

SRX5800 Firewall

Published
2023-10-20

RELEASE

Table of Contents

About This Guide

Step 1: Prepare the Site for SRX5800 Firewall Installation

Rack-Mounting Requirements | 2

Tools Required to Unpack and Prepare the SRX5800 Firewall for Installation | 4

Step 2: Install the Mounting Hardware

Install the Mounting Hardware in a Four-Post Rack or Cabinet | 5

Install the Mounting Hardware in an Open-Frame Rack | 6

Step 3: Install the Firewall

Remove Components | 8

Install the Firewall | 10

Reinstall Components | 12

Step 4: Connect the Grounding Cable

Step 5: Connect External Devices and Network Cables

Connect to a Network for Out-of-Band Management | 14

Connect a Management Console | 14

Connect the Network Cables | 15

Step 6: Connect Power Cables

Connect Power to an AC-Powered Firewall | 17

Connect Power to a DC-Powered Firewall | 20

Step 7: Perform the Initial Software Configuration

Enter Configuration Mode | 25

Configure User Accounts and Passwords | 25

Configure System Attributes | 26

Commit the Configuration | 27

Safety Warnings

SRX5800 Firewall Compliance Statements for EMC Requirements

About This Guide

This guide contains information that you need to install and configure the SRX5800 Firewall quickly. For complete installation instructions, see the SRX5800 Firewall Hardware Documentation at www.juniper.net/documentation/.



WARNING: This guide contains a summary of safety warnings in "Safety Warnings" on [page 30](#). For a complete list of warnings for this firewall, including translations, see the SRX5800 Firewall Hardware Documentation at www.juniper.net/documentation/.

The SRX5800 Firewall is a high-performance, highly scalable, carrier-class security device with multiprocessor architecture. The firewall is 16 rack units (RU) tall. Three firewalls can be stacked in a single floor-to-ceiling rack, for increased port density per unit of floor space. The firewall provides 14 slots that can be populated with up to 12 Services Processing Cards (SPCs) and interface cards and two Switch Control Boards (SCBs) in nonredundant fabric configurations. The interface cards can be any of the following types:

- I/O cards (IOCs) have fixed ports on their front panels.
- Flex I/O cards (Flex IOCs) have two slots on their front panels for smaller cards called port modules that add additional ports to the firewall.
- Modular Port Concentrators (MPCs) have two slots on their front panels for smaller cards called Modular Interface Cards (MICs) that add additional ports to the firewall.

The SRX5800 Firewall provides redundancy and resiliency. The hardware system is fully redundant, including power supplies and SCBs.

By installing various combinations of interface cards 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 minimum system configuration for the SRX5800 Firewall.

Table 1: Minimum System Configuration

Component	Minimum
SPC	1
Interface card (IOC, Flex IOC, or MPC)	1

Table 1: Minimum System Configuration (Continued)

Component	Minimum
SCB	1
Routing Engine	1

For detailed information about the 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 SRX5800 Firewall Installation

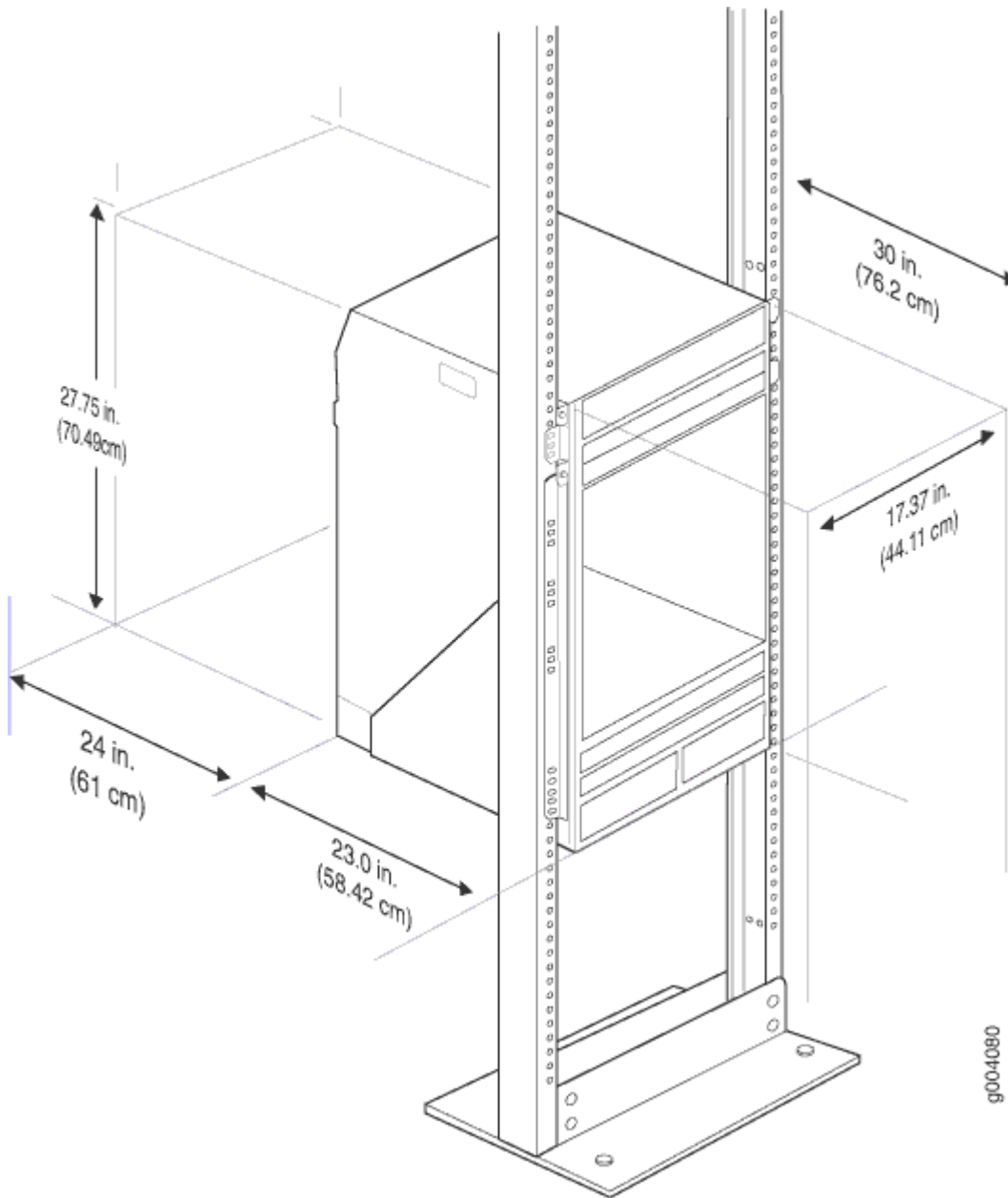
IN THIS SECTION

- [Rack-Mounting Requirements | 2](#)
- [Tools Required to Unpack and Prepare the SRX5800 Firewall for Installation | 4](#)

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's external dimensions: 27.75 in. (70.5 cm) high, 23.0 in. (58.4 cm) to 27.7 in. (70.6 cm) deep (depending on power supply type), and 17.37 in. (44.11 cm) wide. The outer edges of the mounting brackets extend the width to 19 in. (48.3 cm). See [Figure 1 on page 3](#).

Figure 1: SRX5800 Firewall Rack Clearance and Chassis Dimensions



- The rack must be strong enough to support the weight of the fully configured firewall, up to 400 lb (180 kg). If you stack three fully configured firewalls in one rack, it must be capable of supporting about 1,200 lb (542 kg).
- 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 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.

Tools Required to Unpack and Prepare the SRX5800 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" on page 4](#).

Step 2: Install the Mounting Hardware

IN THIS SECTION

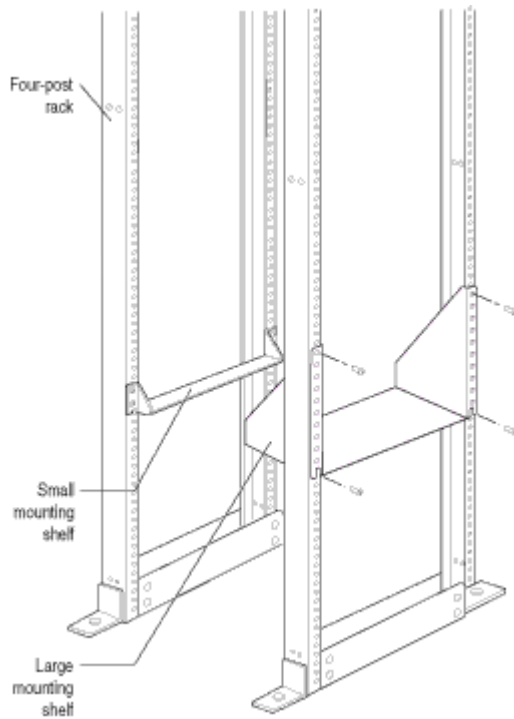
- [Install the Mounting Hardware in a Four-Post Rack or Cabinet | 5](#)
- [Install the Mounting Hardware in an Open-Frame Rack | 6](#)

Install the Mounting Hardware in a Four-Post Rack or Cabinet

To install the mounting shelf as shown in [Figure 2 on page 6](#):

1. On the front rack rails, install cage nuts in the holes specified in the *SRX5800 Firewall Hardware Guide* for the large shelf.
2. On the front of each front rack rail, partially insert a mounting screw into the hole containing the lowest cage nut.
3. Install the large shelf on the front rack rails. Rest the bottom slot of each ear on a mounting screw.
4. Partially insert a mounting screw into the top hole in each ear of the large shelf.
5. Tighten all the screws completely.
6. On the rear rack rails, install cage nuts in the holes specified in the *SRX5800 Firewall Hardware Guide* for the small shelf.
7. On the back of each rear rack rail, partially insert a mounting screw into the hole containing the lowest cage nut.
8. Install the small shelf on the back rack rails. Rest the bottom slot of each ear on a mounting screw. The small shelf installs on the back of the rear rails, extending toward the center of the rack. The bottom of the small shelf should align with the bottom of the large shelf.
9. Partially insert screws into the open holes in the ears of the small shelf.
10. Tighten all the screws completely.

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

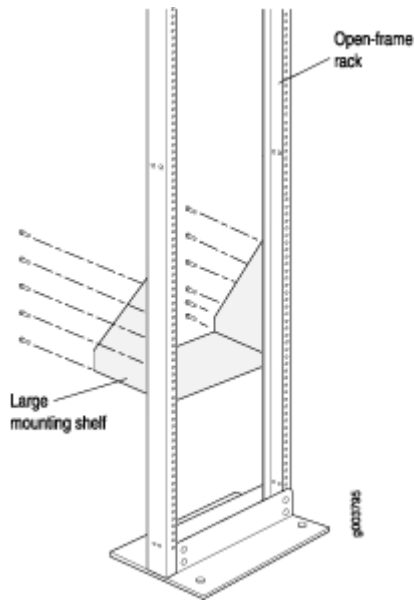


Install the Mounting Hardware in an Open-Frame Rack

To install the mounting shelf as shown in [Figure 3 on page 7](#):

1. On the rear of each rack rail, partially insert a mounting screw into the highest hole specified in the *SRX5800 Firewall Hardware Guide* for the large shelf.
2. Install the large shelf on the rack. Hang the shelf over the mounting screws using the keyhole slots located near the top of the large shelf flanges.
3. Partially insert screws into the open holes in the ears of the large shelf.
4. Tighten all the screws completely.

Figure 3: Mount Hardware for an Open-Frame Rack



Proceed to ["Step 3: Install the Firewall" on page 7](#).

Step 3: Install the Firewall

IN THIS SECTION

- [Remove Components | 8](#)
- [Install the Firewall | 10](#)
- [Reinstall Components | 12](#)

Because of the firewall's size and weight, you must use a mechanical lift to install the firewall in the rack. Also, you must remove all components, as shown in [Figure 4 on page 8](#) and [Figure 5 on page 9](#), before you install the firewall.

Remove Components

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

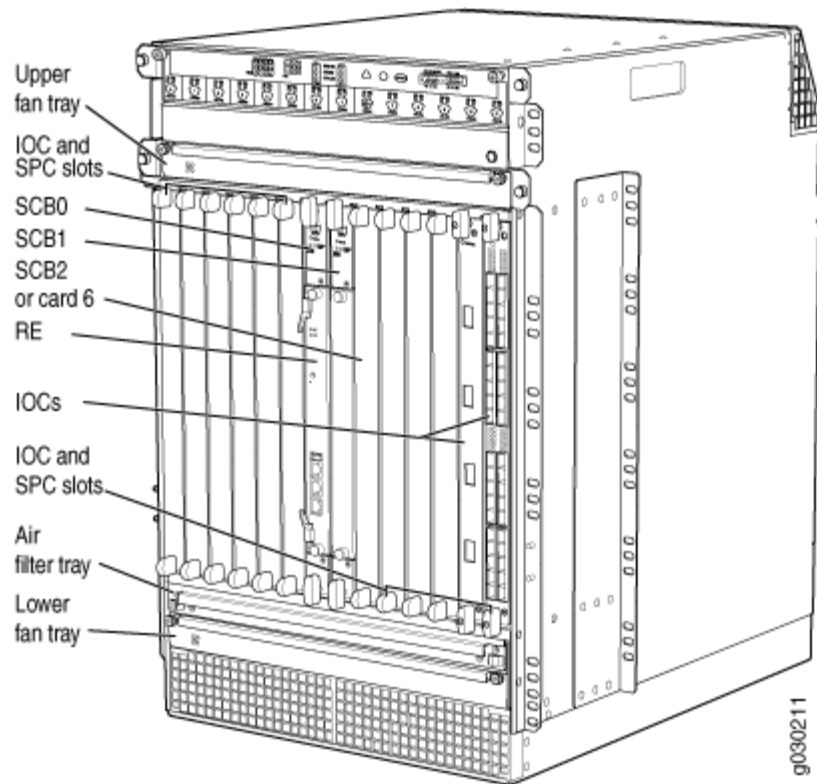
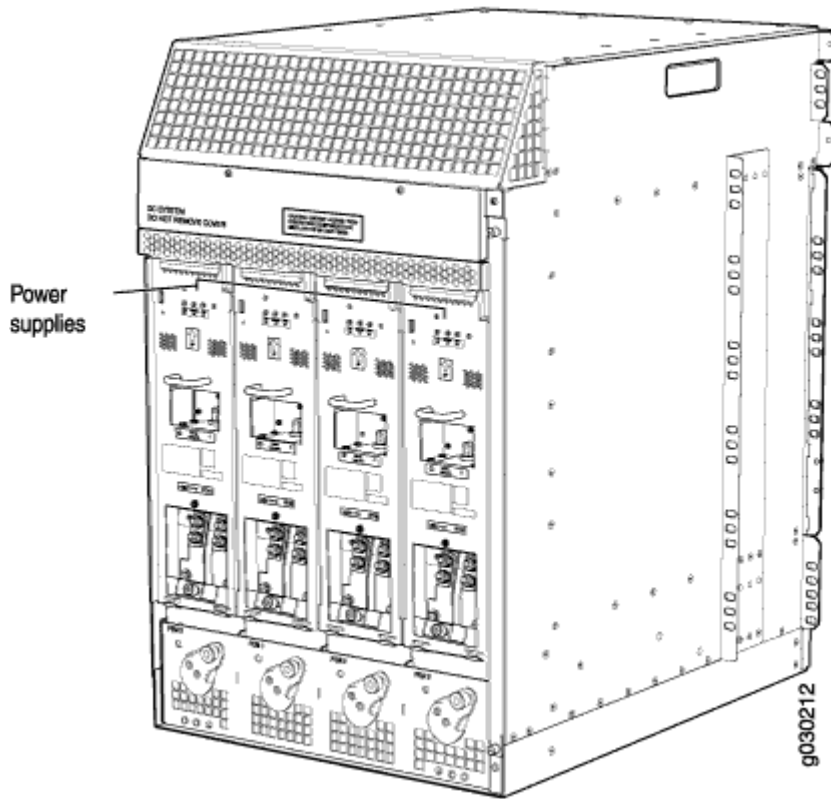


Figure 5: Components to Remove from the Rear of the Firewall



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

- Power supplies
- Cards (SCBs, SPCs, IOCs, Flex IOCs, and MPCs)
- Air filter
- Fan trays
- Cable management system

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.

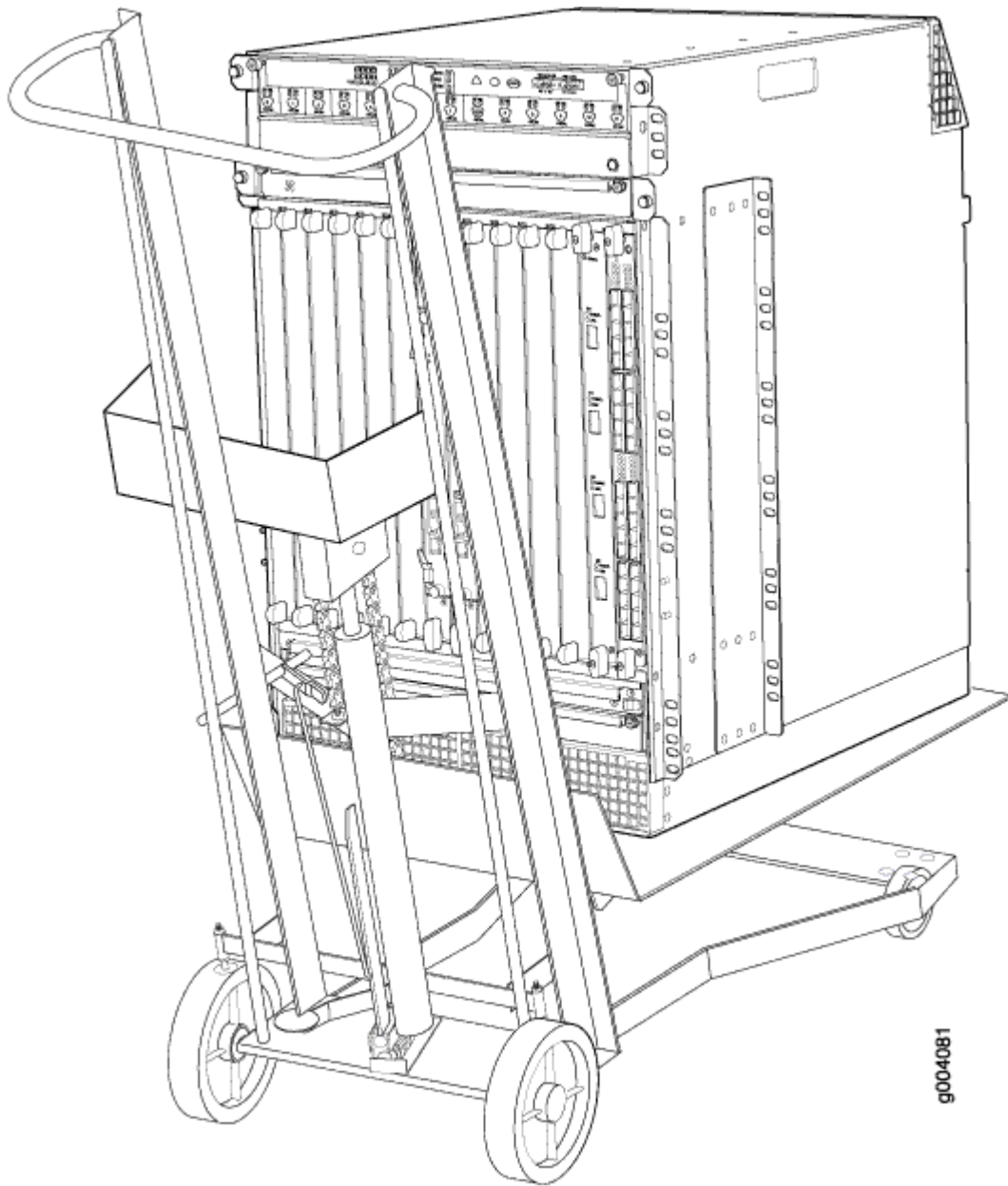
NOTE: For complete instructions on removing firewall components, see the SRX5800 Firewall Hardware Documentation at www.juniper.net/documentation/.

Install the Firewall

Before you install the firewall, you must remove all components (see "Remove Components" on page 8). 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 SRX5800 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 shelves.
4. Lift the chassis approximately 0.75 in. above the surface of the mounting shelves, and position it as close as possible to the shelves.
5. Carefully slide the firewall onto the mounting shelves so that the bottom of the chassis and the mounting shelves overlap by approximately 2 in.

6. Slide the firewall onto the mounting shelves until the mounting brackets or front-mounting flanges contact the rack rails. The shelves ensure 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. To install the firewall in an open-frame rack, 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.

Reinstall Components

To reinstall the components in the firewall:

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 SRX5800 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 for each component.

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 12.

Step 4: Connect the Grounding Cable

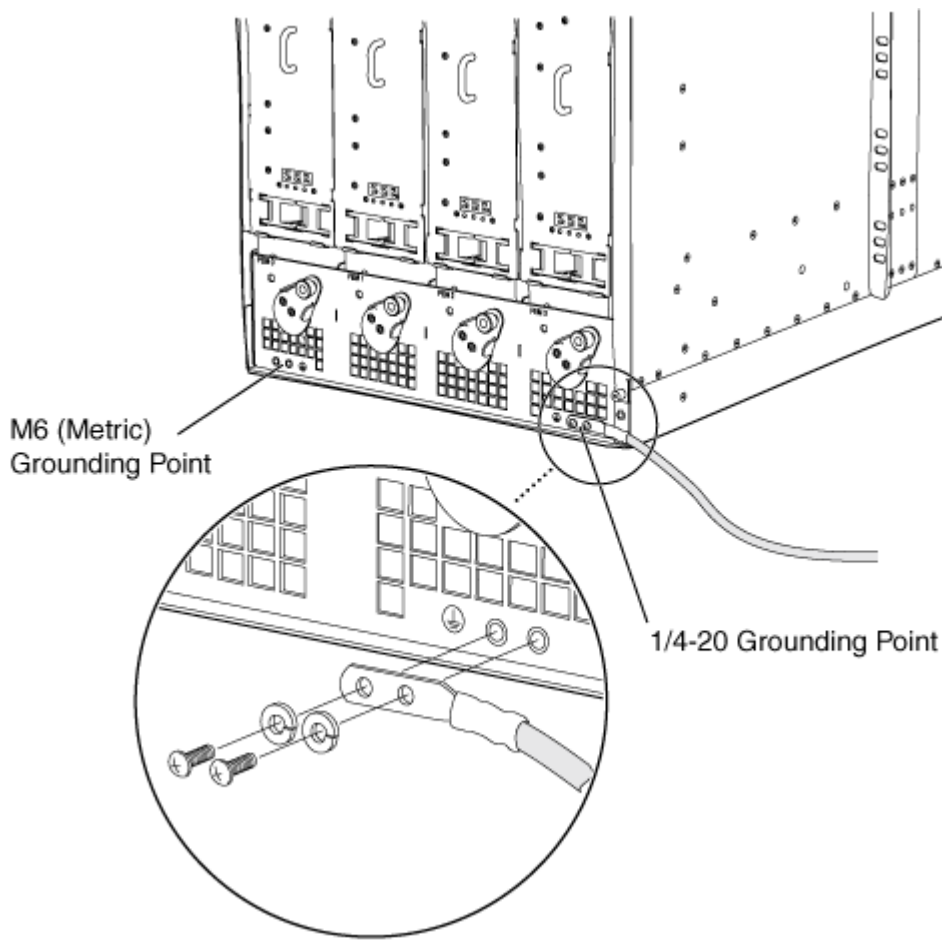


WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must properly ground the firewall chassis before connecting power.

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 SRX5800 Firewall Hardware Documentation at www.juniper.net/documentation/.
6. Place the grounding cable lug over one of the two grounding points. The right pair is sized for UNC 1/4-20 screws and 1/4 in. split washers, which are provided in the accessory box. The left pair is sized for M6 metric screws. If you wish to use the metric-sized grounding point, you must provide appropriate screws and split washers.
7. Secure the grounding cable lug to the grounding point, first with the washers, and then with the screws as shown in Figure 7 on page 13.

Figure 7: Connecting the Grounding Cable



9030295

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 14.](#)

Step 5: Connect External Devices and Network Cables

IN THIS SECTION

- [Connect to a Network for Out-of-Band Management | 14](#)
- [Connect a Management Console | 14](#)
- [Connect the Network Cables | 15](#)

To connect external devices and network cables:

Connect to a Network for Out-of-Band Management

1. Plug the RJ-45 end of the serial cable into the appropriate **CONSOLE** or **AUX** port on the firewall Routing Engine.
2. Plug the other end of the cable into the network device.

Connect a Management Console

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).

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 SRX5800 Firewall Hardware Documentation at www.juniper.net/documentation/.
2. If the cable connector port is covered by a rubber safety plug, remove the plug.



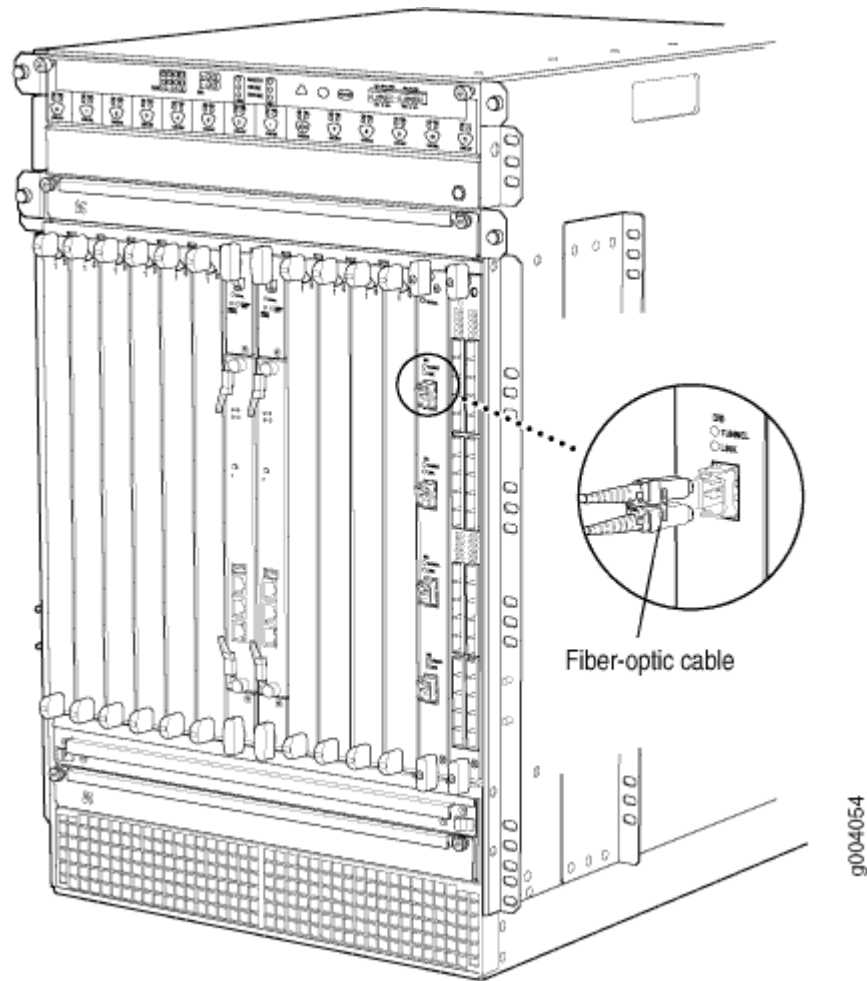
LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.



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 8 on page 16](#).

Figure 8: 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

- [Connect Power to an AC-Powered Firewall | 17](#)
- [Connect Power to a DC-Powered Firewall | 20](#)

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

This procedure addresses connecting power to firewalls equipped with either standard-capacity or high-capacity AC 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 12 for instructions.

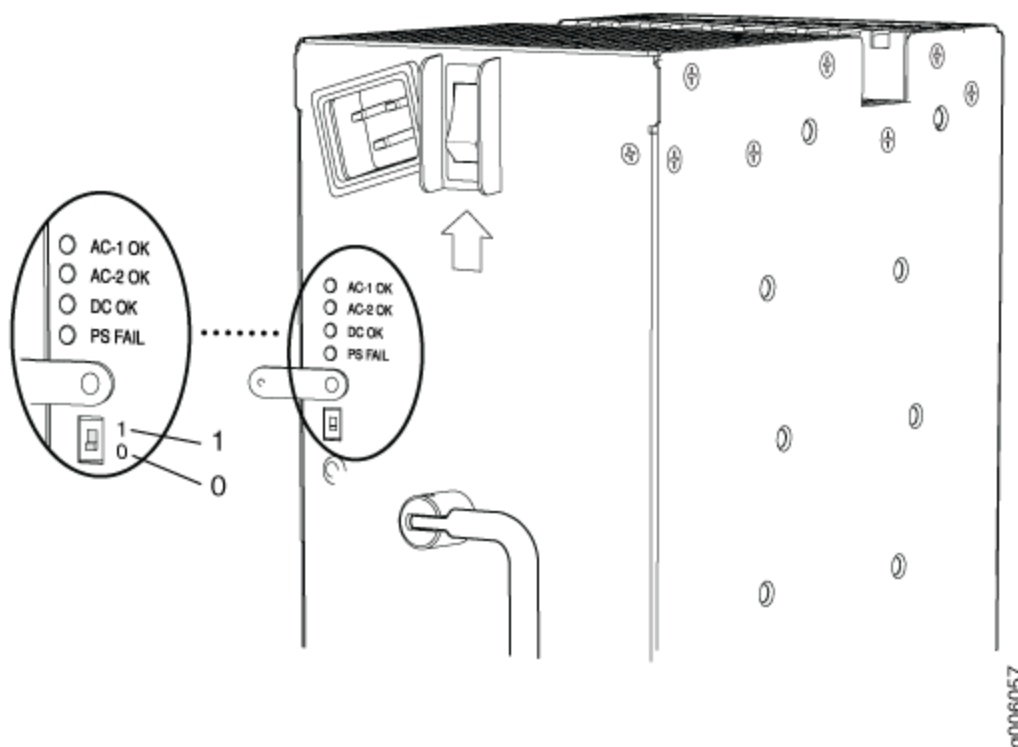
NOTE: The firewall must be running Junos OS Release 10.4 or later in order to use high-capacity AC power supplies.

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. Locate the power cords you will use to connect the device to AC power. See the SRX5800 Firewall Hardware Documentation at www.juniper.net/documentation/ for specifications.

2. 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 SRX5800 Firewall Hardware Documentation at www.juniper.net/documentation/.
3. For high-capacity AC power supplies, check the setting of the input mode switch:
 - a. 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.
 - b. Use a sharp, nonconductive object to slide the switch to the desired position. Move the input mode switch on each power supply to position **0** for one feed or position **1** for two feeds (see [Figure 9 on page 18](#)). We recommend that you use two AC power feeds and set the mode input switch to **1**.

Figure 9: High-Capacity AC Power Supply Input Mode Switch



NOTE: Do not use a pencil to set the mode switch, because fragments can break off and cause damage to the power supply.

- c. Restore the metal plate to its original position over the input mode switch.
4. For each power supply:

- a. Move the power switch above the power supply to the **OFF** position (**O**). For high-capacity AC power supplies, also move the switch on the power supply itself to the **OFF** position (**O**).
- b. Insert the appliance coupler end of a power cord into the appliance inlet above the power supply. For high-capacity power supplies, also insert the appliance coupler end of a power cord into the appliance inlet on the power supply itself.
- c. Insert each power cord plug into an external AC power source receptacle (Figure 10 on page 19 and Figure 11 on page 20).

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.

Figure 10: Connecting AC Power to the Firewall (Standard-Capacity AC Power Supplies)

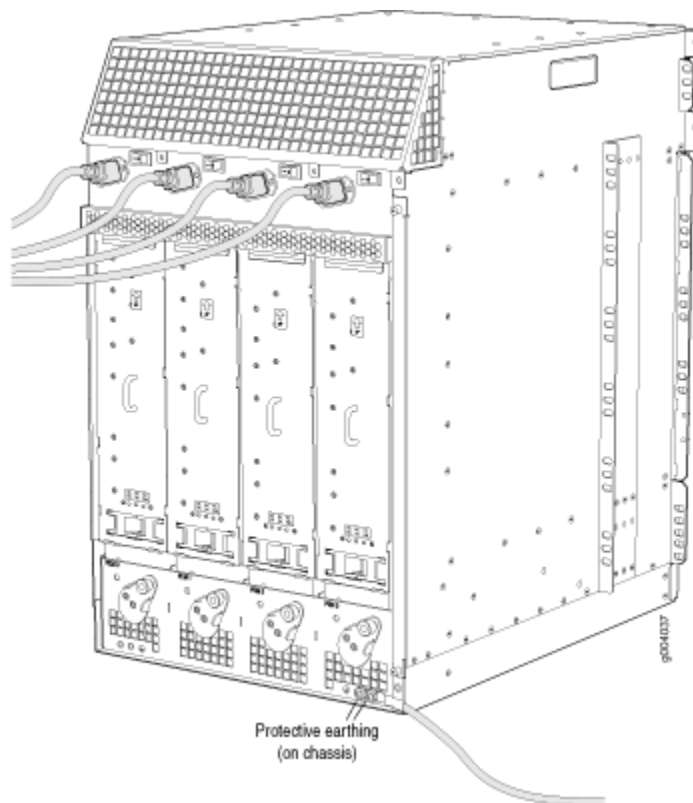
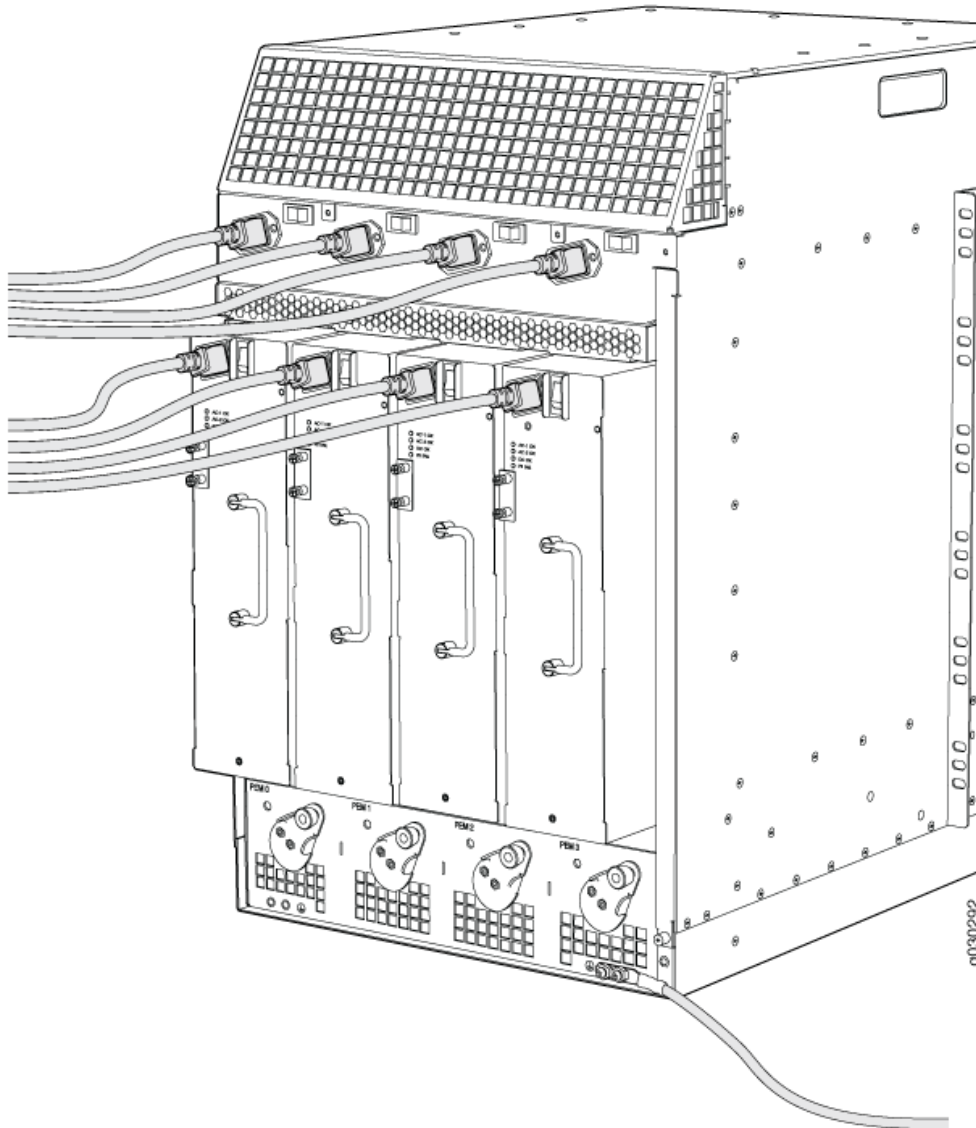


Figure 11: Connecting AC Power to the Firewall (High-Capacity Power Supplies)



- d. Dress each 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.

Connect Power to a DC-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 12](#) for instructions.

[Table 2 on page 21](#) describes the firewall input voltage requirements.

Table 2: SRX5800 Firewall DC Power System Input Voltage

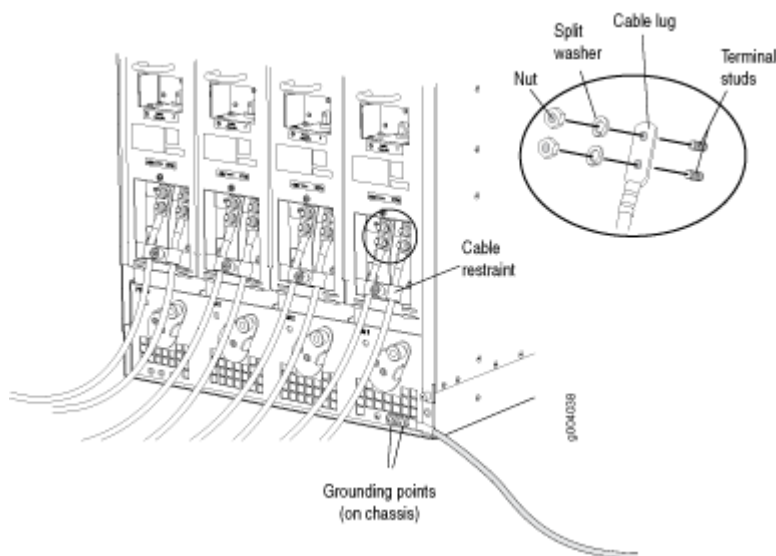
Item	Specification
DC input voltage	Operating range: -40 to -72 VDC

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. For high-capacity DC power supplies, check the setting of the input mode switch:
 - a. 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.
 - b. Use a sharp, nonconductive object to slide the switch to the desired position. Move the input mode switch on each power supply to position **0** for one feed or position **1** for two feeds (see [Figure 12 on page 22](#)). We recommend that you use two DC power feeds and set the mode input switch to **1**.

NOTE: Do not use a pencil to set the mode switch, because fragments can break off and cause damage to the power supply.

- c. Restore the metal plate to its original position over the input mode switch.
3. For standard-capacity DC power supplies, 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 22](#). 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.)
 - a. Attach the positive (+) DC source power cable lug to the **RTN** (return) terminal.
 - b. Attach the negative (-) DC source power cable lug to the **-48V** (input) terminal.
 - c. Loosen the captive screw on the cable restraint on the lower edge of the power supply faceplate.
 - d. Engage the DC power cables with the cable restraint, and tighten the captive screw.

Figure 12: Connecting Power Cables (Standard-Capacity DC Power Supplies)



CAUTION: Ensure that each power cable lug seats flush against the surface of the terminal block as you are tightening the nuts. Ensure that each nut is properly threaded onto the terminal stud. The nut should be able to spin freely with your fingers when it is first placed onto the terminal stud. Applying installation torque to the nut when it is improperly threaded might result in damage to the terminal stud.



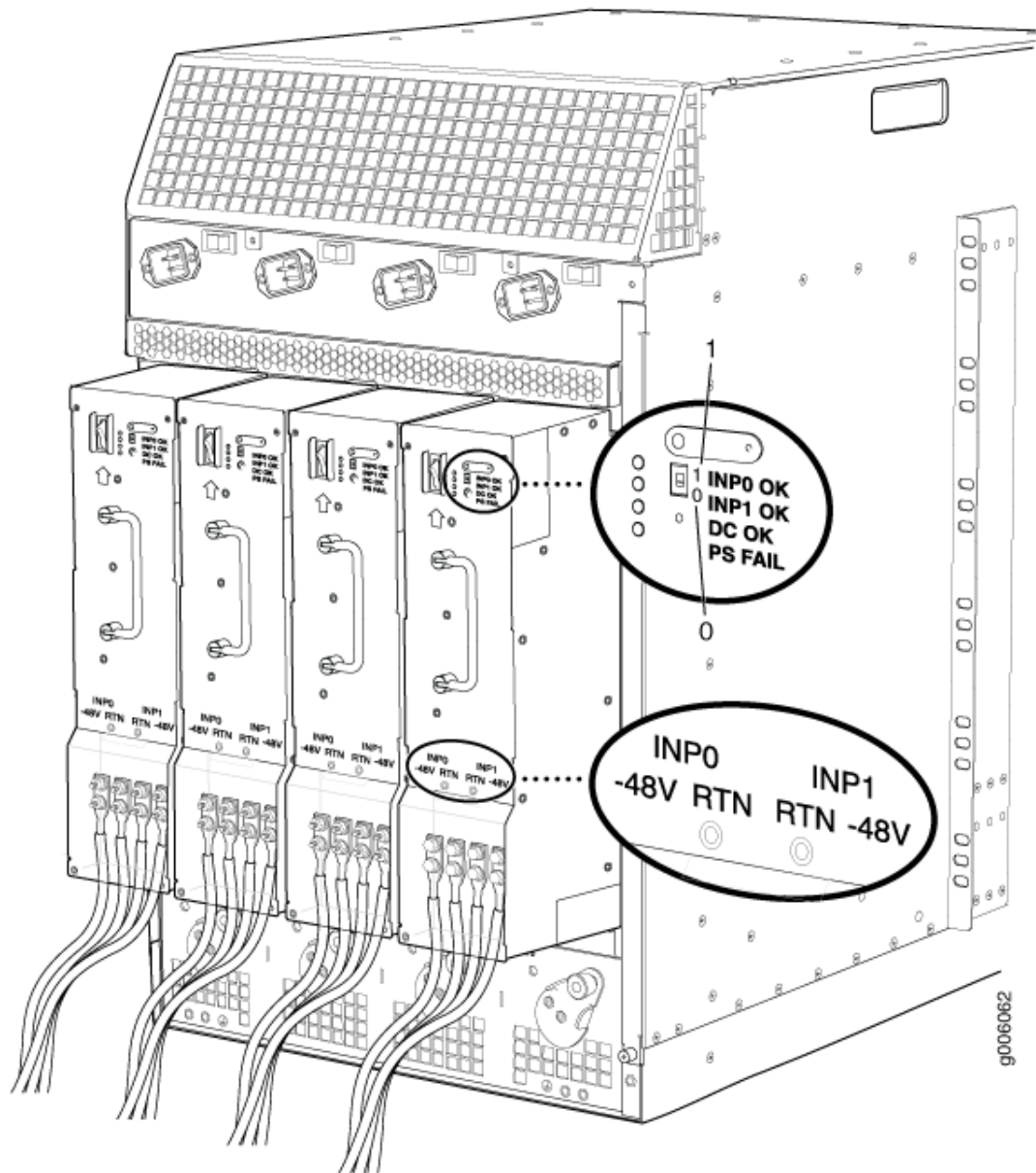
CAUTION: The maximum torque rating of the terminal studs on the DC power supply is 58 lb-in. (6.5 Nm). The terminal studs might be damaged if excessive torque is applied. Use only a torque-controlled driver or socket wrench to tighten nuts on the DC power supply terminal studs.

NOTE: For information about connecting to external DC power sources, see the SRX5800 Firewall Hardware Documentation at www.juniper.net/documentation/.

4. For high-capacity DC power supplies, secure the power cable lugs to the terminal studs, first with the split washers, then with the nuts as shown in [Figure 13 on page 23](#). 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.)
 - a. Attach the positive (+) DC source power cable lugs to the **RTN** (return) terminals for the **INP0** and **INP1** connector pairs.

- b. Attach the negative (-) DC source power cable lug to the **-48V** (input) terminals for the **INP0** and **INP1** connector pairs.

Figure 13: Input Mode Switch and Power Cable Connectors (High-Capacity DC Power Supplies)



CAUTION: Ensure that each power cable lug seats flush against the surface of the terminal block as you are tightening the nuts. Ensure that each nut is properly threaded

onto the terminal stud. The nut should be able to spin freely with your fingers when it is first placed onto the terminal stud. Applying installation torque to the nut when improperly threaded might result in damage to the terminal stud.



CAUTION: The maximum torque rating of the terminal studs on the DC power supply is 58 lb-in. (6.5 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.

NOTE: For information about connecting to DC power sources, see the SRX5800 Firewall Hardware Documentation at www.juniper.net/documentation/.

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

NOTE: For information about connecting to external DC power sources, see the SRX5800 Firewall Hardware Documentation at www.juniper.net/documentation/.

6. Switch on the external circuit breakers to provide voltage to the DC power source cable leads.

Proceed to "[Step 7: Perform the Initial Software Configuration](#)" on page 24.

Step 7: Perform the Initial Software Configuration

IN THIS SECTION

- [Enter Configuration Mode | 25](#)
- [Configure User Accounts and Passwords | 25](#)
- [Configure System Attributes | 26](#)
- [Commit the Configuration | 27](#)

This procedure connects the firewall to the network but does not enable it to forward traffic. For complete information about enabling the firewall to forward traffic, including examples, see the appropriate Junos operating system (Junos OS) configuration guides at www.juniper.net/techpubs/.

To configure the software:

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-4/2/0 unit 0 family inet address address/prefix-length
admin@# set interfaces ge-4/3/5 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-4/3/5
admin@# set security zones security-zone untrust interfaces ge-4/2/0
```

7. Configure basic security policies.

```
[edit]
admin@# set security policies from-zone trust to-zone untrust policy policy-name match source-
address any destination-address any application any
admin@# set security policies from-zone trust to-zone untrust policy policy-name then permit
```

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 SRX5800 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 metalically 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 metalically 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 *SRX5800 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 *SRX5800 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 *SRX5800 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.

注意

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

06/77263

SRX5800 Firewall Compliance Statements for EMC Requirements

IN THIS SECTION

- [Canada | 33](#)
- [European Community | 33](#)
- [Japan | 33](#)
- [United States | 34](#)

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 might cause radio interference in which case the user might be required to take adequate measures.

Japan

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

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.

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. Copyright © 2023 Juniper Networks, Inc. All rights reserved.