JUNIPER NETWORKS | Engineering Simplicity

SRX300 Firewall Hardware Guide

Published
2023-08-15

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

SRX300 Firewall Hardware Guide
Copyright © 2023 Juniper Networks, Inc. All rights reserved.

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 | vii

1 Overview

SRX300 Firewall Overview | 2

- SRX300 Firewall Description | 2
- Benefits of the SRX300 Firewall | 2

SRX300 Chassis | 3

- SRX300 Firewall Chassis Overview | 3
- Understanding the SRX300 Firewall Front Panel | 4
- Understanding the SRX300 Firewall Back Panel | 8

SRX300 Power System | 9

- Understanding the SRX300 Firewall Power Supply | 9
- SRX300 Firewall Power Specifications and Requirements | 10

2 Site Planning, Preparation, and Specifications

Site Preparation Checklist for the SRX300 Firewall | 12

SRX300 Site Guidelines and Requirements | 15

- General Site Installation Guidelines for the SRX300 Firewall | 15
- SRX300 Firewall Environmental Specifications | 16
- SRX300 Firewall Electrical Wiring Guidelines | 16
- SRX300 Firewall Grounding Specifications | 18
- SRX300 Firewall Physical Specifications | 19
- SRX300 Firewall Clearance Requirements for Airflow and Hardware Maintenance | 20
- Rack Requirements | 20
- Cabinet Requirements | 21

SRX300 Transceiver Specifications and Pinouts | 22

SRX300 Transceiver Support | 22

RJ-45 Connector Pinouts for the SRX300 Firewall Ethernet Port | 22

RJ-45 Connector Pinouts for the SRX300 Firewall Console Port | 23

Mini-USB Connector Pinouts for the SRX300 Firewall Console Port | 24

3 Initial Installation and Configuration

SRX300 Installation Overview | 27

SRX300 Firewall Installation Overview | 27

SRX300 Firewall Autoinstallation Overview | 28

Unpacking and Mounting the SRX300 | 29

Unpacking the SRX300 Firewall | 29

Verifying Parts Received with the SRX300 Firewall | 30

Installing the SRX300 Firewall on a Desk | 31

Installing the SRX300 Firewall on a Wall | 31

Installing the SRX300 Firewall in a Rack | 33

Connecting the SRX300 to Power | 37

Required Tools and Parts for Grounding the SRX300 Services Gateway | 37

Connecting the SRX300 Firewall Grounding Cable | 37

Connecting the SRX300 Firewall to the Power Supply | 39

Powering On the SRX300 Services Gateway | 39

Powering Off the SRX300 Services Gateway | 40

Connecting the SRX300 to External Devices | 41

Connecting the Dial-Up Modem to the Console Port on the SRX300 Services Gateway | 41

Connecting to the SRX300 Firewall CLI Using a Dial-Up Modem | 42

Configuring Junos OS on the SRX300 | 43

SRX300 Firewall Factory-Default Settings | 44

Initial Configuration Using the CLI | 45

Connect to the Serial Console Port | 46

Connect to the Mini-USB Console Port | 47

Configure the SRX300 Using the CLI | 48

Initial Configuration Using J-Web | 49

Configure Using J-Web | 49

Customize the Configuration for Junos OS Release 19.2 | 51

Customize the Configuration for Junos OS Release 15.1X49-D170 | 52

Configure the Device Using ZTP with Juniper Networks Network Service Controller | 53

4 Maintaining Components

Maintaining the SRX300 Components | 56

Routine Maintenance Procedures for the SRX300 Services Gateway | 56

Maintaining the SRX300 Firewall Power Supply | 56

5 Troubleshooting Hardware

Troubleshooting the SRX300 | 58

Troubleshooting Resources for the SRX300 Firewall Overview | 58

Troubleshooting Chassis and Interface Alarm Messages on the SRX300 Firewall | 59

Troubleshooting the Power System on the SRX300 Services Gateway | 60

Using the RESET CONFIG Button | 61

Changing the RESET CONFIG Button Behavior | 62

6 Contacting Customer Support and Returning the Chassis or Components

Returning the SRX300 Chassis or Components | 64

Contacting Customer Support | 64

Returning a SRX300 Firewall Component to Juniper Networks | 65

Locating the SRX300 Firewall Chassis Serial Number and Agency Labels | 65

Listing the SRX300 Firewall Component Details with the CLI | 66

Required Tools and Parts for Packing the SRX300 Firewall | 66

Packing the SRX300 Firewall for Shipment | 66

Packing SRX300 Firewall Components for Shipment | 67

7

Safety and Compliance Information

Definitions of Safety Warning Levels | 69

General Safety Guidelines and Warnings | 70

Restricted Access Warning | 72

Qualified Personnel Warning | 73

Prevention of Electrostatic Discharge Damage | 74

Fire Safety Requirements | 75

Laser and LED Safety Guidelines and Warnings | 77

Radiation from Open Port Apertures Warning | 79

Battery-Handling Warning | 80

Lightning Activity Warning | 82

Jewelry Removal Warning | 83

Operating Temperature Warning | 84

Product Disposal Warning | 86

Action to Take After an Electrical Accident | 87

General Electrical Safety Guidelines and Warnings | 87

SRX300 Agency Approvals and Compliance Statements | 88

- SRX300 Firewall Agency Approvals | 88
- SRX300 Firewall EMC Requirements | 90

About This Guide

Use this guide to install hardware and perform initial software configuration, routine maintenance, and troubleshooting for the SRX300 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 SRX300 (Quick Start)
- SRX300 Series and SRX550 High Memory Gateway Interface Modules Reference

1

CHAPTER

Overview

SRX300 Firewall Overview | 2

SRX300 Chassis | 3

SRX300 Power System | 9

SRX300 Firewall Overview

IN THIS SECTION

- SRX300 Firewall Description | 2
- Benefits of the SRX300 Firewall | 2

SRX300 Firewall Description

The SRX300 Firewall consolidates networking and security capabilities for small retail offices. The services gateway provides cost-effective, scalable integration of routing, security, and switching in a single device. The SRX300 Firewall provides firewall support with key features such as IP security (IPsec) VPN and Content Security .

With a desktop form-factor chassis, the SRX300 Firewall has eight 1 G Ethernet ports, two 1 G SFP ports, 4 GB of DRAM memory, and 8 GB of flash memory.

The SRX300 Firewall runs the Junos operating system (Junos OS) and supports the following features:

- Firewall support with key features such as IPsec and VPN
- Intrusion Detection and Prevention (IDP)
- High availability
- QoS
- MPLS

You can manage the SRX300 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.

Benefits of the SRX300 Firewall

- **High performance**—The SRX300 supports up to 1-Gbps firewall and 300-Mbps IPsec VPN, and is suited for small branch and retail office deployments.

- **Simplified deployment with minimal manual intervention**—The Zero Touch Provisioning (ZTP) feature enables you to provision and configure the SRX300 line automatically, thereby reducing operational complexity and simplifying the provisioning of new sites.
- **Threat protection**—The SRX300 line supports IPsec VPN, Media Access Control Security (MACsec), Juniper Juniper Advanced Threat Prevention Cloud, and Trusted Platform Module (TPM) to protect against potential vulnerabilities.

SRX300 Chassis

IN THIS SECTION

- SRX300 Firewall Chassis Overview | 3
- Understanding the SRX300 Firewall Front Panel | 4
- Understanding the SRX300 Firewall Back Panel | 8

SRX300 Firewall Chassis Overview

The SRX300 Firewall chassis weighs 4.38 lb. and measures 1.37 in. high, 12.63 in. wide, and 7.52 in. deep.



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 rear of the chassis is provided to connect the services gateway to ground.

Understanding the SRX300 Firewall Front Panel

IN THIS SECTION

- Network Port LEDs | 7

Figure 1 on page 4 shows the front panel of the SRX300 Firewall.

Figure 1: SRX300 Firewall Front Panel

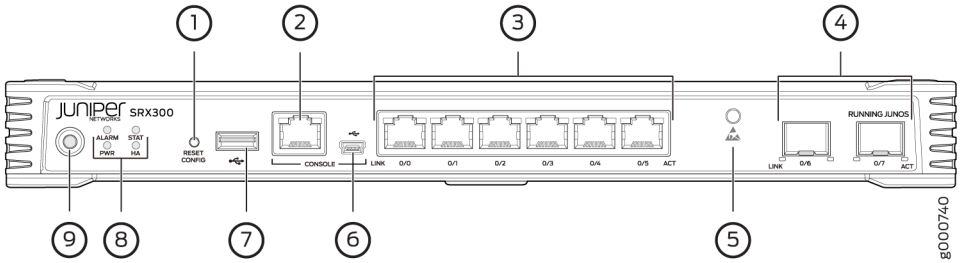


Table 1 on page 4 provides details about the front panel components.

Table 1: SRX300 Firewall Front Panel Components

Number	Component	Description
1	Reset Config button	Returns the services gateway to the rescue configuration or the factory-default configuration.
2	Serial Console port	Connects a laptop to the services gateway for CLI management. The port uses an RJ-45 serial connection and supports the RS-232 (EIA-232) standard.

Table 1: SRX300 Firewall Front Panel Components *(Continued)*

Number	Component	Description
3	1-GbE Ethernet ports	Six LAN ports (0/0 to 0/5) 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
4	1-GbE small form-factor pluggable (SFP) ports	Two 1-GbE MACsec-capable SFP ports for network traffic.
5	ESD point	For personal safety, while working on the services gateway, use the ESD outlet to plug in an ESD grounding strap to prevent your body from sending static charges to the services gateway.

Table 1: SRX300 Firewall Front Panel Components *(Continued)*

Number	Component	Description
6	Mini-USB console port	Connects a laptop to the services gateway for CLI management through a USB interface. The 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.
7	USB port	The services gateway has one USB port that accepts a USB storage device.
8	LEDs	Indicates component and system status at a glance.
9	Power button	Use the Power button to power on or power off the services gateway.

Figure 2 on page 6 shows the LEDs on the front panel.

Figure 2: SRX300 Firewall Front Panel LEDs

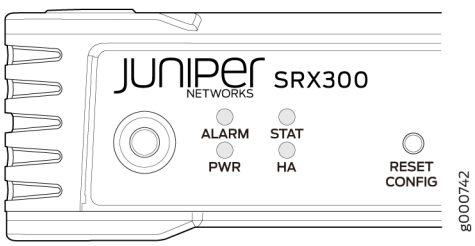


Table 2 on page 7 lists the front panel LEDs.

Table 2: SRX300 Firewall Front Panel LEDs

Component	Description
ALARM	• Solid amber (noncritical alarm) • Solid red (critical alarm) • Off (no alarms)

STAT	• Solid green (operating normally)
	• Solid amber
	  • Device is starting up
	  • Committing rescue configuration
	  • Committing clear configuration
	• Solid red (error detected)

PWR	• Solid green (receiving power) • Solid red (power failure) • Off (no power)
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)

Network Port LEDs

The SFP and Ethernet ports have two status LEDs, LINK and ACT, located above the port.

Table 3: Network Port LEDs

LED	Description
LINK (LED on the left)	• Solid green—There is link activity. • Off—There is no link established.
ACT (LED on the right)	• Blinking green—There is activity on the 1 G link. • Off—There is no link activity.

Understanding the SRX300 Firewall Back Panel

Figure 3 on page 8 shows the back panel of the SRX300 Firewall and Table 4 on page 8 lists the back panel components.

Figure 3: SRX300 Firewall Back Panel

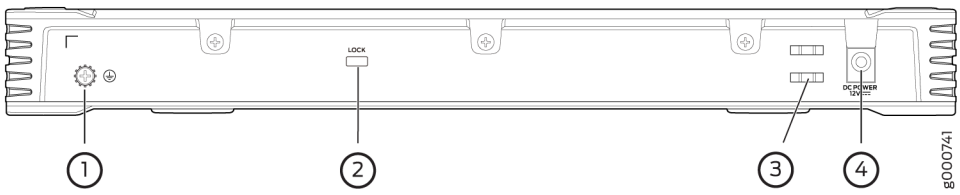


Table 4: SRX300 Firewall Back Panel Components

Number	Component	Description
1	Grounding point	Connects the services gateway chassis to earth ground (optional). **NOTE**: We recommend connecting the services gateway to ground if required.

Table 4: SRX300 Firewall Back Panel Components *(Continued)*

Number	Component	Description
2	Lock	Provides the capability to lock and secure the device at the installation site.
3	Cable tie holder	Secures the DC power cord connection to the adapter.
4	Power supply input	Connects the services gateway to the external power supply.

RELATED DOCUMENTATION

SRX300 Installation Overview | 27

SRX300 Power System

IN THIS SECTION

- Understanding the SRX300 Firewall Power Supply | 9
- SRX300 Firewall Power Specifications and Requirements | 10

Understanding the SRX300 Firewall Power Supply

The power supply for the SRX300 Firewall is external. You must use the AC to DC, 60 W power supply adapter provided by Juniper Networks to provide power to the services gateway. The adapter provides an output of 12 VDC, 5 A.

SEE ALSO

Connecting the SRX300 Firewall to the Power Supply | 39

Powering On the SRX300 Services Gateway | 39

Powering Off the SRX300 Services Gateway | 40

SRX300 Firewall Power Specifications and Requirements

Table 5 on page 10 lists the power specifications for the SRX300 Firewall power supply adapter.

Table 5: Power Specifications for the SRX300 Firewall Power Supply Adapter

Power Supply Adapter Requirement	Specification
AC input	100 to 240 VAC
AC input line frequency	50 to 60 Hz
AC system current rating	1 A maximum
Maximum AC inrush current	7 A at 220 V/50 Hz

WARNING: The AC power cord for the services gateway is intended for use with only the power supply adapter provided with the device .

SEE ALSO

SRX300 Firewall Electrical Wiring Guidelines | 16

CHAPTER 2

Site Planning, Preparation, and Specifications

Site Preparation Checklist for the SRX300 Firewall | 12

SRX300 Site Guidelines and Requirements | 15

SRX300 Transceiver Specifications and Pinouts | 22

Site Preparation Checklist for the SRX300 Firewall

Table 6 on page 12 provides a checklist of tasks you need to perform when preparing a site for installing the SRX300 Firewall.

Table 6: Site Preparation Checklist for SRX300 Firewall Installation

Item or Task	Additional Information	Performed By	Date	Notes
Environment				
Verify that environmental factors such as temperature and humidity do not exceed device tolerances.	"SRX300 Services Gateway Environmental Specifications" on page 16			
Power				
• Measure the distance between the external power sources and the device installation site. • Locate sites for connection of system grounding. • Calculate the power consumption and requirements.	"SRX300 Services Gateway Electrical Wiring Guidelines" on page 16 "SRX300 Services Gateway Power Specifications and Requirements" on page 10			
Rack Requirements				

Table 6: Site Preparation Checklist for SRX300 Firewall Installation *(Continued)*

Item or Task	Additional Information	Performed By	Date	Notes
Verify that your rack meets the minimum requirements.	SRX300 Services Gateway Rack-Mounting Requirements and Warnings			
Rack Installation				
• Plan the rack location, including required space clearances. • Secure the rack to the floor and building structure.	Preparing the SRX300 Services Gateway for Rack-Mount Installation			
Cabinet Requirements				
• Verify that your cabinet meets the minimum requirements. • Plan the cabinet location, including required space clearances.	SRX300 Services Gateway Cabinet Size and Clearance Requirements			
Wall Installation				

Table 6: Site Preparation Checklist for SRX300 Firewall Installation *(Continued)*

Item or Task	Additional Information	Performed By	Date	Notes
• Verify that the area selected meets the minimum requirements. • Verify that you have the required hardware to proceed with the installation.	Preparing the SRX300 Services Gateway for Wall-Mount Installation			
Desktop Installation				
• Verify that the area selected meets the minimum requirements. • Plan the installation location, including required space clearances and airflow requirements.	Preparing the SRX300 Services Gateway for Desk-Mount Installation			
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.				

RELATED DOCUMENTATION

General Site Installation Guidelines for the SRX300 Firewall | 15

SRX300 Site Guidelines and Requirements

IN THIS SECTION

- General Site Installation Guidelines for the SRX300 Firewall | 15
- SRX300 Firewall Environmental Specifications | 16
- SRX300 Firewall Electrical Wiring Guidelines | 16
- SRX300 Firewall Grounding Specifications | 18
- SRX300 Firewall Physical Specifications | 19
- SRX300 Firewall Clearance Requirements for Airflow and Hardware Maintenance | 20
- Rack Requirements | 20
- Cabinet Requirements | 21

General Site Installation Guidelines for the SRX300 Firewall

The following precautions help you plan an acceptable operating environment for your SRX300 Firewall and avoid environmentally caused equipment failures:

- For the operating temperature of the services gateway to be optimal, 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 ESD procedures to avoid damaging equipment. Static discharge can cause components to fail completely or intermittently over time. For more information, see Preventing Electrostatic Discharge Damage to the SRX300 Services Gateway.

NOTE: The SRX300 Firewall does not include a fan and does not generate any acoustic noise.

SRX300 Firewall Environmental Specifications

Table 7 on page 16 provides the required environmental conditions for normal SRX300 Firewall operations.

Table 7: Environmental Specifications for the SRX300 Firewall

Description	Value
Altitude	No performance degradation up to 10,000 ft (3048 m)
Relative humidity	5% to 95%, noncondensing
Temperature	• Operational temperature— -4° F (-20° C) to 140° F (60° C) • Nonoperational temperature— 4° F (20° C) to 158° F (70° C)
Average power consumption	24.9 W
DC Input rating	12 VDC, 2.8 A maximum
Average heat dissipation	85 BTU/hr
Noise level	0 dB (fanless)

SRX300 Firewall Electrical Wiring Guidelines

Table 8 on page 17 describes the factors you must consider while planning the electrical wiring for the services gateway at your site.

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

Table 8: Site Electrical Wiring Guidelines for the SRX300 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 cable 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 may want to seek expert advice.

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

SEE ALSO

SRX300 Firewall Power Specifications and Requirements | 10

General Electrical Safety Guidelines and Warnings

SRX300 Firewall Grounding Specifications

To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, the SRX300 Firewall must be adequately grounded before power is connected. You must provide a grounding lug to connect the services gateway to earth ground.

WARNING: Before you connect power to the services gateway, a licensed electrician must attach a cable lug to the grounding and power cables that you supply. A cable with an incorrectly attached lug can damage the services gateway (for example, by causing a short circuit).

The services gateway chassis has one grounding point on the back panel.

Table 9 on page 18 lists the specifications of the grounding cable used with the device.

You must install the SRX300 in a restricted-access location and ensure that the chassis is always properly grounded. The SRX300 device has a one-hole protective grounding terminal provided on the chassis. 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 one-hole grounding lug connection. This tested system meets or exceeds all applicable EMC regulatory requirements with the one-hole protective grounding terminal.

Table 9: Grounding Cable Specifications for the Services Gateway

Grounding Requirement	Specification
Grounding cable	14 AWG single-strand wire cable

Table 9: Grounding Cable Specifications for the Services Gateway *(Continued)*

Grounding Requirement	Specification
Amperage of grounding cable	Up to 4 A
Grounding lug	Ring-type, vinyl-insulated TV14-6R lug or equivalent

SEE ALSO

Connecting the SRX300 Firewall Grounding Cable | 37

SRX300 Firewall Physical Specifications

Table 10 on page 19 lists the physical specifications for the services gateway.

Table 10: Physical Specifications for the SRX300 Firewall

Physical Specification of Chassis	Value
Height	1.37 in.
Width	12.63 in.
Depth	7.52 in.
Weight	4.38 lb

SEE ALSO

Understanding the SRX300 Firewall Front Panel | 4

Understanding the SRX300 Firewall Back Panel | 8

SRX300 Firewall Clearance Requirements for Airflow and Hardware Maintenance

When planning the installation site for the SRX300 Firewall, you need to allow sufficient clearance around the device. Consider the following:

- The SRX300 Firewall does not include a fan and uses natural convection cooling. For the operating temperature of the services gateway to be optimal, the airflow around the chassis must be unrestricted.
- 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, or if you are placing it on the desktop near other equipment, ensure that the exhaust from other equipment does not blow into the intake vents of the chassis.

Rack Requirements

When installing the services gateway in a rack, you must ensure that the rack complies with a 1U (19 in. or 48.7 cm) rack as defined in Cabinets, Racks, Panels, and Associated Equipment (document number EIA-310-D), published by the Electronic Industries Alliance (http://www.ecaus.org/eia/site/index.html).

When selecting a rack, ensure that the physical characteristics of the rack comply with the following specifications:

- The outer edges of the mounting brackets extend the width of either chassis to 19 in. (48.3 cm).
- The front of the chassis extends approximately 0.5 in. (1.27 cm) beyond the mounting ears.
- Maximum permissible ambient temperature when two devices are placed side by side in a 19 in. rack is 40° C.

The spacing of the mounting brackets and flange holes on the rack and device mounting brackets are as follows:

- The holes within each rack set are spaced at 1 U (1.75 in. or 4.5 cm).
- The mounting brackets and front-mount flanges used to attach the chassis to a rack are designed to fasten to holes spaced at rack distances of 1 U (1.75 in.).
- The mounting holes in the mounting brackets provided with the device are spaced 1.25 in. (3.2 cm) apart (top and bottom mounting hole).

Always secure the rack in which you are installing the services gateway to the structure of the building. If your geographical area is subject to earthquakes, bolt the rack to the floor. For maximum stability, also secure the rack to ceiling brackets.

Cabinet Requirements

You can install the services gateway in a 19 in. (48.7 cm) cabinet as defined in Cabinets, Racks, Panels, and Associated Equipment (document number EIA-310-D) published by the Electronic Industries Alliance (http://www.ecaus.org/eia/site/index.html). You must mount the services gateway horizontally in the cabinet using appropriate rack adapters.

When selecting a cabinet, ensure that it meets the following specifications:

- The cabinet is at least 1U (3.50 in. or 8.89 cm) and can accommodate the services gateway.
- The outer edges of the mounting brackets extend the width of either chassis to 19 in. (48.7 cm), and the front of the chassis extends approximately 0.5 in. (1.27 cm) beyond the mounting brackets.
- The minimum total clearance inside the cabinet is 30.7 in. (78 cm) between the inside of the front door and the inside of the rear door.

NOTE: A cabinet larger than the minimum required provides better airflow and reduces the chance of overheating.

When you mount the services gateway in a cabinet, you must ensure that ventilation through the cabinet is sufficient to prevent overheating. Consider the following when planning for chassis cooling:

- Ensure that the cool air supply you provide through the cabinet can adequately dissipate the thermal output of the services gateway.
- Install the services gateway as close as possible to the front of the cabinet so that the cable management system clears the inside of the front door. Installing the chassis close to the front of the cabinet maximizes the clearance in the rear of the cabinet for critical airflow.
- Route and dress all cables to minimize the blockage of airflow to and from the chassis.

RELATED DOCUMENTATION

SRX300 Installation Overview | 27

SRX300 Transceiver Specifications and Pinouts

IN THIS SECTION

- SRX300 Transceiver Support | 22
- RJ-45 Connector Pinouts for the SRX300 Firewall Ethernet Port | 22
- RJ-45 Connector Pinouts for the SRX300 Firewall Console Port | 23
- Mini-USB Connector Pinouts for the SRX300 Firewall Console Port | 24

SRX300 Transceiver Support

You can find information about the pluggable transceivers supported on your Juniper Networks device by using the Hardware Compatibility Tool. In addition to transceiver and connector type, the optical and cable characteristics—where applicable—are documented for each transceiver. The Hardware Compatibility Tool enables you to search by product, displaying all the transceivers supported on that device, or category, by interface speed or type. The list of supported transceivers for the SRX300 is located at https://apps.juniper.net/hct/product/#prd=SRX300.

RJ-45 Connector Pinouts for the SRX300 Firewall Ethernet Port

Table 11 on page 22 describes the RJ-45 connector pinouts for the Ethernet port.

Table 11: RJ-45 Connector Pinouts for the SRX300 Firewall Ethernet Port

Pin	Signal
1	BI_DA+
2	BI_DA
3	BI_DB+

Table 11: RJ-45 Connector Pinouts for the SRX300 Firewall Ethernet Port *(Continued)*

Pin	Signal
4	BI_DC+
5	BI_DC
6	BI_DB
7	BI_DD+
8	BI_DD

RJ-45 Connector Pinouts for the SRX300 Firewall Console Port

Table 12 on page 23 describes the RJ-45 connector pinouts for the console port.

Table 12: RJ-45 Connector Pinouts for the SRX300 Firewall Console Port

Pin	Signal	Description
1	RTS	Request to Send
2	DTR	Data Terminal Ready
3	TXD	Transmit Data
4	Ground	Signal Ground
5	Ground	Signal Ground
6	RXD	Receive Data

Table 12: RJ-45 Connector Pinouts for the SRX300 Firewall Console Port *(Continued)*

Pin	Signal	Description
7	DSR/DCD	Data Set Ready
8	CTS	Clear to Send

Mini-USB Connector Pinouts for the SRX300 Firewall Console Port

The SRX300 Firewall has two console ports: an RJ-45 Ethernet port and a mini-USB Type-B port. If your management device (laptop or PC) does not have a DB-9 plug connector pin or an RJ-45 connector pin, you can connect your management device to the Mini-USB Type-B console port of the services gateway by using a cable that has a standard Type-A USB connector on one end and a Mini-USB Type-B (5-pin) connector on the other end. Table 13 on page 24 describes the Mini-USB Type-B connector pinouts for the console port.

NOTE: By design, the mini-USB console port has higher priority over the RJ-45 console port. If the mini-USB and RJ-45 console ports are both connected, then the mini-USB console port will be active.

Table 13: Mini-USB Type-B Connector Pinouts for the Services Gateway Console Port

Pin	Signal	Cable Color	Description
1	VCC	Red	+5 VDC
2	D-	White	Data -
3	D+	Green	Data +

Table 13: Mini-USB Type-B Connector Pinouts for the Services Gateway Console Port *(Continued)*

Pin	Signal	Cable Color	Description
X	N/C		Could be not connected (N/C), connected to ground (GND), or used as an attached device presence indicator
4	GND	Black	Ground

CHAPTER 3

Initial Installation and Configuration

SRX300 Installation Overview | 27

Unpacking and Mounting the SRX300 | 29

Connecting the SRX300 to Power | 37

Connecting the SRX300 to External Devices | 41

Configuring Junos OS on the SRX300 | 43

SRX300 Installation Overview

IN THIS SECTION

- SRX300 Firewall Installation Overview | 27
- SRX300 Firewall Autoinstallation Overview | 28

SRX300 Firewall Installation Overview

After you have prepared the site for installation and unpacked the SRX300 Firewall, you are ready to install the device. It is important to proceed through the installation process in the following order:

1. Review the safety guidelines explained in SRX300 Services Gateway General Safety Guidelines and Warnings.
2. Prepare your site for the installation of the services gateway as described in "Site Preparation Checklist for the SRX300 Services Gateway" on page 12.
3. Install the services gateway. See:
   - "Installing the SRX300 Services Gateway in a Rack" on page 33
   - "Installing the SRX300 Services Gateway on a Wall" on page 31
   - "Installing the SRX300 Services Gateway on a Desk" on page 31
4. Connect the grounding cable as described in "Connecting the SRX300 Services Gateway Grounding Cable" on page 37.
5. Power on the services gateway as described in "Powering On the SRX300 Services Gateway" on page 39.

SEE ALSO

Site Preparation Checklist for the SRX300 Firewall | 12

General Site Installation Guidelines for the SRX300 Firewall | 15

SRX300 Firewall Autoinstallation Overview

The autoinstallation process begins any time a services gateway is powered on and cannot locate a valid configuration file in the internal flash. Typically, a configuration file is unavailable when a services gateway is powered on for the first time or if the configuration file is deleted from the internal flash. The autoinstallation feature enables you to deploy multiple services gateways from a central location in the network.

If you are setting up many devices, autoinstallation can help automate the configuration process by loading configuration files onto new or existing devices automatically over the network. You can use either the J-Web interface or the CLI to configure a device for autoinstallation.

For the autoinstallation process to work, you must store one or more host-specific or default configuration files on a configuration server in the network and have a service available—typically Dynamic Host Configuration Protocol (DHCP)—to assign an IP address to the services gateway.

Autoinstallation takes place automatically when you connect an Ethernet port on a new services gateway to the network and power on the device. To simplify the process, you can explicitly enable autoinstallation on a device and specify a configuration server, an autoinstallation interface, and a protocol for IP address acquisition.

> **NOTE**: If the USB autoinstallation feature is enabled (the default configuration), removal of a USB storage device immediately after insertion is not supported.
>
> After you insert a USB storage device, Junos OS scans the device to check whether it contains the USB autoinstallation file. This process might take up to 50 seconds to complete depending on the quality of the USB storage device and the number and size of the files in the device. Removing the USB storage device while this process is running might cause the services gateway to reboot, the USB port to stop working, and data loss on the USB. We recommend that after inserting a USB storage device, you wait for at least 60 seconds before removing it.
>
> By issuing the `set system autoinstallation usb disable` command (which disables the USB autoinstallation feature) before you insert the USB device, you can reduce the waiting interval between insertion and removal of a USB storage device from 60 seconds to 20 seconds.

For more information about configuring autoinstallation, see the following topics:

- Installation and Upgrade Guide for Security Devices
- Monitoring and Troubleshooting Guide

Unpacking and Mounting the SRX300

IN THIS SECTION

- Unpacking the SRX300 Firewall | 29
- Verifying Parts Received with the SRX300 Firewall | 30
- Installing the SRX300 Firewall on a Desk | 31
- Installing the SRX300 Firewall on a Wall | 31
- Installing the SRX300 Firewall in a Rack | 33

Unpacking the SRX300 Firewall

The SRX300 Firewall is shipped in a cardboard carton and secured with foam packing material. The carton also contains an accessory box and quick-start instructions.

To unpack the SRX300 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 SRX300 Services Gateway" 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 SRX300 Firewall

The SRX300 Firewall shipment package contains a packing list. Check the parts in the shipment against the items on the packing list. The packing list specifies the part numbers and carries a brief description of each part in your order.

If any part is missing, contact a customer service representative.

Table 14 on page 30 lists the inventory of components supplied with the SRX300 device.

NOTE: The parts shipped with your services gateway can vary depending on the configuration you ordered. To know the part numbers for ordering the separately orderable mounting kits, see the SRX300 Line of Services Gateways for the Branch Platform Datasheet.

Table 14: Parts List for a Fully Configured SRX300 Firewall

Component	Quantity
SRX300 services gateway	1
USB console cable with Type-A and Mini-B USB plugs	1
Documentation Roadmap	1
How to Set Up Your SRX300 Firewall (Quick Start)	1
Power supply adapter and power cord	1
End User License Agreement	1

Installing the SRX300 Firewall on a Desk

You can mount an SRX300 Firewall on a desk or any other level surface horizontally or vertically. The four rubber feet attached to the chassis provide stability. Before mounting an SRX300 Firewall on a desk or level surface:

Follow these guidelines when installing the SRX300 Firewall on a desk:

- Verify that the installation site meets the requirements described in "Site Preparation Checklist for the SRX300 Services Gateway" on page 12.
- Place the desk in its permanent location, allowing adequate clearance for airflow and maintenance, and secure it to the building structure.

The horizontal position is the standard installation position. To install the device in a horizontal position:

1. Make sure that the rubber feet are attached to the chassis.
2. Place the device on a desk with the Juniper Networks logo, which is embossed on the top cover, facing up.

Installing the SRX300 Firewall on a Wall

You can mount an SRX300 Firewall on a wall. The four rubber feet attached to the chassis provide stability. Before mounting the SRX300 Firewall on a wall:

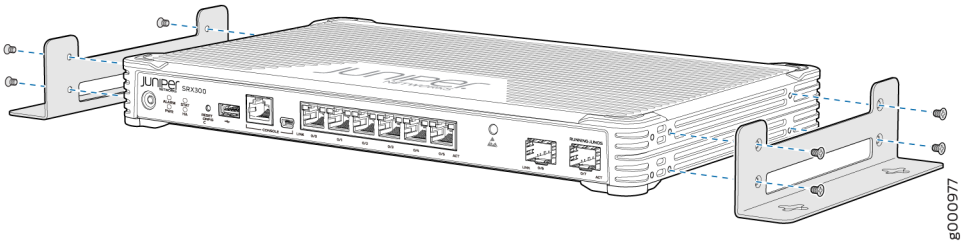
- Verify that the installation site meets the requirements described in "Site Preparation Checklist for the SRX300 Services Gateway" on page 12.
- Verify that you have the following parts available in your wall-mounting kit:
  - Wall-mounting brackets
  - Screws

NOTE: The wall-mounting kit is not shipped with the device and must be ordered separately.

To install the device on a wall:

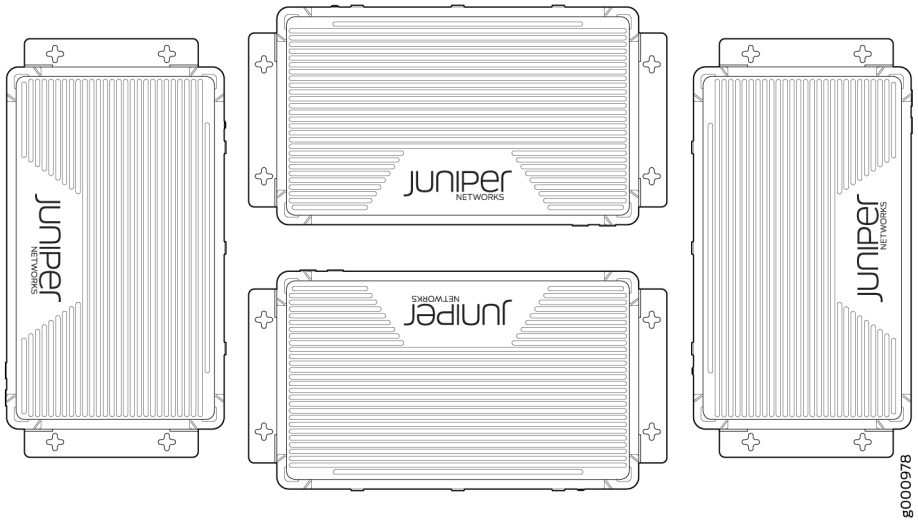
1. Place the device on a flat, level surface with the Juniper Networks logo, which is embossed on the top cover, facing up. Ensure that the rubber feet are attached to the bottom of the chassis.
2. Position a mounting bracket on each side of the chassis as shown in Figure 4 on page 32.

Figure 4: Attaching Wall-Mount Brackets



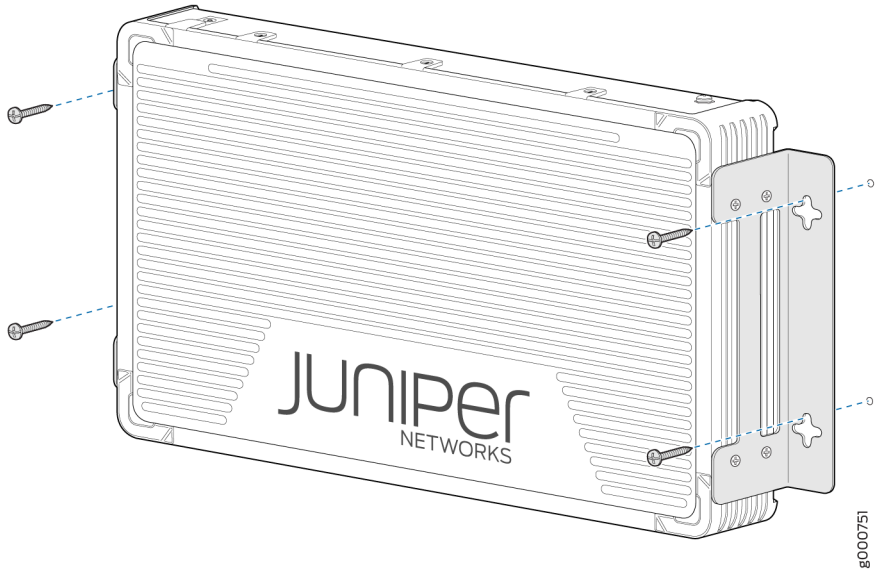
3. Use a number-2 Phillips screwdriver to install the screws that secure the mounting brackets to the chassis.
4. If you are using wall anchors to support the chassis, install two pairs of anchors on the wall with the mounting brackets attached.
5. Have one person grasp the sides of the device, lift it, and position it on the wall. Figure 5 on page 32 shows the four different orientations in which you can mount the services gateway on a wall.

Figure 5: Orienting the SRX300 Firewall on a Wall



6. Have a second person install two pairs of mounting screws through the bracket holes on either side of the device to secure it to the wall.
7. Verify that the mounting screws on one side are aligned with the mounting screws on the opposite side and that the device is level (see Figure 6 on page 33).

Figure 6: Mounting the SRX300 Firewall on a Wall



Installing the SRX300 Firewall in a Rack

You can front-mount the SRX300 Firewall in a rack. Many types of racks are acceptable, including four-post (telco) racks, enclosed cabinets, and open-frame racks. For more information about the type of rack or cabinet the SRX300 Firewall can be installed in, see SRX300 Services Gateway Rack Size and Strength Requirements.

NOTE: The rack-mounting kit is not shipped with the device and must be ordered separately.

NOTE: If you are installing multiple devices in one rack, install the lowest one first and proceed upward in the rack. Ensure that the rubber feet from the base of the chassis are removed for rack installation.

Before mounting the SRX300 Firewall in a rack:

- Verify that the installation site meets the requirements described in "Site Preparation Checklist for the SRX300 Services Gateway" on page 12.

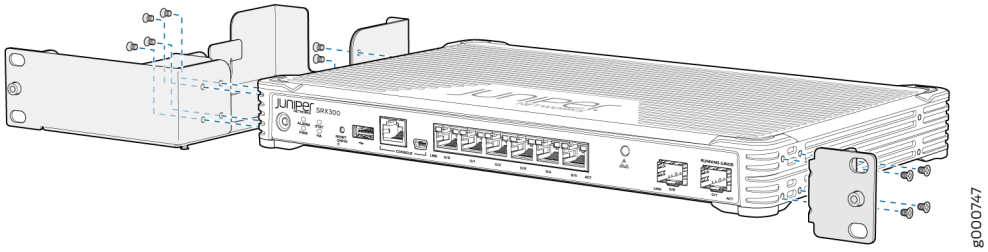
- Verify that the racks or cabinets meet the specific requirements described in SRX300 Services Gateway Rack-Mounting Requirements and Warnings.
- Place the rack or cabinet in its permanent location, allowing adequate clearance for airflow and maintenance, and secure it to the building structure. For more information, see "SRX300 Services Gateway Clearance Requirements for Airflow and Hardware Maintenance" on page 20.
- Verify that you have the following parts available in your rack-mounting kit:
  - Rack-mount tray
  - Screws

To install the device in a rack:

1. Position a mounting bracket on each side of the chassis as shown in Figure 7 on page 34.

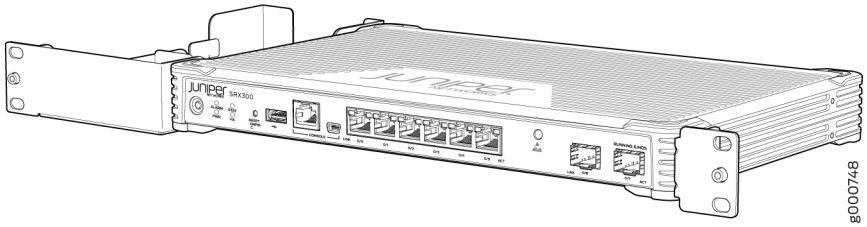
> **NOTE**: The SRX300 Firewall cannot be center-mounted in racks.

Figure 7: SRX300 Firewall Rack Installation — Positioning the Mounting Brackets



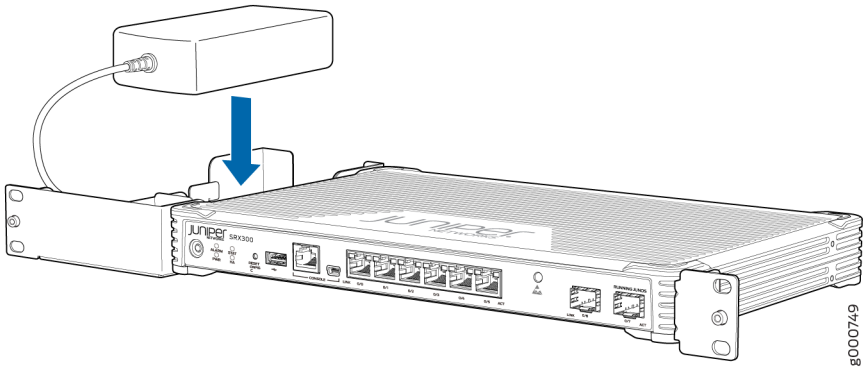
2. Use a number-2 Phillips screwdriver to install the screws that secure the mounting brackets and power supply adapter tray to the chassis as shown in Figure 8 on page 34.

Figure 8: SRX300 Firewall Rack Installation — Securing the Mounting Brackets and Power Supply Adapter Tray



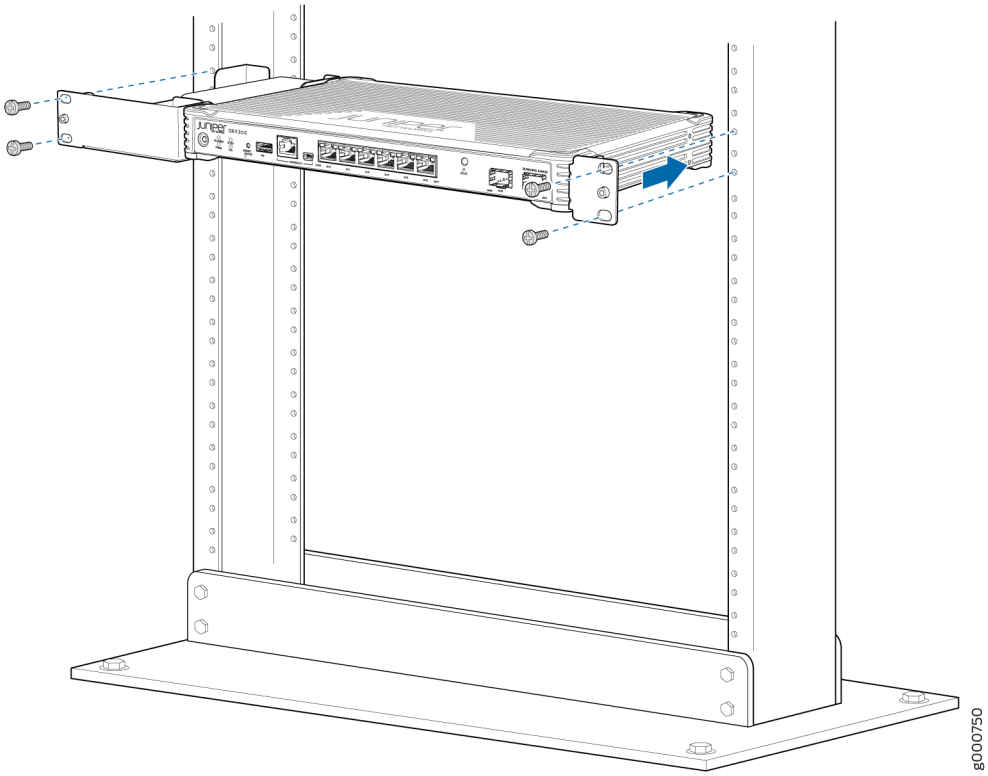
3. Place the power supply adapter in the tray as shown in Figure 9 on page 35.

Figure 9: SRX300 Firewall Rack Installation — Positioning the Power Supply Adapter Tray



4. Have one person grasp the sides of the device, lift it, and position it in the rack.
5. Align the bottom hole in each mounting bracket with a hole in each rack rail as shown in Figure 10 on page 36, making sure the chassis is level.

Figure 10: SRX300 Firewall Rack Installation — Positioning the SRX300 Firewall in a Rack



6. Have a second person install a mounting screw into each of the two aligned holes. Tighten the mounting screws.
7. Install the second screw in each mounting bracket.
8. Verify that the mounting screws on one side of the rack are aligned with the mounting screws on the opposite side and that the device is level.

RELATED DOCUMENTATION

SRX300 Site Guidelines and Requirements | 15

Connecting the SRX300 to Power

IN THIS SECTION

- Required Tools and Parts for Grounding the SRX300 Services Gateway | 37
- Connecting the SRX300 Firewall Grounding Cable | 37
- Connecting the SRX300 Firewall to the Power Supply | 39
- Powering On the SRX300 Services Gateway | 39
- Powering Off the SRX300 Services Gateway | 40

Required Tools and Parts for Grounding the SRX300 Services Gateway

To ground and to provide power to the services gateway, you need the following tools:

- Phillips (+) screwdrivers, numbers 1 and 2
- Electrostatic discharge (ESD) grounding wrist strap
- Wire cutters

Connecting the SRX300 Firewall Grounding Cable

You ground the services gateway by connecting a grounding cable to earth ground and then attaching it to the chassis grounding point located on the back panel of the device using a M4 screw. You must install the SRX300 in a restricted-access location and ensure that the chassis is always properly grounded. The SRX300 device has a single-hole protective grounding terminal provided on the chassis. See Figure 11 on page 38. 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 single-hole grounding lug connection. This tested system meets or exceeds all applicable EMC regulatory requirements with the single-hole protective grounding terminal.

You must provide the following items:

- One M4 screw
- Grounding cables

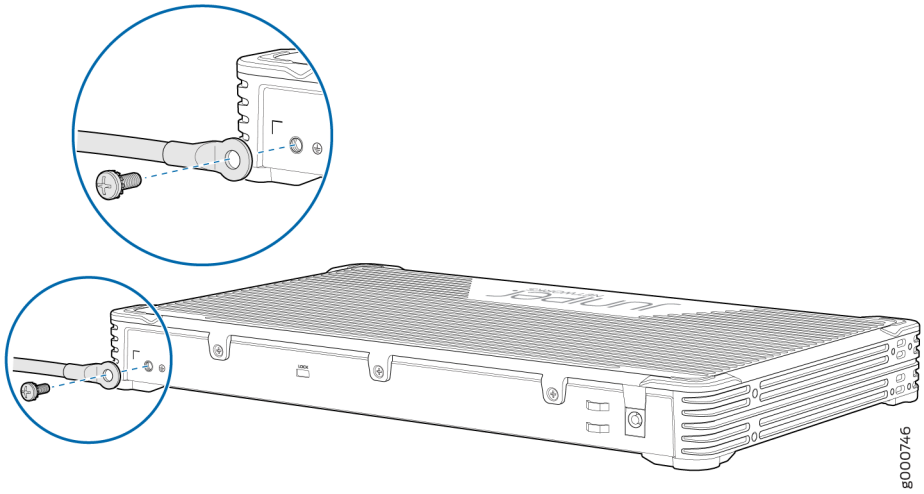
- Cable lugs (for example, Panduit LCC6-10A-L)

> **CAUTION**: Before you connect power to the services gateway, a licensed electrician must attach a cable lug to the grounding and power cables that you supply. A cable with an incorrectly attached lug can damage the services gateway (for example, by causing a short circuit).

To ground the device:

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strap to the ESD point on the chassis. For more details, see Preventing Electrostatic Discharge Damage to the SRX300 Services Gateway.
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.
4. Place the grounding cable lug over the grounding point (sized for M4 screws) on the rear of the chassis as shown in Figure 11 on page 38.

Figure 11: Connecting the Grounding Cable to the SRX300 Firewall



5. Secure the grounding cable lug to the grounding point, first with the washer, then with the screw. Apply between 6 in.-lb (0.67 Nm) and 8 in.-lb (0.9 Nm) of torque to the screw.
6. 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.

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

SEE ALSO

SRX300 Firewall Grounding Specifications | 18

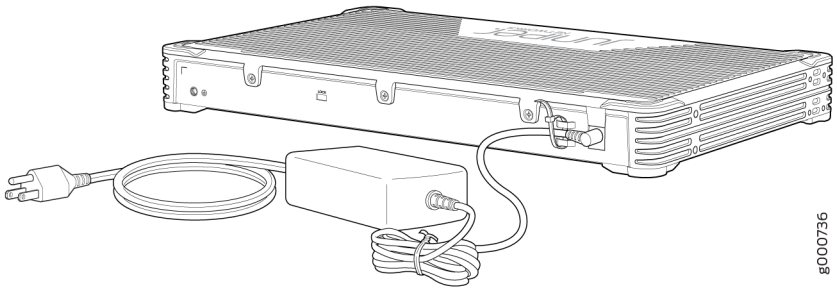
Connecting the SRX300 Firewall to the Power Supply

To connect the device to the power supply:

CAUTION: Before connecting the device to the power supply, attach an ESD strap to an ESD point and place the other end of the strap around your bare wrist.

1. Plug the DC connector end of the power cable into the power connector on the back of the device as shown in Figure 12 on page 39.
2. Plug the AC adapter end of the power cable into an AC power outlet.

Figure 12: Connecting the SRX300 Firewall to the Power Supply



Powering On the SRX300 Services Gateway

To power on the services gateway:

1. Ensure that you have connected the power supply to the device.

2. Insert the plug of the power supply adapter into an AC power source receptacle.
3. Turn on the power to the AC power receptacle.

The device starts automatically as the power supply completes its startup sequence. The PWR LED lights 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.

NOTE: When the system is completely powered off and you turn on the power supply, the device starts as the power supply completes its startup sequence. If the device finishes starting and you need to power off the system again, first issue the CLI `request system power-off` command.

Powering Off the SRX300 Services Gateway

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.

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

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

  WARNING: 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.

CAUTION: Forced shutdown can result in data loss and corruption of the file system.

NOTE: 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 SRX300 to External Devices

IN THIS SECTION

- Connecting the Dial-Up Modem to the Console Port on the SRX300 Services Gateway | **41**
- Connecting to the SRX300 Firewall CLI Using a Dial-Up Modem | **42**

Connecting the Dial-Up Modem to the Console Port on the SRX300 Services Gateway

To connect the dial-up modem to the console port on the services gateway:

1. Turn off power to the services gateway.
2. Turn off power to the modem.
3. Connect one end of the Ethernet cable into the console port on the services gateway.
4. Connect the other end of the CAT-5e cable (Ethernet cable) into the RJ-45 to DB-9 serial port adapter.
5. Connect the serial port adapter to a separately purchased DB-9 socket to DB-25 plug adapter or other adapter appropriate for your modem.
6. Plug the modem adapter into the DB-25 connector on the modem.
7. Connect the modem to your telephone network.
8. Turn on the power to the modem.
9. Power on the services gateway by pressing the Power button on the front panel. Verify that the PWR LED on the front panel turns green.

> **NOTE**: Most modems have an RS-232 DB-25 connector. You must separately purchase an adapter to connect your modem to the RJ-45 to DB-9 adapter and the Ethernet cable.

> **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).

Connecting to the SRX300 Firewall CLI Using a Dial-Up Modem

To remotely connect to the CLI through a dial-up modem connected to the console port on the services gateway:

1. Connect a modem at your remote location to a management device such as a PC or laptop computer.
2. Start your asynchronous terminal emulation application (such as Microsoft Windows HyperTerminal) on the PC or laptop computer.
3. Select the COM port to which the modem is connected (for example, COM1).
4. Configure the port settings :
   - Bits per second—9600
   - Data bits—8
   - Parity—None

- Stop bits—1
- Flow control—None

5. In the HyperTerminal window, enter **AT**.

   An **OK** response verifies that the modem can communicate successfully with the COM port on the PC or laptop.

6. Dial the modem that is connected to the console port on the services gateway by entering **ATDT *remote-modem-number***. For example, if the number of the modem connected to the console port on the services gateway is 0013033033030, enter **ATDT 0013033033030**.

   The services gateway login prompt appears.

7. Log in as the root user. No password is required at initial connection, but you must assign a root password before committing any configuration settings.

Configuring Junos OS on the SRX300

IN THIS SECTION

- SRX300 Firewall Factory-Default Settings | **44**
- Initial Configuration Using the CLI | **45**
- Initial Configuration Using J-Web | **49**
- Configure the Device Using ZTP with Juniper Networks Network Service Controller | **53**

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 the browser-based setup wizard or by using the command-line interface (CLI).

SRX300 Firewall Factory-Default Settings

IN THIS SECTION

- How to View Factory-Default Settings | 45

The SRX300 device is shipped with the following factory-default settings:

Table 15: Security Policies

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

Table 16: NAT Rules

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

Table 17: Interfaces

Port Label	Interface	Security Zone	DHCP State	IP Address
0/0 and 0/7	ge-0/0/0 and ge-0/0/7	untrust	Client	Unassigned
0/1 to 0/6	VLAN Interface irb.0 (ge-0/0/1 to ge-0/0/6)	trust	Server	192.168.1.1/24

The SRX300 device is shipped with the following services and protocols enabled by default.

Table 18: 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.

How to View Factory-Default Settings

To view the factory-default settings on your device:

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

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

3. View the required default configuration 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.

Initial Configuration Using the CLI

IN THIS SECTION

- Connect to the Serial Console Port | 46
- Connect to the Mini-USB Console Port | 47

Configure the SRX300 Using the CLI | 48

You can use either the serial or the mini-USB console port on the device.

Connect to the Serial Console Port

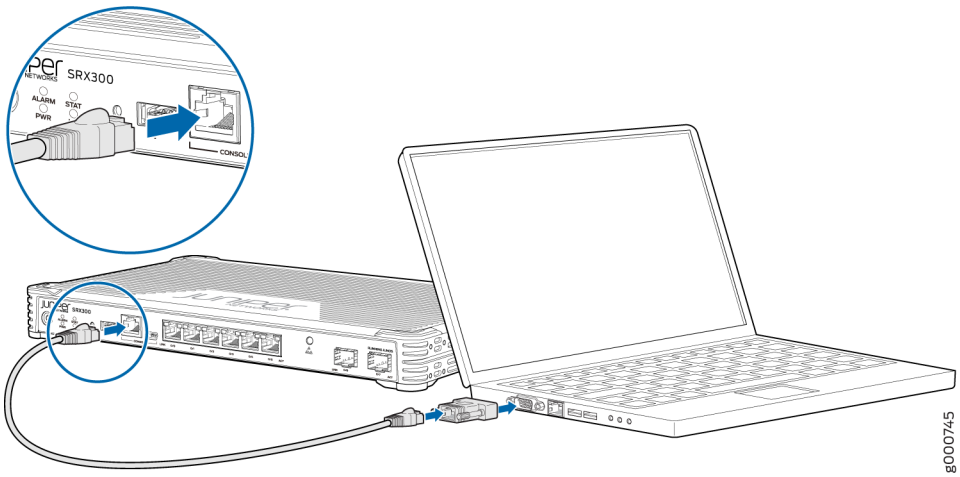
To connect to the serial console port:

1. Plug one end of the Ethernet cable into the RJ-45 to DB-9 serial port 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).

2. Plug the RJ-45 to DB-9 serial port adapter into the serial port on the management device.
3. Connect the other end of the Ethernet cable to the serial console port on the SRX300.

Figure 13: Connect to the Console Port on the SRX300



4. Start your asynchronous terminal emulation application (such as Microsoft Windows HyperTerminal) and select the appropriate COM port to use (for example, COM1).
5. Configure the serial port settings with the following values:
   - Baud rate—9600
   - Parity—N

- Data bits—8
- Stop bits—1
- Flow control—none

Connect to the Mini-USB Console Port

To connect to the mini-USB console port:

1. Download the USB driver to the management device from the Downloads page. To download the driver for Windows OS, select **6.5** from the **Version** drop-down list. To download the driver for macOS, select **4.10** from the **Version** drop-down list.
2. Install the USB console driver software:

   NOTE: Install the USB console driver software before attempting to establish a physical connection between the SRX300 and the management device, otherwise the connection will fail.

   a. Copy and extract the **.zip** file to your local folder.

   b. Double-click the **.exe** file. The installer screen appears.

   c. Click **Install**.

   d. Click **Continue Anyway** on the next screen to complete the installation.

      If you chose to stop the installation at any time during the process, then all or part of the software will fail to install. In such a case, we recommend that you uninstall the USB console driver and then reinstall it.

   e. Click **OK** when the installation is complete.
3. Plug the large end of the USB cable supplied with the SRX300 into a USB port on the management device.
4. Connect the other end of the USB cable to the mini-USB console port on the SRX300.
5. Start your asynchronous terminal emulation application (such as Microsoft Windows HyperTerminal) and select the new COM port installed by the USB console driver software. In most cases, this is the highest-numbered COM port in the selection menu.

   You can locate the COM port under **Ports (COM & LPT)** in **Windows Device Manager** after the driver is installed and initialized. This might take several seconds.
6. Configure the port settings with the following values:
   - Bits per second—9600

- Parity—None
- Data bits—8
- Stop bits—1
- Flow control—None

7. If you have not already done so, power on the SRX300 by pressing the **Power** button on the front panel. Verify that the **PWR** LED on the front panel turns green.

   The terminal emulation screen on your management device displays the startup sequence. When the SRX300 has finished starting up, a login prompt appears.

Configure the SRX300 Using the CLI

To configure the SRX300 by using the CLI:

1. Start the CLI.

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

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

2. Enter configuration mode.

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

3. 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
```

4. Commit the configuration to activate it on the device.

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

Initial Configuration Using J-Web

IN THIS SECTION

- Configure Using J-Web | 49
- Customize the Configuration for Junos OS Release 19.2 | 51
- Customize the Configuration for Junos OS Release 15.1X49-D170 | 52

Configure Using J-Web

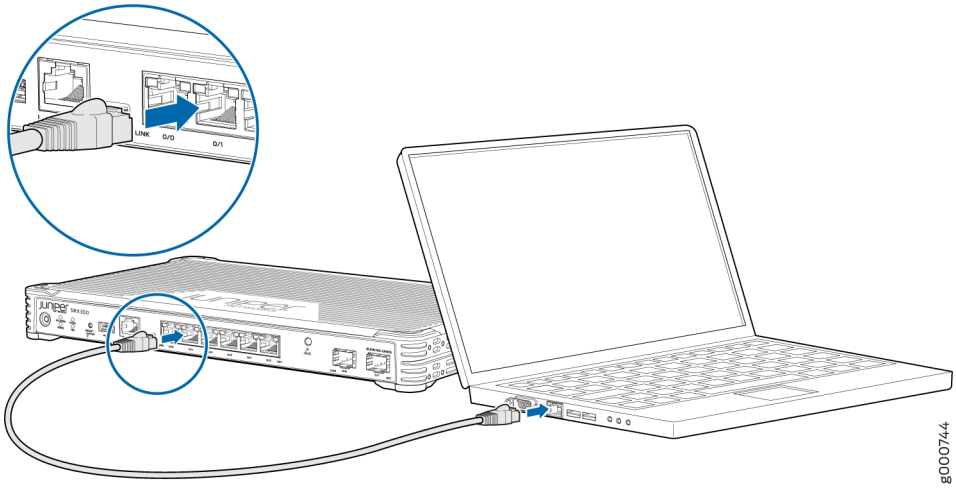
To configure the device by using J-Web:

1. Connect one end of the Ethernet cable to any of the network ports numbered **0/1** through **0/6** on the device.

   NOTE: The ge-0/0/0 and ge-0/0/7 interfaces (ports **0/0** and **0/7**) are WAN interfaces. Do not use these ports for the initial configuration procedure.

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

Figure 14: Connect the SRX300 to a Management Device



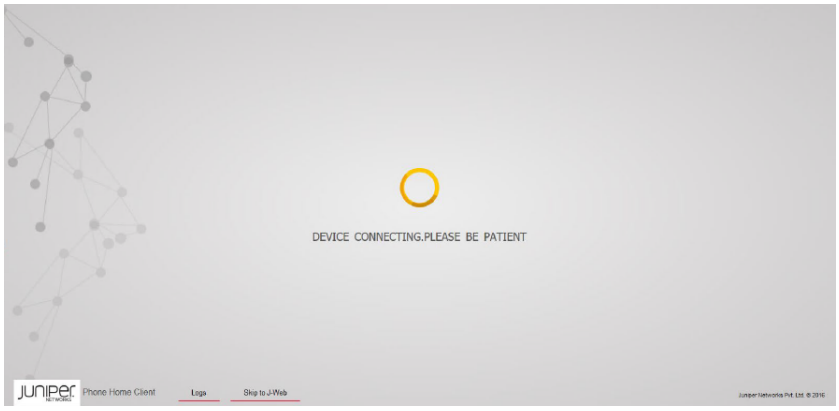
The SRX300 functions as a DHCP server and automatically assigns an IP address to the laptop.

3. Ensure that the management device acquires an IP address on the 192.168.1.0/24 network from the device.

   If an IP address is not assigned to the management device, manually configure an IP address in the 192.168.1.0/24 network.

> **NOTE**: Do not assign the 192.168.1.1 IP address to the management device, as this IP address is assigned to the SRX300.

4. Open a browser and type https://192.168.1.1. The Phone Home Client page appears.

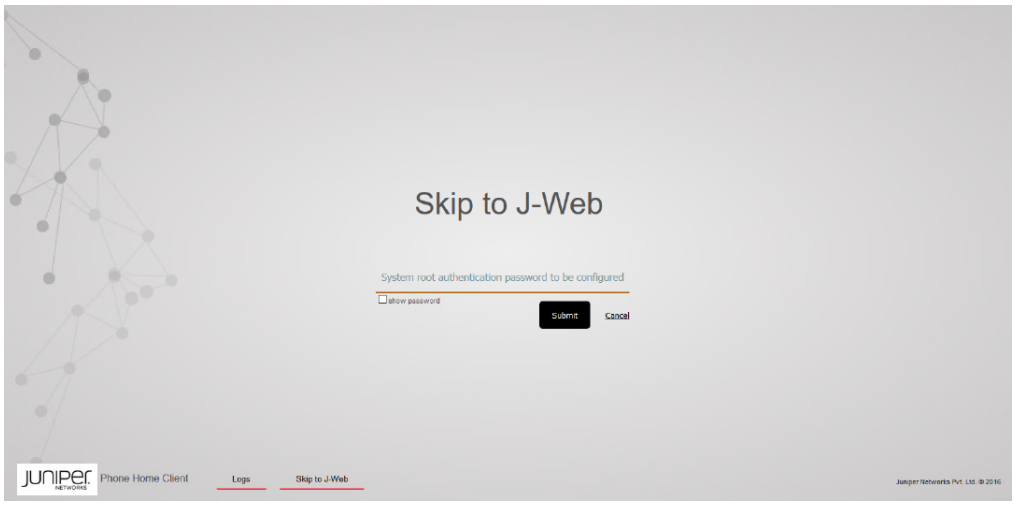


5. To configure the device:

   - Using zero-touch provisioning (ZTP)—Follow the procedure in "Configure the Device Using ZTP with Juniper Networks Network Service Controller" on page 53

- Using J-Web—Click **Skip to J-Web**.

6. Set a root authentication password in the Skip to J-Web page and click **Submit**.



   The J-Web login page appears. The SRX300 already has factory-default settings configured to make it a plug-and-play device. So all you have to do to get the SRX300 up and running is connect it to your LAN and WAN networks.

7. Connect the WAN network to port **0/0** to obtain a dynamic IP address.
8. Connect the LAN network to any of the ports from **0/1** through **0/6**.
9. Check to see if the SRX300 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 SRX300 on your network right away.

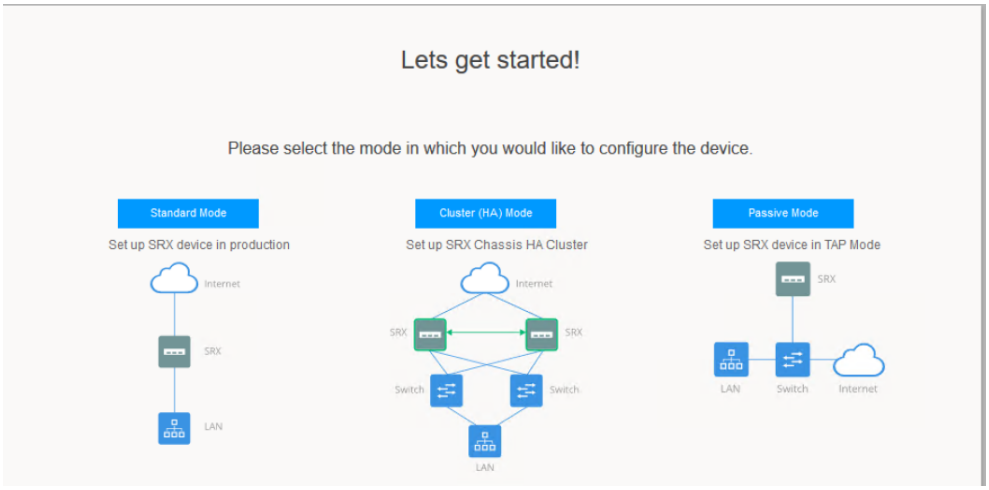
You can continue to customize the settings by logging in to J-Web and selecting the configuration mode that's right for you. You can then follow the screens as they appear in the Setup wizard.

- To customize the configuration in Junos OS Release 19.2, see "Customize the Configuration for Junos OS Release 19.2" on page 51.
- To customize the configuration in Junos OS Release 15.1X49-D170, see "Customize the Configuration for Junos OS Release 15.1X49-D170" on page 52.

Customize the Configuration for Junos OS Release 19.2

You can select any one of the configuration modes to customize the configuration:

- Standard—Configure basic security settings for the SRX300.
- Cluster (HA)—Set up the SRX300 in chassis cluster mode.
- Passive—Set up the SRX300 in Tap mode. Tap mode enables the SRX300 to passively monitor traffic flows across a network.



Customize the Configuration for Junos OS Release 15.1X49-D170

You can select any one of the configuration modes to customize the configuration:

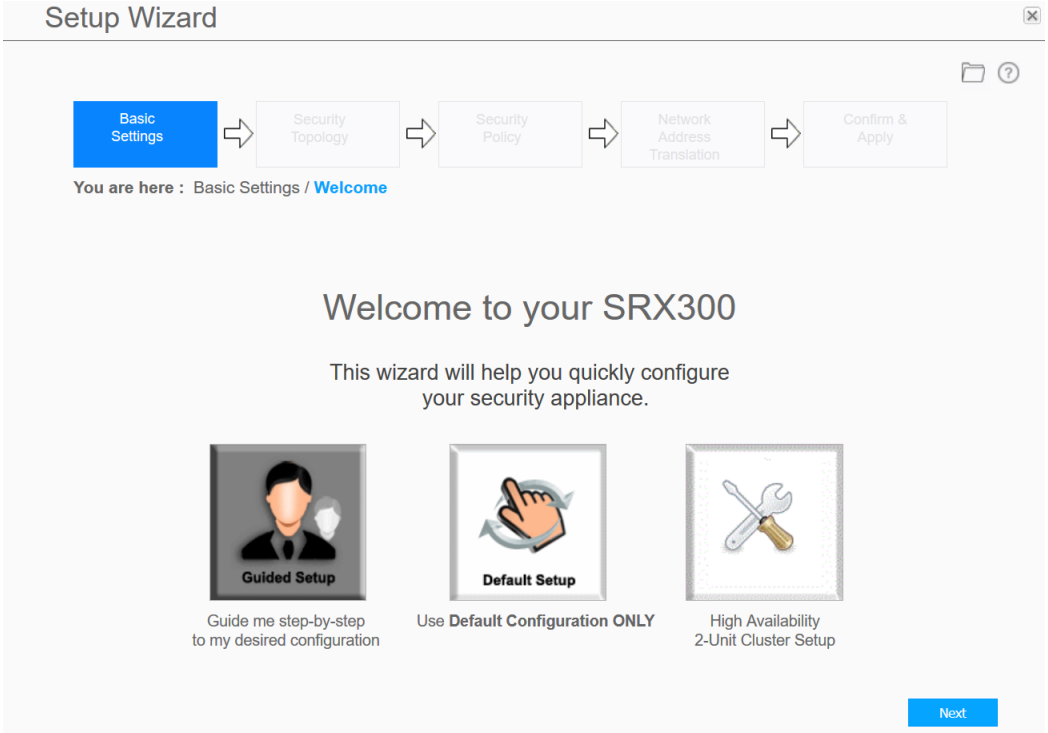
- Guided Setup (uses a dynamic IP address)—Enables you to set up the SRX300 in a custom security configuration. You can select either the Basic or the Expert option.

  The following table compares the Basic and Expert levels:

Options	Basic	Expert
Number of internal zones allowed	3	≥ 3
Internet zone configuration options	• Static IP • Dynamic IP	• Static IP • Static pool • Dynamic IP
Internal zone service configuration	Allowed	Allowed
Internal destination NAT configuration	Not Allowed	Allowed

NOTE: If you change the IP address of the port to which the laptop is connected, you might lose connectivity to the device when applying the configuration in the Guided Setup mode. To access J-Web again, open a new browser window and type https:// *new IP address*.

- Default Setup (uses a dynamic IP address)—Enables you to quickly set up the SRX300 with the default configuration. Any additional configuration can be done after the wizard setup is completed.
- High Availability—Enables you to set up a chassis cluster with a default basic configuration.



Configure the Device Using ZTP with Juniper Networks Network Service Controller

NOTE: You can configure using ZTP for Junos OS Release 19.2 and earlier releases.

You can use ZTP to complete the initial configuration of the SRX300 in your network automatically, with minimum intervention.

Network Service Controller is a component of the Juniper Networks Contrail Service Orchestration platform that simplifies and automates the design and implementation of custom network services that use an open framework.

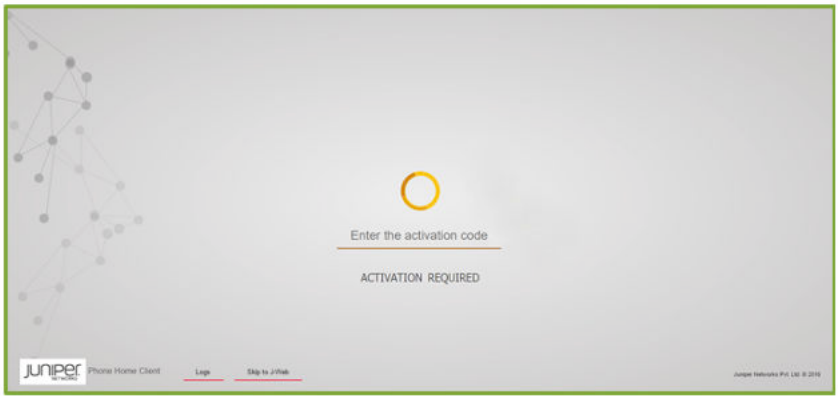
For more information, refer to the Network Service Controller section in the datasheet at http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000559-en.pdf.

To configure the device automatically using ZTP:

NOTE: To complete the ZTP process, ensure that the SRX300 is connected to the Internet.

- If you already have the authentication code, enter the code in the webpage displayed.

Figure 15: Authentication Code Page



On successful authentication, the initial configuration is applied and committed on the SRX300. Optionally, the latest Junos OS image is installed on the SRX300 before the initial configuration is applied.

- If you do not have the authentication code, you can use the J-Web setup wizard to configure the SRX300. Click **Skip to J-Web** and configure the SRX300 using J-Web.

4

CHAPTER

Maintaining Components

Maintaining the SRX300 Components | 56

Maintaining the SRX300 Components

IN THIS SECTION

- Routine Maintenance Procedures for the SRX300 Services Gateway | 56
- Maintaining the SRX300 Firewall Power Supply | 56

Routine Maintenance Procedures for the SRX300 Services Gateway

For optimum performance of the services gateway, 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 device and into the air intake vents.
- Check the status LEDs on the front panel of the services gateway.

Maintaining the SRX300 Firewall Power Supply

To maintain the power supply on the services gateway:

- Make sure that the power and grounding cables are arranged so that they do not obstruct access to other device components.
- Routinely check the PWR LED on the front panel. If this LED is solid green, the power supplies are functioning normally.
- Periodically inspect the site to ensure that the grounding and power cables connected to the services gateway are securely in place and that there is no moisture accumulating near the services gateway.



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

5
CHAPTER

Troubleshooting Hardware

Troubleshooting the SRX300 | 58

Troubleshooting the SRX300

IN THIS SECTION

- Troubleshooting Resources for the SRX300 Firewall Overview | 58
- Troubleshooting Chassis and Interface Alarm Messages on the SRX300 Firewall | 59
- Troubleshooting the Power System on the SRX300 Services Gateway | 60
- Using the RESET CONFIG Button | 61
- Changing the RESET CONFIG Button Behavior | 62

Troubleshooting Resources for the SRX300 Firewall Overview

To troubleshoot a services gateway, you use the Junos OS command-line interface (CLI) and LEDs on the components:

- LEDs—When the services gateway detects an alarm condition, the alarm LED on the interfaces glows red or yellow.
- CLI—The CLI is the primary tool for controlling and troubleshooting hardware, Junos OS, and network connectivity. Use the CLI to display more information about alarms. CLI commands display information about network connectivity derived from the ping and traceroute utilities. For information about using the CLI to troubleshoot Junos OS, see the appropriate Junos OS configuration guide.
- JTAC—If you need assistance during troubleshooting, you can contact the Juniper Networks Technical Assistance Center (JTAC) by using the Web or by telephone. If you encounter software problems, or problems with hardware components not discussed here, contact JTAC.

SEE ALSO

Troubleshooting Chassis and Interface Alarm Messages on the SRX300 Firewall | 59

Troubleshooting the Power System on the SRX300 Services Gateway | 60

Troubleshooting Chassis and Interface Alarm Messages on the SRX300 Firewall

When the services gateway detects an alarm condition, the alarm LED on the front panel turns red or amber as appropriate. To view a more detailed description of the alarm cause, issue the `show chassis alarms` CLI command.

Table 19 on page 59 describes alarms that can occur for an SRX300 Firewall chassis component.

Table 19: SRX300 Firewall Chassis Alarm Conditions and Corrective Actions

Component	Alarm Conditions	Action	Alarm Severity
Boot media	The services gateway boots from an alternate boot device.	• If the internal flash memory fails at startup, the services gateway automatically boots itself from the alternative boot device (USB storage device). **NOTE**: If you configured your services gateway to boot from an alternative boot device, ignore this alarm condition. • Reformat the internal flash memory and install a bootable image. (See the Installation and Upgrade Guide and Network Monitoring and Troubleshooting Guide) • If you did not configure the services gateway to boot from an alternative boot device, contact JTAC.	Amber (minor)
Hardware components on the services gateway	The services gateway chassis temperature or chassis is too warm	Check the room temperature. See "SRX300 Services Gateway Environmental Specifications" on page 16.	Amber (minor)

Table 19: SRX300 Firewall Chassis Alarm Conditions and Corrective Actions *(Continued)*

Component	Alarm Conditions	Action	Alarm Severity
	The services gateway temperature is too high, either because of an internal overheating condition or because the maximum recommended room temperature has been exceeded.	The services gateway shuts down automatically in 4 minutes.	Red (major)

Troubleshooting the Power System on the SRX300 Services Gateway

The LEDs on the services gateway enable you to determine the performance and operation. The PWR LED, located on the front panel of the services gateway, indicates the different settings with respect to the power system.

Table 20 on page 60 describes different PWR LED status settings and their corrective actions.

Table 20: Services Gateway Power LED Status

LED Status	Meaning	Possible Cause and Corrective Action
Green	Device is receiving power.	Normal indication. No action is required.
Amber	Indicates that the power button has been pressed and quickly released.	Normal indication. No action is required.

Table 20: Services Gateway Power LED Status *(Continued)*

LED Status	Meaning	Possible Cause and Corrective Action
Off	Indicates that the device is not receiving power.	• Verify that the AC power cord from the power source to the device is not damaged. If the insulation is cracked or broken, immediately replace the cord or cable. • Ensure that the socket you plug in is in working condition. • Ensure the device has an AC input voltage between 100 and 240 VAC. • If you cannot determine the cause of the problem or need additional assistance, contact JTAC.

SEE ALSO

Troubleshooting Chassis and Interface Alarm Messages on the SRX300 Firewall | 59

Using the RESET CONFIG Button

If a configuration fails or denies management access to the services gateway, you can use the RESET CONFIG button to restore the device to the factory-default configuration or a rescue configuration. For example, if someone inadvertently commits a configuration that denies management access to a services gateway, you can delete the invalid configuration and replace it with a rescue configuration by pressing the RESET CONFIG button.

NOTE: The RESET CONFIG button is recessed to prevent it from being pressed accidentally.

The rescue configuration is a previously committed, valid configuration. You must have previously set the rescue configuration through the J-Web interface or the CLI. To press the RESET CONFIG button, insert a small probe (such as a straightened paper clip) into the pinhole on the front panel.

- By default, pressing and quickly releasing the RESET CONFIG button loads and commits the rescue configuration through the J-Web interface or the CLI. The Status LED is solid amber during this time.
- By default, pressing and holding the RESET CONFIG button for 15 seconds or more—until the Status LED is solid amber — deletes all configurations on the device, including the backup configurations and rescue configuration, and loads and commits the factory configuration.

> **NOTE**: Resetting the configuration does not trigger a reboot automatically. Thus, configuration changes that require a reboot, such as Ethernet switching configurations, do not take effect after you reset the configuration. As a result, connectivity to the device might be lost. For the configuration to take effect, power off and power on the device after resetting the configuration.

Changing the RESET CONFIG Button Behavior

You can change the default operation of the RESET CONFIG button by limiting how the button resets the services gateway:

- To prevent the RESET CONFIG button from setting the device to the factory-default configuration and deleting all other configurations:

  ```
  admin@host# set chassis config-button no-clear
  ```

  You can still press and quickly release the button to reset it to the rescue configuration.

- To prevent the RESET CONFIG button from setting the device to the rescue configuration:

  ```
  admin@host# set chassis config-button no-rescue
  ```

  You can still press and hold the button for 15 seconds or more to reset the gateway to the factory-default configuration.

- To disable the button and prevent the device from resetting to either the factory-default or rescue configuration:

  ```
  admin@host# set chassis config-button no-clear no-rescue
  ```

The **no-clear** option prevents the RESET CONFIG button from deleting all configurations on the services gateway. The **no-rescue** option prevents the RESET CONFIG button from loading the rescue configuration.

To return the function of the RESET CONFIG button to its default behavior, remove the **config-button** statement from the device configuration.

CHAPTER 6

Contacting Customer Support and Returning the Chassis or Components

Returning the SRX300 Chassis or Components | 64

Returning the SRX300 Chassis or Components

IN THIS SECTION

- Contacting Customer Support | 64
- Returning a SRX300 Firewall Component to Juniper Networks | 65
- Locating the SRX300 Firewall Chassis Serial Number and Agency Labels | 65
- Listing the SRX300 Firewall Component Details with the CLI | 66
- Required Tools and Parts for Packing the SRX300 Firewall | 66
- Packing the SRX300 Firewall for Shipment | 66
- Packing SRX300 Firewall Components for Shipment | 67

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 a SRX300 Firewall Component to Juniper Networks

To return an SRX300 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. Refused shipments are returned to the customer via collect freight.

3. Pack the SRX300 Firewall 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 SRX300 Firewall Chassis Serial Number and Agency Labels

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

Listing the SRX300 Firewall Component Details with the CLI

Before contacting Juniper Networks to request an RMA, you must find the serial number on the SRX300 Firewall or component.

To list all of the SRX300 Firewall components and their serial numbers, enter the following command:

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                CV3315AN0010      SRX300
Routing Engine   REV 02   650-065039   CV3315AN0010      RE-SRX300
FPC 0                                                     FPC
  PIC 0                                                   6xGE,2xGE SFP Base PIC
Power Supply 0
```

Required Tools and Parts for Packing the SRX300 Firewall

To remove the components from the SRX300 Firewall 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 SRX300 Firewall for Shipment

To pack the SRX300 Firewall 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. Attach 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. For more information about ESD, see Preventing Electrostatic Discharge Damage to the SRX300 Services Gateway.

3. On the console or other management device connected to the services gateway, enter CLI operational mode and issue the following command to 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 SRX300 Firewall Components for Shipment

Follow these guidelines for packing and shipping individual components of the services gateway:

- When you return a component, make sure that it is adequately protected with packing materials and packed so that the pieces are prevented from moving around inside the carton.
- Use the original shipping materials if they are available.
- Place the individual component in an electrostatic bag.
- Write the Return Materials Authorization (RMA) number on the exterior of the box to ensure proper tracking.

CHAPTER 7

Safety and Compliance Information

Definitions of Safety Warning Levels | 69

General Safety Guidelines and Warnings | 70

Restricted Access Warning | 72

Qualified Personnel Warning | 73

Prevention of Electrostatic Discharge Damage | 74

Fire Safety Requirements | 75

Laser and LED Safety Guidelines and Warnings | 77

Radiation from Open Port Apertures Warning | 79

Battery-Handling Warning | 80

Lightning Activity Warning | 82

Jewelry Removal Warning | 83

Operating Temperature Warning | 84

Product Disposal Warning | 86

Action to Take After an Electrical Accident | 87

General Electrical Safety Guidelines and Warnings | 87

SRX300 Agency Approvals and Compliance Statements | 88

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 16 on page 75) 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).

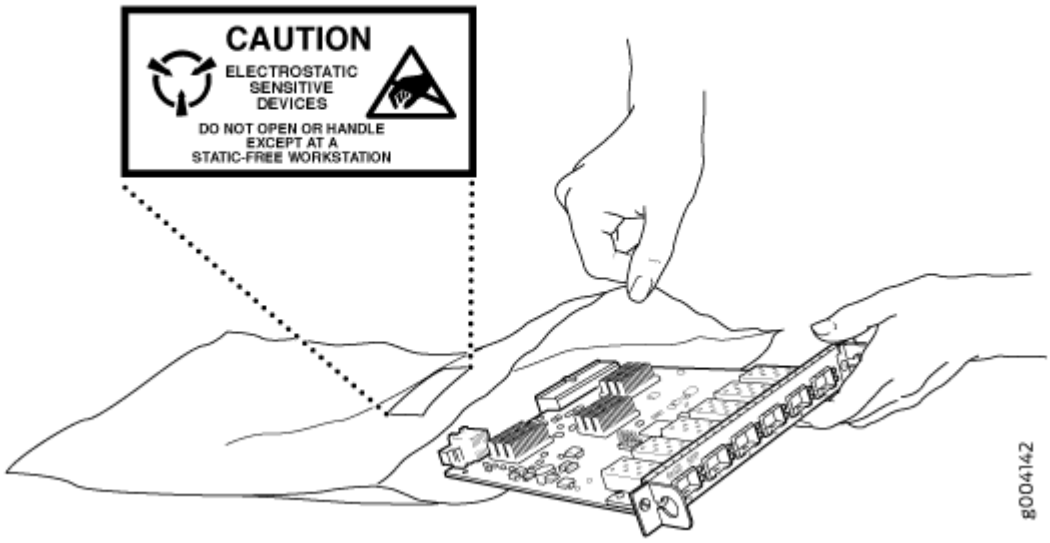
- When handling any component that is subject to ESD damage and that is removed from the device, make sure the equipment end of your ESD wrist strap is attached to the ESD point on the chassis.

  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 16 on page 75). If you are returning a component, place it in an antistatic bag before packing it.

Figure 16: 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

- Fire Suppression | 76
- Fire Suppression Equipment | 76

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

- General Laser Safety Guidelines | 77
- Class 1 Laser Product Warning | 78
- Class 1 LED Product Warning | 78
- Laser Beam Warning | 79

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.

Battery-Handling Warning



WARNING: Replacing the battery incorrectly might result in an explosion. Replace the 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.

Attention 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.

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.

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.

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 batería 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.

RELATED DOCUMENTATION

- Lightning Activity Warning | **82**
- Jewelry Removal Warning | **83**
- Operating Temperature Warning | **84**
- Product Disposal Warning | **86**

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.

Attention 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.

RELATED DOCUMENTATION

- Battery-Handling Warning | 80
- Jewelry Removal Warning | 83
- Operating Temperature Warning | 84
- Product Disposal Warning | 86

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 weld the metal object 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.

Attention 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.

RELATED DOCUMENTATION

Battery-Handling Warning | 80
Lightning Activity Warning | 82
Operating Temperature Warning | 84
Product Disposal Warning | 86

Operating Temperature Warning



WARNING: To prevent the services gateway from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 104°F (40°C). To prevent airflow restriction, allow at least 6 in. (15.2 cm) of clearance around the ventilation openings.

Waarschuwing Om te voorkomen dat welke services gateway van de Juniper Networks services gateway 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 services gateway-sarjan reititin ylikuumentuisi, sitä ei saa käyttää tilassa, jonka lämpötila ylittää korkeimman suositellun ympäristölämpötilan

40ºC. Ettei ilmanvaihto estyisi, tuuletusaukkojen ympärille on jätettävä ainakin 15,2 cm tilaa.

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

Warnung Um einen services gateway der services gateway vor Überhitzung zu schützen, darf dieser nicht in einer Gegend betrieben werden, in der die Umgebungstemperatur das empfohlene Maximum von 40ºC 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 services gateway, non adoperateli in un locale che ecceda la temperatura ambientale massima di 40ºC. 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 services gateway Disse skal ikke brukes på steder der den anbefalte maksimale omgivelsestemperaturen overstiger 40ºC. Sørg for at klaringen rundt lufteåpningene er minst 15,2 cm for å forhindre nedsatt luftsirkulasjon.

Aviso Para evitar o sobreaquecimento do encaminhador Juniper Networks services gateway, não utilize este equipamento numa área que exceda a temperatura máxima recomendada de 40ºC. 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 services gateway se recaliente, no lo haga funcionar en un área en la que se supere la temperatura ambiente máxima recomendada de 40ºC. 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 services gateway överhettas genom att inte använda den i ett område där den maximalt rekommenderade omgivningstemperaturen på 40ºC överskrids. Förhindra att luftcirkulationen inskränks genom att se till att det finns fritt utrymme på minst 15,2 cm omkring ventilationsöppningarna.



WARNING: Power off the device before installing or removing components. Check the device temperature before touching the device.

RELATED DOCUMENTATION

Battery-Handling Warning | 80
Lightning Activity Warning | 82
Jewelry Removal Warning | 83
Product Disposal Warning | 86

Product Disposal Warning



WARNING: Disposal of this product 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.

Attention 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.

RELATED DOCUMENTATION

Battery-Handling Warning | 80

Lightning Activity Warning | 82

Jewelry Removal Warning | 83

Operating Temperature Warning | 84

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

SRX300 Agency Approvals and Compliance Statements

IN THIS SECTION

SRX300 Firewall Agency Approvals | 88

SRX300 Firewall EMC Requirements | 90

SRX300 Firewall Agency Approvals

IN THIS SECTION

Compliance Statement for Argentina | 90

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
- EMC
  - EN 300 386 V1.6.1 Telecom Network Equipment - EMC requirements
  - EN 55032:2012 + EN55032:2012/AC:2013 Electromagnetic compatibility of multimedia equipment - Emission requirements
  - CISPR 32:2012
  - EN 55022:2010/AC:2011 European Radiated Emissions
  - CISPR 22 edition 6.0 : 2008-09
  - EN 55024: 2010 Information Technology Equipment Immunity Characteristics
  - CISPR 24 edition 2b :2010 COREC 2011 IT Equipment Immunity Characteristics
- EMI
  - FCC 47CFR , Part 15 Class A (2012) USA Radiated Emissions
  - ICES-003 Issue 5, August 2012 Canada Radiated Emissions
  - VCCI-V-3/2013.04 and V-4/2012.04 Japanese Radiated Emissions
  - BSMI CNS 13438 and NCC C6357 Taiwan Radiated Emissions
- Immunity
  - EN-61000-3-2 Power Line Harmonics
  - EN-61000-3-3 Voltage Fluctuations and Flicker
  - EN-61000-4-2 Electrostatic Discharge
  - EN-61000-4-3 Radiated Immunity
  - EN-61000-4-4 (2004) Electrical Fast Transients

- EN-61000-4-5 (2006) Surge
- EN-61000-4-6 (2007) Low Frequency Common Immunity
- EN-61000-4-11 (2004) Voltage Dips and Sags
- EN 55024 +A1+A2 (1998) Information Technology Equipment Immunity Characteristics

- Environmental
  - Reduction of Hazardous Substances (ROHS) 6
- Telco
  - Common Language Equipment Identifier (CLEI) code

Compliance Statement for Argentina

EQUIPO DE USO IDÓNEO.

SEE ALSO

SRX300 Firewall EMC Requirements | 90

SRX300 Firewall EMC Requirements

IN THIS SECTION

- Canada | 91
- European Community | 91
- Israel | 91
- Japan | 91
- United States | 91

Canada

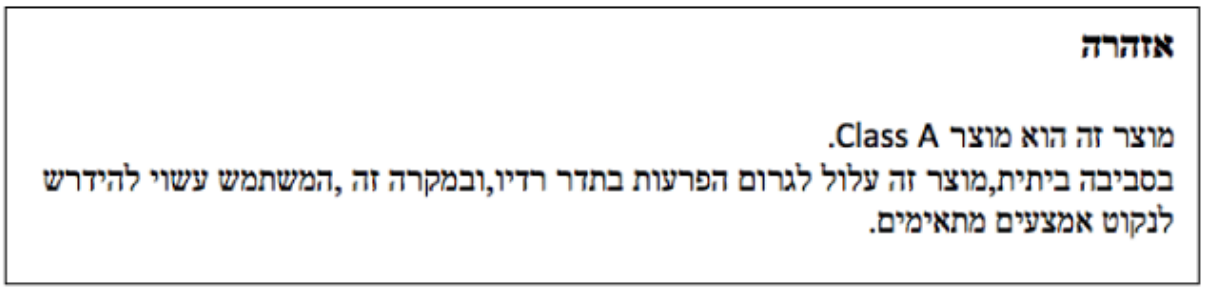
This Class A digital apparatus complies with Canadian ICES-003.

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.

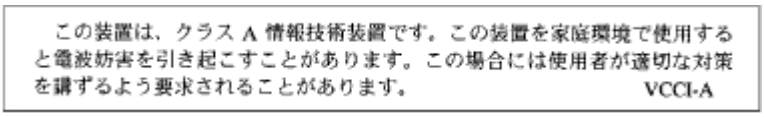
Israel



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.