have six PIM slots. Table 4 shows the PIM types you can install in the slots of an SSG 520. Table 5 on page 7 shows the PIM types you can install in the slots of an SSG 520.

**Table 4: PIM Slots, SSG 520**

| Slot | PIM Types | Slot | PIM Types |
|---|---|---|---|
| **1** | **WAN Connectivity**<br>Serial, T1/E1, DS3 | **4** | **WAN Connectivity**<br>Serial, T1/E1, DS3 |
| **2** | **WAN Connectivity**<br>Serial, T1/E1, DS3 | **5** | **WAN Connectivity**<br>Serial, T1/E1, DS3 |
| **3** | **LAN or WAN Connectivity**<br>10/100/1000, SFP,<br>FE Serial, T1/E1, DS3 | **6** | **LAN or WAN Connectivity**<br>10/100/1000, SFP,<br>FE Serial, T1/E1, DS3 |

**Table 5: PIM Slots, SSG 550**

| Slot | PIM Types | Slot | PIM Types |
|---|---|---|---|
| **1** | **WAN Connectivity**<br>Serial, T1/E1, DS3 | **4** | **WAN Connectivity**<br>Serial, T1/E1, DS3 |
| **2** | **LAN or WAN Connectivity**<br>10/100/1000, SFP,<br>FE Serial, T1/E1, DS3 | **5** | **LAN or WAN Connectivity**<br>10/100/1000, SFP,<br>FE Serial, T1/E1, DS3 |
| **3** | **LAN or WAN Connectivity**<br>10/100/1000, SFP,<br>FE Serial, T1/E1, DS3 | **6** | **LAN or WAN Connectivity**<br>10/100/1000, SFP,<br>FE Serial, T1/E1, DS3 |

Each Physical Interface Module (PIM) supported on an SSG 500 series device has the following components:

- One or more cable connector ports—Accepts a network media connector.
- Status LED—Indicates port status. Table 6 describes the meaning of the LEDs.

**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. |

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

## Ethernet PIMs

There are four built-in 10/100 Gigabit Ethernet ports on an SSG 500 series device, and you can also add additional Ethernet ports by installing Ethernet PIMs. For an SSG 520 device, you can install up to two Ethernet PIMs in slots 3 and 6. For an SSG 550 device, you can install up to four Ethernet PIMs in slots 2, 3, 5, and 6.

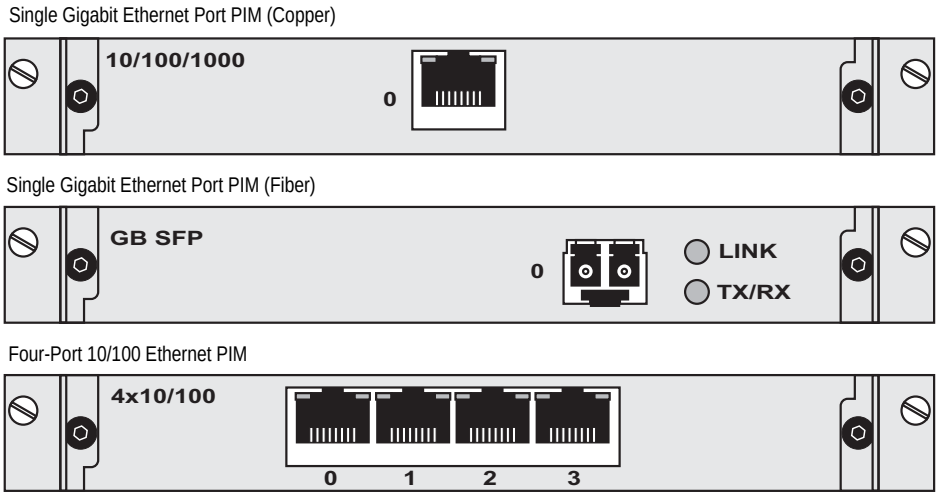
SSG devices support Ethernet PIMs with one of the following port configurations:

- One Gigabit Ethernet port (copper or fiber)
- Four 10/100 Fast Ethernet ports

The PIM with one Gigabit Ethernet port provides connectivity to Gigabit Ethernet LANs. Connect the module using a single-mode or multimode optical cable.

Figure 5 shows the available Ethernet PIMs.

**Figure 5: Ethernet PIMs**




## Wide Area Network Physical Interface Modules

Wide Area Network (WAN) PIMs allow you to connect an SSG device to geographically dispersed networks. These networks can be privately owned, but more often include public or shared networks. You can install up to six WAN PIMs in either SSG model.

SSG 500 series devices support WAN PIMs with one of the following port configurations:

- Two serial ports—Serial PIM
- Two T1 ports—T1 PIM
- Two E1 ports—E1 PIM
- One T3 port—T3 PIM

The PIM with two serial ports provides full-duplex, synchronous data transmission at up to 8 Mbps over serial links. Figure 6 shows the Two-port serial WAN PIM.

**Figure 6: Two-Port Serial Wide Area Network Physical Interface Module**

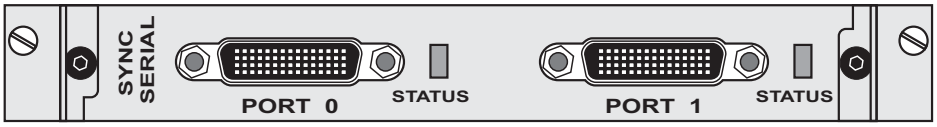


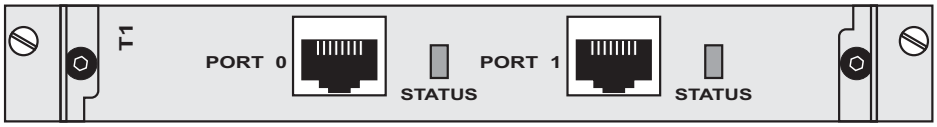
Table 7 lists the cables that you can order from Juniper Networks to connect to a port on the serial PIM. The device to which you are connecting and the serial interface type determine which cable you need.

**Table 7: 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 |

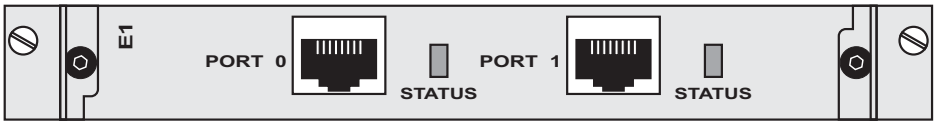
The PIM with two T1 ports provides connection to T1 or fractional T1 network media types.

**Figure 7: T1 Wide Area Network Physical Interface Module**



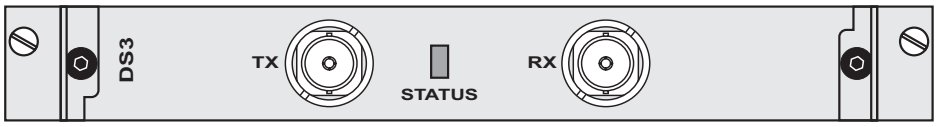

The PIM with two E1 ports provides connection to E1 or fractional E1 network media types.

**Figure 8: E1 Wide Area Network Physical Interface Module**




The PIM with a single T3 port pair provides connection to T3 network media types.

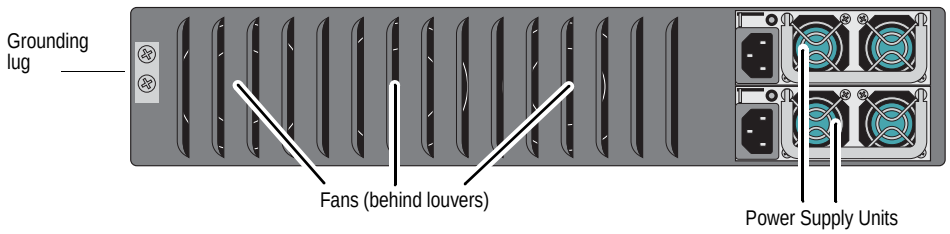
**Figure 9: T3 Wide Area Network Physical Interface Module**



## Back Panel

The back panel of the device contains the fan tray and power supply unit(s). The back panel also includes a two-hole grounding lug (at the left edge).

**Figure 10: Back Panel of an SSG 500 Series Device**




### *Fans*

SSG 500 series devices have a single fixed-mounted three-fan tray.

### *Power Supplies*

Power supplies are located at the right side of the rear panel of an SSG 500 series device:

- The SSG 520 is equipped with a single permanently-installed AC or DC power supply unit (PSU).
- The SSG 550 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.

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

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

The input power light on the faceplate of an SSG 550 AC or DC PSU indicates the power and system status. Table 8 describes the LED states:

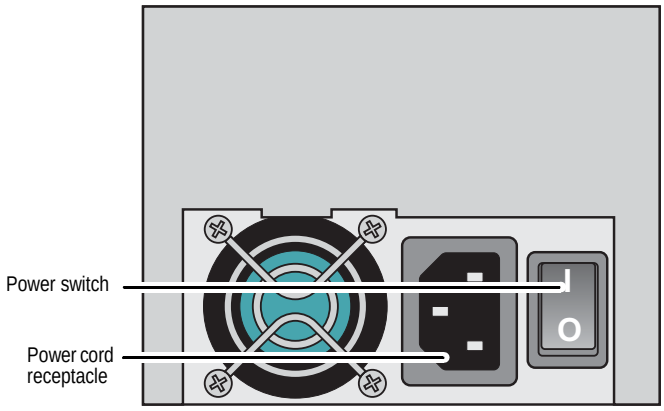
**Table 8: Input Power LED Descriptions**

| Color | Status | Description |
|---|---|---|
| Green | On steadily | Input power is On and system is On |
| Amber | On steadily | Input power is On and system is Off |
| | Off | Input power is Off |

## AC Power Supply

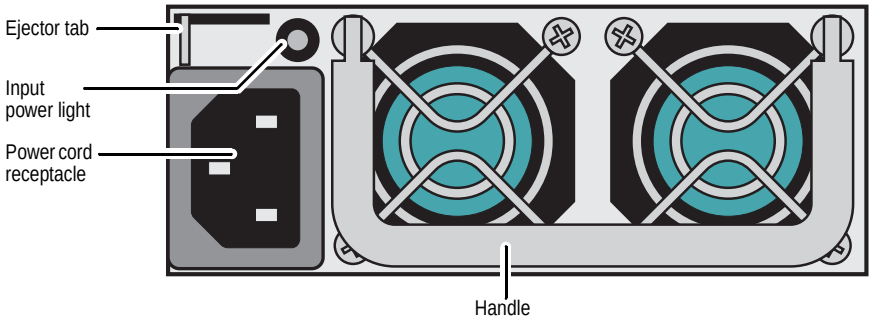
The AC PSU faceplate for an SSG 520 contains a power switch and a male power cord receptacle.

**Figure 11: SSG 520 AC Power Supply Faceplate**




Each AC PSU faceplate for an SSG 550 contains an ejector tab and a power cord receptacle.

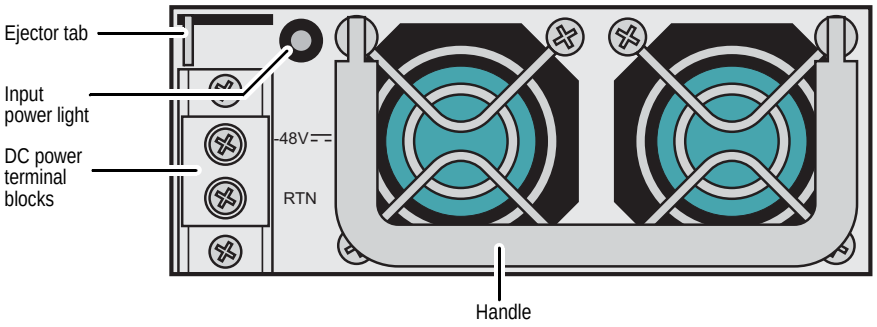
**Figure 12: SSG 550 AC Power Supply Faceplate**




## DC Power Supply

The DC PSU faceplate contains two DC power terminal blocks that connect to power cables.

**Figure 13: SSG 550 DC Power Supply Faceplate**



### *Grounding Lug*

A two-hole grounding lug is provided on the rear of the chassis to connect the device to earth ground (see Figure 10 on page 10).

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 16.

Chapter 2

# Installing and Connecting the Device

This chapter describes how to install an SSG 500 series device in a standard 19-inch equipment rack and how to connect cables and power to the device. Topics in this chapter include:



**NOTE:** For safety warnings and instructions, please 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 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 system 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 3 feet (1 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.

## Equipment Rack Installation

You can mount an SSG 500 series device into a standard 19-inch equipment rack. The device is shipped with mounting brackets.

**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 an SSG 500 series device, you need a 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 500 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 500 series device into a rack:

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 14: Mid-mount Rack Installation**


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

## Connecting the Interface Cable to the 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 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, an SSG 500 series 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 10 on page 10).

**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 AC Power to the Device

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 power to the device:

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:

    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 500 series device.

4. For each power supply:

    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.

## Connecting DC Power to the Device

Each DC power supply 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 power supply, 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 earthing 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 power to the device:

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:

   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.

3. For each power supply:

   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.

   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 the Device On and Off

To power on an SSG 500 series device, press the power button. ScreenOS boots as the power supply completes its startup sequence. The POWER LED lights during startup and remains on steadily when the device is operating normally.

**NOTE:** The power supply unit in the rear panel of the device may include a power switch. If included, make sure this switch is in the ON position.

To power off an SSG 500 series device, do one of the following:

- Graceful shutdown—Press and release the power button. The device shuts down the operating system and then powers itself off.
- Immediate shutdown—Press the power button and hold it for more than 5 seconds. The device immediately powers itself off without shutting down the operating system.

To remove power completely from the device, unplug the power cord. The power button on an SSG 500 series 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.

## Connect the Device to a Network

An SSG 500 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:

- Connect an SSG 500 Series Device to an Untrusted Network
- Connect WAN PIMs to an Untrusted Network
- Connect the Device to an Internal Network or a Workstation

## *Connect an SSG 500 Series Device to an Untrusted Network*

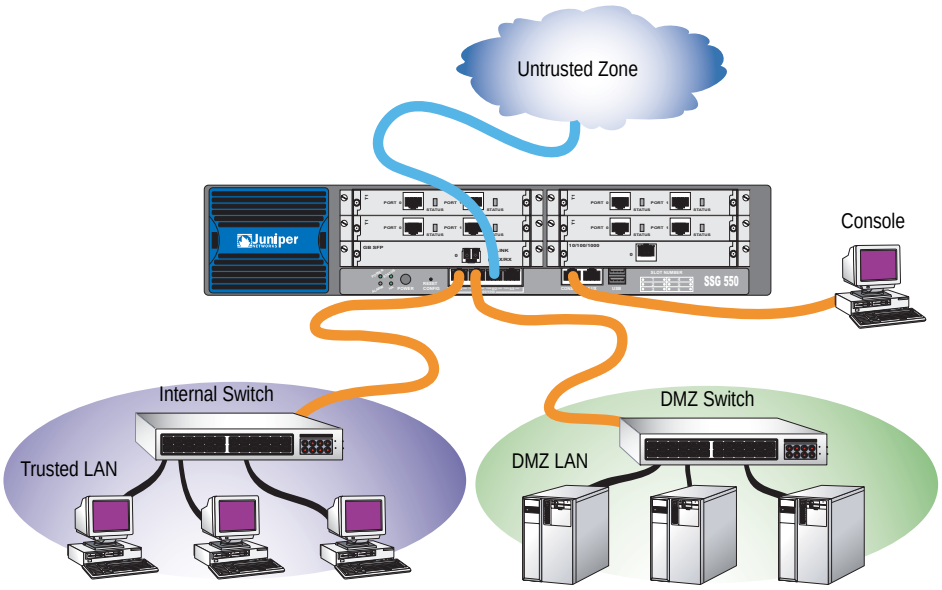
You can connect your SSG 500 series device to the untrusted network in one of the following ways:

- Connecting Ethernet Ports
- Connecting Serial AUX/Console Ports
- Connect WAN PIMs to an Untrusted Network

Figure 15 shows an SSG 500 series device with basic network cabling connections and the 10/100 Ethernet ports cabled as follows:

- The port labeled 0/0 (ethernet0/0 interface) is connected to a switch that connects workstations to the trusted network and is prebound to the Trust security zone.
- The port labeled 0/1 (ethernet0/1 interface) is connected to a switch that connects workstations on the DMZ LAN and is prebound to the DMZ security zone.
- The port labeled 0/2 (ethernet0/2 interface) is connected to the untrusted network and is prebound to the Untrust security zone.
- The console port is connected to a serial terminal for management access.

**Figure 15: Basic Networking Example**




### Connecting Ethernet Ports

To establish a high-speed connection, connect the provided Ethernet cable from the Ethernet port marked 0/0 on an SSG 500 series to the external router. The device autosenses the correct speed, duplex, and MDI/MDIX settings.

### Connecting Serial AUX/Console 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.

## *Connect WAN PIMs to an Untrusted Network*

This section explains how to connect WAN PIMs to an untrusted network.

### T1, E1, E3, and Serial PIMs

To connect the 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 T1, E1, T3, or Serial PIM, see "WAN PIM Interface Configuration" on page 30.

## *Connect the 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. An SSG 500 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 Settings" on page 25 for the default zone to interface bindings.

Chapter 3
# Configuring the Device

ScreenOS software is preinstalled on SSG 500 series devices. 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 describes the following topics:



**NOTE:** After you configure an SSG 500 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 Signature Service and Anti-Virus, 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.

## Access the Device

You can access, configure, and manage an SSG 500 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 Web browser. To initially use the WebUI, the workstation on which you run the Web 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 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, see the *Administration* volume of the *Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.4.0.

- NetScreen-Security Manager: NetScreen-Security Manager 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*.

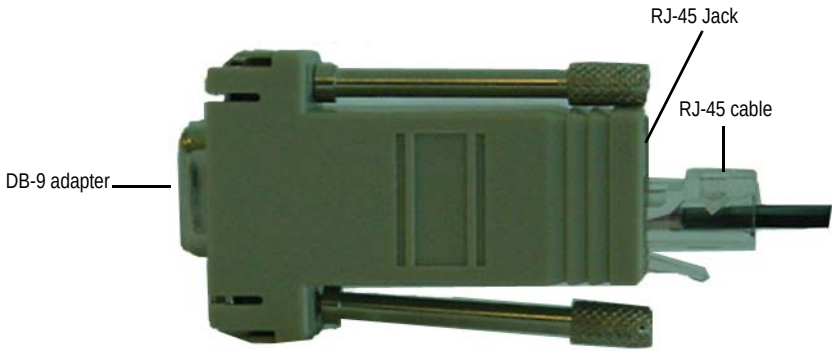
## *Using a Console Connection*

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

To establish a console connection, do the following:

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 16: 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**.

### *Using the WebUI*

To use the WebUI, you must be on the same subnetwork as the device. To access the device with the WebUI browser interface:

1. Connect your workstation to the ethernet0/0 port, 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.)

### *Using Telnet*

To establish a Telnet connection, do the following:

1. Connect your workstation to the ethernet0/0 port on the device.

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**.

## Default Settings

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

Figure 17 shows basic network cabling connections for an SSG 500 series device. This figure shows one T1 Physical Interface Module (PIM) in slot 1 of an SSG 500 series device; port 0 in the PIM (serial1/0) provides connection to the Internet. The built-in 10/100/1000 gigabit Ethernet ports are cabled as follows:

- The left port (ethernet0/0) is connected to a switch that connects workstations on the Trusted LAN.

- The middle left port (ethernet0/1) is connected to a switch that connects workstations on the DMZ LAN; the right and middle right ports (ethernet0/2 and ethernet0/3) are not connected.
- The console port is connected to a serial terminal for management access.

**Figure 17: Basic Cable Connections for a Secure Services Gateway Device**

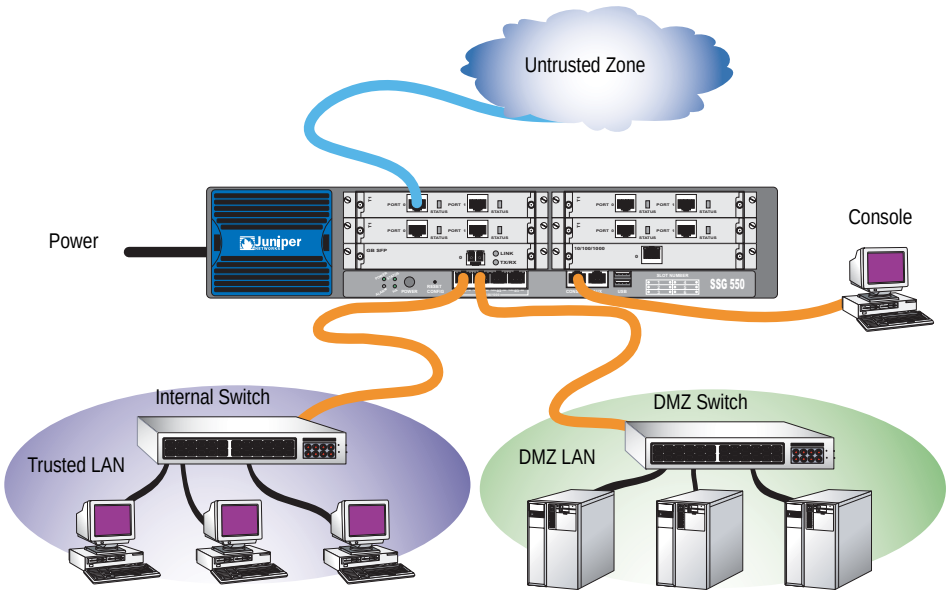



Table 9 describes the default zone bindings for ports on an SSG 500 series device. The cable connections shown in Figure 17 use the default settings of some of the ports.

**Table 9: Default Port and Zone Bindings for an SSG 500 Series Device**

| Port | Zone Binding |
|---|---|
| **Built-in 10/100 Gigabit Ethernet ports:** | |
| ethernet0/0 (default IP address is 192.168.1.1/24) | Trust |
| ethernet0/1 | DMZ |
| ethernet0/2 | Untrust |
| ethernet0/3 | HA |
| WAN PIM ports | Untrust |
| Ethernet PIM 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.

## Configuring the Device

This section describes the basic configurations that you need to perform to allow an SSG 500 series device to connect LAN users to a remote network. For more detailed information about ScreenOS features and how to configure them, see the *Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.4.0.

This section describes the following basic configurations:



### *Changing the Admin Name and Password*

The admin user has complete privileges to configure an SSG 500 series device. We recommend that you change the default admin name (netscreen) and password (netscreen) immediately.

#### *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 an SSG 500 series device if they know the login and password. To configure an SSG 500 series device to be managed only from a specific host on your network, use the WebUI or CLI:

***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 an SSG 500 series 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:

***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
```

## Domain Name System Server

The Domain Name System (DNS) server on the network maintains a database for resolving hostnames and IP addresses. An SSG 500 series 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:

***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
```

## Setting the Date and Time

The time set on an SSG 500 series device affects 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 system clock on the device with the clock on your workstation. To configure the date and time on the device, use the WebUI or CLI:

### 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 CLI set clock command in a Telnet or console session to manually enter the date and time for the device.

## 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 an SSG 500 series device in the network. To configure the hostname and domain name on the device, use the WebUI or CLI:

### WebUI

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

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

### CLI

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

## Management Interface Address

The ethernet0/0 port has the default IP address 192.168.1.1/24 and is configured for management services. If you connect the ethernet0/0 port on an SSG 500 series 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. For example, you might want to change the interface to match IP addresses that already exist on your LAN.

### *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:

#### *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
```

### *Ethernet0/0 IP Address*

You can change the default IP address of the ethernet0/0 interface to match addresses that already exist on your Trusted LAN. To change an interface IP address on the device, use the WebUI or CLI:

#### *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
```

## WAN PIM Interface Configuration

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



Interfaces on WAN PIMs are bound to the Untrust zone by default. See the *Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.4.0 for more information about configuring WAN interfaces.

## The 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 terminal equipment (DTE). DTE is typically where a link terminates.

SSG 500 series serial WAN PIMs support the following serial standards:

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

To configure serial interface characteristics, use the WebUI or CLI:

***WebUI***

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

DTE Options
    Select your options

***CLI***

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

## The 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 devices support the following T1 DS-1 standards:

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

To configure the T1 PIM, use the WebUI or CLI:

***WebUI***

Network > Interfaces > List > Edit (WAN 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

Click **OK**.

***CLI***

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

For information on how to configure the T1 interface, refer to the *Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.4.0.

## The T3 Interface

T3, also known as data signal 3 (DS3), is a high-speed data-transmission medium formed by multiplexing 28 DS1signals into seven separate DS2 signals, and combining the DS2 signals into a single DS3 signal. T3 links operate at 43.736 Mbps.

The devices support the following T3 DS-3 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 PIM, use the WebUI or CLI:

***WebUI***

Network > Interfaces > List > Edit (WAN 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

Click **OK**.

***CLI***

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

For information on how to configure the T3 interface, refer to the *Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.4.0.

## *The 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 PIM, use the WebUI or CLI:

***WebUI***

Network > Interfaces > List > Edit (WAN 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

Click **OK**.

***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* for ScreenOS 5.4.0.

## 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 and Examples ScreenOS Reference Guide* for ScreenOS 5.4.0.

SSG 500 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 an 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:

***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* for ScreenOS 5.4.0.

## Verify 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.

## Reset the 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* for ScreenOS 5.4.0.
- Using the reset pinhole on the back panel of the device, as described in the next section.

### *The Reset Pinhole*

You can reset the device and restore the factory default settings by pressing the reset pinhole. To perform this operation, you need to either view the device status LEDs on the front panel or start a Console session as described in Using a Console Connection on page 24.

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 paper clip), 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 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 the Device

This chapter describes service and maintenance procedures for SSG 500 series devices. It includes the following topics:



**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.

## Tools and Parts Required

To replace a component on an SSG 500 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

## Replacing a Physical Interface Module

Both SSG 500 series models have six slots in the front panel for Ethernet or WAN PIMs. PIMs in an SSG 500 series device are field installable and replaceable. The device must be powered off before PIMs are removed or installed.

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

The PIMs are installed in the front panel of an SSG 500 series device. A PIM weighs less than 1 pound (0.5 kilogram).

### *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 blank faceplates unless you are installing a PIM in the empty slot.

To remove a blank faceplate, do the following:

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 device 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. Loosen and remove the screws on each side of the faceplate using a 1/8-inch slotted screwdriver.
5. Remove the faceplate by grasping the handles on each side of the faceplate. Place it in the electrostatic bag or on the antistatic mat.

### *Removing a Physical Interface Module*

To remove a PIM, do the following:

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:

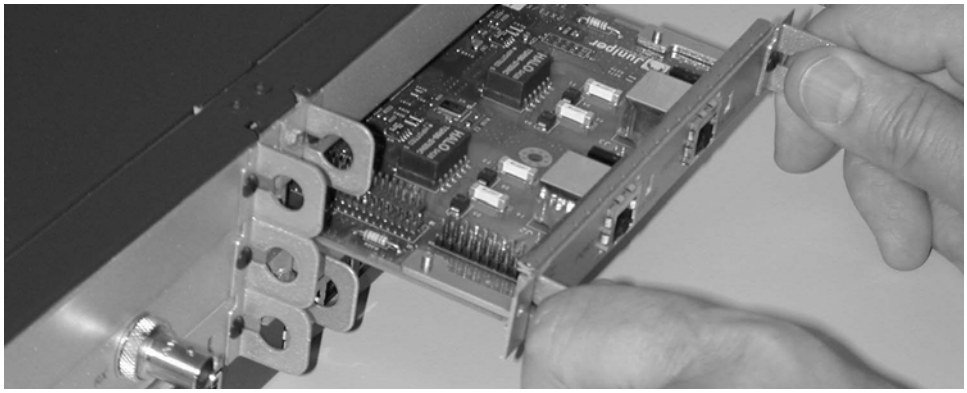
   - Secure the cable so that it is not supporting its own weight as it hangs to the floor.
   - Place excess cable out of the way in a neatly coiled loop.
   - Use fasteners to maintain the shape of cable loops.

7. Loosen and remove the screws on each side of the PIM faceplate using a 1/8-inch slotted screwdriver.

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

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

**Figure 18: Removing/Installing a Physical Interface Module**



## *Installing a Physical Interface Module*

To install a PIM, do the following:

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 the PIM in 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 slotted 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 lights steadily green to confirm that the PIM is online.

## Replacing Power System Components (SSG 550 Devices Only)

The SSG 550 device has one or 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.

Each power supply is hot-insertable and hot-removable. To replace a power supply in an SSG 550 device, use the procedures described in this section.

### *Removing an AC Power Supply*

The power supplies are located at the right rear of the chassis. A power supply weighs 2.4 lb. (1.1 kg.).

**CAUTION:** Do not leave a power supply slot empty for more than a short time while the device is operational. The power supply or a blank power supply panel must remain in the chassis for proper airflow.

To remove an AC power supply from an SSG 550 device, perform the following steps:

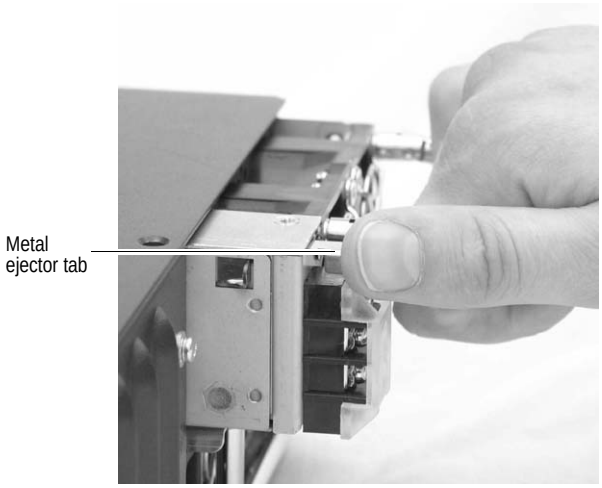
1. Attach an ESD grounding strap to your bare wrist, and connect the strap to the ESD point on the chassis or to an outside ESD point if the SSG device is disconnected from earth ground.

2. Unplug the power cord from the power source receptacle.

3. Unplug the power cord from the appliance inlet on the power supply faceplate.

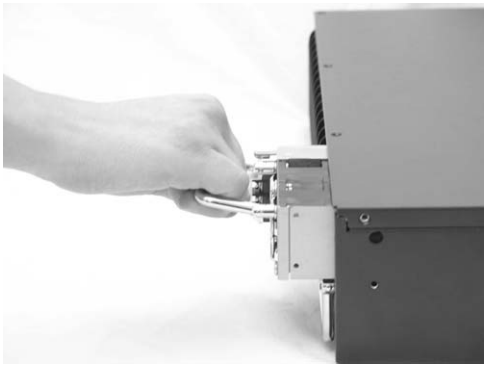
4. With your thumb, slide the metal ejector tab on the power supply faceplate to the right and hold it in place, to unlock the power supply.

**Figure 19: 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.

**Figure 20: Removing/Installing AC/DC Power Supply**



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 panel over the slot.

---

### *Installing an AC Power Supply*

To install an AC power supply in an SSG 550 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 SSG device is disconnected from earth ground.
2. Using both hands, slide the power supply 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 power-supply faceplate is flush with any adjacent power-supply faceplate.
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.

### *Replacing an AC Power Supply Cord*

To replace the 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 SSG 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.

### *Removing a DC Power Supply*

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

To remove a DC power supply 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 SSG device is disconnected from earth ground.
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 as shown in Figure 19.
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 20.
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 panel over the slot.

### *Installing a DC Power Supply*

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

To install a DC power supply into an SSG 550 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 SSG device is disconnected from earth ground.
2. Using both hands, slide the power supply into the chassis until you hear it click into position.
3. Firmly push the power supply into the chassis until it comes to a stop. Make sure that the power supply faceplate is flush with any adjacent power supply faceplate.

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. Turn on the current to the DC feed wires.

## Upgrading Memory

You can upgrade an SSG 500 series device that has a single 256 MB SIMM DRAM memory 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
- Anti-Virus
- Anti-Spam
- Intrusion Protection System (Deep Inspection)

To upgrade the memory on an SSG 500 series device, do the following:

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.

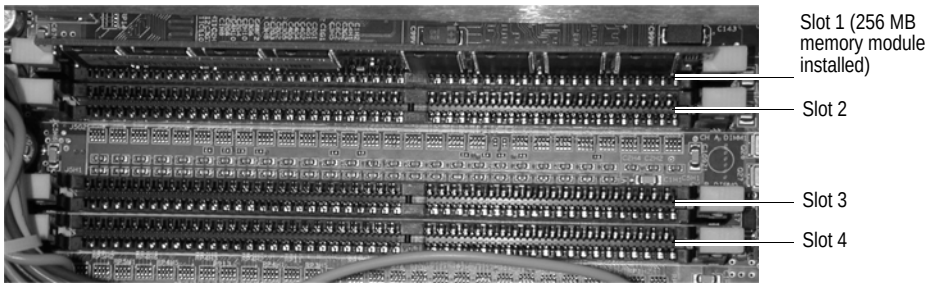
2. Press and release the power button to power off the device. Verify that the POWER LED blinks and then turns off.

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 21: Memory Module Slots**




**NOTE:** Install 512 MB memory modules in either 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 memory module by pressing your thumbs downward on the locking tabs on each side of the module so that the tabs swivel away from it.

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 memory modules into the slot from which you just removed the 256 MB SIMM DRAM memory 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.

**CAUTION:** You must install the two 512 MB memory modules in either slots 1 and 3, or in slots 2 and 4. Do not install memory modules in adjacent slots.

9. Locate the appropriate slot for the second 512 MB SIMM DRAM memory 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 a Filter

The front panel of an SSG 500 series 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 display, 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.

### *Removing a Filter*

The filter is located beneath the filter cover at the left front of the chassis.

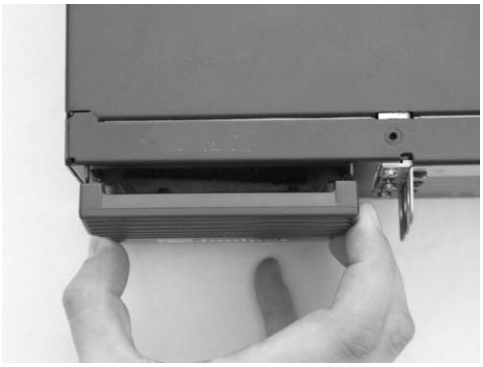
To remove a filter from the device, do the following:

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

**Figure 22: Squeezing Filter Cover Tabs**


2. Pull the filter cover away from the chassis.

**Figure 23: Removing/Installing Filter Cover**



3. Remove the filter.

**Figure 24: Removing/Installing Filter**


## *Installing a Filter*

To install a filter into the device, do the following:

1. Place the new filter into the opening over the air vent on the front of the chassis as shown in Figure 24.

2. Position the filter cover over the filter and slide it into place as shown in Figure 23.

3. 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 25.

**Figure 25: Securing Filter Cover**

Appendix A
# Specifications

This appendix provides general system specifications for SSG 500 series devices.

## Secure Services Gateway 500 Series Physical Specifications

**Table 10: Secure Services Gateway 500 Series Physical Specifications**

| Description | Value |
|---|---|
| Chassis dimensions | 3.44 in. (8.74 cm) high<br>17.44 in. (44.3 cm) wide—19.44 in. (49.38 cm) wide with mounting brackets attached<br>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 500 series device minimum configuration (no PIMs): 23lb (10.4 kg)<br>SSG 500 series device maximum configuration (six PIMs): 25.3 lb (11.5 kg) |

## Electrical Specifications

**Table 11: Secure Services Gateway 500 Series AC 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 500) | 6 A |
| AC system current rating (SSG 520) | 6 A |
| AC system current rating (SSG 550) | 8 A |

**Table 12: Secure Services Gateway 500 Series DC Electrical Specifications**

| Item | Specification |
|---|---|
| DC input voltage | Operating range: -48 to -60 VDC |
| DC system current rating | 20 A |

## Environmental Specifications

**Table 13: Secure Services Gateway 500 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)<br>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 | 2457 BTU/hour (720 W) |

## Certifications

### *Safety*

- CAN/CSA-C22.2 No. 60950-1-03/UL 60950-1 Safety of Information Technology Equipment
- EN 60950-1 Safety of Information Technology Equipment
- 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)

### *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

### *European Telecommunications Standards Institute (ETSI)*

- 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 14 lists the RJ-45 connector pinouts for the Console and AUX ports:

**Table 14: Console and AUX Port Connector Pinouts**

| RJ-45 | Name | I/O | Description | DB-9 |
|---|---|---|---|---|
| 1 | RTS Out | O | Request To Send | 8 |
| 2 | DTR Out | O | Data Terminal Ready | 6 |
| 3 | TxD | O | Transmit Data | 2 |
| 4 | GND | N/A | Chassis Ground | 5 |
| 5 | GND | N/A | Chassis Ground | 5 |
| 6 | RxD | I | Receive Data | 3 |
| 7 | DSR | I | Data Set Ready | 4 |
| 8 | CTS | I | Clear To Send | 7 |

# Index