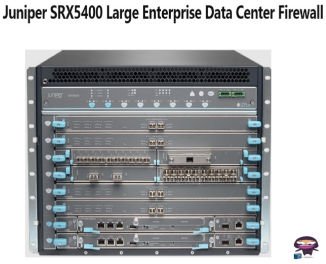
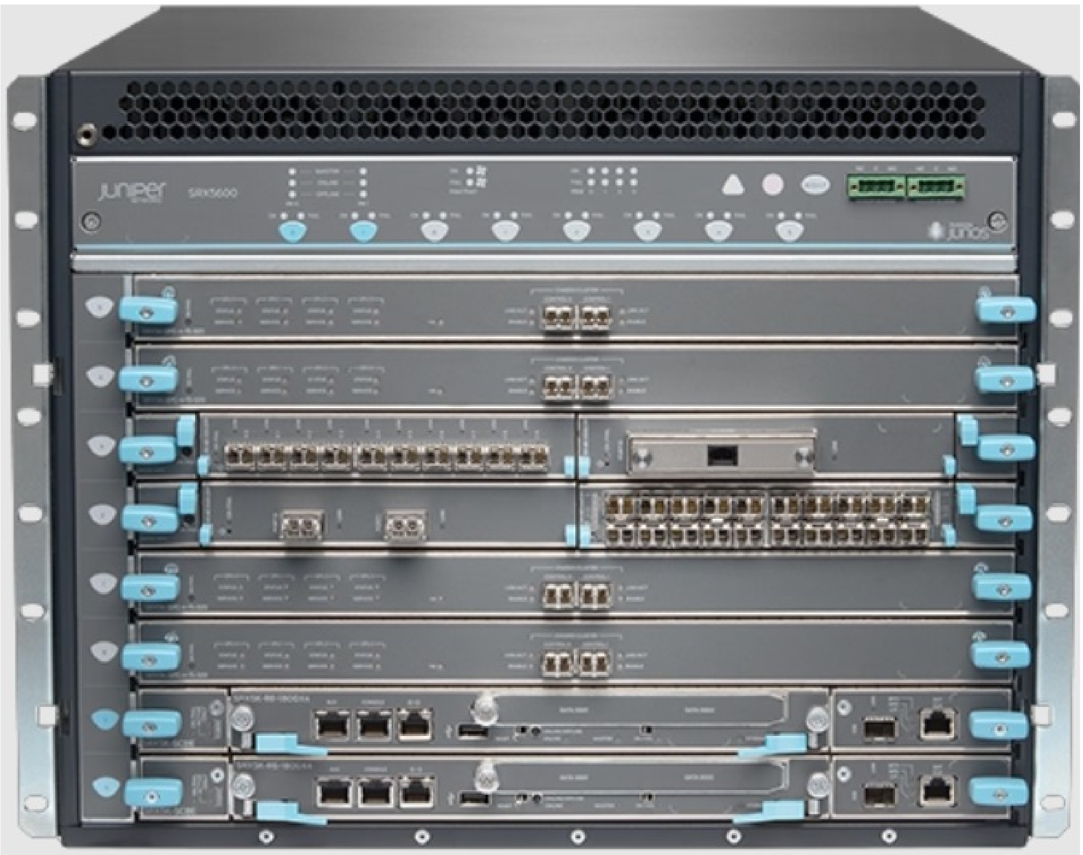


Juniper SRX5400 Large Enterprise Data Center Firewall Instruction Manual

Contents

Juniper SRX5400 Large Enterprise Data Center Firewall



Specifications

- Product: SRX5400 Firewall
- Publish Date: 2024-05-21
- Height: 5 rack units (U)
- Stacking: Up to five devices can be stacked in a single floor-to-ceiling rack
- Slots: Four slots available for configuration
- Power Supplies: Four AC power supplies for full power redundancy

Product Information

The SRX5400 Firewall is a high-performance, highly scalable, carrier-class security device with multiprocessor architecture. It provides flexibility in configuration to suit various network needs.

System Configurations
The SRX5400 Firewall allows for different combinations of MPCs and SPCs to customize the number of ports and services processing capacity. Refer to the documentation for detailed system configurations.

Power Redundancy
The firewall includes four AC power supplies for full power redundancy, ensuring continuous operation even in case of a power supply failure.

Shipping Information
The firewall is securely shipped in a cardboard box strapped to a wooden pallet, ensuring safe delivery. The package includes necessary accessories and documentation.

Product Usage Instructions

Step 1: Prepare the Site for SRX5400 Firewall Installation

Rack-Mounting Requirements
Ensure the rack meets the specified requirements for mounting the SRX5400 Firewall securely.

Tools Required to Unpack and Prepare
Gather the necessary tools as mentioned in the documentation to unpack and prepare the firewall for installation.

FAQ

- **Q: Can I use IOCs or Flex IOCs on the SRX5400 Firewall?**
  A: No, the SRX5400 Firewall only supports MPCs and does not support IOCs or Flex IOCs.
- **Q: How many power supplies are required for a fully configured device in DC configuration?**
  A: In a DC configuration, two power supplies are required to supply power to a fully configured SRX5400 Firewall.

About This Guide

This guide contains information that you need to install and configure the SRX5400 Firewall quickly. For complete installation instructions, see the SRX5400 Firewall hardware documentation at **www.juniper.net/documentation/**.

WARNING: This guide contains a summary of safety warnings in “Safety Warnings” on page 28. For a complete list of warnings for this device, including translations, see the SRX5400 Firewall hardware documentation at **www.juniper.net/documentation/**.

The SRX5400 Firewall is a high-performance, highly scalable, carrier-class security device with multi-processor architecture.
The SRX5400 Firewall is 5 rack units (U) tall. Five of these devices can be stacked in a single floor-to-ceiling rack, for increased port density per unit of floor space.
The firewall provides four slots that you can populate with one Switch Control Board (SCB) and up to three additional cards of the following types:

- Services Processing Cards (SPCs) provide the processing capacity to run integrated services such as firewall, IPsec, and IDP.
- Modular Port Concentrators (MPCs) and the Modular Interface Cards (MICs) that install in them provide Ethernet interfaces that connect the firewall to your data network.

NOTE: The SRX5400 Firewall supports the SRX5K-SPC-4-15-320 SPC only. It does not support the SRX5K-SPC-2-10-40 SPC.

By installing different combinations of MPCs and SPCs, you can tailor both the number of ports and the maximum services processing capacity to suit your network. Table 1 on page 1 describes the possible system configurations for the SRX5400 Firewall.

Table 1: Possible System Configurations

Component	Minimum	Maximum
SPC	1	2
MPC	1	2

Component	Minimum	Maximum
SCB	1	1
Routing Engine	1	1

NOTE: For SPCs and MPCs, there are three slots available allowing for the following SPC and MPC configuration scenarios: 1 SPC and 1 MPC, 2 SPCs and 1 MPC, or 1 SPC and 2 MPCs.

NOTE: MPCs are the only interface cards supported by the SRX5400 Firewall. The SRX5400 Firewall does not support the IOCs or Flex IOCs supported on other firewalls in the SRX5000 line.

Four AC power supplies (PSUs) provide full power redundancy. Each AC power supply provides power to all components in the device. When two or more power supplies are present, they share power almost equally within a fully populated system. However, if using only two AC PSUs, you must insert them into the first and third PSU slots. In the DC configuration, two power supplies are required to supply power to a fully configured device.
For detailed information about the SPCs, MPCs, and other cards supported by the firewall, see the SRX5400, SRX5600, and SRX5800 Firewall Card Reference at www.juniper.net/documentation/.
The firewall is shipped in a cardboard box strapped securely to a wooden pallet. Plastic straps secure the top and bottom in place. The firewall chassis is bolted to this pallet. A printed copy of this document and a cardboard accessory box are also included in the shipping container.

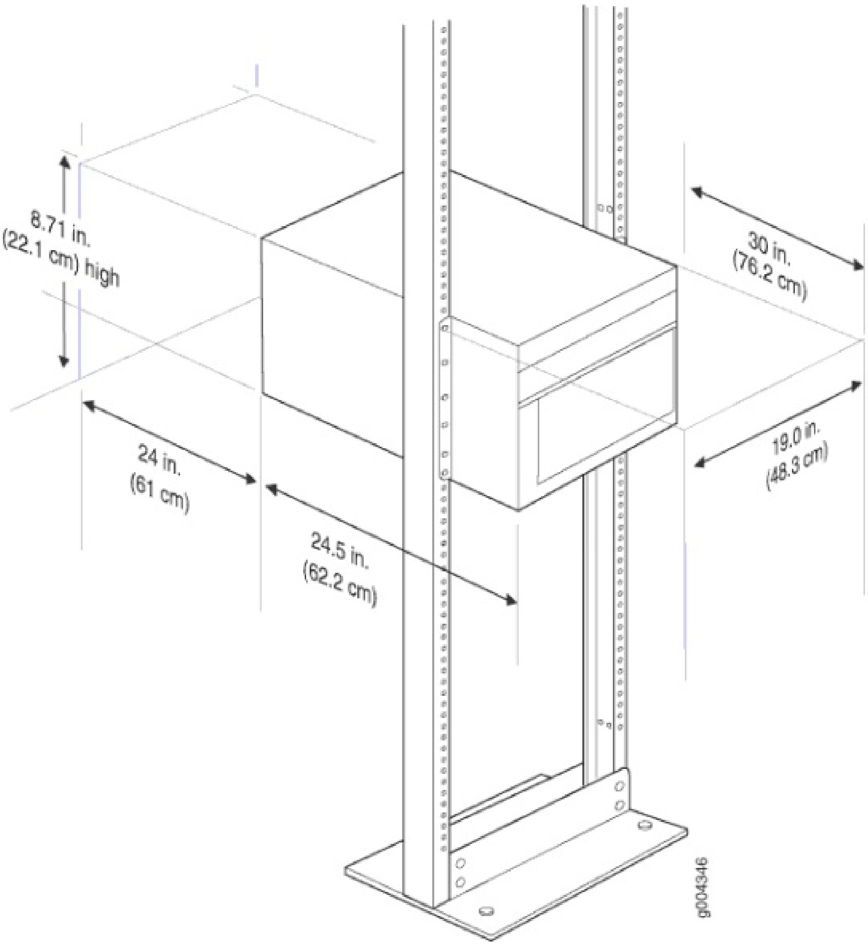
Step 1: Prepare the Site for SRX5400 Firewall Installation

IN THIS SECTION

Rack-Mounting Requirements

- You can install the firewall in a four-post rack or cabinet or an open-frame rack.
- The rack rails must be spaced widely enough to accommodate the firewall chassis' external dimensions: 8.71 in. (22.1 cm) high, 24.5 in. (62.2 cm) deep, and 17.45 in. (44.3 cm) wide. The mounting brackets extend the width to 19 in. (48.3 cm). See Figure 1 on page 4.

Figure 1: Rack Clearance and Chassis Dimensions



- The rack must be strong enough to support the weight of the fully configured firewall, up to 128 lb (58.1 kg).
- For the cooling system to function properly, the airflow around the chassis must be unrestricted. Allow at least 6 in. (15.2 cm) of clearance between side-cooled firewalls. Allow 2.8 in. (7 cm) between the side of the chassis and any non-heat-producing surface such as a wall.
- For service personnel to remove and install hardware components, there must be adequate space at the front and back of the firewall. Allow at least 30 in. (76.2 cm) in front of the firewall and 24 in. (61 cm) behind the firewall.
- The rack or cabinet must have an adequate supply of cooling air.
- Ensure that the cabinet allows the chassis hot exhaust air to exit from the cabinet without recirculating into the firewall.
- The firewall must be installed into a rack that is secured to the building structure.
- Mount the firewall at the bottom of the rack if it is the only unit in the rack.
- When mounting the firewall in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

Tools Required to Unpack and Prepare the SRX5400 Firewall for Installation

To unpack the firewall and prepare for installation, you need the following tools:

- A mechanical lift—recommended
- Phillips (+) screwdrivers, numbers 1 and 2
- 2.5-mm flat-blade (–) screwdriver

- 7/16-in. torque-controlled driver or socket wrench
- 1/2-in. or 13-mm open-end or socket wrench to remove bracket bolts from the shipping pallet
- Electrostatic discharge wrist strap
- Antistatic mat

Proceed to “Step 2: Install the Mounting Hardware in a Four-Post Rack or Cabinet or an Open-Frame Rack” on page 6.

Step 2: Install the Mounting Hardware in a Four-Post Rack or Cabinet or an Open-Frame Rack

To install the mounting shelf on the front rails of a four-post rack or cabinet, or on the rails of an open-frame rack:

1. If needed, install cage nuts in the holes specified in Table 2 on page 6.
2. On the back of each rack rail, partially insert a mounting screw into the lowest hole specified in Table 2 on page 6.
3. Install the mounting shelf on the back of the rack rails. Rest the bottom slot of each flange on a mounting screw.
4. Partially insert screws into the open holes in each flange of the mounting shelf (see Figure 2 on page 7 or Figure 3 on page 8).
5. Tighten all the screws completely.

Table 2: Mounting Shelf Hole Locations

Hole (Starting from U Division)	Distance Above U Division	
4	2.00 in. (5.1 cm)	1.14 U
3	1.51 in. (3.8 cm)	0.86 U
2	0.88 in. (2.2 cm)	0.50 U
1	0.25 in. (0.6 cm)	0.14 U

Figure 2: Mounting Hardware for a Four-Post Rack or Cabinet

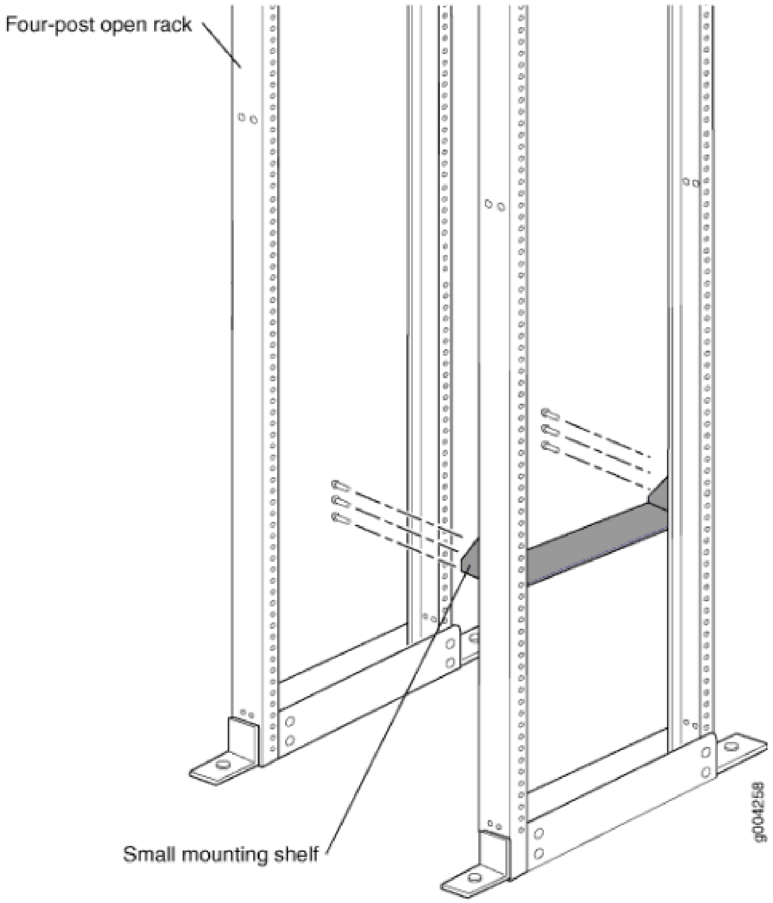
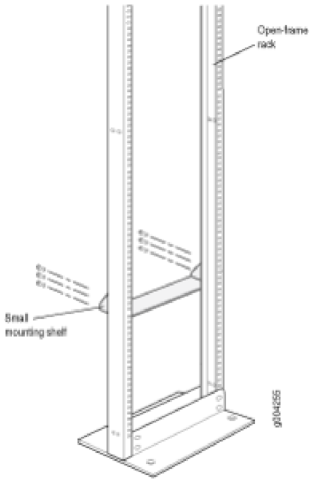


Figure 3: Mounting Hardware for an Open-Frame Rack



Proceed to "Step 3: Install the SRX4600 Firewall" on page 8.

Step 3: Install the SRX4600 Firewall

IN THIS SECTION

Because of the firewall's size and weight, you must remove all components, as shown in Figure 4 on page 9 and Figure 5 on page 9, before you install the firewall. We also recommend using a mechanical lift to install the firewall.

Remove Components

Figure 4: Components to Remove from the Front of the Firewall

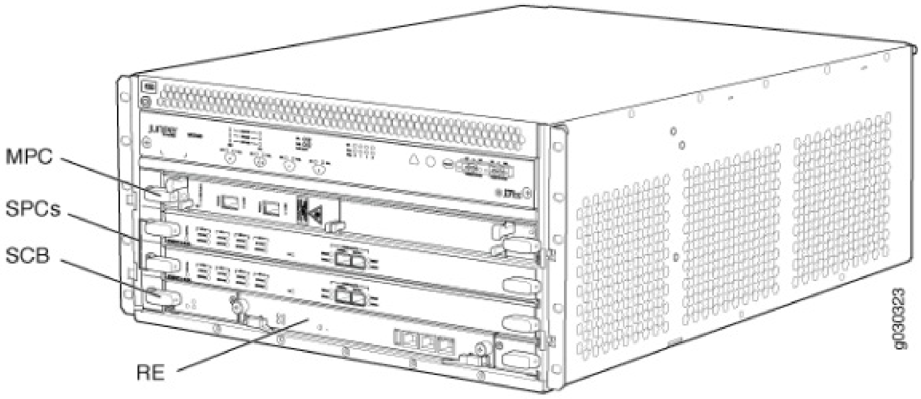
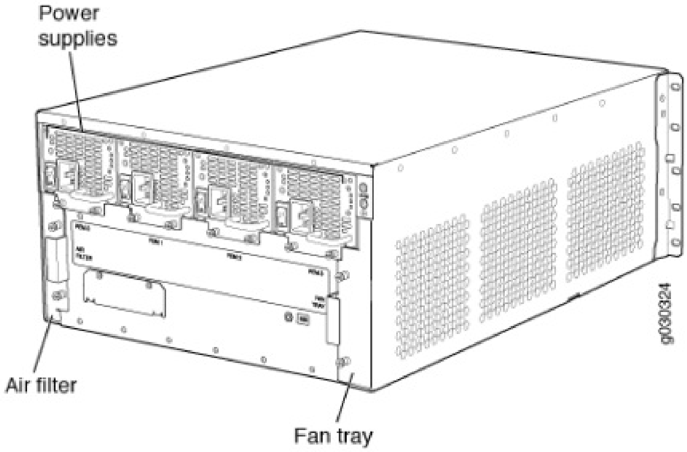


Figure 5: Components to Remove from the Rear of the Firewall



Before you lift the firewall, you must remove the following components:

- Power supplies
- SCB
- Routing Engine
- Air filter
- Fan tray
- SPCs
- MPCs

To remove the components from the firewall:

1. Slide each component out of the chassis evenly so that it does not become stuck or damaged.
2. Label each component as you remove it so you can reinstall it in the correct location.
3. Immediately store each removed component in an electrostatic bag.

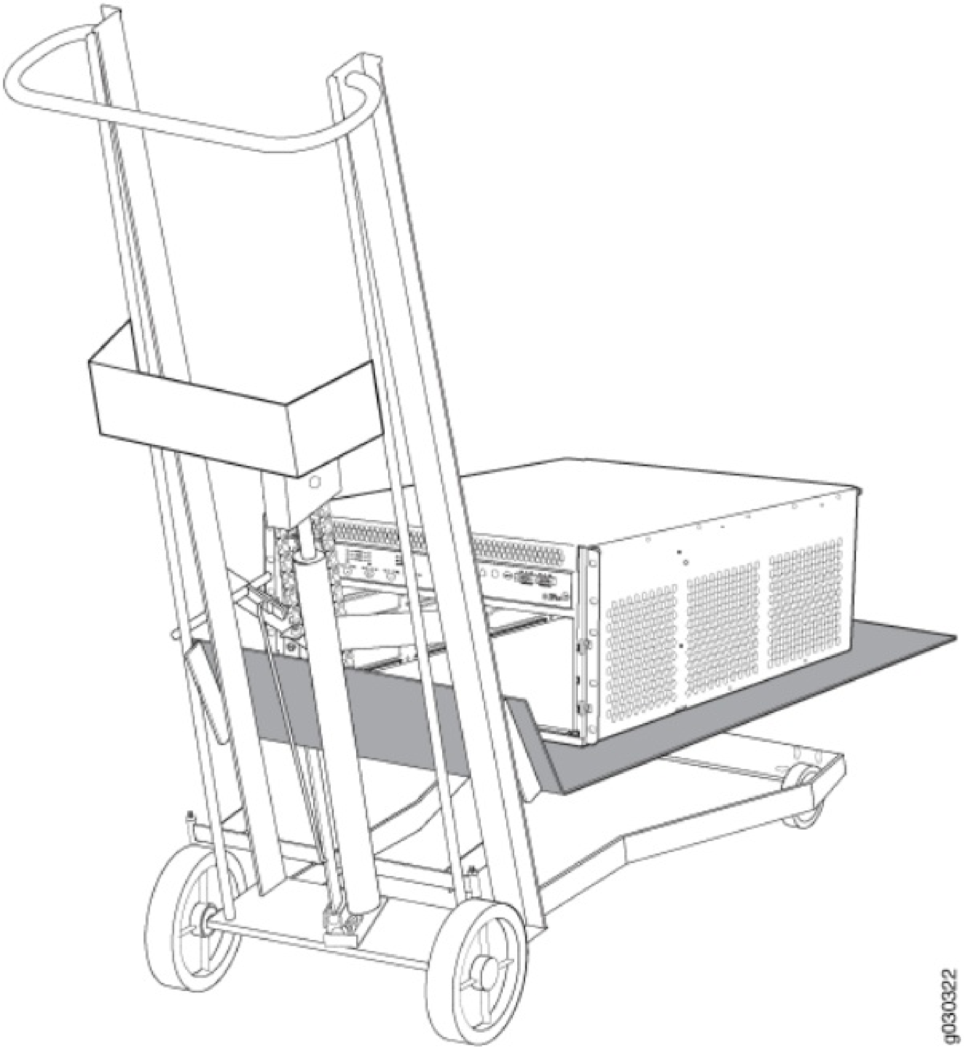
4. Do not stack removed components. Lay each one on a flat surface.

Install the Firewall Using a Lift

To install the firewall using a lift:

1. Ensure that the rack is in its permanent location and is secured to the building. Ensure that the installation site allows adequate clearance for both airflow and maintenance. For details, see the SRX5400 Firewall hardware documentation at www.juniper.net/documentation/.
2. Load the firewall onto the lift, making sure that it rests securely on the lift platform (see Figure 6 on page 11).

Figure 6: Load the Firewall onto the Lift



3. Using the lift, position the firewall in front of the rack or cabinet, centering it in front of the mounting shelf.
4. Lift the chassis approximately 0.75 in. above the surface of the mounting shelf, and position it as close as possible to the shelf.
5. Carefully slide the firewall onto the mounting shelf so that the bottom of the chassis and the mounting shelf overlap by approximately 2 in.
6. Slide the firewall onto the mounting shelf until the mounting brackets contact the rack rails. The shelf ensures that the holes in the mounting brackets and the front-mounting flanges of the chassis align with the holes in the rack rails.
7. Move the lift away from the rack.
8. Install a mounting screw into each of the open mounting holes aligned with the rack, starting from the bottom.
9. Visually inspect the alignment of the firewall. If the firewall is installed properly in the rack, all the mounting

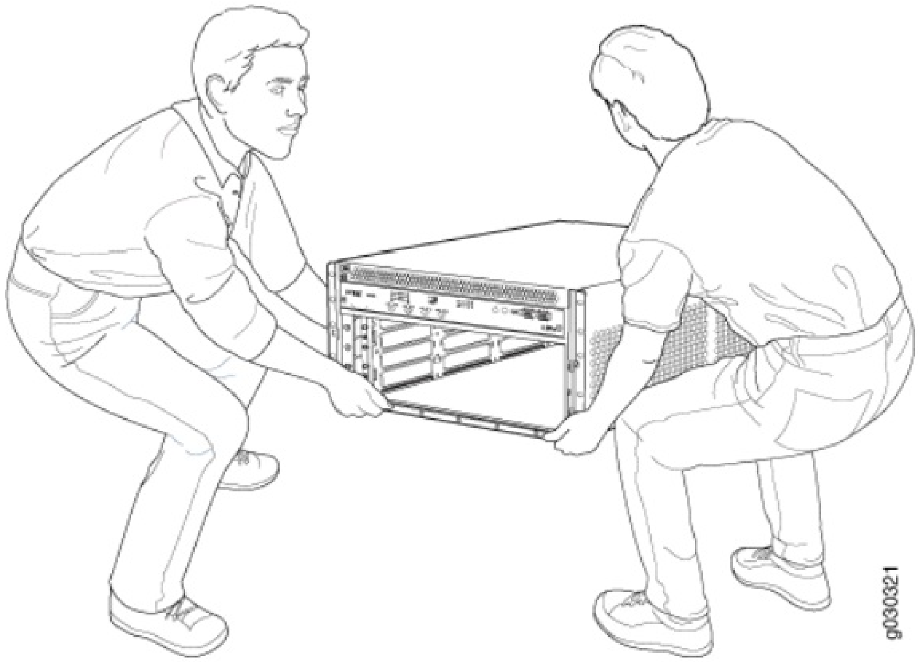
screws on one side of the rack should be aligned with the mounting screws on the opposite side and the firewall should be level.

Install the Firewall Without a Mechanical Lift

Lifting the chassis and mounting it in a rack requires at least two people. The empty chassis weighs approximately 65.5 lb (29.7 kg).

1. Ensure that the rack is in its permanent location and is secured to the building.
2. Position the chassis in front of the rack or cabinet, centering it in front of the mounting shelf. Use a pallet jack if one is available.
3. With one person on each side, hold onto the bottom of the chassis and carefully lift it onto the small mounting shelf. See Figure 7 on page 12.

Figure 7: Lift the Firewall into the Rack



4. Slide the chassis onto the mounting shelf until the mounting brackets contact the rack rails. The shelf ensures that the holes in the mounting brackets and the front-mounting flanges of the chassis align with the holes in the rack rails.
5. To install the chassis in an open-frame rack, install a mounting screw into each of the open mounting holes aligned with the rack, starting from the bottom.
6. Visually inspect the alignment of the chassis. If the chassis is installed properly in the rack, all the mounting screws on one side of the rack should be aligned with the mounting screws on the opposite side and the chassis should be level.

Reinstall Components

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis. For more information about ESD, see the SRX5400 Firewall hardware documentation at www.juniper.net/documentation/.
2. Slide each component into the chassis evenly so that it does not become stuck or damaged.
3. Tighten the captive screws or lock any levers for each component installed.

NOTE: Make sure that all empty slots are covered with blank panels before you operate the firewall.

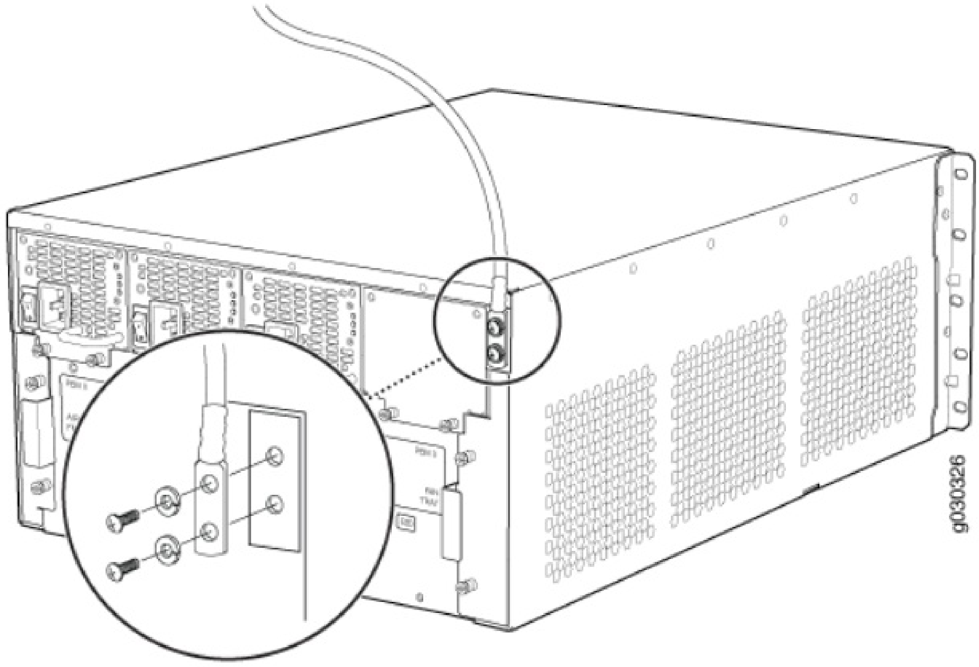
Proceed to “Step 4: Connect the Grounding Cable” on page 13.

Step 4: Connect the Grounding Cable

WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must properly ground the firewall chassis before connecting power.

1. Attach an ESD grounding strap to your bare wrist, and connect the other end of the strap to an approved site ESD grounding point. See the instructions for your site.
2. Connect the grounding cable to a proper earth ground.
3. Verify that a licensed electrician has attached the cable lug provided with the firewall to the grounding cable. The cable must be 6-AWG (13.3 mm2), minimum 60°C wire.
4. Make sure that grounding surfaces are clean and brought to a bright finish before grounding connections are made.
5. Disconnect the ESD grounding strap from the site ESD grounding point, and connect it to one of the ESD points on the chassis. For more information about ESD, see the SRX5400 Firewall hardware documentation at www.juniper.net/documentation/.
6. Place the grounding cable lug over the grounding point. The grounding point is sized for UNC 1/4-20 screws and 1/4 in. split washers, which are provided in the accessory box.
7. Secure the grounding cable lug to the grounding point, first with the washers, and then with the screws as shown in Figure 8 on page 14.

Figure 8: Connecting the Grounding Cable



8. Verify that the grounding cabling is correct, that the grounding cable does not touch or block access to firewall components, and that it does not drape where people could trip over it. Proceed to “Step 5: Connect External Devices and Network Cables” on page 15.

Step 5: Connect External Devices and Network Cables

IN THIS SECTION

To connect external devices and network cables:

Connect to a Network for Out-of-Band Management

1. Turn off the power to the management device.
2. Plug one end of the RJ-45 Ethernet cable into the appropriate ETHERNET port on the firewall Routing Engine.
3. Plug the other end of the cable into the network device.

Connect a Management Console

NOTE: We no longer include the console cable as part of the device package. If the console cable and adapter are not included in your device package, or if you need a different type of adapter, you can order the following separately:

- RJ-45 to DB-9 adapter (JNP-CBL-RJ45-DB9)
- RJ-45 to USB-A adapter (JNP-CBL-RJ45-USBA)
- RJ-45 to USB-C adapter (JNP-CBL-RJ45-USBC)

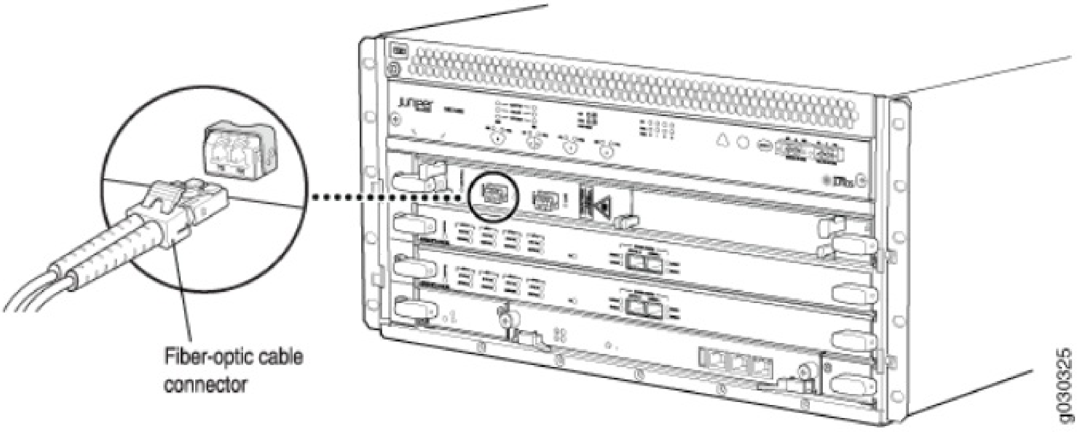
If you want to use an RJ-45 to USB-A or RJ-45 to USB-C adapter, you must have the X64 (64-Bit) Virtual COM port (VCP) driver installed on your PC. See **https://ftdichip.com/drivers/vcp-drivers/** to download the driver.

1. Plug one end of the RJ-45 Ethernet cable into the CONSOLE or AUX port on the firewall Routing Engine.
2. Plug the female DB-9 end into the device’s serial port.

Connect the Network Cables

1. Have ready a length of the type of cable used by the interface. For cable specifications, see the SRX5400 Firewall hardware documentation at **www.juniper.net/documentation/**.
2. If the cable connector port is covered by a rubber safety plug, remove the plug.
   LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.
   CAUTION: Do not leave a fiber-optic transceiver uncovered except when you are inserting or removing cable. The safety cap keeps the port clean and prevents accidental exposure to laser light.
3. Insert the cable connector into the cable connector port on the faceplate as shown in Figure 9 on page 17.

Figure 9: Connect Network Cables



4. Arrange the cable in the cable management system to prevent it from dislodging or developing stress points. Secure the cable so that it is not supporting its own weight as it hangs to the floor. Place excess cable out of the way in a neatly coiled loop in the cable management system. Placing fasteners on the loop helps to maintain its shape.

CAUTION: Avoid bending a fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

CAUTION: Do not let fiber-optic cables hang free from the connector. Do not allow the fastened loops of a cable to dangle, which stresses the cable at the fastening point.

Proceed to “Step 6: Connect Power Cables” on page 17.

Step 6: Connect Power Cables

IN THIS SECTION

Depending on its configuration, the firewall uses either AC or DC power supplies. Perform the appropriate procedures for each power supply in the firewall.

Connect Power to an AC-Powered Firewall

WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must properly ground the firewall chassis before connecting power. See “Step 4: Connect the Grounding Cable” on page 13 for instructions.

NOTE: The device is not shipped with AC power cords. Make sure to order or obtain AC power cords with a plug appropriate for your geographical location.

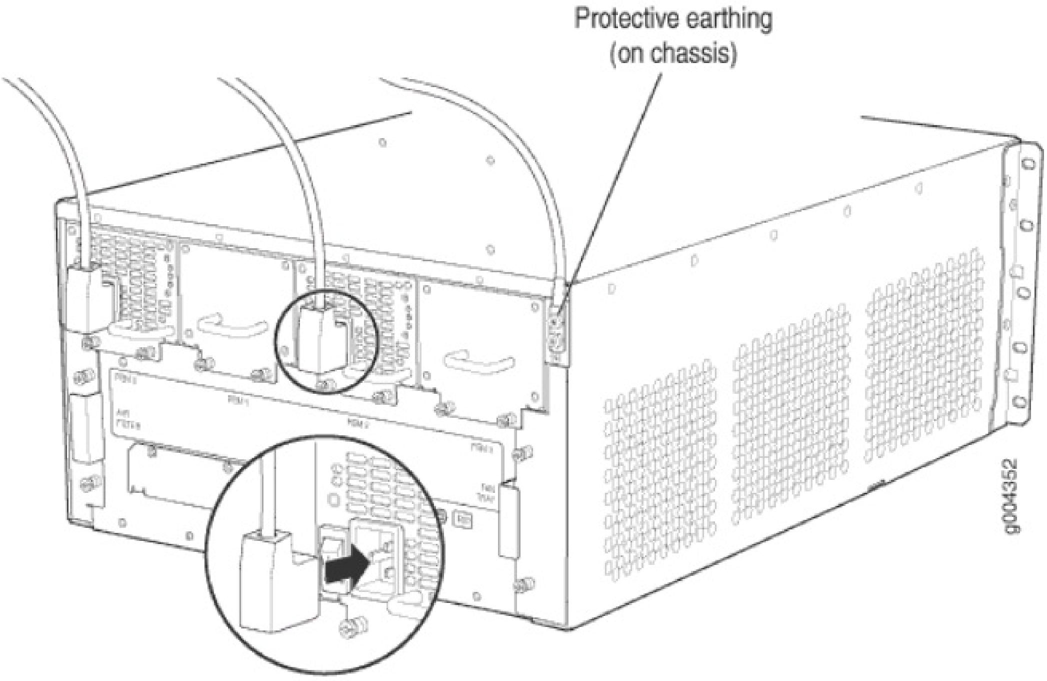
1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis. For more information about ESD, see the SRX5400 Firewall hardware documentation at www.juniper.net/documentation/.
2. Locate the power cords you will use to connect the device to AC power. See the SRX5400 Firewall hardware

documentation at www.juniper.net/documentation/ for specifications.

3. For each power supply:
   - Move the power switch on the power supply faceplate to the OFF position (O).
   - Insert the appliance coupler end of the power cord into the appliance inlet on the power supply (Figure 10 on page 19).
   - Insert the power cord plug into an external AC power source receptacle.

     NOTE: Each power supply must be connected to a dedicated AC power feed and a dedicated customer site circuit breaker. We recommend using a 15-A (250-VAC), circuit breaker minimum, or as permitted by local code.
   - Dress the power cord appropriately. Verify that the power cord does not block the air exhaust or access to firewall components, and that it does not drape where people could trip over it.

Figure 10: Connecting AC Power to the Firewall



Connect Power to a DC-Powered Firewall

This procedure addresses connecting power to firewalls equipped with DC power supplies.

WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must properly ground the firewall chassis before connecting power. See “Step 4: Connect the Grounding Cable” on page 13 for instructions.

Table 3 on page 19 describes the firewall input voltage requirements.

Table 3: DC Power System Input Voltage

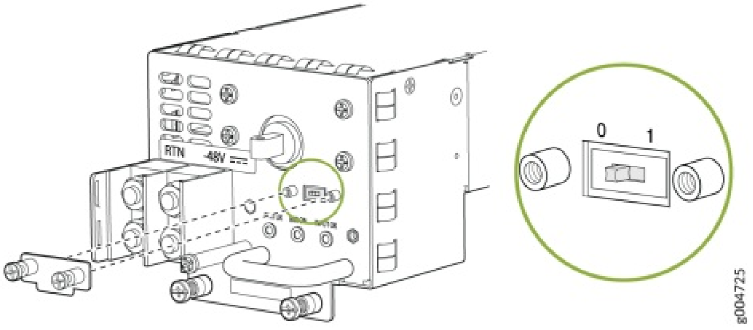
Item	Specification
DC input voltage	Operating range: –40.5 to –72 VDC

1. Ensure that the voltage across the DC power source cable leads is 0 V and that there is no chance that the

cable leads might become active during installation.

2. Check the setting of the input mode switch:
   - Move or remove the metal plate that covers the input mode switch. On some power supply versions, the cover pivots at one end, and you can simply swing it up out of the way. On other versions, the cover is secured with two captive screws that you must loosen.
   - Use a sharp, nonconductive object to slide the switch to the desired position. Set the input mode switch to position 0 for 60-A input and position 1 for 70-A input. This setting is used by the power management software and must be set on the power supply. See Figure 11 on page 20.
   -

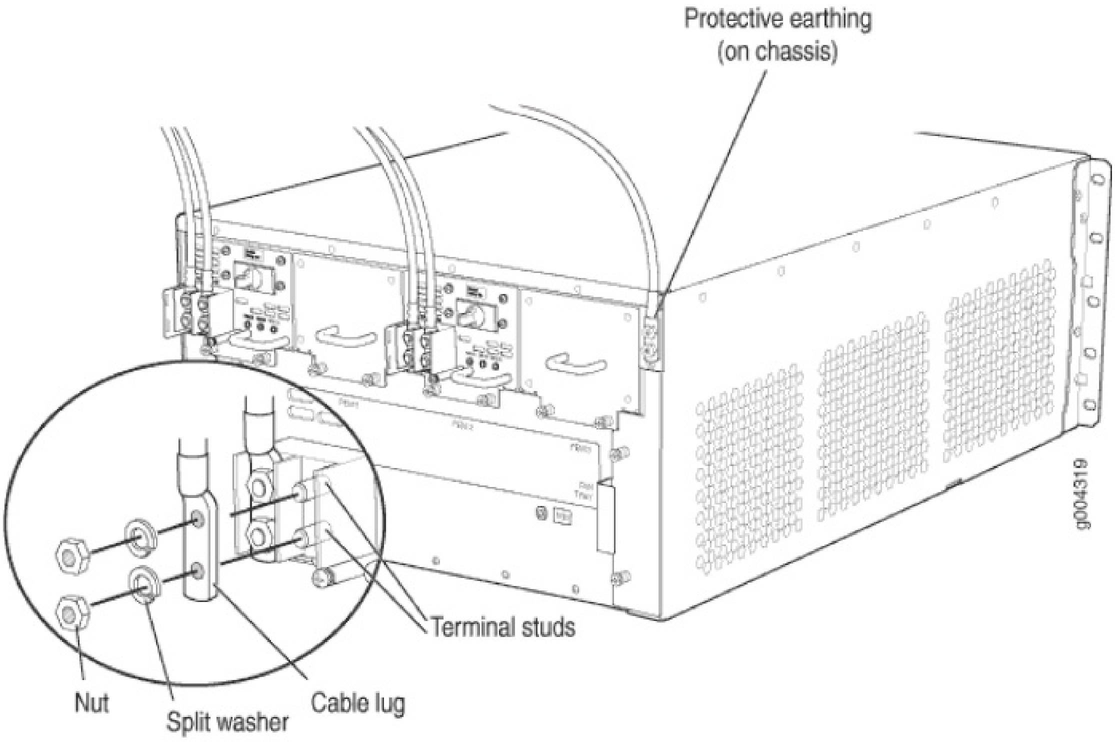
Figure 11: DC Power Supply Input Mode Switch



Restore the metal plate to its original position over the input mode switch.

3. Secure the power cable lugs to the terminal studs, first with the split washers, then with the nuts as shown in Figure 12 on page 21. Apply between 23 lb-in. (2.6 Nm) and 25 lb-in. (2.8 Nm) of torque to each nut. Do not overtighten the nut. (Use a 7/16-in. torque-controlled driver or socket wrench.)
   - Attach the positive (+) DC source power cable lug to the RTN (return) terminal.
   - Attach the negative (–) DC source power cable lug to the –48V (input) terminal.

Figure 12: Connect DC Power Cables



- Secure the power cable lugs to the terminal studs, first with the split washers, then with the nuts as shown in Figure 12 on page 21. Apply between 23 lb-in. (2.6 Nm) and 25 lb-in. (2.8 Nm) of torque to each nut. Do not overtighten the nut. (Use a 7/16-in. torque-controlled driver or socket wrench.)

- Attach the positive (+) DC source power cable lug to the RTN (return) terminal.
- Attach the negative (–) DC source power cable lug to the –48V (input) terminal.

  CAUTION: The maximum torque rating of the terminal studs on the DC power supply is 36 lb-in. (4.0 Nm). The terminal studs might be damaged if excessive torque is applied. Use only a torque-controlled driver or socket wrench to tighten nuts on the DC power supply terminal studs.

4. Connect each DC power cable to the appropriate external DC power source.

   NOTE: For information about connecting to external DC power sources, see the SRX5400 Firewall hardware documentation a **www.juniper.net/documentation/**.
5. Switch on the power supply breakers to provide voltage to the DC power source cable leads. Proceed to "Step 7: Perform the Initial Software Configuration" on page 22.

Step 7: Perform the Initial Software Configuration

IN THIS SECTION

Enter Configuration Mode

1. If you have not already done so, switch the circuit breaker or toggle switch for each power supply to the ON position to start the device. The OK LED on the power supply faceplate should blink, and then light steadily.
2. Log in as the root user. There is no password.
3. Start the CLI.
   - root# cli
   - root@>
4. Enter configuration mode.
   - configure
   - [edit]
   - root@#

Configure User Accounts and Passwords

1. 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
2. Configure an administrator account on the device. When prompted, enter the password for the administrator

account.

- [edit]
- root@# set system login user admin class super-user authentication plain-text-password
- New password: password
- Retype new password: password

3. Commit the configuration to activate it on the firewall.
   - [edit]
   - root@# commit

Configure System Attributes

1. Log in as the administrative user that you configured earlier.
2. Configure the name of the firewall. If the name includes spaces, enclose the name in quotation marks (“ ”).
   - configure
   - [edit]
   - admin@# set system host-name host-name
3. Configure the IP address and prefix length for the firewall Ethernet interface.
   - [edit]
   - admin@# set interfaces fxp0 unit 0 family inet address address/prefix-length
4. Configure the traffic interface.
   - [edit]
   - admin@# set interfaces ge-2/0/0 unit 0 family inet address address/prefix-length
   - admin@# set interfaces ge-2/1/5 unit 0 family inet address address/prefix-length
5. Configure the default route.
   - [edit]
   - admin@# set routing-options static route 0.0.0.0/0 next-hop gateway
6. Configure basic security zones and bind them to traffic interfaces.
   - [edit]
   - admin@# set security zones security-zone trust interfaces ge-2/0/0
   - admin@# set security zones security-zone untrust interfaces ge-2/1/5
7. Configure basic security policies.
   - [edit]
   - admin@# set security policies from-zone trust to-zone untrust policy policy-name match sourceaddress any destination-address any application any
   - admin@# set security policies from-zone trust to-zone untrust policy policy-name then permit
8. Configure hash-based session distribution.
   - [edit]
   - admin@# set security forwarding-process application-services session-distribution-mode hashbased

Commit the Configuration

1. Check the configuration for validity.

```
[edit]
admin@# commit check
configuration check succeeds
```

2. Optionally, display the configuration to verify that it is correct.

```
admin@# show
```

```
## Last changed: 2008-05-07 22:43:25 UTC
version "9.2I0 [builder]";
system {
    autoinstallation;
    host-name henbert;
    root-authentication {
        encrypted-password "$1$oTVn2KY3$uQe4xzQCxpR2j7sKuV.Pa0"; ## SECRET-DATA
    }
    login {
        user admin {
            uid 928;
            class super-user;
            authentication {
                encrypted-password "$1$cdOPmACd$QvreBsJkNR1EF0uurTBkE."; ## SECRET-DATA
            }
        }
    }
    services {
        ssh;
        web-management {
            http {
                interface ge-0/0/0.0;
            }
        }
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any any;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
}
    interfaces {
        ge-0/0/0 {
            unit 0;
        }
        ge-2/0/0 {
            unit 0 {
                family inet {
                    address 5.1.1.1/24;
                }
            }
        }
        ge-2/1/5 {
            unit 0 {
                family inet {
                    address 192.1.1.1/24;
                }
            }
        }
        fxp0 {
            unit 0 {
                family inet {
                    address 192.168.10.2/24;
                }
            }
        }
    }
    routing-options {
        static {
            route 0.0.0.0/0 next-hop 5.1.1.2;
        }
```

```
}
security {
    zones {
        security-zone trust {
            interfaces {
                ge-2/1/5.0;
            }
        }
        security-zone untrust {
            interfaces {
                ge-2/0/0.0;
            }
        }
    }
    policies {
        from-zone trust to-zone untrust {
            policy bob {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
    }
}
```

3. Commit the configuration to activate it on the firewall.
    - [edit]
    - admin@# commit
4. Optionally, configure additional properties by adding the necessary configuration statements. Then commit the changes to activate them on the firewall.
    - [edit]
    - admin@# commit
5. When you have finished configuring the firewall, exit configuration mode.
    - [edit]
    - admin@# exit
    - admin@>

Safety Warnings

WARNING: See installation instructions before you connect the firewall. This is a summary of safety warnings. For a complete list of warnings for the firewall, including translations, see the SRX5400 Firewall hardware documentation at **www.juniper.net/documentation/**.

WARNING: The intrabuilding port(s) of the firewall is suitable for connection to intrabuilding or unexposed wiring or cabling only. The intrabuilding port(s) of the firewall MUST NOT be metallically connected to interfaces that connect to the outside plant (OSP) or its wiring. These interfaces are designed for use as intrabuilding interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 4) and require isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

CAUTION: Before you remove or install components of a firewall, attach an 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 firewall.

CAUTION: An external surge protective device (SPD) should be used at the AC input of the firewall.

- Only trained and qualified personnel should install or replace the firewall.
- Perform only the procedures described in this guide or the SRX5400 Firewall Hardware Guide. Other services should be performed by authorized service personnel only.
- Read the installation instructions before you connect the firewall to a power source.
- Before you install the firewall, read the guidelines for site preparation in the SRX5400 Firewall
- Hardware Guide to make sure that the site meets power, environmental, and clearance requirements for the firewall.
- For the cooling system to function properly, the airflow around the chassis must be unrestricted. Allow at least 6 in. (15.2 cm) of clearance between side-cooled devices. Allow 2.8 in. (7 cm) between the side of the chassis and any non-heat-producing surface such as a wall.
- When you are installing the firewall, do not use a ramp inclined more than 10 degrees.
- Manually installing the firewall requires at least two people to lift the chassis. Before you lift the chassis, remove components as described in the SRX5400
- Firewall Hardware Guide. To prevent injury, keep your back straight and lift with your legs, not your back. Do not attempt to lift the chassis by the power supply handles.
- The firewall should be mounted at the bottom of the rack if it is the only unit in the rack.
- When you are mounting the firewall in a partially filled rack, load the rack from the bottom to the top, with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the firewall in the rack.
- When you are removing or installing an electrical component, always place it component-side up on a flat antistatic surface or in an electrostatic bag.
- When you are installing the firewall, always make the ground connection first and disconnect it last.
- Wire the DC power supply using the appropriate lugs. When you are connecting power, the proper wiring sequence is ground to ground, +RTN to +RTN, and then –48 V to –48 V. When you are disconnecting power, the proper wiring sequence is –48 V to –48 V, +RTN to +RTN, and then ground to ground. Always connect the ground wire first and disconnect it last.
- Do not work on the system or connect or disconnect cables during electrical storms.
- Before you work on equipment that is connected to power lines, remove jewelry, including rings, necklaces, and watches. Metal objects heat up when they are connected to power and ground and can cause serious burns or become welded to the terminals.
- Failure to observe these safety warnings can result in serious physical injury.
- AC power cable warning (Japan):

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

SRX5400 Firewall Compliance Statements for EMC Requirements

IN THIS SECTION

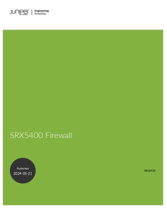
Canada
This Class A digital apparatus complies with Canadian ICES-003.

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

Japan
The preceding translates as follows:
This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this product is used near a radio or television receiver in a domestic environment, it might cause radio interference. Install and use the equipment according to the instruction manual.

United States
The firewall 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, might 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.

Documents / Resources

	**Juniper SRX5400 Large Enterprise Data Center Firewall** [pdf] Instruction Manual SRX5400 Large Enterprise Data Center Firewall, SRX5400, Large Enterprise Data Center Fire wall, Enterprise Data Center Firewall, Data Center Firewall, Center Firewall, Firewall

References

- Documentation | Juniper Networks
- Documentation | Juniper Networks
- User Manual

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.