JUNIPER NETWORKS | Engineering Simplicity

SRX380 Firewall Hardware Guide

Published
2023-08-15

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

SRX380 Firewall Hardware Guide

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use this guide to install hardware and perform initial software configuration, routine maintenance, and troubleshooting for the SRX380 Firewall. After completing the installation and basic configuration procedures covered in this guide, refer to the Junos OS documentation for information about further software configuration.

RELATED DOCUMENTATION

- Day One+ for SRX380 (Quick Start)
- SRX300 Series and SRX550 High Memory Gateway Interface Modules Reference
- Wi-Fi Mini-PIM Installation Guide
- LTE Mini-PIM and Antenna Installation Guide

1

CHAPTER

Overview

SRX380 Firewall Overview

IN THIS SECTION

Overview

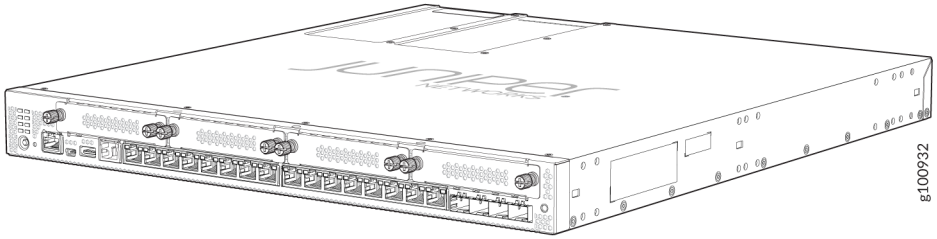
The Juniper Networks SRX380 Firewall consolidates security, routing, and switching to provide an all-in-one networking platform for software-defined WAN (SD-WAN) and next-generation firewall (NGFW) deployments. The SRX380 is designed for enterprise (large branch offices, small campus, SD-WAN) and service provider (managed WAN CPE, SD-WAN) deployments.

The SRX380 Firewall is 1 rack unit (U) tall and provides high port density with 16 on-board PoE-enabled 1-Gigabit Ethernet ports and 4 10-Gigabit Ethernet ports that support small form-factor pluggable plus (SFP+) transceivers. All the ports support AES-256 MACsec encryption. The SRX380 has a 100 GB on-board Serial Advanced Technology Attachment (SATA) solid-state drive (SSD).

The SRX380 supports dual power supplies and up to four Mini-Physical Interface Modules (Mini-PIMs).

Figure 1 on page 2 shows the SRX380 Firewall.

Figure 1: SRX380 Firewall



Key features supported on the SRX380 include VPN, Intrusion Detection and Prevention (IDP), AppSecure, Juniper Networks Juniper Advanced Threat Prevention Cloud (ATP Cloud), and Content

Security. For more information about the features supported on the SRX380 Firewall, see Feature Explorer.

You can manage the SRX380 Firewall by using the same interfaces that you use for managing other devices that run Junos OS—the CLI, the J-Web graphical interface, and Junos Space.

The first supported version of Junos OS for the SRX380 Firewall is Release 20.1R1.

This video provides a brief overview of the SRX380.

Video: SRX380 Hardware Overview

SRX380 Firewall FRUs

Field-replaceable units (FRUs) are components that you can replace at your site. The FRUs in the SRX380 Firewall are:

- Power supplies

  If only one power supply is installed in your device, you must power off the device before removing the power supply.

- Mini-PIMs

  The Mini-PIMs are not hot-swappable. You must power off the device before removing or installing Mini-PIMs.

NOTE: If you have a Juniper J-Care service contract, register any addition, change, or upgrade of hardware components at https://www.juniper.net/customers/support/tools/updateinstallbase/. Failure to do so can result in significant delays if you need replacement parts. This note does not apply if you replace existing components with the same type of component.

Benefits of the SRX380 Firewall

- **Multiple WAN connectivity options**—The SRX380 supports multiple options such as Ethernet, serial, T1/E1, VDSL2, Wi-Fi, and 3G/4G LTE wireless for WAN or Internet connectivity to link sites.

- **Comprehensive security**—The SRX380 provides security in every layer with AES-256 MACsec encryption, IPS, Content Security, Juniper Juniper Advanced Threat Prevention Cloud, and Application Security for protection against potential vulnerabilities.

SRX380 Chassis

IN THIS SECTION

The SRX380 Firewall chassis is a rigid sheet metal structure that houses all of the other components.

SRX380 Chassis Overview

The SRX380 chassis installs in standard 800–mm (or larger) enclosed cabinets, 19-in. equipment racks, or telecommunications open-frame racks.

CAUTION: Before removing or installing components of a functioning services gateway, attach an electrostatic discharge (ESD) strap to an ESD point and place the other end of the strap around your bare wrist. Failure to use an ESD strap could result in damage to the device.

The services gateway must be connected to earth ground during normal operation. The protective earthing terminal on the side of the chassis is provided to connect the services gateway to ground.

SRX380 Front Panel

IN THIS SECTION

Figure 2 on page 5 shows the front panel of the SRX380. Table 1 on page 5 provides details about the front panel components.

Figure 2: SRX380 Firewall Front Panel

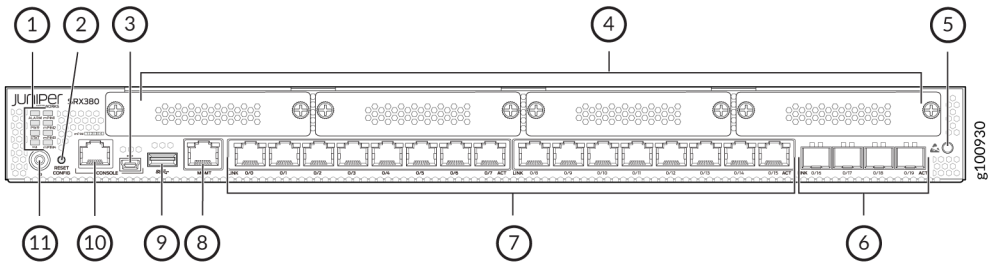


Table 1: SRX380 Firewall Front Panel Components

Callout	Component	Description
1	LEDs	Indicate component and system status.
2	Reset Config button	Returns the services gateway to the rescue configuration or the factory-default configuration.

Table 1: SRX380 Firewall Front Panel Components *(Continued)*

Callout	Component	Description
3	Mini-USB console port	Accepts a Mini-B type USB cable plug. A USB cable with Mini-B and Type A USB plugs is supplied with the services gateway. To use the mini-USB console port, you must download a USB driver to the management device from the Downloads page at https://www.juniper.net/support/downloads/?p=junos-srx#sw. To download the driver for Windows OS, select 6.5 from the **Version** drop-down list. To download the driver for Mac OS, select 4.10 from the **Version** drop-down list.
4	Mini-PIM slots	Four slots for Mini-PIMs, which can provide LAN and WAN functionality along with connectivity to various media types.
5	ESD outlet	
6	1-Gigabit Ethernet or 10-Gigabit Ethernet SFP or SFP+ ports	Four 1 or 10-Gigabit Ethernet SFP or SFP+ ports for network traffic.

Table 1: SRX380 Firewall Front Panel Components *(Continued)*

Callout	Component	Description
7	1-Gigabit Ethernet ports	Sixteen 1-Gigabit Ethernet LAN ports that are PoE-enabled. The ports have the following characteristics: • Use an RJ-45 connector • Operate in full-duplex and half-duplex modes • Support autonegotiation The ports can be used to: • Function as front-end network ports • Provide LAN and WAN connectivity to hubs, switches, local servers, and workstations • Forward incoming data packets to the services gateway • Receive outgoing data packets from the services gateway
8	Management port	Use the management (MGMT) port to connect to the device over the network.
9	USB port	One USB port that accepts a USB storage device.
10	RJ-45 console port	Supports RS-232 serial ports.
11	Power button	Use the Power button to shut down the services gateway.

NOTE: The SRX380 ships with tamperproof labels for the Mini-PIM slots and SSD slots.

Chassis Status LEDs

Figure 3 on page 8 shows the LEDs on the front panel of the SRX380.

Figure 3: SRX380 Firewall Front Panel LEDs

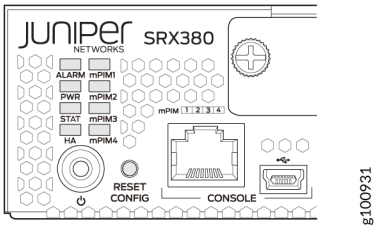


Table 2 on page 8 lists the front panel LEDs.

Table 2: SRX380 Firewall Front Panel LEDs

Component	Description
ALARM	• Solid amber (noncritical alarm) • Solid red (critical alarm) • Off (no alarms)
STAT	• Solid green (operating normally) • Solid red (error detected)
PWR	• Solid green (receiving power) • Solid amber (Power-off triggered) • Off (no power)

Table 2: SRX380 Firewall Front Panel LEDs *(Continued)*

Component	Description
HA	• Solid green (all HA links are available) • Solid amber (some HA links are unavailable) • Solid red (HA links are not functional) • Off (HA is disabled)
mPIM1, mPIM2, mPIM3, and mPIM4	• Solid green (Mini-PIM is functioning normally) • Solid red (Mini-PIM hardware failure) • Off (Mini-PIM is not installed or Mini-PIM is not detected by the device)

Management Port and Network Port LEDs

The management port and network port have two LEDs each that indicate the link activity and status of the ports. Figure 4 on page 9 shows the LEDs.

Table 3 on page 10 describes the management port and network port LEDs.

Figure 4: SRX380 Management Port and Network Port LEDs

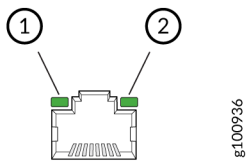


Table 3: Management Port and Network Port LEDs

Callout	LED	Description
1	Link	• Solid green—There is link activity. • Off—There is no link established.
2	Activity	• Blinking green—There is activity on the link. • Off—There is no link established.

SRX380 Back Panel

Figure 5 on page 10 shows the back panel of the SRX380 Firewall. Table 4 on page 10 lists the components on the back panel.

Figure 5: SRX380 Firewall Back Panel

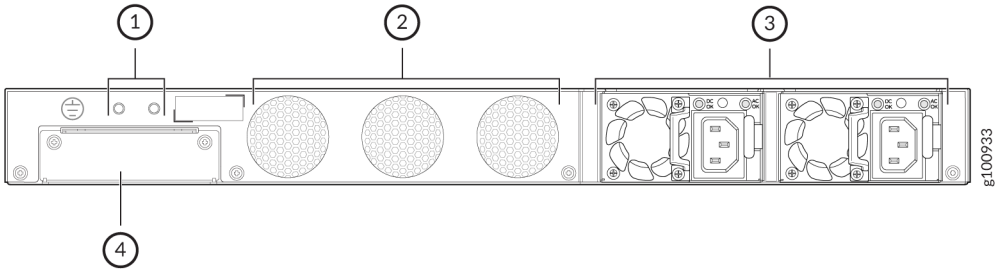


Table 4: SRX380 Firewall Back Panel Components

Callout	Component	Description
1	Grounding point	The grounding point consists of two threaded holes, which fit two 10-32 x .25 in. screws.

Table 4: SRX380 Firewall Back Panel Components *(Continued)*

Callout	Component	Description
2	Fans	The fans are fixed and provide front-to-back cooling.
3	Power supply input	One power supply is preinstalled.
4	SSD slot	Slot for second SSD. Currently, the SRX380 does not support a second SSD.

SRX380 Interface Modules Overview

Mini-Physical Interface Modules (Mini-PIMs) are field-replaceable network interface cards (NICs) supported on the SRX300 line of services gateways. You can easily insert or remove Mini-PIMs from the front slots of the SRX380 chassis. The Mini-PIMs provide physical connections to a LAN or WAN. The Mini-PIMs receive incoming packets from the network and transmit outgoing packets to the network. During this process, they perform framing and line-speed signaling for the medium type.

CAUTION: The Mini-PIMs are not hot-swappable. You must power off the services gateway before removing or installing Mini-PIMs.

The following Mini-PIMs are supported on the SRX380 Firewall:

- 1-Port Serial Mini-PIM (SRX-MP-1SERIAL-R)
- 1-Port T1/E1 Mini-PIM (SRX-MP-1T1E1-R)
- 1-Port VDSL2 (Annex A) Mini-PIM (SRX-MP-1VDSL2-R)
- LTE Mini-PIM (SRX-MP-LTE-AE and SRX-MP-LTE-AA)
- Wi-Fi Mini-PIM (SRX-MP-WLAN-US, SRX-MP-WLAN-IL, and SRX-MP-WLAN-WW)

NOTE: Gigabit-Backplane Physical Interface Modules (GPIMs) are not supported on the SRX380 Firewall.

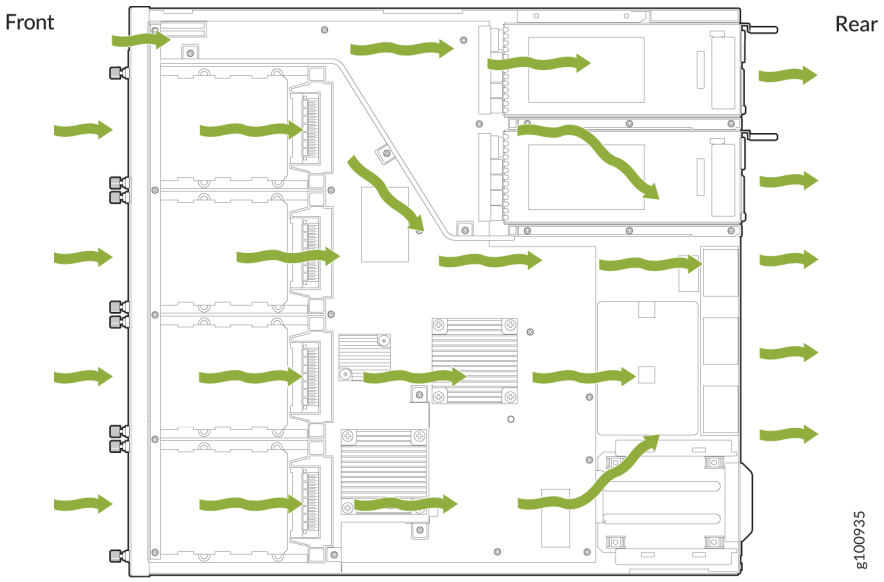
For more information on Mini-PIMs, see SRX300 Series and SRX550 High Memory Gateway Interface Modules Reference.

SRX380 Cooling System

The cooling system for the SRX380 Firewall includes three fixed fans. The fans draw air through vents on the front of the chassis and exhaust the air through the back of the chassis. The airflow produced by the fans keeps the device components within the acceptable temperature range.

Figure 6 on page 12 shows the airflow through the SRX380 Firewall chassis.

Figure 6: Airflow Through the SRX380 Firewall Chassis



SRX380 Power System

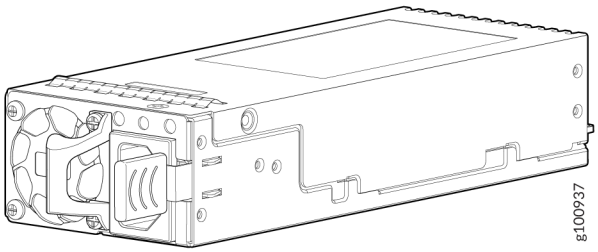
IN THIS SECTION

SRX380 Firewall Power Supply

You can install two power supplies in the slots located at the rear of the chassis. Each power supply provides an output power of 600 W. The SRX380 ships with one power supply installed.

Figure 7 on page 13 shows the power supply for the SRX380.

Figure 7: SRX380 Power Supply



The power supplies in the SRX380 Firewall are hot-insertable and hot-removable field-replaceable units (FRUs). You can replace them without powering off the device. If only one power supply is installed in your device, you need to power off the device before removing the power supply.

Table 5 on page 14 lists the power consumed by the SRX380. The maximum power available on a PoE port is 30 W.

Table 5: Power Consumed by the SRX380 Firewall

Device	Number of PoE-Enabled Ports	Maximum Power Consumed by the Device	Maximum System Power Available for PoE
SRX380	16	• 525.23 W @100V (with one power supply installed and 300-W PoE device) • 738.04 W @100V (with two power supplies installed and 480-W PoE device) • 172 W @100V (with one power supply installed and without a PoE device)	• 300 W (with one power supply installed) • 480 W (with two power supplies installed, without redundancy)

AC Power Supply LEDs on SRX380 Services Gateways

Each power supply has two LEDs on the faceplate that indicate the status of the power supply. Table 6 on page 14 describes the AC power supply LEDs.

Table 6: AC Power Supply LEDs on the SRX380 Firewall

LED	Color	Description
AC OK	Off	No AC power input.
	Red	Power supply failure.
	Green	The power supply is delivering power and is functioning correctly.
DC OK	Off	No AC power input
	Red	Power supply failure.
	Green	The power supply is delivering power and is functioning correctly.

Power Specifications for SRX380 Services Gateways

Table 7 on page 15 provides the AC power supply electrical specifications for SRX380 devices.

Table 7: AC Power Supply Electrical Specifications for SRX380 Devices

Power Requirement	Specification
AC input voltage	100 to 240 VAC
AC input line frequency	50 Hz/60 Hz nominal
AC system current rating	8.5 A at 100 VAC 4.25 A at 240 VAC
Maximum AC inrush current	11 A at 220 V/50 Hz (with four Mini-PIMs installed)

AC Power Cord Specifications for SRX380

A detachable AC power cord is supplied with the AC power supplies. The coupler is type C13 as described by International Electrotechnical Commission (IEC) standard 60320. The plug end of the power cord fits into the power source outlet that is standard for your geographical location.

CAUTION: The AC power cord provided with each power supply is intended for use with that power supply only and not for any other use.

NOTE: In North America, AC power cords must not exceed 4.5 meters (approximately 14.75 feet) in length, to comply with National Electrical Code (NEC) Sections 400-8 (NFPA 75, 5-2.2) and 210-52 and Canadian Electrical Code (CEC) Section 4-010(3). The cords supplied with the device are in compliance.

Table 8 on page 16 lists the AC power cord specifications for the countries and regions listed in the table.

Table 8: AC Power Cord Specifications

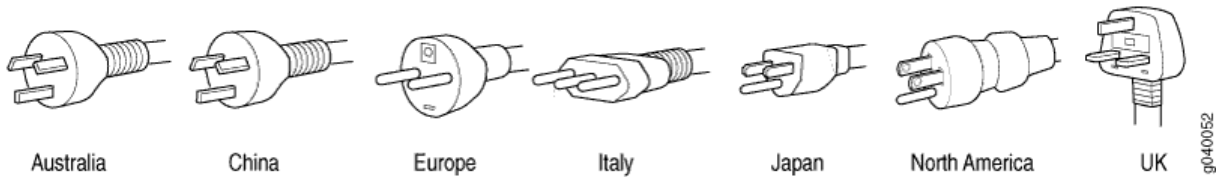
Country/Region	Electrical Specifications	Plug Standards	Juniper Model Number
Argentina	250 VAC, 10 A, 50 Hz	IRAM 2073 Type RA/3	CBL-EX-PWR-C13-AR
Australia	250 VAC, 10 A, 50 Hz	AS/NZZS 3112 Type SAA/3	CBL-EX-PWR-C13-AU
Brazil	250 VAC, 10 A, 50 Hz	NBR 14136 Type BR/3	CBL-EX-PWR-C13-BR
China	250 VAC, 10 A, 50 Hz	GB 1002-1996 Type PRC/3	CBL-EX-PWR-C13-CH
Europe (except Italy, Switzerland, and United Kingdom)	250 VAC, 10 A, 50 Hz	CEE (7) VII Type VIIG	CBL-EX-PWR-C13-EU
India	250 VAC, 10 A, 50 Hz	IS 1293 Type IND/3	CBL-EX-PWR-C13-IN
Israel	250 VAC, 10 A, 50 Hz	SI 32/1971 Type IL/3G	CBL-EX-PWR-C13-IL
Italy	250 VAC, 10 A, 50 Hz	CEI 23-16 Type I/3G	CBL-EX-PWR-C13-IT
Japan	125 VAC, 12 A, 50 Hz or 60 Hz	SS-00259 Type VCTF	CBL-EX-PWR-C13-JP
Korea	250 VAC, 10 A, 50 Hz or 60 Hz	CEE (7) VII Type VIIGK	CBL-EX-PWR-C13-KR
North America	125 VAC, 13 A, 60 Hz	NEMA 5-15 Type N5-15	CBL-EX-PWR-C13-US
South Africa	250 VAC, 10 A, 50 Hz	SABS 164/1:1992 Type ZA/13	CBL-EX-PWR-C13-SA
Switzerland	250 VAC, 10 A, 50 Hz	SEV 6534-2 Type 12G	CBL-EX-PWR-C13-SZ

Table 8: AC Power Cord Specifications *(Continued)*

Country/Region	Electrical Specifications	Plug Standards	Juniper Model Number
Taiwan	125 VAC, 13 A, 60 Hz	NEMA 5-15 Type N5-15	CBL-EX-PWR-C13-US
United Kingdom	250 VAC, 10 A, 50 Hz	BS 1363/A Type BS89/13	CBL-EX-PWR-C13-UK

Figure 8 on page 17 illustrates the plug on the power cord for some of the countries or regions listed in Table 8 on page 16.

Figure 8: AC Plug Types



2

CHAPTER

Site Planning, Preparation, and Specifications

SRX380 Site Preparation Checklist

Table 9 on page 19 provides a checklist of the tasks you need to perform when preparing a site for installing the SRX380 Firewall.

Table 9: Site Preparation Checklist for SRX380 Firewall Installation

Item or Task	Additional Information
Environment	
Verify that environmental factors such as temperature and humidity do not exceed device tolerances.	"SRX380 Firewall Environmental Specifications" on page 21
Power	
Measure the distance between the external power sources and the device installation site.	"SRX380 Firewall Electrical Wiring Guidelines" on page 22
Locate sites to connect system grounding.	"Connecting the SRX380 Grounding Cable" on page 35
Calculate the power consumption and requirements.	Table 5 on page 14
Rack Requirements	
Verify that your rack meets the minimum requirements.	"Rack Requirements" on page 25
Rack Installation	

Table 9: Site Preparation Checklist for SRX380 Firewall Installation *(Continued)*

Item or Task	Additional Information
Plan the rack location, including required space clearances.	"Rack Requirements" on page 25
Secure the rack to the floor and building structure.	
Cabinet Requirements	
Verify that your cabinet meets the minimum requirements.	"Cabinet Requirements" on page 26
Plan the cabinet location, including required space clearances.	
Cables	
• Acquire cables and connectors. • Review the maximum distance allowed for each cable. Choose the length of cable based on the distance between the hardware components being connected. • Plan the cable routing and management.	

SRX380 Site Guidelines and Requirements

IN THIS SECTION

General Site Installation Guidelines for the SRX380 Firewall

The following precautions help you plan an acceptable operating environment for your SRX380 Firewall and avoid environmentally caused equipment failures:

- For the cooling system to function properly, the airflow around the chassis must be unrestricted. Allow sufficient clearance between the front and back of the chassis and adjacent equipment. Ensure that there is adequate circulation in the installation location.
- Follow the prescribed electrostatic discharge (ESD) prevention procedures to prevent damaging the equipment. Static discharge can cause components to fail completely or intermittently over time.
- Ensure that blank Mini-PIM panels are installed in all empty Mini-PIM slots to prevent any interruption or reduction in the flow of air across internal components.

SRX380 Firewall Environmental Specifications

Table 10 on page 22 provides the required environmental conditions for normal operations of the SRX380 Firewall.

Table 10: Environmental Specifications for the SRX380 Firewall

Description	Value
Altitude	2000 m (6561 ft)
Relative humidity	5% to 90%, noncondensing
Temperature	• Operational temperature with Mini-PIMs—32° F (0° C) to 104° F (40° C) @ 2000 meters. • Operational temperature without Mini-PIMs—32° F (0° C) to 122° F (50° C) @ 2000 meters. • Nonoperational temperature— -4° F (-20° C) to 158° F (70° C)
Average power consumption	150 W (without PoE)

SRX380 Firewall Electrical Wiring Guidelines

Table 11 on page 23 describes the factors you must consider while planning the electrical wiring for the SRX380 at your site.

CAUTION: It is particularly important to provide a properly grounded and shielded environment and to use electrical surge-suppression devices.

Table 11: Site Electrical Wiring Guidelines for the SRX380 Firewall

Site Wiring Factor	Guideline
Signaling Limitations	To ensure that signaling functions optimally: • Install wires correctly. Improperly installed wires can emit radio interference. • Do not exceed the recommended distances or pass wires between buildings. The potential for damage from lightning strikes increases if wires exceed recommended distances or if wires pass between buildings. • Shield all conductors. The electromagnetic pulse (EMP) caused by lightning can damage unshielded conductors and destroy electronic devices.
Radio Frequency Interference (RFI)	To reduce or eliminate the emission of RFI from your site wiring: • Use twisted-pair cables with a good distribution of grounding conductors. • Use a high-quality twisted-pair cable with one ground conductor for each data signal when applicable, if you must exceed the recommended distances.
Electromagnetic Compatibility (EMC)	Provide a properly grounded and shielded environment and use electrical surge-suppression devices. Strong sources of electromagnetic interference (EMI) can cause the following damage: • Destroy the signal drivers and receivers in the device • Conduct power surges over the lines into the equipment, resulting in an electrical hazard **NOTE**: If your site is susceptible to problems with EMC, particularly from lightning or radio transmitters, you might want to seek expert advice.

CAUTION: To comply with intrabuilding lightning or surge requirements, the intrabuilding wiring must be shielded. The shielding for the wiring must be grounded at both ends.

To reduce the risk of fire, use 26 AWG telecommunication line wire.

SRX380 Firewall Physical Specifications

Table 12 on page 24 lists the physical specifications for the SRX380.

Table 12: Physical Specifications for the SRX380 Firewall

Physical Specification of Chassis	Value
Depth	With handles—20.47 in. (52 cm) Without handles—18.7 in. (47.5 cm)
Width	17.36 in. (44.09 cm)
Height	1.72 in. (4.37 cm)
Weight (with single power supply unit)	15 lb (6.80 kg)

SRX380 Firewall Clearance Requirements for Airflow and Hardware Maintenance

When planning the installation site for the SRX380 Firewall, you must allow sufficient clearance around the device. Consider the following requirements:

- For the operating temperature of the services gateway to be optimal, the airflow around the chassis must be unrestricted. The three fixed fans provide front-to-back chassis cooling.
- For service personnel to remove and install hardware components, there must be adequate space at the front and back of the device. Allow at least 24 in. (61 cm) both in front of and behind the device.

- If you are mounting the device in a rack with other equipment, ensure that the exhaust from other equipment does not blow into the intake vents of the chassis.

For information on the airflow through the SRX380 Firewall chassis, see "SRX380 Cooling System" on page 12.

Rack Requirements

The SRX380 Firewall is designed to be installed on four-post racks. Table 13 on page 25 provides the rack requirements and specifications for the SRX380.

Table 13: Rack Requirements for the SRX380 Firewall

Rack Requirement	Guidelines
Rack type	Use a four-post rack that provides bracket holes or hole patterns spaced at 1-U (1.75 in. or 4.45 cm) increments and that meets the size and strength requirements to support the weight of the device.
Mounting bracket hole spacing	The holes in the mounting brackets are spaced at 1-U (1.75 in. or 4.45 cm) increments. The device can be mounted in any four-post rack that provides holes spaced at that distance.
Rack size and strength	• Ensure that the rack complies with the standards for a 19-in. rack as defined in Cabinets, Racks, Panels, and Associated Equipment (document number EIA-310–D) published by the Electronics Industry Association. • Ensure that the rack rails are spaced widely enough to accommodate the external dimensions of the chassis. The outer edges of the front-mounting brackets extend the width to 19 in. (48.26 cm). • Space the front and rear rack rails between 23 in. (58.5 cm) to 36 in. (91.4 cm) front-to-back. • The rack must be strong enough to support the weight of the device. • Ensure that the spacing of rails and adjacent racks provides for proper clearance around the device and rack.

Table 13: Rack Requirements for the SRX380 Firewall *(Continued)*

Rack Requirement	Guidelines
Rack connection to building structure	• Secure the rack to the building structure. • If earthquakes are a possibility in your geographical area, secure the rack to the floor. • Secure the rack to the ceiling brackets and to wall or floor brackets for maximum stability.

Cabinet Requirements

You can mount the SRX380 in an enclosure or cabinet that contains a four-post 19-in. open rack as defined in Cabinets, Racks, Panels, and Associated Equipment (document number EIA-310-D) published by the Electronics Industry Association.

Table 14 on page 26 provides the cabinet requirements and specifications for the SRX380.

Table 14: Cabinet Requirements for the SRX380

Cabinet Requirement	Guidelines
Cabinet size and clearance	The minimum cabinet size for accommodating an SRX380 device is 36 in. (91.4 cm) deep. Large cabinets improve airflow and reduce the chance of overheating.

Table 14: Cabinet Requirements for the SRX380 *(Continued)*

Cabinet Requirement	Guidelines
Cabinet airflow requirements	When you mount the device in a cabinet, ensure that ventilation through the cabinet is sufficient to prevent overheating. • Ensure that the cool air supply you provide through the cabinet adequately dissipates the thermal output of the device. • Ensure that the cabinet allows the hot exhaust air from the chassis to exit the cabinet without recirculating into the device. An open cabinet (without a top or doors) that employs hot air exhaust extraction from the top allows the best airflow through the chassis. If the cabinet contains a top or doors, perforations in these elements assist with removing the hot air exhaust. • The SRX380 device fans exhaust hot air through the fans and power supplies. Install the device in the cabinet in a way that maximizes the open space on the FRU side of the chassis. This maximizes the clearance for critical airflow. • Route and dress all cables to minimize the blockage of airflow to and from the chassis. • Ensure that the spacing of rails and adjacent cabinets allows for proper clearance around the device and cabinet.

CHAPTER 3

Initial Installation and Configuration

Unpacking and Mounting the SRX380

IN THIS SECTION

Unpacking the SRX380 Firewall

The SRX380 Firewall is shipped in a cardboard carton and secured with foam packing material. The carton also contains an accessory box and quick start instructions.

NOTE: The services gateway is maximally protected inside the cardboard carton. Do not unpack it until you are ready to begin installation.

To unpack the SRX380 Firewall:

1. Move the cardboard carton to a staging area as close to the installation site as possible, where you have enough room to remove the components from the chassis.
2. Position the cardboard carton with the arrows pointing up.
3. Carefully open the top of the cardboard carton.
4. Remove the foam covering the top of the services gateway.
5. Remove the accessory box.
6. Verify the parts received against the lists in "Verifying Parts Received with the SRX380 Firewall" on page 30.
7. Store the brackets and bolts inside the accessory box.
8. Save the shipping carton and packing materials in case you need to move or ship the services gateway at a later time.

Verifying Parts Received with the SRX380 Firewall

The shipment includes a packing list. Check the parts you receive in the shipping carton against the items on the packing list. The parts shipped depend on the configuration you order.

If any part on the packing list is missing, contact your customer service representative or contact Juniper customer care from within the U.S. or Canada by telephone at 1-888-314-5822. For international-dial or direct-dial options in countries without toll-free numbers, see https://www.juniper.net/support/requesting-support.html.

Table 15: Parts List for a Fully Configured SRX380 Firewall

Component	Quantity
SRX380 with one power supply (includes blank covers for Mini-PIM slots)	1
USB console cable with Type-A and Mini-B USB plugs	1
Power cord appropriate for your geographical location	1
Power cord retainer clip	1
Rack mounting kit	• 6 flat-head 4-40 mounting screws • 12 flat-head M4x6-mm Phillips mounting screws • One pair each of flush or 2-in.-recess mounting brackets • One pair of mounting rails • One pair of mounting blades

Table 16: Accessory Parts List for the SRX380 Firewall

Part	Quantity
End User License Agreement	1
Documentation Roadmap and Product Warranty	1

Mounting the SRX380 Firewall in a Rack

You can mount the SRX380 on four posts of a 19-in. rack or cabinet by using the four-post rack-mount kit that is shipped with the device. (The remainder of this topic uses *rack* to mean *rack or cabinet*.)

Space the front and rear rack rails between 23 in. (58.5 cm) to 36 in. (91.4 cm) front-to-back.

NOTE: If you need to mount the device in a recessed position on a four-post rack, you can use the 2-in.-recess mounting brackets provided with the rack-mount kit.

Before mounting the device on a four-post rack:

- Ensure that you have the following parts and tools available:
  - Phillips (+) screwdriver, number 2
  - Six flat-head 4-40 mounting screws (provided with the four-post rack-mount kit)
  - Twelve flat-head M4x6-mm Phillips mounting screws (provided with the four-post rack-mount kit)
  - One pair each of flush or 2-in.-recess mounting brackets (provided with the four-post rack-mount kit)
  - One pair of mounting rails (provided with the four-post rack-mount kit)
  - One pair of mounting blades (provided with the four-post rack-mount kit)
  - Screws to secure the chassis and the mounting blades to the rack (not provided)
- Verify that the site meets the requirements described in "SRX380 Site Preparation Checklist" on page 19.

- Place the rack in its permanent location, allowing adequate clearance for airflow and maintenance, and secure it to the building structure.
- Read "General Site Installation Guidelines for the SRX380 Firewall" on page 21.

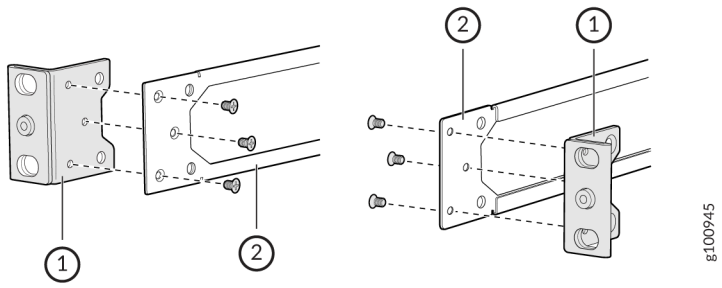
NOTE: One person must be available to lift the device while another secures the device to the rack.

CAUTION: If you are mounting multiple units on a rack, mount the heaviest unit at the bottom of the rack and mount the other units from the bottom of the rack to the top in decreasing order of the weight of the units.

To mount the device on four posts of a rack:

1. Remove the device from the shipping carton (see "Unpacking the SRX380 Firewall" on page 29).
2. Place the device on a flat, stable surface.
3. Attach the mounting brackets (either the flush or the 2-in.-recess mounting brackets) to the mounting rails by using the six 4-40 flat-head Phillips mounting screws. See Figure 9 on page 32.

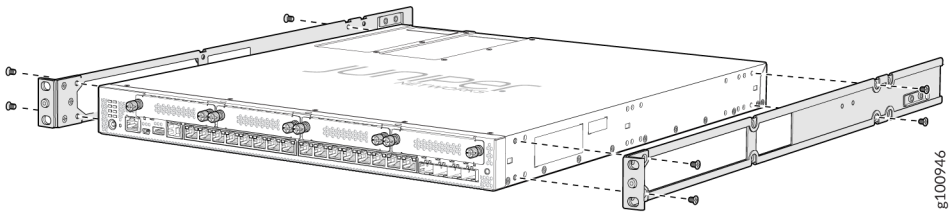
Figure 9: Attaching the Front-Mounting Bracket to the Side Mounting-Rail



1– Mounting bracket	2– Mounting rail

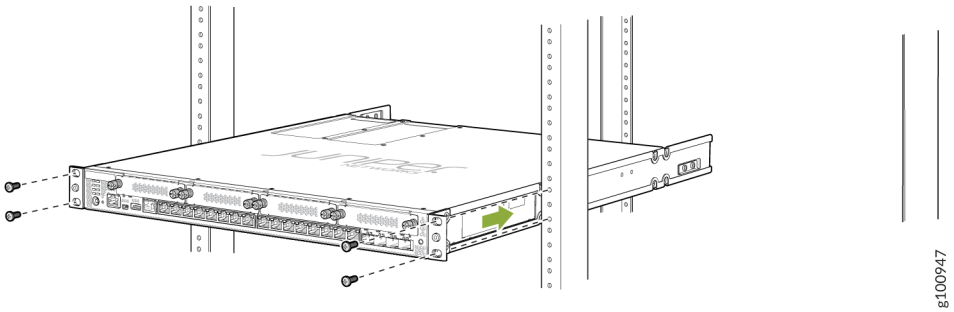
4. Align the holes in the mounting rail with the screw holes on the side of the chassis. See Figure 10 on page 33.

Figure 10: Attaching the Mounting-Rail to the Chassis



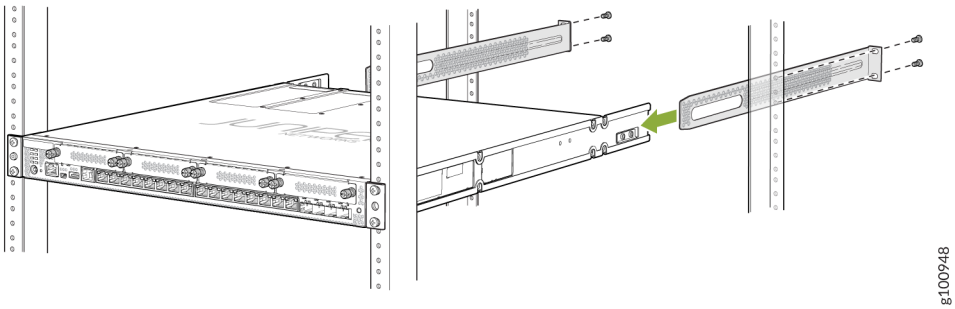
5. Attach the mounting rail to the device using the M4x6-mm Phillips flat-head mounting screws. Tighten the screws.
6. Repeat Step 4 and Step 5 on the opposite side of the device.
7. Have one person grasp both sides of the device, lift it, and position it in the rack so that the front bracket is aligned with the rack holes.
8. Have a second person secure the front of the device to the rack by using 4 mounting screws (and cage nuts and washers if the rack requires them). Tighten the screws. See Figure 11 on page 33.

Figure 11: Securing the Device to the Rack



9. Continue to support the SRX380 while sliding the mounting blades into the channel of the mounting rails and securing the blades to the rack. Use four mounting screws (and cage nuts and washers if the rack requires them) to attach the blade to the rack. Tighten the screws. See Figure 12 on page 34.

Figure 12: Attaching the Rear-Mounting Blades



10. Ensure that the chassis is level by verifying that all the screws on the front of the rack are aligned with the screws at the back of the rack.

Connecting the SRX380 to Power

IN THIS SECTION

Required Tools and Parts for Grounding the SRX380 Firewall

Table 17 on page 35 lists the earthing terminal location, grounding cable requirements, grounding lug specifications, screws and washers required, and the screwdriver needed for connecting the device to earth ground. Before you begin connecting a device to earth ground, ensure that you have the parts and tools required for your device.

Table 17: Parts and Tools Required for Connecting an SRX380 to Earth Ground

Grounding Cable Requirements	Grounding Lug Specifications	Screws and Washers	Screwdriver
10 AWG or as permitted by the local code	Panduit LCD10-10AF-L or equivalent—not provided	• Two 10-32 x .25 in. screws with #10 split-lock washer—not provided • Two #10 flat washers—not provided	Phillips (+) number 2

Connecting the SRX380 Grounding Cable

To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must connect the chassis to earth ground before you connect it to power.

NOTE: Ensure that a licensed electrician has attached an appropriate grounding lug to the grounding cable you supply. Using a grounding cable with an incorrectly attached lug can damage the device.

You ground the services gateway by connecting a grounding cable to earth ground and then attaching the grounding cable to the chassis grounding point located on the rear of the device.

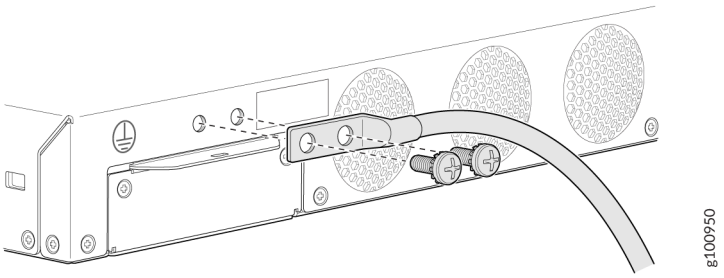
You must install the SRX380 in a restricted-access location and ensure that the chassis is always properly grounded. The SRX380 has a two-hole protective grounding terminal provided on the chassis. See Figure 13 on page 36. Under all circumstances, use this grounding connection to ground the chassis. For AC-powered systems, you must also use the grounding wire in the AC power cord along with the two-hole grounding lug connection. This tested system meets or exceeds all applicable EMC regulatory requirements with the two-hole protective grounding terminal.

To ground the device:

1. Wrap and fasten one end of the ESD grounding strap around your wrist and connect the other end to a site ESD point. For more details, see "Prevention of Electrostatic Discharge Damage" on page 71.
2. Ensure that all grounding surfaces are clean and brought to a bright finish before grounding connections are made.

3. Connect the grounding cable to a proper earth ground, such as the rack in which the device is mounted.
4. Remove the two screws on the chassis using a Phillips screwdriver.
5. Place the grounding cable lug attached to the grounding cable over the grounding point on the rear of the chassis.

Figure 13: Connecting the Grounding Cable to the SRX380 Firewall



6. Secure the grounding cable lug to the grounding point with the washers and screws.
7. Dress the grounding cable and verify that it does not touch or block access to the services gateway components and that it does not drape where people could trip on it. Ensure that the cable does not obstruct the air flow of the fans.

NOTE: The device should be permanently connected to ground during operation.

Connecting the SRX380 Firewall to an AC Power Supply

Ensure that you have the following parts and tools available:

- A power cord appropriate for your geographical location
- A power cord retainer clip (provided with the device)

To connect AC power to the device:

1. Push the end of the power cord retainer strip into the slot above the power cord inlet until the strip snaps into place. Ensure that the loop in the retainer strip faces the power cord (see Figure 14 on page 37).

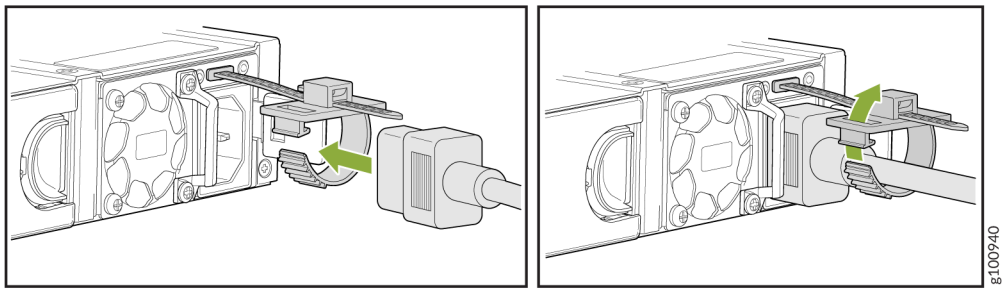
   The power cord retainer clip extends out of the chassis by 3 in. (7.62 cm).

2. Press the small tab on the retainer strip to loosen the loop. Slide the loop until there is enough space to insert the power cord coupler into the power cord inlet.
3. Locate the power cord or cords shipped with the device; the cords have plugs appropriate for your geographical location. See Table 8 on page 16.

> **WARNING**: Ensure that the power cord does not drape where people can trip on it or block access to device components.

4. Insert the power cord coupler firmly into the power cord inlet (see Figure 14 on page 37).
5. Slide the loop toward the power supply until it is snug against the base of the coupler.

Figure 14: Connecting an AC Power Cord



6. Press the tab on the loop and draw out the loop into a tight circle.
7. If the AC power source outlet has a power switch, set it to the OFF (**0**) position.
8. Insert the power cord plug into an AC power source outlet.
9. If the AC power source outlet has a power switch, set it to the ON (**|**) position.

   If the power supply is installed correctly and functioning normally, the LED on the faceplate of the power supply glows solid green.

   The device starts automatically as the power supply completes its startup sequence. The PWR LED lights up during startup and remains on when the device is operating normally.

> **NOTE**: After the power supply is turned on, it can take up to 60 seconds for status indicators —such as the STAT and PWR LEDs—to show that the power supply is functioning normally. Ignore error indicators that appear during the first 60 seconds.

Powering Off the SRX380 Firewall

You can power off the services gateway in one of the following ways:

- Graceful shutdown—Press and immediately release the Power button. The device begins gracefully shutting down the operating system and then powers itself off.

  CAUTION: Use the graceful shutdown method to power off or reboot the services gateway.

- Forced shutdown—Press the Power button and hold it down for 10 seconds. The device immediately powers itself off without shutting down the operating system.

  CAUTION: Forced shutdown can result in data loss and corruption of the file system. Use the forced shutdown method as a last resort to recover the services gateway if the services gateway operating system is not responding to the graceful shutdown method.

WARNING: Do not press the Power button while the device is shutting down.

To remove power completely from the device, unplug the power cord or switch off the AC power source.

After powering off a power supply, wait at least 10 seconds before turning it back on. After powering on a power supply, wait at least 10 seconds before turning it off.

The Power button on the services gateway is a standby power switch, which will not turn off the input power to the services gateway.

TIP: When you are powering off the device, the CLI displays the following message: `Turning the system power off`. You can now safely remove the power cable to completely power off the device.

NOTE: You can use the **request system reboot** CLI command to schedule a reboot.

Connecting the SRX380 to External Devices

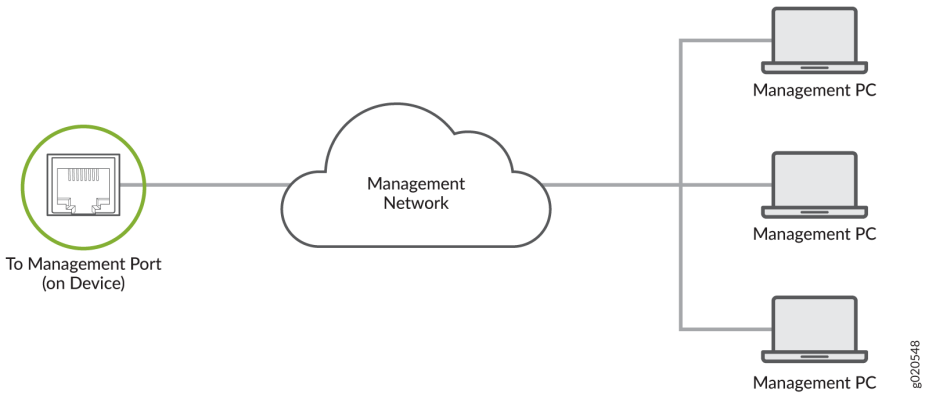
IN THIS SECTION

You can manage the SRX380 by using the management port for out-of-band management or through the console ports.

Connecting an SRX380 to a Network for Out-of-Band Management

You can monitor and manage the SRX380 by using a dedicated management channel. The SRX380 has a management port to which you can connect an Ethernet cable with an RJ-45 connector. Use the management port to connect the device to a network for out-of-band management. Figure 15 on page 39 shows how to connect a device for out-of-band management.

Figure 15: Connecting a Device to a Network for Out-of-Band Management

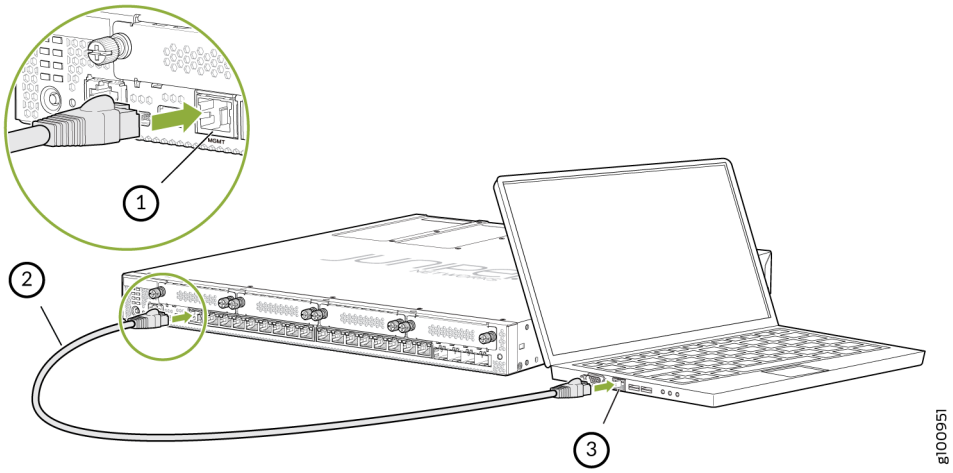


To connect the SRX380 to a network for out-of-band management (see Figure 16 on page 40):

1. Connect one end of the Ethernet cable to the management port (labeled **MGMT**) on the device.

2. Connect the other end of the Ethernet cable to the management device.

Figure 16: Connecting the SRX380 to a Management Device



1– Management port	3– RJ-45 cable connecting to the Ethernet port on the laptop
2– RJ-45 cable connecting to the MGMT port on SRX380	

Connecting an SRX380 to a Management Console by Using an RJ-45 Connector

The SRX380 has an RJ-45 console port. Use the console port to connect the device to a management console or to a console server.

If your laptop or PC does not have a DB-9 plug connector pin and you want to connect your laptop or PC directly to the SRX380, use a combination of the RJ-45 cable and RJ-45 to DB-9 adapter and a USB to DB-9 adapter. You must provide the USB to DB-9 adapter.

NOTE: We no longer include a DB-9 to RJ-45 cable or a DB-9 to RJ-45 adapter with a CAT5E copper cable as part of the device package. If you require a console cable, you can order it separately with the part number JNP-CBL-RJ45-DB9 (DB-9 to RJ-45 adapter with a CAT5E copper cable).

To connect the SRX380 to a management console:

1. Connect one end of the Ethernet cable to the console port (labeled **CON**).
2. Connect the other end of the Ethernet cable into the console server or management console.

Connecting an SRX380 to a Management Console by Using the Mini-USB Type-B Console Port

Before you begin connecting the device by using the Mini-USB Type-B console port:

- Ensure that you have the following parts and tools available:
  - One Mini-USB cable with Standard-A and Mini-USB Type-B (5-pin) connectors (not provided)
- Ensure that the USB to Serial driver is installed on the host machine.
- Ensure that the HyperTerminal properties of the console server or laptop are set as follows:
  - Baud rate—9600
  - Flow control—None
  - Data—8
  - Parity—None
  - Stop bits—1
  - DCD state—Disregard

You can configure and manage the SRX380 by using the RJ-45 console port or the Mini-USB Type-B console port. Only one console port is active at a time.

If your laptop or PC does not have a DB-9 plug connector pin or RJ-45 connector pin, you can connect your laptop or PC directly to the device by using a Mini-USB cable that has a Standard-A USB connector on one end and a Mini-USB Type-B (5-pin) connector on the other end.

To connect the device to the console by using the Mini-USB Type-B console port:

1. Connect the host machine to the device using the active console port, which is the RJ-45 console port by default.
2. Set the Mini-USB Type-B console port as the active console port by using the `port-type` command.

   By default, the RJ-45 port is set as an active console port and the Mini-USB Type-B port is the passive console port.
3. Reboot the device.
4. Connect the Standard-A connector of the Mini-USB cable to the host machine (PC or laptop).

5. Connect the Mini-USB Type-B (5-pin) connector of the Mini-USB cable to the Mini-USB Type-B console port (labeled **CON**) on the device.

After the connection is established, the Mini-USB Type-B console port becomes the active console port. The host machine connected to the Mini-USB Type-B console port displays log messages and enables you to control the device functionality through it.

Configuring Junos OS on the SRX380

IN THIS SECTION

The services gateway is shipped with the Juniper Networks Junos operating system (Junos OS) preinstalled and ready to be configured when the device is powered on. You can perform the initial software configuration of the services gateway by using any one of the following methods:

- J-Web Setup wizard
- Command-line interface (CLI)

Understanding SRX380 Firewall Factory-Default Settings

The SRX380 device is shipped with the with the factory-default settings listed in Table 18 on page 43, Table 19 on page 43, Table 20 on page 43, and Table 21 on page 43.

Table 18: Security Policies

Source Zone	Destination Zone	Policy Action
trust	trust	permit
trust	untrust	permit

Table 19: NAT Rules

Source Zone	Destination Zone	Policy Action
trust	untrust	Source NAT to untrust zone interface

Table 20: Ethernet Interfaces

Port Label	Interface	Security Zone	DHCP State	IP Address
0/0 and 0/19	ge-0/0/0 and xe-0/0/19	untrust	Client	Unassigned
0/1 to 0/18	VLAN Interface irb.0 (ge-0/0/1 to ge-0/0/15) (xe-0/0/16 to xe-0/0/18)	trust	Server	192.168.2.1/24
MGMT	fxp0		Server	192.168.1.1/24

Table 21: LTE Interfaces

Interface	Security Zone	IP Address
cl-1/0/0	N/A	N/A
dl0 (logical)	untrust	ISP assigned*

*Only if the LTE Mini-PIM is present

The SRX380 device is shipped with the following services and protocols enabled by default:

Table 22: Services, Protocols, and Startup Mode

Services	Protocols	Device Startup Mode
SSH HTTPS NETCONF over SSH	RSTP (all interfaces)	Switching

To provide secure traffic, a basic set of screens are configured on the untrust zone.

Initial Configuration

IN THIS SECTION

You can configure the device using either the J-Web or CLI:

Initial Configuration Using J-Web

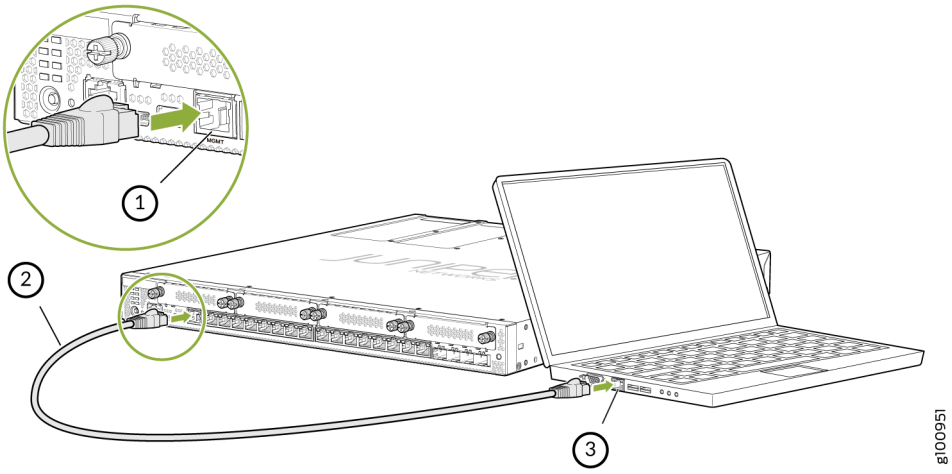
To configure root authentication:

1. Connect one end of the Ethernet cable to the management port (labeled **MGMT**) on the device.

   NOTE: You can also connect any of the network ports numbered 0/1 through 0/15 to the Ethernet port on the management device.

2. Connect the other end of the Ethernet cable to the management device.

Figure 17: Connecting the SRX380 to a Management Device



The SRX380 functions as a DHCP server and automatically assigns an IP address to the laptop.

3. Ensure that the laptop acquires an IP address on the 192.168.1.0/24 network.
4. If the laptop is unable to acquire an IP address, manually configure an IP address in the 192.168.1.0/24 network.

> **NOTE**: Be sure you don't assign the IP address 192.168.1.1 to the laptop as this is the IP address assigned to the SRX380.

5. Open a browser and type https://192.168.1.1. No login is required.

   The J-Web Setup wizard opens on your screen.
6. Click **Skip** in the upper-right corner of the Setup wizard.
7. Set a root authentication password and click OK.

   The J-Web login page appears.
8. Log in using the root authentication password.

   The J-Web Setup application displays.

Configuring the SRX380 Firewall Using CLI

To configure Junos OS on the SRX380 using CLI:

1. Connect the console port to a laptop or PC by using the RJ-45 to DB-9 serial port adapter.

   An Ethernet cable that has an RJ-45 connector at either end and an RJ-45 to DB-9 serial port adapter.

2. Start the CLI.

```
root@% cli
root>
```

> **NOTE**: You can view the factory-default settings by using the show configuration command.

3. Enter configuration mode.

```
root> configure
[edit]
root#
```

4. Set the root authentication password by entering a cleartext password, an encrypted password, or an SSH public key string (DSA or RSA).

```
[edit]
root# set system root-authentication plain-text-password
New password: password
Retype new password: password
```

5. Commit the configuration to activate it on the services gateway.

```
[edit]
root# commit
```

Plug and Play

The SRX380 already has factory-default settings configured to make it a plug and play device. So all you have to do to get the SRX380 up and running is connect it to your LAN and WAN networks.

1. Connect the WAN network to port **0/0**.
2. Connect the LAN network to any of the ports from **0/1** through **0/18**.
3. Check to see if the SRX380 is connected to the Internet. Go to http://www.juniper.net. If the page does not load, check the Internet connection.

After you complete these steps, you can start using the SRX380 on your network right away. You can go back and customize settings at anytime. The J-Web Setup wizard is always available to you.

Configure the SRX380 Using J-Web

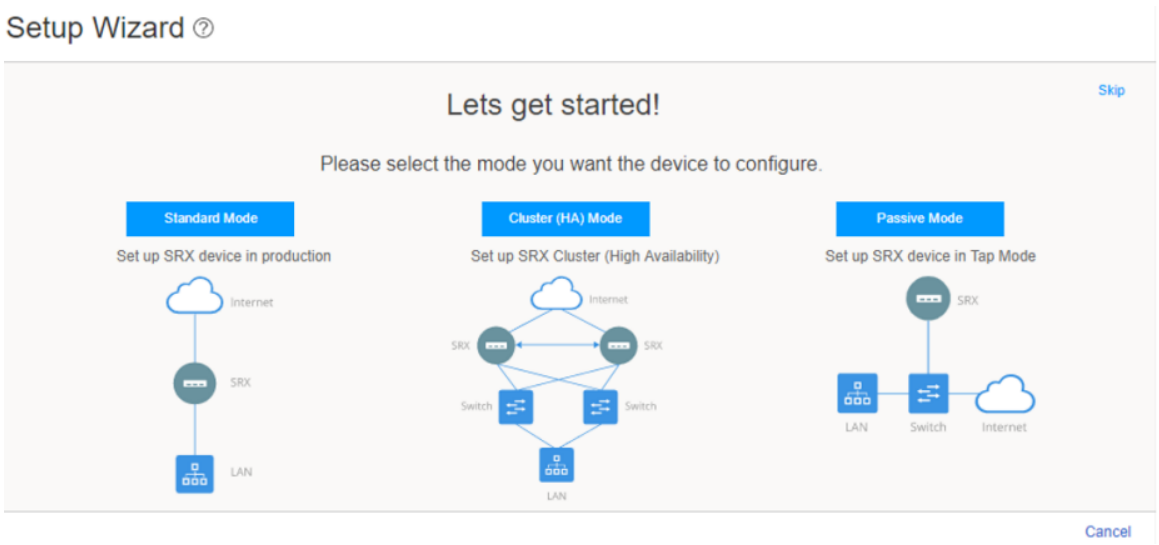
You can modify the configuration using J-Web. Have the following information ready before you start the configuration process:

- Hostname
- Root authentication password
- IP address for the NTP server
- IP address for the DNS server
- IP address for the management interface

To modify the configuration using J-Web:

1. In the J-Web application, select **Configure > Setup Wizard**. The Setup wizard opens on your screen.

Figure 18: Setup Wizard Page



2. Select **Standard**.
3. Configure the device and users:
   a. Enter the hostname.

b. (Optional) Allow root access.

c. Enter the root authentication password.

d. (Optional) Add user accounts.

e. Click **Next**.

> **NOTE**: Once you specify the hostname and root password, you can skip all the other steps and apply the configuration.

4. Set the time and configure the DNS server:

   a. Set the time manually or configure an NTP server.

   b. Select the time zone from the drop-down box.

   c. Type the IP address for the DNS server.

   d. Click **Next**.

5. Configure the management interface:

   a. Select the management port.

   b. Type the IP address for the management interface and the static route if it is needed to reach the SRX380 via the management interface.

   c. Click **Next**.

6. Configure zones and associate interfaces to the zones. You can use the default settings and click **Next**.

7. Set up additional services and security policies, or just click **Finish** and set it up later.

   The Setup Wizard displays a summary of your configuration settings.

8. You can edit any setting or click **OK**.

   Once you click **OK**, the Setup Wizard applies your configuration.

   > **NOTE**: You might lose connectivity to the SRX380 device if you changed the IP address of the port to which the laptop is connected. If you lose connectivity, open a new browser window and type https://<new IP address> to access J-Web again.

9. Click **Close** to end the Setup Wizard.

   The J-Web login screen automatically displays on your screen. You can now log in with the root authentication password.

Viewing Factory-Default Settings

To view the factory-default settings on your services gateway:

1. Log in as the root user and provide your credentials.
2. View the list of default config files:

```
user@host>file list /etc/config
```

3. View the required default config file.

```
user@host> file show /etc/config/<config file name>
```

When you commit changes to the configuration, a new configuration file is created, which becomes the active configuration. If the current active configuration fails, you can use the `load factory-default` command to revert to the factory-default configuration.

CHAPTER 4

Maintaining Components

Maintaining SRX380 Components

IN THIS SECTION

Routine Maintenance Procedures for the SRX380 Firewall

For optimum performance of the SRX380, perform the following preventive maintenance procedures regularly:

- Inspect the installation site for moisture, loose wires or cables, and excessive dust.
- Make sure that airflow is unobstructed around the services gateway and into the air intake vents.
- Check the status LEDs on the front panel of the services gateway.

Maintaining the SRX380 Firewall Cooling System Components

The fan controller works to maintain an optimal temperature for the services gateway. If the fan controller fails, the temperature of the services gateway will exceed the maximum working temperature and the device will fail. Make sure that you maintain the recommended clearances behind the services gateway to enable the fan controller to function optimally.

Maintaining the SRX380 Firewall Power Supply

To maintain the power supplies of the services gateway:

- Make sure that all power cables are arranged so that they do not obstruct access to other components of the services gateway.

- Routinely check the LEDs on the power supplies at the rear of the chassis. If the LEDs are lit solid green, then the power supplies are functioning normally.
- Periodically inspect the site to ensure that the power cables connected to the services gateway are securely in place and that there is no moisture accumulating near the services gateway.
- Check the status of the power supplies on the device by using the `show chassis environment` or `show chassis hardware` command. The output is similar to the following:

```
user@host> show chassis environment
Class Item                          Status     Measurement
Temp  Routing Engine                OK         42 degrees C / 107 degrees F
      Routing Engine CPU            OK         59 degrees C / 138 degrees F
Fans  SRX380 Chassis fan 0          OK         Spinning at normal speed
      SRX380 Chassis fan 1          OK         Spinning at normal speed
      SRX380 Chassis fan 2          OK         Spinning at normal speed
Power Power Supply 0                OK
      Power Supply 1                Absent
```

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                EW4519AF0040      SRX380-POE-AC
Routing Engine   REV 03   650-097090   EW4519AF0040      RE-SRX380-POE-AC
FPC 0                                                     FPC
  PIC 0                                                   16xGE,4*SFP+ Base PIC
Power Supply 0   REV 04   640-060602   1EDX933076P       JPSU-600W-AC-AFO
```

Removing and Installing SRX380 Power System Components

IN THIS SECTION

Remove an AC Power Supply on SRX380 Devices

The power supplies in an SRX380 are hot-removable and hot-insertable field-replaceable units (FRUs) installed in the rear panel of the device. You can remove and replace the power supplies without powering off the device.

NOTE: If only one power supply is installed in the device, you must power off the device before removing the power supply.

Before you remove a power supply, ensure that you have taken the necessary precautions to prevent electrostatic discharge (ESD) damage (see "Prevention of Electrostatic Discharge Damage" on page 71).

Ensure that you have the following parts and tools available:

- ESD grounding strap
- Phillips (+) screwdriver, number 2 (not provided)
- Antistatic bag or an antistatic mat
- Replacement power supply or a cover panel for the power supply slot

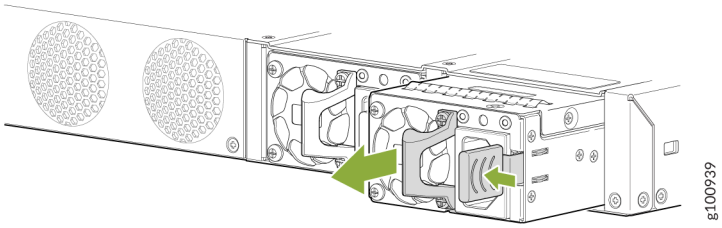
CAUTION: We recommend that you install either a replacement power supply or a cover panel in the empty power supply slot to prevent chassis overheating and dust accumulation.

To remove an AC power supply from the device (see Figure 19 on page 54):

1. Place the antistatic bag or the antistatic mat on a flat, stable surface.
2. Wrap and fasten one end of the ESD grounding strap around your wrist and connect the other end to a site ESD point.
3. If the AC power source outlet has a power switch, set it to the OFF (**O**) position.
4. Gently pull out the plug end of the power cord connected to the power source outlet.
5. Remove the power cord from the power supply faceplate by detaching the power cord retainer and gently pulling out the socket end of the power cord connected to the power supply faceplate.
6. Slide the ejector lever toward the left until the power supply is unseated.

7. Grasp the power supply handle and pull firmly to slide the power supply halfway out of the chassis.
8. Place one hand under the power supply to support it and slide it completely out of the chassis. Take care not to touch power supply components, pins, leads, or solder connections.
9. Place the power supply in the antistatic bag or on the antistatic mat placed on a flat, stable surface.
10. If you are not replacing the power supply, install a cover panel over the slot.

Figure 19: Removing an AC Power Supply from an SRX380 Device



Install an AC Power Supply on SRX380 Devices

Before you install an AC power supply in the device:

- Ensure that you have the following parts and tools available to install the power supply:
  - ESD grounding strap
  - Phillips (+) screwdriver, number 2
- Ensure you understand how to prevent electrostatic discharge (ESD) damage. See "Prevention of Electrostatic Discharge Damage" on page 71.

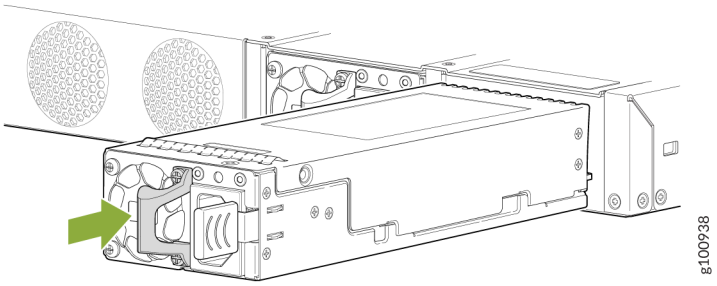
NOTE: Each power supply must be connected to a dedicated power source outlet. The device is shipped with one power supply preinstalled. You can order additional power supplies separately. You can install up to two power supplies in the device.

To install an AC power supply in the device (see Figure 20 on page 55):

1. Wrap and fasten one end of the ESD grounding strap around your wrist and connect the other end to a site ESD point.

2. If the power supply slot has a cover panel on it, loosen the captive screws on the cover panel by using your fingers or the screwdriver. Hold the captive screws and gently pull the screws outward to remove the cover panel. Save the cover panel for later use.
3. Taking care not to touch power supply pins, leads, or solder connections, remove the power supply from the bag.
4. Using both hands, place the power supply in the power supply slot on the rear panel of the device and slide it in until it is fully seated and the ejector lever fits into place.

Figure 20: Installing an AC Power Supply in an SRX380 Device



NOTE: If you have a Juniper J-Care service contract, register any addition, change, or upgrade of hardware components at https://www.juniper.net/customers/support/tools/updateinstallbase/. Failure to do so can result in significant delays if you need replacement parts. This note does not apply if you replace existing components with the same type of component.

Removing and Installing Mini-PIMs

IN THIS SECTION

Before you begin, power off the services gateway.

CAUTION: The Mini-Physical Interface Modules (Mini-PIMs) are not hot-swappable. You must power off the services gateway before removing or installing Mini-PIMs.

To maintain proper airflow through the services gateway, cover any empty Mini-PIM slot with a blank faceplate.

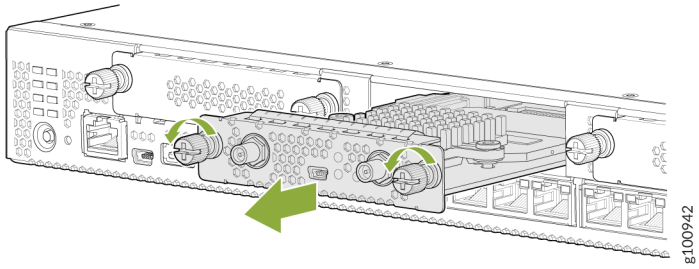
CAUTION: Do not remove a blank faceplate that covers an empty Mini-PIM slot unless you are installing a Mini-PIM in the empty slot.

Remove a Mini-Physical Interface Module

To remove a Mini-PIM from the services gateway (see Figure 21 on page 57):

1. Place an electrostatic bag or antistatic mat on a flat, stable surface on which you intend to place the Mini-PIM.
2. Wrap and fasten one end of the ESD grounding strap around your wrist and connect the other end to a site ESD point.
3. Unplug the power adapter from the services gateway.
4. Verify that the Power LED is off.
5. Label the cables connected to the Mini-PIM so that you can reconnect each cable correctly.
6. Disconnect the cables from the Mini-PIM.
7. If necessary, arrange the cables to prevent them from dislodging or developing stress points.
8. Remove the screws on each side of the Mini-PIM faceplate.
9. Grasp the screws on each side of the Mini-PIM faceplate and slide the Mini-PIM out of the services gateway.

Figure 21: Removing a Mini-PIM from an SRX380 Device



10. Place the Mini-PIM in the electrostatic bag or on the antistatic mat.
11. If you are not installing a replacement Mini-PIM into the empty slot, install a blank faceplate over the slot to maintain proper airflow.

Install a Mini-Physical Interface Module

To install a Mini-Physical Interface Module (Mini-PIM) in the services gateway (see Figure 22 on page 58):

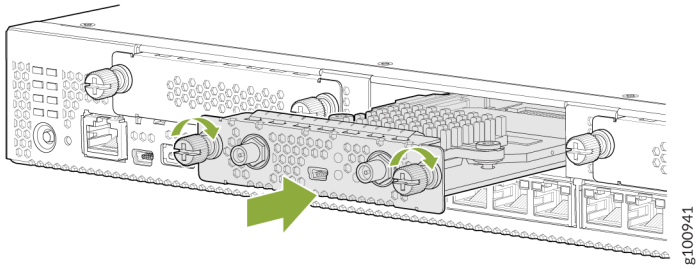
1. Wrap and fasten one end of the ESD grounding strap around your wrist and connect the other end to a site ESD point.
2. Power off the services gateway by briefly pressing the Power button on the front panel. Wait for the Power LED to turn off before proceeding. Disconnect the services gateway from its power source.
3. Remove the Mini-PIM from the electrostatic bag.
4. Grasp the screws on each side of the Mini-PIM faceplate and align the notches in the connector at the rear of the Mini-PIM with the notches in the Mini-PIM slot in the device.

> ⚠ **CAUTION**: Slide the Mini-PIM straight into the slot to avoid damaging the components of the Mini-PIM.

5. Slide the Mini-PIM in until it is fully seated in the services gateway.
6. Tighten the screws on each side of the Mini-PIM faceplate.
7. Insert the appropriate cables into the cable connectors on the Mini-PIM.
8. If necessary, arrange the cables to prevent them from dislodging or developing stress points:
   - Secure the cables so that they are not supporting their own weight as they hang to the floor.
   - Place any excess cables out of the way in neatly coiled loops.

- Use fasteners to maintain the shape of the cable loops.

Figure 22: Installing a Mini-PIM in an SRX380 Device



9. Reconnect the power adapter to the services gateway. Verify that the Power LED glows steadily green after you press the power button.
10. Verify that the Mini-PIM LED on the device chassis glows steadily green to confirm that the Mini-PIM is online.

5

CHAPTER

Contacting Customer Support and Returning the Chassis or Components

Returning the SRX380 Chassis or Components

IN THIS SECTION

Contacting Customer Support

Once you have located the serial numbers of the device or component, you can return the device or component for repair or replacement. For this, you need to contact Juniper Networks Technical Assistance Center (JTAC).

You can contact JTAC 24 hours a day, 7 days a week, using any of the following methods:

- On the Web: Using the Service Request Manager link at https://support.juniper.net/support/
- By telephone:
  - From the US and Canada: 1-888-314-JTAC
  - From all other locations: 1-408-745-9500

> **NOTE**: If contacting JTAC by telephone, enter your 12-digit service request number followed by the pound (#) key if this is an existing case, or press the star (*) key to be routed to the next available support engineer.

When requesting support from JTAC by telephone, be prepared to provide the following information:

- Your existing service request number, if you have one

- Details of the failure or problem
- Type of activity being performed on the firewall when the problem occurred
- Configuration data displayed by one or more `show` commands
- Your name, organization name, telephone number, fax number, and shipping address

The support representative validates your request and issues a Return Materials Authorization (RMA) number for return of the device or component.

Returning an SRX380 Firewall or Component to Juniper Networks

To return an SRX380 Firewall or component to Juniper Networks for repair or replacement:

1. Determine the part number and serial number of the services gateway or component.
2. Obtain a Return Materials Authorization (RMA) number from JTAC.

   NOTE: Do not return the services gateway or any component to Juniper Networks unless you have first obtained an RMA number. Juniper Networks reserves the right to refuse shipments that do not have an RMA number. Refused shipments are returned to the customer via collect freight.

3. Pack the services gateway or component for shipping.

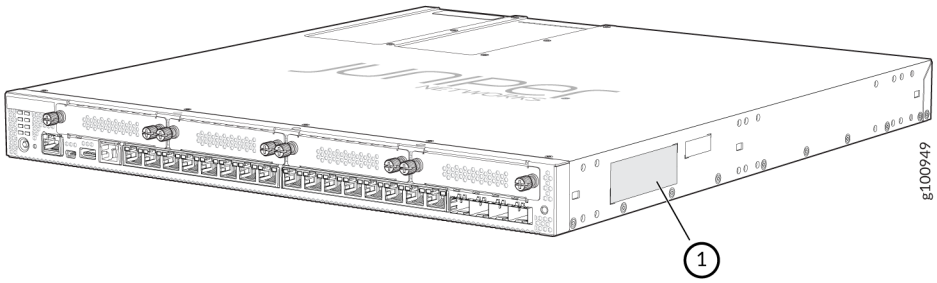
For more information about return and repair policies, see the customer support webpage at https://www.juniper.net/support/guidelines.html.

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

Locating the Chassis Serial Number

The chassis serial number is located on the side of the chassis.

Figure 23: Location of the Serial Number Label



Locating the Mini-PIM Serial Number Label

Mini-Physical Interface Modules (Mini-PIMs) are field-replaceable and each Mini-PIM has a unique serial number. The serial number label is located on the right side of the Mini-PIM, when the Mini-PIM is horizontally oriented (as it would be when installed on the device). The exact location might be slightly different on different Mini-PIMs, depending on the placement of components on the Mini-PIM.

Listing the SRX380 Firewall Component Details by Using the CLI

Before contacting Juniper Networks to request an RMA, you must find the serial number of the SRX380 Firewall or component.

Use the `show chassis hardware` command to view all the components of an SRX380 Firewall and the corresponding serial numbers.

```
user@host>
```

NOTE: In the output of the `show chassis hardware` command, the Mini-PIM slot number is reported as an FPC number, and the Mini-PIM number (always 0) is reported as the PIC number.

Most components also have a serial number ID label affixed to the component body.

Required Tools and Parts for Packing the SRX Series Services Gateway

To remove one or more components from the SRX Series Services Gateway or to remove the services gateway from a rack, you need the following tools and parts:

- Electrostatic bag or antistatic mat for each component
- Electrostatic discharge (ESD) grounding wrist strap
- Flat-blade screwdriver, approximately 1/4 in. (6 mm)
- Phillips (+) screwdrivers, numbers 1 and 2

Packing the SRX Series Services Gateway for Shipment

To pack the SRX Series Services Gateway for shipment:

1. Retrieve the shipping carton and packing materials in which the services gateway was originally shipped. If you do not have these materials, contact your Juniper Networks representative about approved packaging materials.
2. Wrap and fasten an electrostatic discharge (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. On the console or other management device connected to the services gateway, enter CLI operational mode, and then shut down the services gateway software:

   ```
   user@host> request system halt
   ```

   Wait until a message appears on the console confirming that the operating system has halted.
4. Shut down power to the services gateway by pressing the Power button on the front of the services gateway.
5. Disconnect power from the services gateway.
6. Remove the cables that connect to all external devices.
7. If the device is installed on a wall or rack, have one person support the weight of the device while another person unscrews and removes the mounting screws.
8. Place the services gateway in the shipping carton.
9. Cover the services gateway with an ESD bag, and place the packing foam on top of and around the device.
10. Replace the accessory box on top of the packing foam.
11. Securely tape the box closed.

12. Write the Return Materials Authorization (RMA) number on the exterior of the box to ensure proper tracking.

Packing SRX Series Services Gateway Components for Shipment

To pack and ship individual components of the services gateway:

1. Make sure that it is adequately protected with packing materials and securely packed so that the pieces do not move around inside the carton.
2. Use the original shipping materials if they are available.
3. Place each component in an individual electrostatic bag.
4. Write the Return Materials Authorization (RMA) number on the exterior of the box to ensure proper tracking.

CAUTION: Do not stack any of the services gateway components while packing them.

CHAPTER 6

Safety and Compliance Information

Definitions of Safety Warning Levels

The documentation uses the following levels of safety warnings (there are two *Warning* formats):

NOTE: You might find this information helpful in a particular situation, or you might overlook this important information if it was not highlighted in a Note.

CAUTION: You need to observe the specified guidelines to prevent minor injury or discomfort to you or severe damage to the device.

Attention Veillez à respecter les consignes indiquées pour éviter toute incommodité ou blessure légère, voire des dégâts graves pour l'appareil.

LASER WARNING: This symbol alerts you to the risk of personal injury from a laser.

Avertissement Ce symbole signale un risque de blessure provoquée par rayon laser.

WARNING: This symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry, and familiarize yourself with standard practices for preventing accidents.

Waarschuwing Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen.

Varoitus Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista.

Avertissement Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents.

Warnung Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt.

Avvertenza Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti.

Advarsel Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker.

Aviso Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes.

¡Atención! Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes.

Varning! Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador.

General Safety Guidelines and Warnings

The following guidelines help ensure your safety and protect the device from damage. The list of guidelines might not address all potentially hazardous situations in your working environment, so be alert and exercise good judgment at all times.

- Perform only the procedures explicitly described in the hardware documentation for this device. Make sure that only authorized service personnel perform other system services.
- Keep the area around the device clear and free from dust before, during, and after installation.
- Keep tools away from areas where people could trip over them while walking.

- Do not wear loose clothing or jewelry, such as rings, bracelets, or chains, which could become caught in the device.
- Wear safety glasses if you are working under any conditions that could be hazardous to your eyes.
- Do not perform any actions that create a potential hazard to people or make the equipment unsafe.
- Never attempt to lift an object that is too heavy for one person to handle.
- Never install or manipulate wiring during electrical storms.
- Never install electrical jacks in wet locations unless the jacks are specifically designed for wet environments.
- Operate the device only when it is properly grounded.
- Follow the instructions in this guide to properly ground the device to earth.
- Replace fuses only with fuses of the same type and rating.
- Do not open or remove chassis covers or sheet-metal parts unless instructions are provided in the hardware documentation for this device. Such an action could cause severe electrical shock.
- Do not push or force any objects through any opening in the chassis frame. Such an action could result in electrical shock or fire.
- Avoid spilling liquid onto the chassis or onto any device component. Such an action could cause electrical shock or damage the device.
- Avoid touching uninsulated electrical wires or terminals that have not been disconnected from their power source. Such an action could cause electrical shock.
- Some parts of the chassis, including AC and DC power supply surfaces, power supply unit handles, SFB card handles, and fan tray handles might become hot. The following label provides the warning for hot surfaces on the chassis:

- Always ensure that all modules, power supplies, and cover panels are fully inserted and that the installation screws are fully tightened.

Restricted Access Warning

WARNING: This unit is intended for installation in restricted access areas. A restricted access area is an area to which access can be gained only by service personnel through the use of a special tool, lock and key, or other means of security, and which is controlled by the authority responsible for the location.

Waarschuwing Dit toestel is bedoeld voor installatie op plaatsen met beperkte toegang. Een plaats met beperkte toegang is een plaats waar toegang slechts door servicepersoneel verkregen kan worden door middel van een speciaal instrument, een slot en sleutel, of een ander veiligheidsmiddel, en welke beheerd wordt door de overheidsinstantie die verantwoordelijk is voor de locatie.

Varoitus Tämä laite on tarkoitettu asennettavaksi paikkaan, johon pääsy on rajoitettua. Paikka, johon pääsy on rajoitettua, tarkoittaa paikkaa, johon vain huoltohenkilöstö pääsee jonkin erikoistyökalun, lukkoon sopivan avaimen tai jonkin muun turvalaitteen avulla ja joka on paikasta vastuussa olevien toimivaltaisten henkilöiden valvoma.

Avertissement Cet appareil est à installer dans des zones d'accès réservé. Ces dernières sont des zones auxquelles seul le personnel de service peut accéder en utilisant un outil spécial, un mécanisme de verrouillage et une clé, ou tout autre moyen de sécurité. L'accès aux zones de sécurité est sous le contrôle de l'autorité responsable de l'emplacement.

Warnung Diese Einheit ist zur Installation in Bereichen mit beschränktem Zutritt vorgesehen. Ein Bereich mit beschränktem Zutritt ist ein Bereich, zu dem nur Wartungspersonal mit einem Spezialwerkzeugs, Schloß und Schlüssel oder anderer Sicherheitsvorkehrungen Zugang hat, und der von dem für die Anlage zuständigen Gremium kontrolliert wird.

Avvertenza Questa unità deve essere installata in un'area ad accesso limitato. Un'area ad accesso limitato è un'area accessibile solo a personale di assistenza tramite un'attrezzo speciale, lucchetto, o altri dispositivi di sicurezza, ed è controllata dall'autorità responsabile della zona.

Advarsel Denne enheten er laget for installasjon i områder med begrenset adgang. Et område med begrenset adgang gir kun adgang til servicepersonale som bruker et spesielt verktøy, lås og nøkkel, eller en annen sikkerhetsanordning, og det kontrolleres av den autoriteten som er ansvarlig for området.

Aviso Esta unidade foi concebida para instalação em áreas de acesso restrito. Uma área de acesso restrito é uma área à qual apenas tem acesso o pessoal de serviço autorizado,

que possua uma ferramenta, chave e fechadura especial, ou qualquer outra forma de segurança. Esta área é controlada pela autoridade responsável pelo local.

¡Atención! Esta unidad ha sido diseñada para instalarse en áreas de acceso restringido. Área de acceso restringido significa un área a la que solamente tiene acceso el personal de servicio mediante la utilización de una herramienta especial, cerradura con llave, o algún otro medio de seguridad, y que está bajo el control de la autoridad responsable del local.

Varning! Denna enhet är avsedd för installation i områden med begränsat tillträde. Ett område med begränsat tillträde får endast tillträdas av servicepersonal med ett speciellt verktyg, lås och nyckel, eller annan säkerhetsanordning, och kontrolleras av den auktoritet som ansvarar för området.

Qualified Personnel Warning

WARNING: Only trained and qualified personnel should install or replace the device.
Waarschuwing Installatie en reparaties mogen uitsluitend door getraind en bevoegd personeel uitgevoerd worden.

Varoitus Ainoastaan koulutettu ja pätevä henkilökunta saa asentaa tai vaihtaa tämän laitteen.

Avertissement Tout installation ou remplacement de l'appareil doit être réalisé par du personnel qualifié et compétent.

Warnung Gerät nur von geschultem, qualifiziertem Personal installieren oder auswechseln lassen.

Avvertenza Solo personale addestrato e qualificato deve essere autorizzato ad installare o sostituire questo apparecchio.

Advarsel Kun kvalifisert personell med riktig opplæring bør montere eller bytte ut dette utstyret.

Aviso Este equipamento deverá ser instalado ou substituído apenas por pessoal devidamente treinado e qualificado.

¡Atención! Estos equipos deben ser instalados y reemplazados exclusivamente por personal técnico adecuadamente preparado y capacitado.

Varning! Denna utrustning ska endast installeras och bytas ut av utbildad och kvalificerad personal.

Prevention of Electrostatic Discharge Damage

Device components that are shipped in antistatic bags are sensitive to damage from static electricity. Some components can be impaired by voltages as low as 30 V. You can easily generate potentially damaging static voltages whenever you handle plastic or foam packing material or if you move components across plastic or carpets. Observe the following guidelines to minimize the potential for electrostatic discharge (ESD) damage, which can cause intermittent or complete component failures:

- Always use an ESD wrist strap when you are handling components that are subject to ESD damage, and make sure that it is in direct contact with your skin.

  If a grounding strap is not available, hold the component in its antistatic bag (see Figure 24 on page 72) in one hand and touch the exposed, bare metal of the device with the other hand immediately before inserting the component into the device.

  WARNING: For safety, periodically check the resistance value of the ESD grounding strap. The measurement must be in the range 1 through 10 Mohms.
  Avertissement Par mesure de sécurité, vérifiez régulièrement la résistance du bracelet antistatique. Cette valeur doit être comprise entre 1 et 10 mégohms (Mohms).

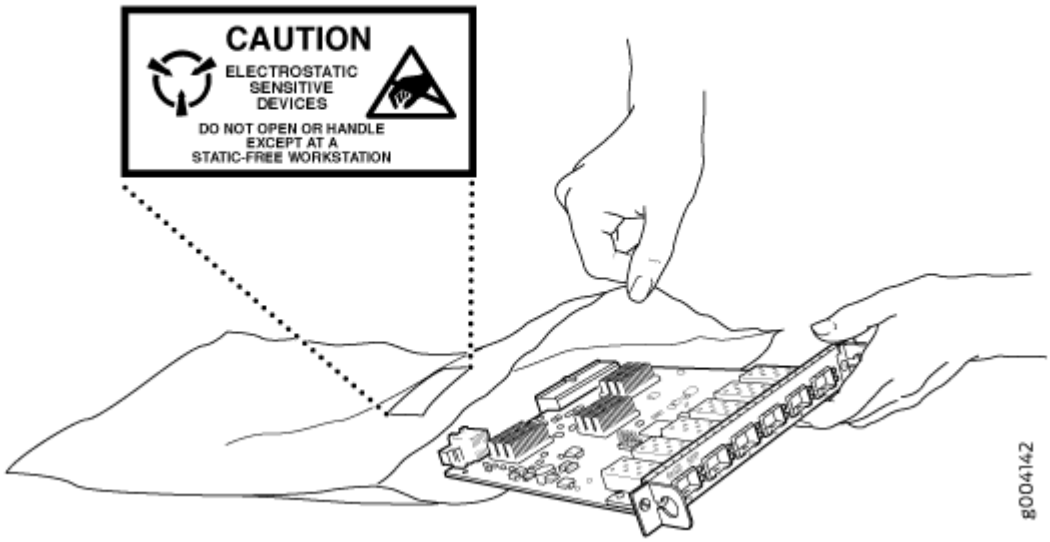
- When handling any component that is subject to ESD damage and that is removed from the device, make sure the equipment end of your ESD wrist strap is attached to the ESD point on the chassis.

  If no grounding strap is available, touch the exposed, bare metal of the device to ground yourself before handling the component.

- Avoid contact between the component that is subject to ESD damage and your clothing. ESD voltages emitted from clothing can damage components.

- When removing or installing a component that is subject to ESD damage, always place it component-side up on an antistatic surface, in an antistatic card rack, or in an antistatic bag (see Figure 24 on page 72). If you are returning a component, place it in an antistatic bag before packing it.

Figure 24: Placing a Component into an Antistatic Bag



CAUTION: ANSI/TIA/EIA-568 cables such as Category 5e and Category 6 can get electrostatically charged. To dissipate this charge, always ground the cables to a suitable and safe earth ground before connecting them to the system.

Attention Les câbles ANSI/TIA/EIA-568, par exemple Cat 5e et Cat 6, peuvent emmagasiner des charges électrostatiques. Pour évacuer ces charges, reliez toujours les câbles à une prise de terre adaptée avant de les raccorder au système.

Fire Safety Requirements

IN THIS SECTION

In the event of a fire emergency, the safety of people is the primary concern. You should establish procedures for protecting people in the event of a fire emergency, provide safety training, and properly provision fire-control equipment and fire extinguishers.

In addition, you should establish procedures to protect your equipment in the event of a fire emergency. Juniper Networks products should be installed in an environment suitable for electronic equipment. We recommend that fire suppression equipment be available in the event of a fire in the vicinity of the equipment and that all local fire, safety, and electrical codes and ordinances be observed when you install and operate your equipment.

Fire Suppression

In the event of an electrical hazard or an electrical fire, you should first turn power off to the equipment at the source. Then use a Type C fire extinguisher, which uses noncorrosive fire retardants, to extinguish the fire.

Fire Suppression Equipment

Type C fire extinguishers, which use noncorrosive fire retardants such as carbon dioxide and Halotron™, are most effective for suppressing electrical fires. Type C fire extinguishers displace oxygen from the point of combustion to eliminate the fire. For extinguishing fire on or around equipment that draws air from the environment for cooling, you should use this type of inert oxygen displacement extinguisher instead of an extinguisher that leaves residues on equipment.

Do not use multipurpose Type ABC chemical fire extinguishers (dry chemical fire extinguishers). The primary ingredient in these fire extinguishers is monoammonium phosphate, which is very sticky and difficult to clean. In addition, in the presence of minute amounts of moisture, monoammonium phosphate can become highly corrosive and corrodes most metals.

Any equipment in a room in which a chemical fire extinguisher has been discharged is subject to premature failure and unreliable operation. The equipment is considered to be irreparably damaged.

NOTE: To keep warranties effective, do not use a dry chemical fire extinguisher to control a fire at or near a Juniper Networks device. If a dry chemical fire extinguisher is used, the unit is no longer eligible for coverage under a service agreement.

We recommend that you dispose of any irreparably damaged equipment in an environmentally responsible manner.

Laser and LED Safety Guidelines and Warnings

IN THIS SECTION

Juniper Networks devices are equipped with laser transmitters, which are considered a Class 1 Laser Product by the U.S. Food and Drug Administration and are evaluated as a Class 1 Laser Product per IEC/EN 60825-1 requirements.

Observe the following guidelines and warnings:

General Laser Safety Guidelines

When working around ports that support optical transceivers, observe the following safety guidelines to prevent eye injury:

- Do not look into unterminated ports or at fibers that connect to unknown sources.
- Do not examine unterminated optical ports with optical instruments.
- Avoid direct exposure to the beam.

LASER WARNING: Unterminated optical connectors can emit invisible laser radiation. The lens in the human eye focuses all the laser power on the retina, so focusing the eye directly on a laser source—even a low-power laser—could permanently damage the eye.

Avertissement Les connecteurs à fibre optique sans terminaison peuvent émettre un rayonnement laser invisible. Le cristallin de l'œil humain faisant converger toute la puissance du laser sur la rétine, toute focalisation directe de l'œil sur une source laser, —même de faible puissance—, peut entraîner des lésions oculaires irréversibles.

Class 1 Laser Product Warning

LASER WARNING: Class 1 laser product.
Waarschuwing Klasse-1 laser produkt.

Varoitus Luokan 1 lasertuote.

Avertissement Produit laser de classe I.

Warnung Laserprodukt der Klasse 1.

Avvertenza Prodotto laser di Classe 1.

Advarsel Laserprodukt av klasse 1.

Aviso Produto laser de classe 1.

¡Atención! Producto láser Clase I.

Varning! Laserprodukt av klass 1.

Class 1 LED Product Warning

LASER WARNING: Class 1 LED product.
Waarschuwing Klasse 1 LED-product.

Varoitus Luokan 1 valodiodituote.

Avertissement Alarme de produit LED Class I.

Warnung Class 1 LED-Produktwarnung.

Avvertenza Avvertenza prodotto LED di Classe 1.

Advarsel LED-produkt i klasse 1.

Aviso Produto de classe 1 com LED.

¡Atención! Aviso sobre producto LED de Clase 1.

Varning! Lysdiodprodukt av klass 1.

Laser Beam Warning

LASER WARNING: Do not stare into the laser beam or view it directly with optical instruments.
Waarschuwing Niet in de straal staren of hem rechtstreeks bekijken met optische instrumenten.

Varoitus Älä katso säteeseen äläkä tarkastele sitä suoraan optisen laitteen avulla.

Avertissement Ne pas fixer le faisceau des yeux, ni l'observer directement à l'aide d'instruments optiques.

Warnung Nicht direkt in den Strahl blicken und ihn nicht direkt mit optischen Geräten prüfen.

Avvertenza Non fissare il raggio con gli occhi né usare strumenti ottici per osservarlo direttamente.

Advarsel Stirr eller se ikke direkte p strlen med optiske instrumenter.

Aviso Não olhe fixamente para o raio, nem olhe para ele directamente com instrumentos ópticos.

¡Atención! No mirar fijamente el haz ni observarlo directamente con instrumentos ópticos.

Varning! Rikta inte blicken in mot strålen och titta inte direkt på den genom optiska instrument.

Radiation from Open Port Apertures Warning

LASER WARNING: Because invisible radiation might be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to radiation and do not stare into open apertures.
Waarschuwing Aangezien onzichtbare straling vanuit de opening van de poort kan komen als er geen fiberkabel aangesloten is, dient blootstelling aan straling en het kijken in open openingen vermeden te worden.

Varoitus Koska portin aukosta voi emittoitua näkymätöntä säteilyä, kun kuitukaapelia ei ole kytkettynä, vältä säteilylle altistumista äläkä katso avoimiin aukkoihin.

Avertissement Des radiations invisibles à l'il nu pouvant traverser l'ouverture du port lorsqu'aucun câble en fibre optique n'y est connecté, il est recommandé de ne pas regarder fixement l'intérieur de ces ouvertures.

Warnung Aus der Port-Öffnung können unsichtbare Strahlen emittieren, wenn kein Glasfaserkabel angeschlossen ist. Vermeiden Sie es, sich den Strahlungen auszusetzen, und starren Sie nicht in die Öffnungen!

Avvertenza Quando i cavi in fibra non sono inseriti, radiazioni invisibili possono essere emesse attraverso l'apertura della porta. Evitate di esporvi alle radiazioni e non guardate direttamente nelle aperture.

Advarsel Unngå utsettelse for stråling, og stirr ikke inn i åpninger som er åpne, fordi usynlig stråling kan emiteres fra portens åpning når det ikke er tilkoblet en fiberkabel.

Aviso Dada a possibilidade de emissão de radiação invisível através do orifício da via de acesso, quando esta não tiver nenhum cabo de fibra conectado, deverá evitar an EXposição à radiação e não deverá olhar fixamente para orifícios que se encontrarem a descoberto.

¡Atención! Debido a que la apertura del puerto puede emitir radiación invisible cuando no existe un cable de fibra conectado, evite mirar directamente a las aperturas para no exponerse a la radiación.

Varning! Osynlig strålning kan avges från en portöppning utan ansluten fiberkabel och du bör därför undvika att bli utsatt för strålning genom att inte stirra in i oskyddade öppningar.

Maintenance and Operational Safety Guidelines and Warnings

IN THIS SECTION

While performing the maintenance activities for devices, observe the following guidelines and warnings:

Battery Handling Warning

WARNING: Replacing a battery incorrectly might result in an explosion. Replace a battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Waarschuwing Er is ontploffingsgevaar als de batterij verkeerd vervangen wordt. Vervang de batterij slechts met hetzelfde of een equivalent type dat door de fabrikant aanbevolen is. Gebruikte batterijen dienen overeenkomstig fabrieksvoorschriften weggeworpen te worden.

Varoitus Räjähdyksen vaara, jos akku on vaihdettu väärään akkuun. Käytä vaihtamiseen ainoastaan saman- tai vastaavantyyppistä akkua, joka on valmistajan suosittelema. Hävitä käytetyt akut valmistajan ohjeiden mukaan.

Avertissement Danger d'explosion si la pile n'est pas remplacée correctement. Ne la remplacer que par une pile de type semblable ou équivalent, recommandée par le fabricant. Jeter les piles usagées conformément aux instructions du fabricant.

Warnung Bei Einsetzen einer falschen Batterie besteht Explosionsgefahr. Ersetzen Sie die Batterie nur durch den gleichen oder vom Hersteller empfohlenen Batterietyp. Entsorgen Sie die benutzten Batterien nach den Anweisungen des Herstellers.

Advarsel Det kan være fare for eksplosjon hvis batteriet skiftes på feil måte. Skift kun med samme eller tilsvarende type som er anbefalt av produsenten. Kasser brukte batterier i henhold til produsentens instruksjoner.

Avvertenza Pericolo di esplosione se la batteria non è installata correttamente. Sostituire solo con una di tipo uguale o equivalente, consigliata dal produttore. Eliminare le batterie usate secondo le istruzioni del produttore.

Aviso Existe perigo de explosão se a bateria for substituída incorrectamente. Substitua a bateria por uma bateria igual ou de um tipo equivalente recomendado pelo fabricante. Destrua as baterias usadas conforme as instruções do fabricante.

¡Atención! Existe peligro de explosión si la batería se reemplaza de manera incorrecta. Reemplazar la baterían EXclusivamente con el mismo tipo o el equivalente recomendado por el fabricante. Desechar las baterías gastadas según las instrucciones del fabricante.

Varning! Explosionsfara vid felaktigt batteribyte. Ersätt endast batteriet med samma batterityp som rekommenderas av tillverkaren eller motsvarande. Följ tillverkarens anvisningar vid kassering av använda batterier.

Jewelry Removal Warning

WARNING: Before working on equipment that is connected to power lines, remove jewelry, including rings, necklaces, and watches. Metal objects heat up when connected to power and ground and can cause serious burns or can be welded to the terminals.

Waarschuwing Alvorens aan apparatuur te werken die met elektrische leidingen is verbonden, sieraden (inclusief ringen, kettingen en horloges) verwijderen. Metalen voorwerpen worden warm wanneer ze met stroom en aarde zijn verbonden, en kunnen ernstige brandwonden veroorzaken of het metalen voorwerp aan de aansluitklemmen lassen.

Varoitus Ennen kuin työskentelet voimavirtajohtoihin kytkettyjen laitteiden parissa, ota pois kaikki korut (sormukset, kaulakorut ja kellot mukaan lukien). Metalliesineet kuumenevat, kun ne ovat yhteydessä sähkövirran ja maan kanssa, ja ne voivat aiheuttaa vakavia palovammoja tai hitsata metalliesineet kiinni liitäntänapoihin.

Avertissement Avant d'accéder à cet équipement connecté aux lignes électriques, ôter tout bijou (anneaux, colliers et montres compris). Lorsqu'ils sont branchés à l'alimentation et reliés à la terre, les objets métalliques chauffent, ce qui peut provoquer des blessures graves ou souder l'objet métallique aux bornes.

Warnung Vor der Arbeit an Geräten, die an das Netz angeschlossen sind, jeglichen Schmuck (einschließlich Ringe, Ketten und Uhren) abnehmen. Metallgegenstände erhitzen sich, wenn sie an das Netz und die Erde angeschlossen werden, und können schwere Verbrennungen verursachen oder an die Anschlußklemmen angeschweißt werden.

Avvertenza Prima di intervenire su apparecchiature collegate alle linee di alimentazione, togliersi qualsiasi monile (inclusi anelli, collane, braccialetti ed orologi). Gli oggetti metallici si riscaldano quando sono collegati tra punti di alimentazione e massa: possono causare ustioni gravi oppure il metallo può saldarsi ai terminali.

Advarsel Fjern alle smykker (inkludert ringer, halskjeder og klokker) før du skal arbeide på utstyr som er koblet til kraftledninger. Metallgjenstander som er koblet til kraftledninger og jord blir svært varme og kan forårsake alvorlige brannskader eller smelte fast til polene.

Aviso Antes de trabalhar em equipamento que esteja ligado a linhas de corrente, retire todas as jóias que estiver a usar (incluindo anéis, fios e relógios). Os objectos metálicos aquecerão em contacto com a corrente e em contacto com a ligação à terra, podendo causar queimaduras graves ou ficarem soldados aos terminais.

¡Atención! Antes de operar sobre equipos conectados a líneas de alimentación, quitarse las joyas (incluidos anillos, collares y relojes). Los objetos de metal se calientan cuando se conectan a la alimentación y a tierra, lo que puede ocasionar quemaduras graves o que los objetos metálicos queden soldados a los bornes.

Varning! Tag av alla smycken (inklusive ringar, halsband och armbandsur) innan du arbetar på utrustning som är kopplad till kraftledningar. Metallobjekt hettas upp när de kopplas ihop med ström och jord och kan förorsaka allvarliga brännskador; metallobjekt kan också sammansvetsas med kontakterna.

Lightning Activity Warning

WARNING: Do not work on the system or connect or disconnect cables during periods of lightning activity.

Waarschuwing Tijdens onweer dat gepaard gaat met bliksem, dient u niet aan het systeem te werken of kabels aan te sluiten of te ontkoppelen.

Varoitus Älä työskentele järjestelmän parissa äläkä yhdistä tai irrota kaapeleita ukkosilmalla.

Avertissement Ne pas travailler sur le système ni brancher ou débrancher les câbles pendant un orage.

Warnung Arbeiten Sie nicht am System und schließen Sie keine Kabel an bzw. trennen Sie keine ab, wenn es gewittert.

Avvertenza Non lavorare sul sistema o collegare oppure scollegare i cavi durante un temporale con fulmini.

Advarsel Utfør aldri arbeid på systemet, eller koble kabler til eller fra systemet når det tordner eller lyner.

Aviso Não trabalhe no sistema ou ligue e desligue cabos durante períodos de mau tempo (trovoada).

¡Atención! No operar el sistema ni conectar o desconectar cables durante el transcurso de descargas eléctricas en la atmósfera.

Varning! Vid åska skall du aldrig utföra arbete på systemet eller ansluta eller koppla loss kablar.

Operating Temperature Warning

WARNING: To prevent the device from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature. To prevent airflow restriction, allow at least 6 in. (15.2 cm) of clearance around the ventilation openings.

Waarschuwing Om te voorkomen dat welke switch van de Juniper Networks router dan ook oververhit raakt, dient u deze niet te bedienen op een plaats waar de maximale aanbevolen omgevingstemperatuur van 40° C wordt overschreden. Om te voorkomen dat de luchtstroom wordt beperkt, dient er minstens 15,2 cm speling rond de ventilatie-openingen te zijn.

Varoitus Ettei Juniper Networks switch-sarjan reititin ylikuumentuisi, sitä ei saa käyttää tilassa, jonka lämpötila ylittää korkeimman suositellun ympäristölämpötilan 40° C. Ettei ilmanvaihto estyisi, tuuletusaukkojen ympärille on jätettävä ainakin 15,2 cm tilaa.

Avertissement Pour éviter toute surchauffe des routeurs de la gamme Juniper Networks switch, ne l'utilisez pas dans une zone où la température ambiante est supérieure à 40° C. Pour permettre un flot d'air constant, dégagez un espace d'au moins 15,2 cm autour des ouvertures de ventilations.

Warnung Um einen Router der switch vor Überhitzung zu schützen, darf dieser nicht in einer Gegend betrieben werden, in der die Umgebungstemperatur das empfohlene

Maximum von 40° C überschreitet. Um Lüftungsverschluß zu verhindern, achten Sie darauf, daß mindestens 15,2 cm lichter Raum um die Lüftungsöffnungen herum frei bleibt.

Avvertenza Per evitare il surriscaldamento dei switch, non adoperateli in un locale che ecceda la temperatura ambientale massima di 40° C. Per evitare che la circolazione dell'aria sia impedita, lasciate uno spazio di almeno 15.2 cm di fronte alle aperture delle ventole.

Advarsel Unngå overoppheting av eventuelle rutere i Juniper Networks switch Disse skal ikke brukes på steder der den anbefalte maksimale omgivelsestemperaturen overstiger 40° C (104° F). Sørg for at klaringen rundt lufteåpningene er minst 15,2 cm (6 tommer) for å forhindre nedsatt luftsirkulasjon.

Aviso Para evitar o sobreaquecimento do encaminhador Juniper Networks switch, não utilize este equipamento numa área que exceda a temperatura máxima recomendada de 40° C. Para evitar a restrição à circulação de ar, deixe pelo menos um espaço de 15,2 cm à volta das aberturas de ventilação.

¡Atención! Para impedir que un encaminador de la serie Juniper Networks switch se recaliente, no lo haga funcionar en un área en la que se supere la temperatura ambiente máxima recomendada de 40° C. Para impedir la restricción de la entrada de aire, deje un espacio mínimo de 15,2 cm alrededor de las aperturas para ventilación.

Varning! Förhindra att en Juniper Networks switch överhettas genom att inte använda den i ett område där den maximalt rekommenderade omgivningstemperaturen på 40° C överskrids. Förhindra att luftcirkulationen inskränks genom att se till att det finns fritt utrymme på minst 15,2 cm omkring ventilationsöppningarna.

Product Disposal Warning

WARNING: Disposal of this device must be handled according to all national laws and regulations.

Waarschuwing Dit produkt dient volgens alle landelijke wetten en voorschriften te worden afgedankt.

Varoitus Tämän tuotteen lopullisesta hävittämisestä tulee huolehtia kaikkia valtakunnallisia lakeja ja säännöksiä noudattaen.

Avertissement La mise au rebut définitive de ce produit doit être effectuée conformément à toutes les lois et réglementations en vigueur.

Warnung Dieses Produkt muß den geltenden Gesetzen und Vorschriften entsprechend entsorgt werden.

Avvertenza L'eliminazione finale di questo prodotto deve essere eseguita osservando le normative italiane vigenti in materia

Advarsel Endelig disponering av dette produktet må skje i henhold til nasjonale lover og forskrifter.

Aviso A descartagem final deste produto deverá ser efectuada de acordo com os regulamentos e a legislação nacional.

¡Atención! El desecho final de este producto debe realizarse según todas las leyes y regulaciones nacionales

Varning! Slutlig kassering av denna produkt bör skötas i enlighet med landets alla lagar och föreskrifter.

Action to Take After an Electrical Accident

If an electrical accident results in an injury, take the following actions in this order:

1. Use caution. Be aware of potentially hazardous conditions that could cause further injury.
2. Disconnect power from the device.
3. If possible, send another person to get medical aid. Otherwise, assess the condition of the victim, and then call for help.

General Electrical Safety Guidelines and Warnings

- Install the services gateway in compliance with the following local, national, or international electrical codes:
  - United States—National Fire Protection Association (NFPA 70), United States National Electrical Code

  - Canada—Canadian Electrical Code, Part 1, CSA C22.1
  - Other countries—International Electromechanical Commission (IEC) 60364, Part 1 through Part 7
  - Evaluated to the TN power system
- Locate the emergency power-off switch for the room in which you are working so that if an electrical accident occurs, you can quickly turn off the power.
- Do not work alone if potentially hazardous conditions exist anywhere in your workspace.
- Never assume that power is disconnected from a circuit. Always check the circuit before starting to work.
- Carefully look for possible hazards in your work area, such as moist floors, ungrounded power extension cords, and missing safety grounds.
- Operate the services gateway within marked electrical ratings and product usage instructions.
- For the services gateway and peripheral equipment to function safely and correctly, use the cables and connectors specified for the attached peripheral equipment, and make certain they are in good condition.

RELATED DOCUMENTATION

> In Case of Electrical Accident
>
> AC Power Electrical Safety Guidelines

AC Power Electrical Safety Guidelines

The following electrical safety guidelines apply to AC-powered devices:

- Note the following warnings printed on the device:

  “**CAUTION:** THIS UNIT HAS MORE THAN ONE POWER SUPPLY CORD. DISCONNECT ALL POWER SUPPLY CORDS BEFORE SERVICING TO AVOID ELECTRIC SHOCK.”

  “**ATTENTION:** CET APPAREIL COMPORTE PLUS D'UN CORDON D'ALIMENTATION. AFIN DE PRÉVENIR LES CHOCS ÉLECTRIQUES, DÉBRANCHER TOUT CORDON D'ALIMENTATION AVANT DE FAIRE LE DÉPANNAGE.”

- AC-powered devices are shipped with a three-wire electrical cord with a grounding-type plug that fits only a grounding-type power outlet. Do not circumvent this safety feature. Equipment grounding must comply with local and national electrical codes.
- You must provide an external certified 2-pole circuit breaker rated minimum 20 A for United States (16-20 A for other countries) in the building installation. Install as permitted by the local code.
- The power cord serves as the main disconnecting device for the AC-powered device. The socket outlet must be near the AC-powered device and be easily accessible.
- For devices that have more than one power supply connection, you must ensure that all power connections are fully disconnected so that power to the device is completely removed to prevent electric shock. To disconnect power, unplug all power cords (one for each power supply).

Power Cable Warning (Japanese)

WARNING: The attached power cable is only for this product. Do not use the cable for another product.

注意

附属の電源コードセットはこの製品専用です。
他の電気機器には使用しないでください。

SRX380 Firewall Agency Approvals

IN THIS SECTION

The services gateway complies with the following standards:

- Safety
  - CAN/CSA-C22.2 No.60950-1 (2007) Information Technology Equipment
  - UL 60950-1 (2nd Ed.) Information Technology Equipment

- EN 60950-1 (2006+ A11:2010) Information Technology Equipment - Safety
- IEC 60950-1 (2005 +A1:2009) Information Technology Equipment - Safety (All country deviations): CB Scheme report
- EN 60825-1 (2007) Safety of Laser Products - Part 1: Equipment classification and requirements
- UL 62368-1: 2014
- CAN/CSA C22.2 No. 62368-1-14
- EN 62368-1: 2014 + A11: 2017
- IEC 62368-1: 2014

- EMC

  Emission

  - EN 55032:2015, Class A
  - CISPR 32:2015, Class A
  - EN 55022:2010, Class A
  - CISPR 22:2008, Class A
  - Australian Communications and Media Authority (ACMA) AS/NZS CISPR 32: 2015 Class A
  - FCC Part 15, Subpart B, for Class A digital devices
  - Innovation, Science and Economic Development Canada ICES 003, dated January 2016 Class A + ICES-Gen
  - VCCI-CISPR32:2016
  - BSMI CNS 13438 Taiwan Radiated and Conducted Emissions (at 10 Meter)
  - KN32 Korea Radiated Emission Characteristics (at 10 Meter)
  - EN 300 386, V1.6.1 (2012-09), Class A
  - EN 300386 V2.1.1 (2016-07), Class A
  - TEC/SD/DD/EMC/221/05/OCT-16, Class A

  Immunity

  - EN 300 386, V1.6.1 (2012-09)
  - EN 300386 V2.1.1 (2016-07)

- EN 55024:2010
- CISPR 24:2010
- CISPR 35:2016
- KN35 Korea Radiated Immunity Characteristics
- TEC/SD/DD/EMC-221/05/OCT-16 India EMC standard

Energy Efficiency requirements

- AT&T TEER (ATIS-06000015.03.2013)
- ECR 3.0.1
- Energy Star
- ETSI ES 203 136 (2013-05)
- Verizon TEEER (VZ.TPR.9205 Issue 6)
- Amazon Customer Requirements

- **Environmental**
  - Reduction of Hazardous Substances (ROHS) 6
- **RF standards**
  - EN 301489-1: V2.1.1
  - EN 301 489-17: V3.1.1
  - EN 301908-1: V11.1.1
  - EN 301489-52: V1.1.0

For Maximum Permissible Exposure (MPE) regulation:

- EN 62311: 2008
- EN50665: 2017
- EN 50385: 2017
- RSS-102 Issue 5
- 47 CFR Part 2.1091
- NCC LP002 section 5.20

- AS/NZS 2772 :2016

- **Telco**
  - Common Language Equipment Identifier (CLEI) code

Compliance Statement for Argentina

EQUIPO DE USO IDÓNEO.

SRX380 Firewall EMC Requirements

IN THIS SECTION

Canada

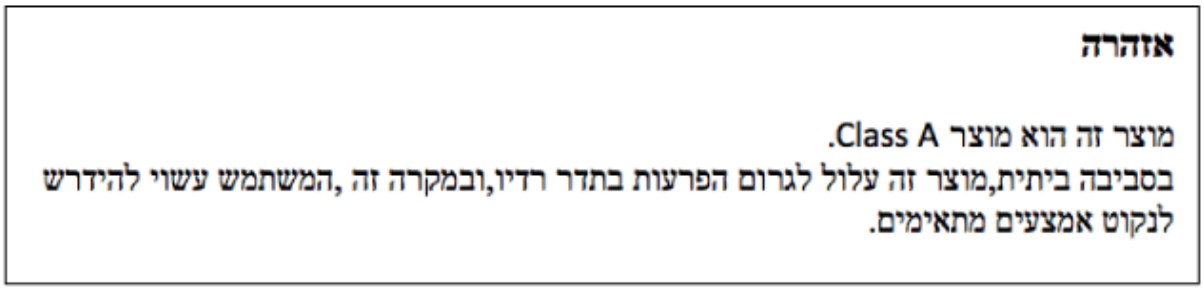
This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

European Community

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

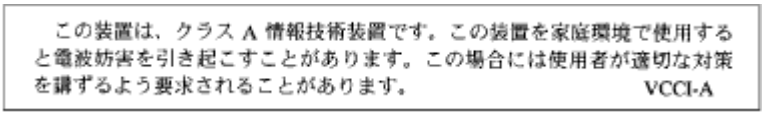
Israel



The preceding translates as follows:

This product is Class A. In residential environments, the product may cause radio interference, and in such a situation, the user may be required to take adequate measures.

Japan



The preceding translates as follows:

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

VCCI-A

United States

The services gateway has been tested and found to comply with the limits for a Class A digital device of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference

when the equipment is operated in a commercial environment. This 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 the user will be required to correct the interference at his own expense.

BSMI Statement (Taiwan)

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，
在這種情況下，使用者會被要求採取某些適當的對策。