Overview

Features

The Cisco Secure Firewall 3100 is a standalone modular security services platform that includes the Secure Firewall 3105, 3110, 3120, 3130, and 3140.

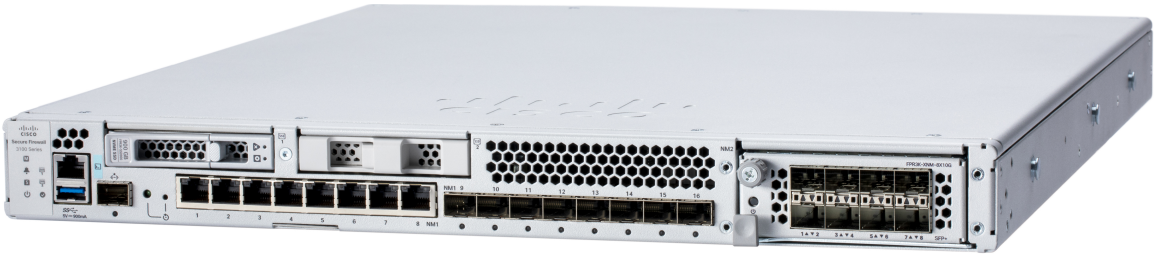
See Product ID Numbers, on page 35 for a list of the product IDs (PIDs) associated with the 3100 series.

The Secure Firewall 3100 supports Cisco Firepower Threat Defense and Cisco ASA software. See the Cisco Secure Firewall Threat Defense Compatibility Guide and the Cisco Secure Firewall ASA Compatibility guide, which provide Cisco software and hardware compatibility, including operating system and hosting environment requirements, for each supported version.

Note The Secure Firewall 3105 is first supported in Cisco Firepower Threat Defense 7.3 and Cisco ASA 9.19 and later.

The following figure shows the Secure Firewall 3100.

Figure 1: Secure Firewall 3100



The following table lists the features for the Secure Firewall 3100.

Table 1: Secure Firewall 3100 Features

Feature	3105	3110	3120	3130	3140
Form factor	1 RU Fits a standard 19-inch (48.3-cm) square-hole rack				
Rack mount	(Optional) Two 2-post mount brackets and/or two slide rails 4-post Electronic Industries Association (EIA)-310-D rack **Note** We recommend that you order the slide rails for your Secure Firewall 3100.				
Airflow	Front to rear (I/O side to non-I/O side) Cold aisle to hot aisle				
Processor	AMD 7272		AMD 7282	AMD 7352	AMD 7452
Core count	12		16	24	32
Core clock	2.9 GHz		2.8 GHz	2.3 GHz	2.35 GHz
System memory	2 x 32 GB		2 x 64 GB	4 x 32 GB	4 x 64 GB
Management port	One 1/10-Gb small form-factor pluggable (SFP) port				
Console port	One RJ-45 serial port				
USB port	USB 3.1 Type A (900 mA) port				
Network ports	8 SFP+ fixed ports and 8 copper RJ-45 ports Named Ethernet 1/1 through 1/16				

Feature	3105	3110	3120	3130	3140
Network module ports	Eight 1/10/25-Gb SFP ports Four 40-Gb QSFP ports				
Network module slots	One **Note** Hot-swapping of identical modules is supported, but if you replace a network module with another type, you must reboot the system so that the new network module is recognized.				
Network modules	• 8-port 1Gb/10Gb SFP+ (FPR3K-XNM-8X10G) • 6-port 1-Gb SFP SX multimode hardware bypass (FPR3K-XNM-6X1SXF) • 6-port 10-Gb SFP SR multimode hardware bypass (FPR3K-XNM-6X10SRF) • 6-port 10-Gb SFP LR single mode hardware bypass (FPR3K-XNM-6X10LRF) • 8-port 10/100/1000Base-T hardware bypass (FPR3K-XNM-8X1GF)			• 8-port 1Gb/10Gb/25Gb SFP+ (FPR3K-XNM-8X25G) • 8-port 1Gb/10Gb SFP+ (FPR3K-XNM-8X10G) • 4-port 40-Gb QSFP+ (FPR3K-XNM-4X40G) • 6-port 1-Gb SFP SX multimode hardware bypass(FPR3K-XNM-6X1SXF) • 6-port 10-Gb SFP SR multimode hardware bypass (FPR3K-XNM-6X10SRF) • 6-port 10-Gb SFP LR single mode hardware bypass (FPR3K-XNM-6X10LRF) • 6-port 25-Gb SFP SR multimode hardware bypass (FPR3K-XNM-6X25SRF) • 6-port 25-Gb SFP LR single mode hardware bypass (FPR3K-XNM-6X25LRF) • 8-port 10/100/1000Base-T hardware bypass (FPR3K-XNM-8X1GF) • 2-port 100-Gb QSFP+ (FPR3K-XNM-2X1000G)	
AC power supply	Two power supply slots Ships with one 400-W AC power supply module Hot-swappable			Two power supply slots Ships with two 400-W AC power supply modules Hot-swappable	

Feature	3105	3110	3120	3130	3140
DC power supply	Yes (optional) Hot-swappable				
Redundant power	No **Note** Yes, if you order an extra power supply.			Yes **Note** Ships with two power supplies.	
Fans	Two dual fan module slots (3 + 1) **Note** The dual fan modules are hot-swappable.				
Storage	Two Nonvolatile Memory Express (NVMe) SSD slots Ships with one 900-GB SSD installed in slot 1. You can order a second RAID1 SSD for slot 2. The RAID1 SSD is preconfigured for RAID1. **Note** Slot 2 is reserved for the optional software RAID1 configuration. **Note** Hot-swapping is supported with 2 SSDs. However, you must enter a CLI command to remove one disk from the RAID before hot swapping. See the CLI configuration guide for your software for the procedure.				
Pullout asset card	Displays the serial number and a QR code that points to the low touch provisioning (LTP) guide.				
Grounding lug	On rear panel				
Power switch	On rear panel				
Reset button	Resets the system to factory default without requiring serial console access **Note** The reset button is recessed. Press with a pin and hold longer than 5 seconds to set the system back to the factory default.				

Deployment Options

Here are some examples of how you can deploy the Secure Firewall 3100:

- As a firewall:
  - At the enterprise internet edge in a redundant configuration
  - At branch offices in either a high availability pair or standalone
  - At data centers in a high availability pair or clustered, which serves the needs of smaller enterprises
- As a device that provides additional application control, URL filtering, or IPS/threat-centered capabilities:
  - Behind an enterprise internet edge firewall in an inline configuration or as a standalone (requires hardware fail-open network module support)

- Deployed passively off a SPAN port on a switch or a tap on a network, or standalone

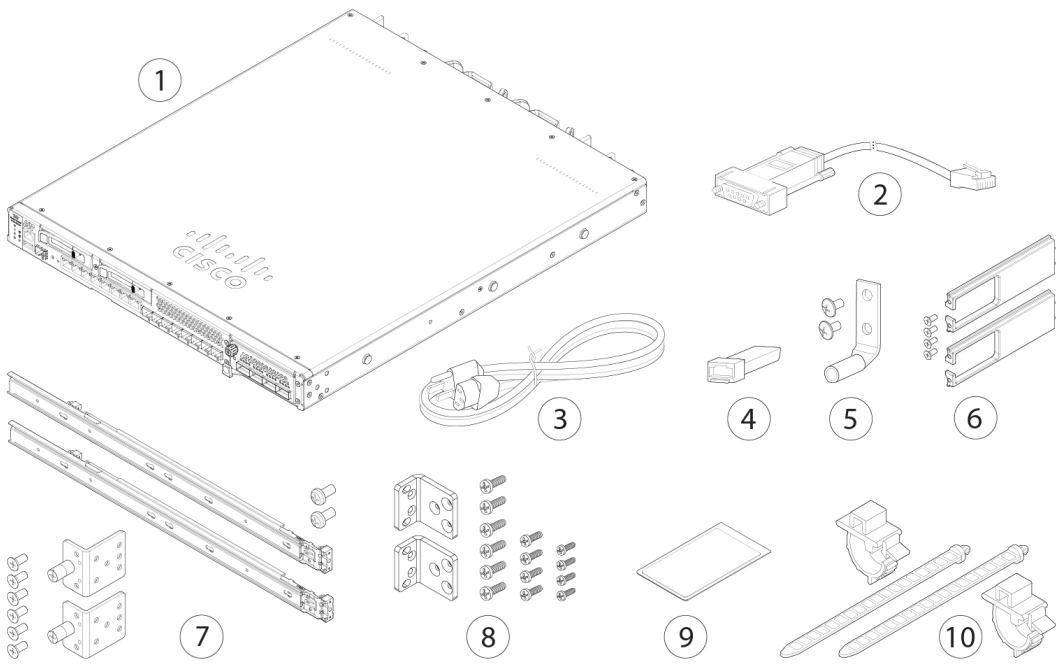
- As a branch native SD-WAN solution that offers remote deployment and is managed over a 4G LTE
- As a VPN device:
  - For remote access VPN
  - For site-to-site VPN

Package Contents

The following figure shows the package contents for the Secure Firewall 3100. The contents are subject to change and your exact contents contain additional or fewer items depending on whether you order the optional parts. See Product ID Numbers for a list of PIDs associated with the package contents.

Note There are two sets of four screws that you can use to secure the chassis to your rack. Chose the screws that fit your rack.

Figure 2: Secure Firewall 3100 Package Contents



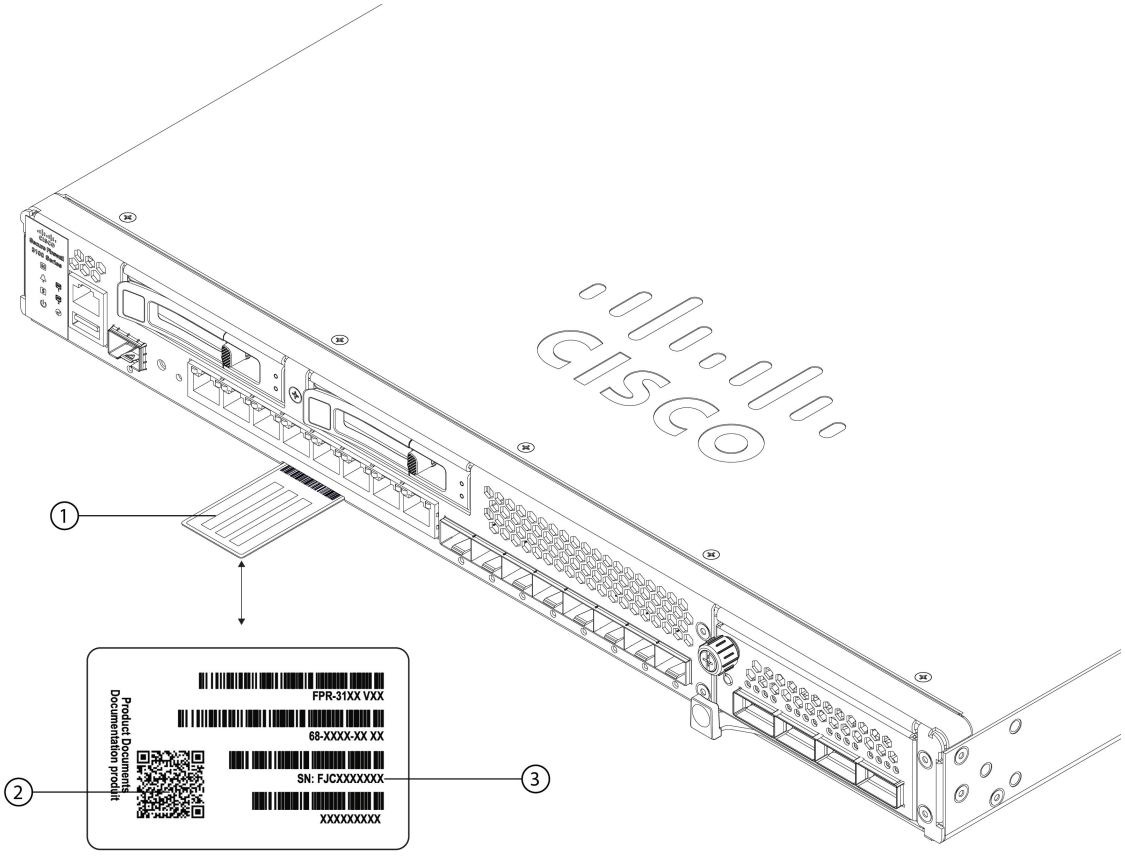
1	Secure Firewall 3100 chassis	**2**	Console cable RJ-45 to DB-9 (part number 72-3383-01)

3	One or two power cords (country-specific) See Power Cord Specifications, on page 37 for a list of supported power cords.	**4**	SFP transceiver (Optional; in package if ordered)
5	One ground lug kit (part number 69-100359-01) • One #6 AWG, 90 degree, #10 post ground lug (part number 32-0608-01) • Two 10-32 x 0.38-inch Phillips screws (part number 48-0700-01)	**6**	Cable management bracket kit (part number 69-100376-01) • Two cable management brackets (part number 700-128334-01) • Four 8-32 x 0.375-inch Phillips screws (part number 48-2696-01) (Optional; in package if ordered)
7	Two slide rails (800-110033-01) Slide rail accessories kit (53-101509-02): • Two slide rail locking brackets (part number 700-121935-01) • Six 8-32 x 0.302-inch slide rail locking bracket Phillips screws (part number 48-102184-01) • Two M3 x 0.5 x 6-mm Phillips screws (part number 48-101144-01) (Optional; in package if ordered)	**8**	Rack-mount bracket kit (53-101510-02): • Two rack-mount brackets (700-127244-01) • Six 8-32 x 0.375-inch Phillips screws (part number 48-2286) for securing the brackets to the chassis • Four 10-32 x 0.75-inch Phillips screws (part number 48-0441-01) for securing the chassis to your rack • Four 12-24 x 0.75-inch Phillips screws (part number 48-0440-01) for securing the chassis to your rack (Optional; in package if ordered)
9	*Cisco Secure Firewall 3100* This document has a URL and QR code that point to the Digital Documentation Portal. The portal contains links to the Product Information page, the Hardware Installation Guide, the Regulatory and Safety Information Guide, the Getting Started Guide, and the Easy Deployment Guide.	**10**	Two power supply module tie wraps and clamps (part number 52-100162-01)

Serial Number and Digital Documentation Portal QR Code

The pullout asset card on the front panel of your Secure Firewall 3100 chassis contains the chassis serial number and the Digital Documentation Portal QR code, which points to the getting started guide, the regulatory and compliance guide, the easy deployment guide, and the hardware installation guide.

Figure 3: Pullout Asset Card



1	Pullout asset tag	**2**	Documentation Portal QR code
3	Chassis serial number		—

The compliance label on the bottom of the chassis contains the chassis serial number, regulatory compliance marks, and the Digital Documentation Portal QR code that points to the guides listed above. The following figure shows an example compliance label found on the bottom of the chassis.

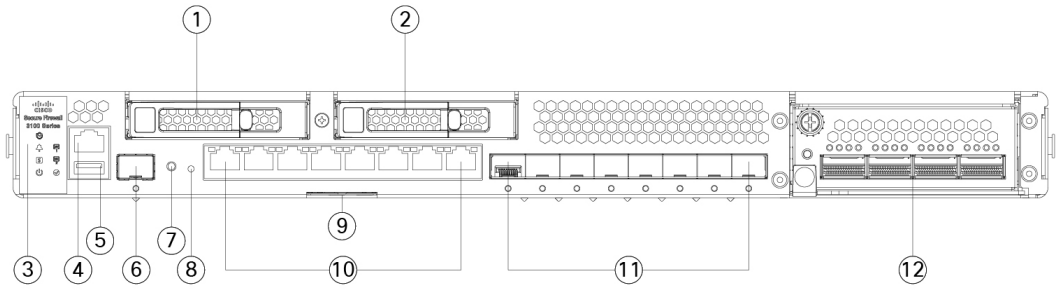
Figure 4: Example Compliance Label

1	Chassis model number	**2**	Chassis serial number
3	Documentation Portal QR code		—

Front Panel

The following figure shows the front panel of the Secure Firewall 3100. See Front Panel LEDs, on page 11 for a description of the LEDs.

Figure 5: Secure Firewall 3100 Front Panel



1	SSD-1	**2**	SSD-2
3	System LEDs	**4**	RJ-45 console port
5	Type A USB 3.1 port	**6**	Gigabit Ethernet management port: • Secure Firewall Threat Defense—Management 0 (also referred to as Management 1/1 and Diagnostic 1/1) • ASA—Management 1/1
7	Reset button LED	**8**	Recessed factory reset button
9	Pullout asset card with chassis serial number, getting started guide QR code, and LTP QR code	**10**	Fixed copper SFP ports (NM-1) Copper SFP ports named Ethernet 1/1 through 1/8 left to right
11	Fixed fiber SFP ports (NM-1) Fiber SFP ports named Ethernet 1/9 through 1/16 left to right	**12**	Network module (NM-2)

Management Port

The Secure Firewall 3100 chassis management port is a 1/10-Gb fiber SFP port.

RJ-45 Console Port

The Secure Firewall 3100 chassis has a standard RJ-45 console port. You can use the CLI to configure your 3100 through the RJ-45 serial console port by using a terminal server or a terminal emulation program on a computer.

The RJ-45 (8P8C) port supports RS-232 signaling to an internal UART controller. The console port does not have any hardware flow control, and does not support a remote dial-in modem. The baud rate is 9600. You can use the standard cable found in your accessory kit to convert the RJ-45 to DB-9 if necessary.

Type A USB 3.1 Port

You can use the external Type A USB port to attach a data-storage device. The external USB drive identifier is `usb:`. The Type A USB port supports the following:

- Hot swapping
- USB drive formatted with FAT32
- Boot kickstart image from ROMMON for discovery recovery purposes
- Copy files to and from workspace:/ and volatile:/ within local-mgmt. The most relevant files are:
  - Core files
  - Ethanalyzer packet captures
  - Tech-support files
  - Security module log files
- Platform bundle image upload using **download image usbA:**

The Type A USB port does *not* support Cisco Secure Package (CSP) image upload support.

Network Ports

The Secure Firewall 3100 chassis has a network module slot that supports the following network modules:

- 8-port 1/10-Gb SFP
- 8-port 1/10/25-Gb SFP
- 6-port 1-Gb SFP SX multimode hardware bypass
- 6-port 10-Gb SFP SR multimode hardware bypass
- 6-port 10-Gb SFP LR single mode hardware bypass
- 6-port 25-Gb SFP SR multimode hardware bypass
- 6-port 25-Gb SFP LR single mode hardware bypass
- 8-port 10/100/1000Base-T hardware bypass; first supported on FTD 7.2.1 and ASA 9.18.2
- 2-port 100-Gb QSFP; first supported on FTD 7.6 and ASA 9.22
- 4-port 40-Gb QSFP; first supported on FTD 7.2.1 and ASA 9.18.2

Note The 4-port 40-Gb and 8-port 25-Gb network modules are supported only on the 3130 and 3140.

Factory Reset Button

The Secure Firewall 3100 chassis has a recessed reset button that resets the system to the factory default. All previous configuration is erased after pressing the button down for five seconds. The following occurs:

- ROMMON NVRAM is cleared and returned to default.
- All extra images are removed; the current running image remains.
- FXOS logs, core files, SSH keys, certificates, FXOS configuration, and Apache configuration are removed.

Note If power is lost between when you pushed the reset button and when the reset process is complete, the process stops and you have to push the button again after the system powers back on.

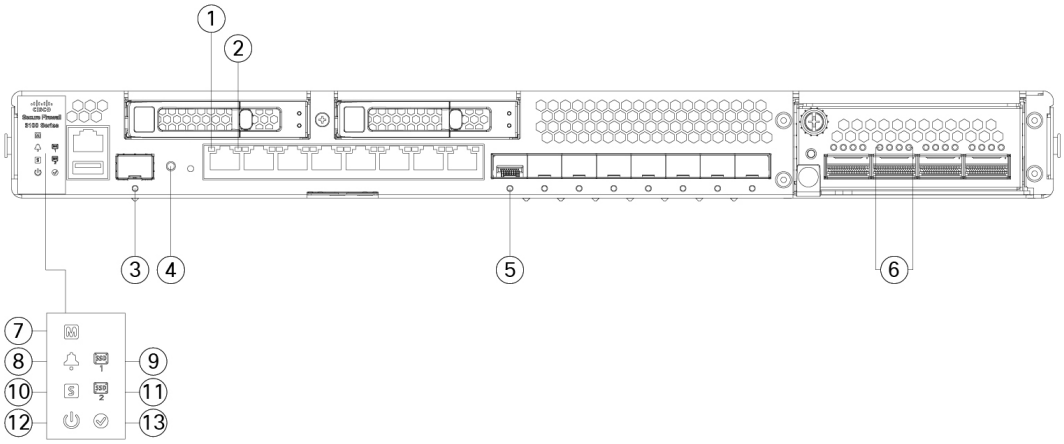
For More Information

- See Remove and Replace the SSD for the procedure for removing a replacing the SSD.
- See Install, Remove, and Replace the Network Module for the procedure for installing network modules.
- See 8-Port 1/10/25-Gb Network Module, on page 15 for more information about the network module.
- See 6-Port 1-Gb SX/10-Gb SR/10-Gb LR/25-Gb SR/25-Gb LR Network Module with Hardware Bypass , on page 22 for more information about the network module.
- See 8-Port 10/100/1000Base-T Network Module with Hardware Bypass, on page 20 for more information about the network module.
- See 4-Port 40-Gb Network Module, on page 16 for more information about the network module.

Front Panel LEDs

The following figure shows the Secure Firewall 3100 front panel LEDs.

Figure 6: Secure Firewall 3100 Front Panel LEDs



1	**RJ-45 Copper Port Link Status** • Off—No link. • Green—Link is up.	2	**RJ-45 Copper Port Activity Status** • Off—No activity • Green, flashing—The number of flashes determines the link speed; 1 flash=10 Mb, 2=100 Mb, 3=1 Gb.

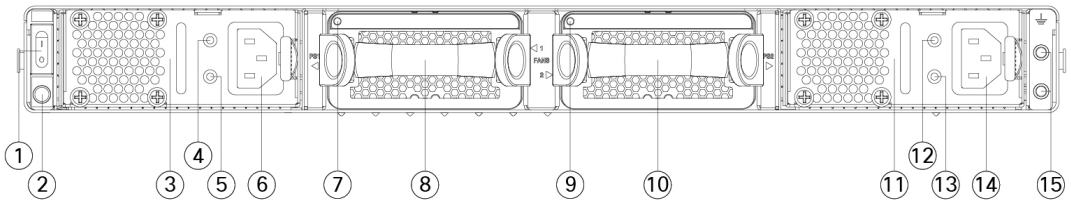
3	**Management Port Status** The 1/10-Gb fiber management port has a bicolor LED under the SFP cage that indicates link/activity/fault: • Off—No SFP. • Green—Link up. • Green, flashing—Network activity. • Amber—SFP present, but no link.	4	**Factory Reset Button Status** • Green, flashing—Flashes 5 seconds after you depress the button. • Off—Reset is complete.
5	**Fiber Port Link/Activity Status** Each fiber port has one dual color LED under the SFP cage. • Off—No SFP. • Green—Link up. • Green, flashing—Network activity at >1G is detected. • Amber—No link or network failure.	6	**Network Module 2 Port Status** • Green—Port is enabled, the link partner is detected. • Amber—Port is enabled, but the link partner is not detected. • Green, flashing—Port is enabled; network activity is detected.
7	**Managed Status** • Green, flashing slowly (twice in 5 seconds)—Cloud is connected. • Green and amber, flashing—Cloud connection failure. • Green—Cloud is disconnected. **Note** See the Easy Deployment Guide for 1000, 2100, or 3100 Series Cisco Secure Firewalls for more information on LTP.	8	**Alarm Status** • Off—No alarms. • Amber—Environmental error. • Green—Status is ok.
9	**SSD 1 Status** • Off—The SSD is not present. • Green—The SSD is present; no activity. • Green, flashing—The SSD is active. • Amber—The SSD has a problem or failure.	10	**System Status** • Off—System has not booted up yet. • Green, flashing quickly—System is booting up. • Green—Normal system function. • Amber—System boot up has failed. • Amber, flashing—Alarm condition, system needs service or attention and may not boot properly.

11	**SSD 2 Status** • Off—The SSD is not present. • Green—The SSD is present; no activity. • Green, flashing—The SSD is active. • Amber—The SSD has a problem or failure.	**12**	**Power Status** • Off—Input power is not detected. If the AC power cord is plugged in, and the LED on the power supply is blinking green, standby power is still on. • Green, flashing—The system has detected a power switch toggle event, and initiated the shutdown sequence. If the power switch is in the OFF position, the system powers off after shutdown is completed. Do not remove the AC or DC power source while this LED is blinking so that the system has time to perform a graceful shutdown. • Amber—The system is powering up (before the BIOS boots). This takes one to five seconds at most. • Green—The system is fully powered up.
13	**Activity Status** (Role of a high-availability pair) • Off—The unit is not configured or enabled in a high-availability pair. • Green—The unit is in active mode. • Amber—The unit is in standby mode.		—

Rear Panel

The following figure shows the rear panel of the Secure Firewall 3100.

Figure 7: Secure Firewall 3100 Rear Panel



1	Power on/off switch	**2**	Power LED below **Note** This power LED has the same behavior as the front panel LED. See Front Panel LEDs, on page 11 for more information.

3	Power supply module 1	**4**	Power supply module 1 FAIL LED
5	Power supply module 1 OK LED	**6**	Power supply module 1 connector
7	Dual Fan Module 1 LED	**8**	Dual fan module 1
9	Dual Fan Module 2 LED	**10**	Dual fan module 2
11	Power supply module 2	**12**	Power supply module 2 FAIL LED
13	Power supply module 2 OK LED	**14**	Power supply module 2 connector
15	Two-post grounding pad **Note** The two-post grounding lug and two screws are included in the accessory kit.		—

Power Switch

The power switch is located to the left of power supply module 1 on the rear of the chassis. It is a toggle switch that controls power to the system. If the power switch is off but the power cord is plugged in and the power supply is flashing green, the system is in standby position, and only the 3.3-V standby power is enabled from the power supply module. The 12-V main power is OFF. When the switch is in the ON position, the 12-V main power is turned on and the system boots.

Before you move the power switch to the OFF position, use the **shutdown** commands so that the system can perform a graceful shutdown. This may take several minutes to complete. After the graceful shutdown is complete, the console displays `It is safe to power off now.` Wait until the front panel PWR LED flashes momentarily and is off before removing AC power.

See Front Panel LEDs, on page 11 for the PWR LED description. See the FXOS Configuration Guide for more information on using the **shutdown** commands.

Caution If you remove the system power cords before the graceful shutdown is complete, disk corruption can occur. You can move the power switch to OFF before the shutdown. The system ignores it.

Note After removing power from the chassis by unplugging the power cord, wait at least 10 seconds before turning power back ON. You want to keep the system power off, including the standby power, for 10 seconds.

For More Information

- See Remove and Replace the Power Supply Module for the procedure for removing and replacing the power supply module in the Secure Firewall 3100.
- See Remove and Replace the Dual Fan Module for the procedure for removing and replacing the dual fan module in the Secure Firewall 3100.
- See Ground the Chassis for the procedure for using the grounding lug to ground the chassis.
- See Power Supply Module, on page 25 for a description of the power supply module LEDs.

- See Dual Fan Modules, on page 27 for a description of the fan LEDs.

8-Port 1/10/25-Gb Network Module

The Secure Firewall 3100 chassis has one network module slot named NM-2. Network modules are optional, removable I/O modules that provide either additional ports or different interface types. The network module plugs into the chassis on the front panel. See Front Panel for the location of the network module slot on the chassis.

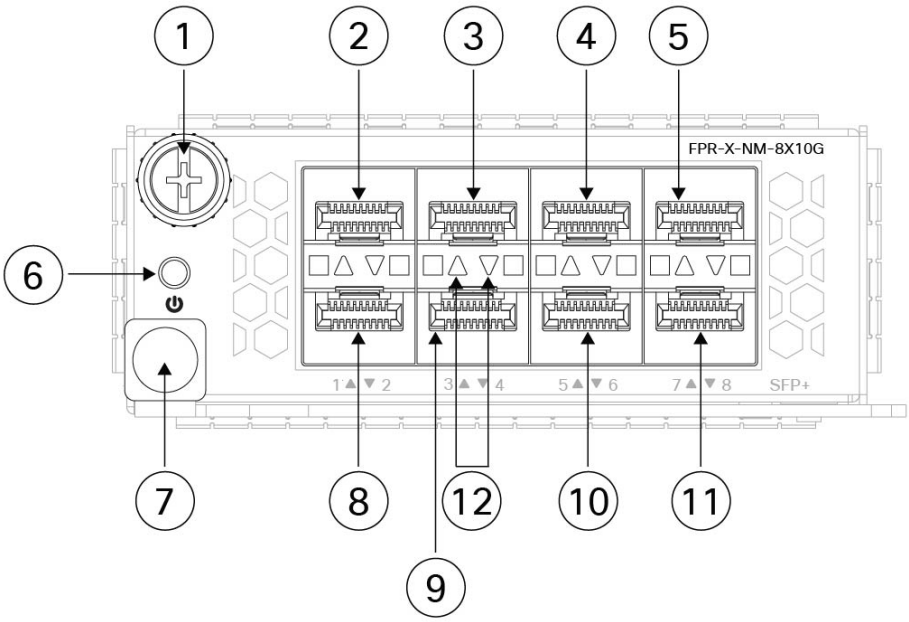
FPR-X-NM-8X10G supports 1 Gb and 10 Gb full-duplex Ethernet traffic per port and is supported on all Secure Firewall 3100s. FPR-X-NM-8X25G supports 1 Gb, 10 Gb, or 25 Gb full-duplex Ethernet traffic per port and is supported *only* on the 3130 and 3140.

The top ports are numbered from left to right—Ethernet 2/1, Ethernet 2/3, Ethernet 2/5, and Ethernet 2/7. The bottom ports are numbered from left to right—Ethernet 2/2, Ethernet 2/4, Ethernet 2/6, and Ethernet 2/8 (see the figure below). Up arrows are the top ports and down arrows are the bottom ports (see the figure below). This network module supports SFP/SFP+/SFP28 transceivers. See Supported SFP/SFP+/QSFP+ Transceivers , on page 30 for the list of Cisco-supported transceivers.

Note The hardware and the system support hot swapping if you are replacing a network module with the same type of network module. You must first disable the network port and then reenable it after replacement. If you replace the 8-port 1/10/25-Gb network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration guide for your operating system for the detailed procedures for managing network modules.

The following figure shows the front panel of the 1/10-Gb and 1/10/25-Gb network module.

Figure 8: 8-Port 1/10-Gb (FPR-X-NM-8X10G) and 8-Port 1/10/25-Gb (FPR-X-NM-8X25G) Network Module



1	Captive screw	**2**	Ethernet 2/1
3	Ethernet 2/3	**4**	Ethernet 2/5
5	Ethernet 2/7	**6**	Power on LED
7	Ejector handle	**8**	Ethernet 2/2
9	Ethernet 2/4	**10**	Ethernet 2/6
11	Ethernet 2/8	**12**	Network activity LEDs The up arrows represent the top ports and the down arrows represent the bottom ports. • Off—No SFP. • Amber—No link or network failure. • Green—Link up. • Green, flashing—Network activity.

For More Information

- See 4-Port 40-Gb Network Module, on page 16 for a description of the 40-Gb network module.
- See 6-Port 1-Gb SX/10-Gb SR/10-Gb LR/25-Gb SR/25-Gb LR Network Module with Hardware Bypass , on page 22 for a description of the 1/10/25-Gb network module.
- See 8-Port 10/100/1000Base-T Network Module with Hardware Bypass, on page 20 for a description of the 10/100/1000Base-T network module.
- See Install, Remove, and Replace the Network Module for the procedure for removing and replacing network modules.

4-Port 40-Gb Network Module

The Secure Firewall 3100 chassis has one network module slot named NM-2. Network modules are optional, removable I/O modules that provide either additional ports or different interface types. The network module plugs into the chassis on the front panel. See Front Panel, on page 8 for the location of the network module slot on the chassis.

The FPR-X-NM-4X40G supports 40-Gb operation and is supported on the 3130 and 3140. This network module provides full-duplex Ethernet traffic per port. The 40-Gb network module has four QSFP+ ports. The 40-Gb ports are numbered left to right, Ethernet 2/1 through Ethernet 2/4. See Supported SFP/SFP+/QSFP+ Transceivers , on page 30 for the list of Cisco-supported transceivers.

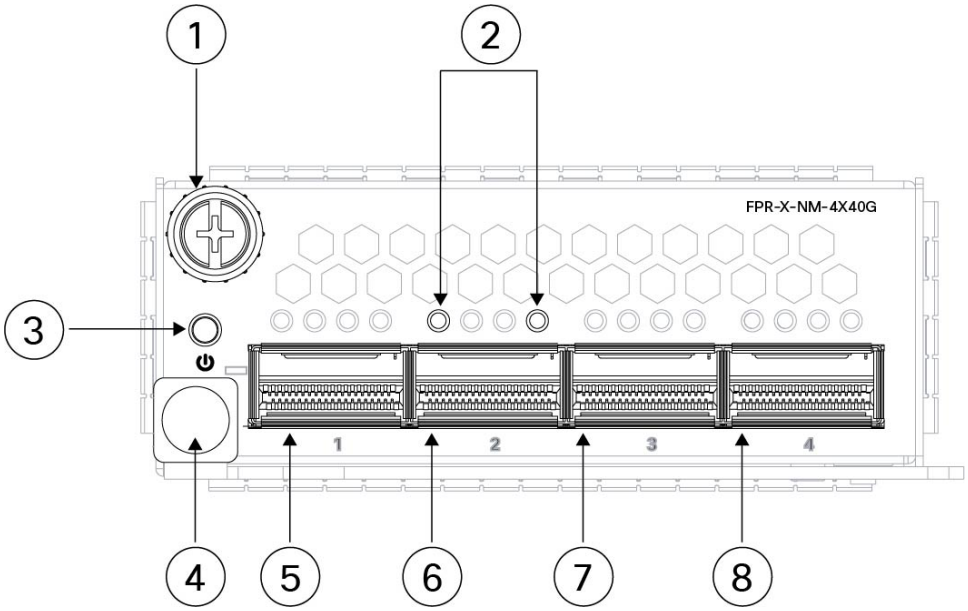
Starting with FTD 7.2 and ASA 7.18.1, you can break each of the four 40-Gb ports into four 10-Gb ports using the supported breakout cables (see Supported SFP/SFP+/QSFP+ Transceivers , on page 30 for a list of the breakout cables). With the four-port 40-Gb network module, you now have 16 10-Gb interfaces. The added interfaces are Ethernet 2/1/1 through Ethernet 2/1/4.

Note The hardware and the system support hot swapping if you are replacing a network module with the same type of network module. If you replace the 4-port 40-Gb network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration guide for your operating system for the detailed procedures for managing network modules.

Note Although you can install the 4-port 40-Gb network in the Secure Firewall 3105, 3110, and 3120, the software does not recognize it because it is not supported.

The following figure shows the front panel of the 4-port 40-Gb network module.

Figure 9: 4-Port 40-Gb Network Module (FPR-X-NM-4X40G)



1	Captive screw	**2**	Network activity LEDs The up arrows represent the top ports and the down arrows represent the bottom ports. • Off—No SFP. • Amber—No link or a network failure. • Green—Link is up. • Green, flashing—Network activity.
3	Power on LED	**4**	Ejector handle
5	Ethernet 2/1	**6**	Ethernet 2/2
7	Ethernet 2/3	**8**	Ethernet 2/4

For More Information

- See 8-Port 1/10/25-Gb Network Module, on page 15 for a description of the 1/10/25-Gb network module.
- See 6-Port 1-Gb SX/10-Gb SR/10-Gb LR/25-Gb SR/25-Gb LR Network Module with Hardware Bypass , on page 22 for a description of the 1/10/25-Gb network module.
- See 8-Port 10/100/1000Base-T Network Module with Hardware Bypass, on page 20 for a description of the 1-Gb network module.
- See Install, Remove, and Replace the Network Module for the procedure for removing and replacing network modules.

2-Port 100-Gb Network Module

The Secure Firewall 3100 chassis has one network module slot named NM-2. Network modules are optional, removable I/O modules that provide either additional ports or different interface types. The network module plugs into the chassis on the front panel. See Front Panel, on page 8 for the location of the network module slot on the chassis.

The FPR-X-NM-2X100G supports 40/100-Gb operation and is supported on the 3130 and 3140. This network module has two QSFP/QSFP28 ports and provides full-duplex Ethernet traffic per port. The maximum bandwidth supported is 200 Gb full duplex, where each port operates at 100 Gb. The 100-Gb ports are numbered left to right, Ethernet 2/1 through Ethernet 2/2. See Supported SFP/SFP+/QSFP+ Transceivers , on page 30 for the list of Cisco-supported transceivers.

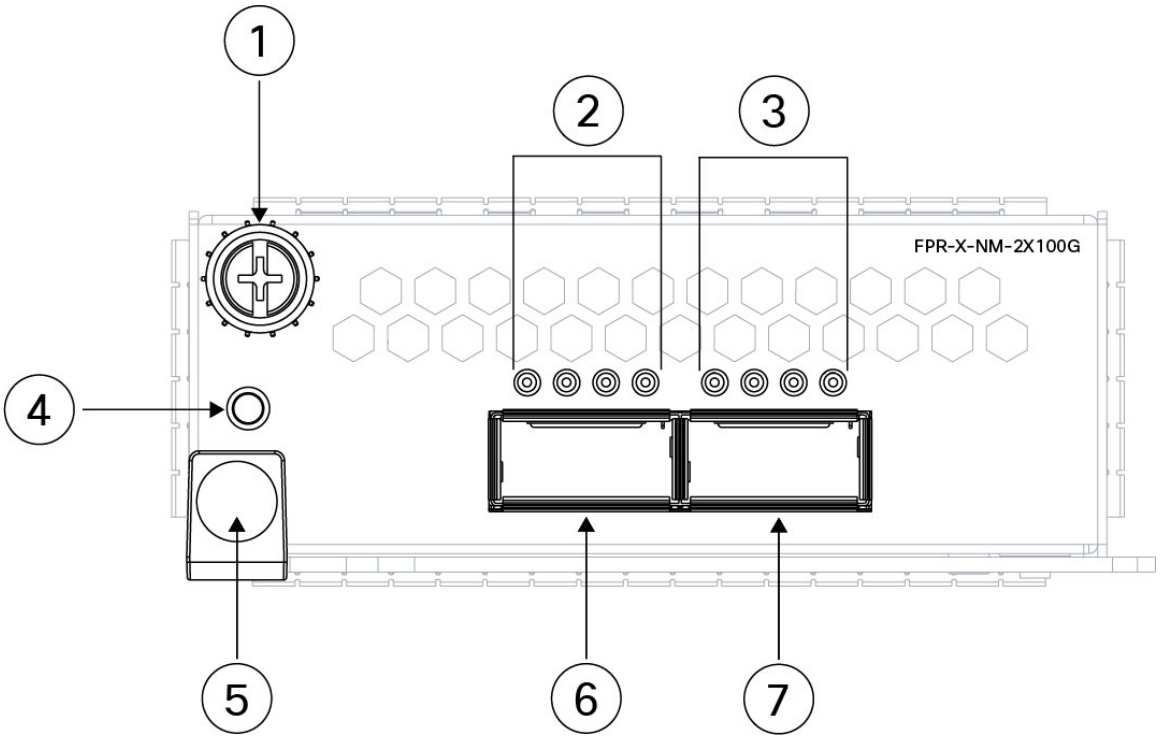
The network module has two 100-Gb ports named E2/1 and E2/2. You can break each 100-Gb port into four 10-Gb or four 25-Gb ports using the supported breakout cables. For E2/1 the new interfaces are named E2/1/1, E2/1/2, E2/1/3 and E2/1/4. For E2/2 the new interfaces are named E2/1/2, E2/2/2, E2/2/3, and E2/2/4.

Note The hardware and the system support hot swapping if you are replacing a network module with the same type of network module. If you replace the 100-Gb network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration guide for your operating system for the detailed procedures for managing network modules.

Note Although you can install the 2-port 100-Gb network module in the Secure Firewall 3105, 3110, and 3120, the software does not recognize it because it is not supported.

The following figure shows the front panel of the 2-port 100-Gb network module.

Figure 10: 2-Port 100-Gb Network Module (FPR-X-NM-2X100G)



1	Captive screw	**2**	Network activity LEDs • Off—No SFP. • Amber—No link or a network failure. • Green—Link is up. • Green, flashing—Network activity.
3	Network activity LEDs • Off—No SFP. • Amber—No link or a network failure. • Green—Link is up. • Green, flashing—Network activity.	**4**	Power on LED
5	Ejector handle	**6**	Ethernet 2/1
7	Ethernet 2/2		—

For More Information

- See 8-Port 1/10/25-Gb Network Module, on page 15 for a description of the 1/10/25-Gb network module.

- See 6-Port 1-Gb SX/10-Gb SR/10-Gb LR/25-Gb SR/25-Gb LR Network Module with Hardware Bypass , on page 22 for a description of the 1/10/25-Gb network module.
- See 8-Port 10/100/1000Base-T Network Module with Hardware Bypass, on page 20 for a description of the 1-Gb network module.
- See Install, Remove, and Replace the Network Module for the procedure for removing and replacing network modules.

8-Port 10/100/1000Base-T Network Module with Hardware Bypass

The Secure Firewall 3100 chassis has one network module slot named NM-2. Network modules are optional, removable I/O modules that provide either additional ports or different interface types. The network module plugs into the chassis on the front panel. See Front Panel, on page 8 for the location of the network module slot on the chassis.

FPR3K-XNM-8X1GF is an 8-port 10/100/1000Base-T hardware bypass network module. The eight ports are numbered from top to bottom, left to right. Ports 1 and 2, 3 and 4, 5 and 6, and 7 and 8 are paired for hardware bypass mode. In hardware bypass mode, data is not processed by the Secure Firewall 3100 but is routed to the paired port.

Hardware bypass (also known as fail-to-wire) is a physical layer (Layer 1) bypass that allows paired interfaces to go into bypass mode so that the hardware forwards packets between these port pairs without software intervention. Hardware bypass provides network connectivity when there are software or hardware failures. Hardware bypass is useful on ports where the secure firewall is only monitoring or logging traffic. The hardware bypass network modules have a switch that is capable of connecting the two ports when needed.

Note Hardware bypass is only supported with threat defense, although you can use these modules in nonbypass mode in threat defense or ASA.

Hardware bypass is supported only on a fixed set of ports. You can pair Port 1 with Port 2, Port 3 with Port 4, but you cannot pair Port 1 with Port 4 for example.

When the appliance switches from normal operation to hardware bypass or from hardware bypass back to normal operation, traffic may be interrupted for several seconds. A number of factors can affect the length of the interruption; for example, behavior of the link partner such as how it handles link faults and debounce timing; spanning tree protocol convergence; dynamic routing protocol convergence; and so on. During this time, you may experience dropped connections.

Note If you have an inline interface set with a mix of hardware bypass and nonhardware bypass interfaces, you cannot enable hardware bypass on this inline interface set. You can only enable hardware bypass on an inline interface set if all the pairs in the inline set are valid hardware bypass pairs.

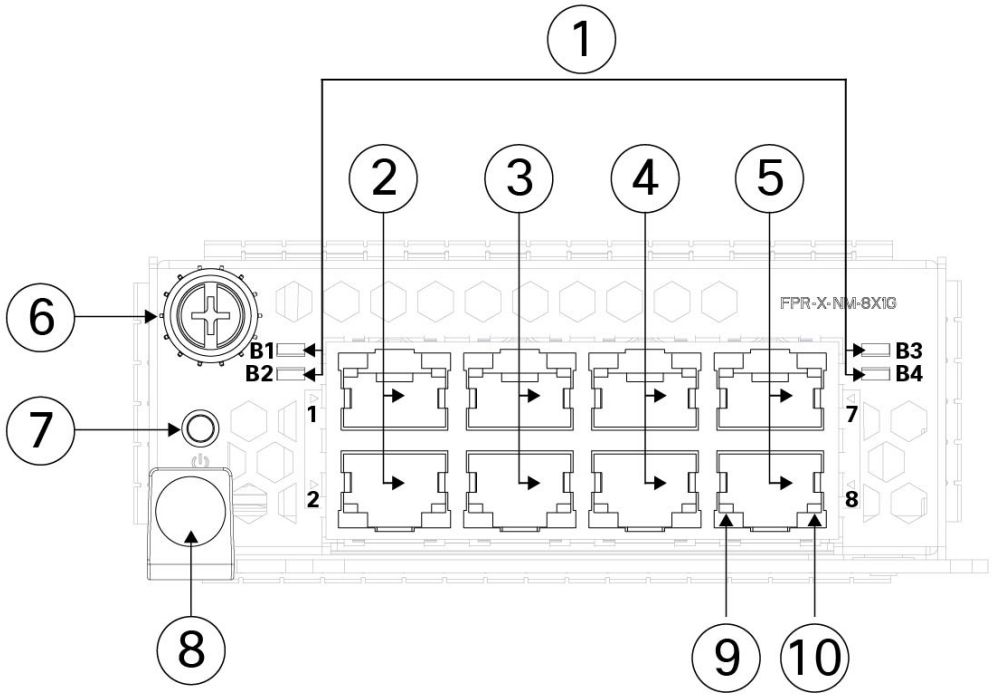
Note The 8-port 10/100/1000Base-T network module is supported beginning with FTD 7.2.3 and ASA 9.18.2.

The hardware and the system support hot swapping if you are replacing a network module with the same type of network module. If you replace the 8-port 10/100/1000Base-T network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration guide for your operating system for the detailed procedures for managing network modules.

Make sure you have the correct firmware package and software version installed to support this network module. See the configuration guide for your software for the procedures for updating the firmware package and verifying the software version. See the Cisco Secure Firewall Threat Defense Compatibility Guide and the Cisco Secure Firewall ASA Compatibility guide, which provide Cisco software and hardware compatibility, including operating system and hosting environment requirements, for each supported version.

The following figure shows the front panel of the 8-port 10/100/1000Base-Tnetwork module.

8-Port 10/100/1000Base-T Network Module



1	Bypass LEDs B1 through B4 • Green—In standby mode. • Amber, flashing—Port is in hardware bypass mode, failure event.	**2**	Ethernet 2/1 and Ethernet 2/2 Ports 1 and 2 are paired together to form a hardware bypass pair. LED B1 applies to this paired port.

3	Ethernet 2/3 and Ethernet 2/4 Ports 3 and 4 are paired together to form a hardware bypass pair. LED B2 applies to this paired port.	**4**	Ethernet 2/5 and Ethernet 2/6 Ports 5 and 6 are paired together to form a hardware bypass pair. LED B3 applies to this paired port.
5	Ethernet 2/7 and Ethernet 2/8 Ports 7 and 8 are paired together to form a hardware bypass pair. LED B4 applies to this paired port.	**6**	Captive screw
7	Power LED	**8**	Handle
9	Left Port LED • Unlit—No connection or port is not in use. • Green—Link up. • Green, flashing—Network activity.	**10**	Right Port LED • Unlit—No connection or port is not in use. • Green—Link up. • Green, flashing—Network activity.

For More Information

- See 6-Port 1-Gb SX/10-Gb SR/10-Gb LR/25-Gb SR/25-Gb LR Network Module with Hardware Bypass , on page 22 for a description of the 1/10/25-Gb network module.
- See 4-Port 40-Gb Network Module, on page 16 for a description of the 40-Gb network module.
- See 8-Port 1/10/25-Gb Network Module, on page 15 for a description of the 1/10/25-Gb network module.
- See Install, Remove, and Replace the Network Module for the procedure for removing and replacing network modules.

6-Port 1-Gb SX/10-Gb SR/10-Gb LR/25-Gb SR/25-Gb LR Network Module with Hardware Bypass

The Secure Firewall 3100 chassis has one network module slot named NM-2. Network modules are optional, removable I/O modules that provide either additional ports or different interface types. The network module plugs into the chassis on the front panel. See Front Panel, on page 8 for the location of the network module slot on the chassis.

The FPR-X-NM-6X1SXF, FPR-X-NM-6X10SRF, FPR-X-NM-6X10LRF, FPR-X-NM-6X25SRF, and FPR-X-NM-6X25LRF hardware bypass network modules have six ports that are numbered from top to bottom, left to right. Pair ports 1 and 2, 3 and 4, and 5 and 6 to form hardware bypass paired sets. In hardware bypass mode, data is not processed by the Secure Firewall 3100 but is routed to the paired port. This network module has built-in SFP transceivers. Hot swapping and field replacement of transceivers are not supported.

Hardware bypass (also known as fail-to-wire) is a physical layer (Layer 1) bypass that allows paired interfaces to go into bypass mode so that the hardware forwards packets between these port pairs without software intervention. Hardware bypass provides network connectivity when there are software or hardware failures. Hardware bypass is useful on ports where the secure firewall is only monitoring or logging traffic. The

hardware bypass network modules have a switch that is capable of connecting the two ports when needed. This hardware bypass network module has built-in SFPs.

Note Hardware bypass is only supported with threat defense, although you can use these modules in nonbypass mode in threat defense or ASA.

Hardware bypass is supported only on a fixed set of ports. You can pair Port 1 with Port 2, Port 3 with Port 4, but you cannot pair Port 1 with Port 4 for example.

Note When the appliance switches from normal operation to hardware bypass or from hardware bypass back to normal operation, traffic may be interrupted for several seconds. A number of factors can affect the length of the interruption; for example, behavior of the link partner such as how it handles link faults and debounce timing; spanning tree protocol convergence; dynamic routing protocol convergence; and so on. During this time, you may experience dropped connections.

Note If you have an inline interface set with a mix of hardware bypass and nonhardware bypass interfaces, you cannot enable hardware bypass on this inline interface set. You can only enable hardware bypass on an inline interface set if all the pairs in the inline set are valid hardware bypass pairs.

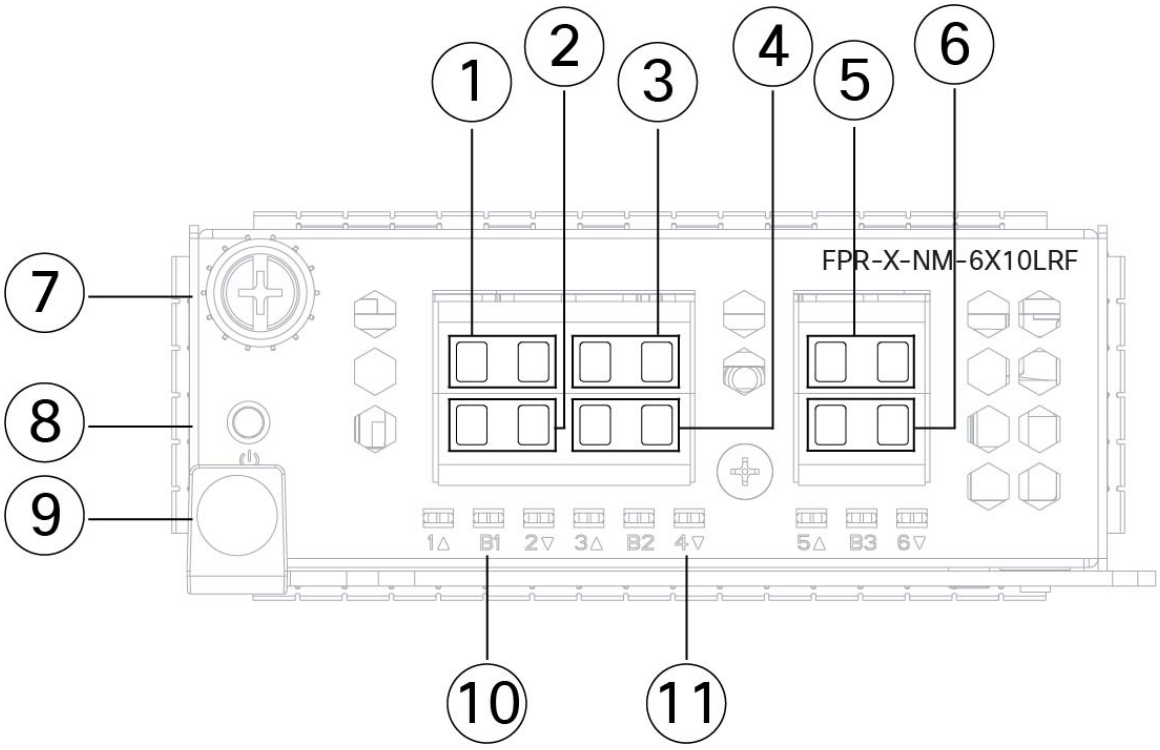
Note The 6-port 1-Gb SX/10-Gb SR/10-Gb LR/25-Gb SR/25-Gb LR network module is supported beginning with FTD 7.2.3 and ASA 9.18.2.

Note The hardware and the system support hot swapping if you are replacing a network module with the same type of network module. If you replace the 6-port 1/10/25-Gb network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration guide for your operating system for the detailed procedures for managing network modules.

Note Make sure you have the correct firmware package and software version installed to support this network module. See the configuration guide for your software for the procedure to verify your firmware package and software version. See the Cisco Secure Firewall Threat Defense Compatibility Guide and the Cisco Secure Firewall ASA Compatibility guide, which provide Cisco software and hardware compatibility, including operating system and hosting environment requirements, for each supported version

The following figure shows the front panel of the 6-port 1/10/25-Gb network module.

Figure 11: 6-Port 1/10/25-Gb Network Module (FPR-X-NM-6X1SXF, FPR-X-NM-6X10SRF, FPR-X-NM-6X10LRF, FPR-X-NM-6X25SRF, and FPR-X-NM-6X25LRF)



1	Port 1 Ethernet 2/1 Ports 1 and 2 are paired together to form a hardware bypass pair.	**2**	Port 2 Ethernet 2/2 Ports 1 and 2 are paired together to form a hardware bypass pair.
3	Port 3 Ethernet 2/3 Ports 3 and 4 are paired together to form a hardware bypass pair.	**4**	Port 4 Ethernet 2/4 Ports 3 and 4 are paired together to form a hardware bypass pair.
5	Port 5 Ethernet 2/5 Ports 5 and 6 are paired together to form a hardware bypass pair.	**6**	Port 6 Ethernet 2/6 Ports 5 and 6 are paired together to form a hardware bypass pair.
7	Captive screw	**8**	Power LED

9	Handle ejector	**10**	Bypass LEDs B1 through B3: • Off—Bypass mode is disabled. • Green—Port is in standby mode. • Amber, flashing—Port is in hardware bypass mode, failure event.
11	Six network activity LEDs: • Amber—No connection, or port is not in use, or no link or network failure. • Green—Link up, no network activity. • Green, flashing—Network activity.		—

For More Information

- See 8-Port 10/100/1000Base-T Network Module with Hardware Bypass, on page 20 for a description of the 1-Gb network module.
- See 8-Port 1/10/25-Gb Network Module, on page 15 for a description of the 1/10/25-Gb network module.
- See 4-Port 40-Gb Network Module, on page 16 for a description of the 40-Gb network module.
- See Install, Remove, and Replace the Network Module for the procedure for removing and replacing network modules.

Power Supply Module

See Product ID Numbers, on page 35 for a list of the PIDs associated with the Secure Firewall 3100 power supply modules.

Note You *cannot* mix AC and DC power supply modules in the chassis.

Note After removing power from the chassis by unplugging the power cord, wait at least 10 seconds before turning power back ON. You want to keep the system power off, including the standby power, for 10 seconds.

Attention Make sure that one power supply module is always active.

Note The system power requirements are lower than the power supply module capabilities. See the following table.

AC Power Supply

The dual power supplies can supply up to 800-W power across the input voltage range. The load is shared when both power supply modules are plugged in and running at the same time.

Note The system does not consume more than the capacity of one power supply module, so it always operate in full redundancy mode when two power supply modules are installed.

Table 2: AC Power Supply Module Hardware Specifications

Input voltage	100 to 240 VAC
Maximum input current	<3 A at 200 VAC <6 A at 100 VAC
Maximum output power	400 W
Frequency	50 to 60 Hz
Efficiency	85% at 50% load
Redundancy	1+1 redundancy with dual power supply modules

DC Power Supply

The power supplies can supply up to 800 W power across the input voltage range. The load is shared when both power supply modules are plugged in and running at the same time.

Note The system does not consume more than the capacity of one power supply module, so it always operate in full redundancy mode when two power supply modules are installed.

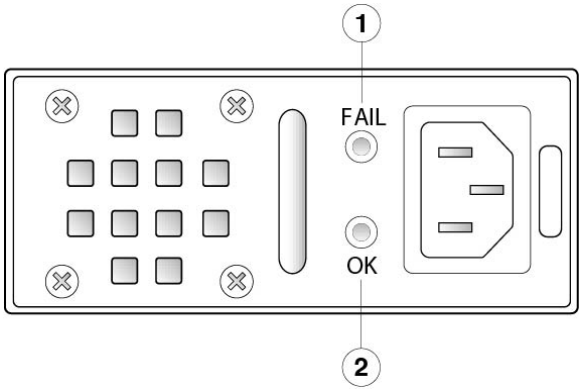
Table 3: DC Power Supply Module Hardware Specifications

Input voltage	-48 to -60 VDC
Maximum input current	< 15 A at -48 V
Redundancy	1+1 redundancy with dual power supply modules
Efficiency	> 88% at 50% load

Power Supply Module LEDs

The following figure shows the bicolor power supply LEDs on the power supply module. The figure shows the AC power supply module. The DC power supply module has the same LEDs.

Figure 12: Power Supply Module LEDs



1	**Amber FAIL LED** Fail LED Status: • Off—No fault detected. • Amber, flashing—Fault warning, power supply may still work but could fail due to high temperature, failing fan, or over current. • Amber—Fault detected; power supply not working properly. Includes over voltage, over current, over temperature, and fan failure.	2	**Green OK LED** OK LED Status: • Off—Input power not present. • Green, flashing—Input power present, but system is not powered up (power switch is off). • Green—The power supply module is enabled and running.

For More Information

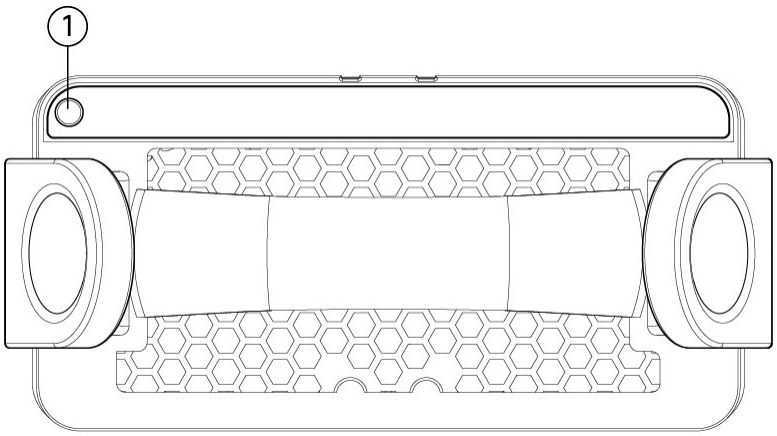
- See Remove and Replace the Power Supply Module for the procedure for removing and replacing the power supply module in the Secure Firewall 3100.

Dual Fan Modules

The Secure Firewall 3100 has two fan modules that provide 3 + 1 redundancy. Each fan module has two fans and each fan has two independent fan rotors. The fan rotors are monitored individually, and this gives 8 fan rotors per system. When one fan rotor fails, all others spin at maximum speed so that the system continues to function. The dual fan modules are hot-swappable and installed in the rear of the chassis.

The following figure shows the location of the fan LED on the fan module.

Figure 13: Fan LED



1	Two-color LED

The fan module has one two-color LED, which is located on the upper left corner of the fan.

- Off—The environmental subsystem is not active yet.
- Green—Fan running normally. It may take up to one minute for the LED status to turn green after power is on.
- Amber—One fan has failed. The system can continue to operate normally, but fan service is required.
- Amber, flashing—Two or more fans have failed. Immediate attention is required.

For More Information

- See Product ID Numbers, on page 35 for a list of the PIDs associated with the Secure Firewall 3100 fans.
- See Remove and Replace the Dual Fan Module for the procedure for removing and replacing the dual fan modules.

SSDs

The Secure Firewall 3100 has two SSD slots that each hold one NVMe 900-GB SSD. By default the Secure Firewall 3100 ships with one 900-GB SSD installed in slot 1. The second SSD slot is reserved for software RAID1. The RAID1 SSD is shipped already configured. If you have two SSDs installed, they form a RAID when you boot up.

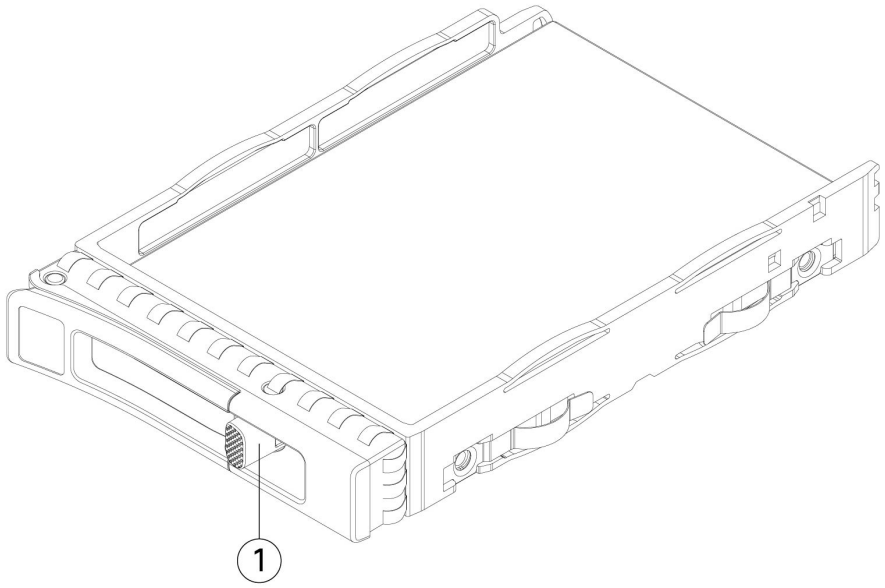
Hot swapping is supported. With two SSDs, you can swap SSD-1 without powering off the chassis. However, you must issue the **raid remove-secure local disk** command to remove SSD-2 from the RAID configuration before hot swapping. Otherwise, you can lose data. If you remove and replace the RAID1 SSD, you must add it again to the RAID1 configuration using the **raid add local-disk 1|2** command. The SSD drive identifiers are `disk0:` and `disk1:`.

Caution If you have only one SSD, you cannot remove it while the firewall is powered on.

Caution You cannot swap SSDs between different platforms. For example, you cannot use a 2100 series SSD in a 3100 series model. If you are swapping SSDs between two Secure Firewall 3100s, use the **remove-secure local disk** command, otherwise sometimes the SED (self-encrypting drive) gets locked. If you get an error message that the SED is locked, you can enter the PSID and the system clears the SED and creates a new set of keys. To avoid this situation, especially if you do not know what the PSIDs are, always use the **remove-secure local disk** when removing SSDs. See Hot Swap an SSD on the Secure Firewall 3100/4200 for the procedures for safely removing an SSD.

See Product ID Numbers, on page 35 for a list of the PIDs associated with the Secure Firewall 3100 SSDs.

Figure 14: SSD



1	SSD release tab		—

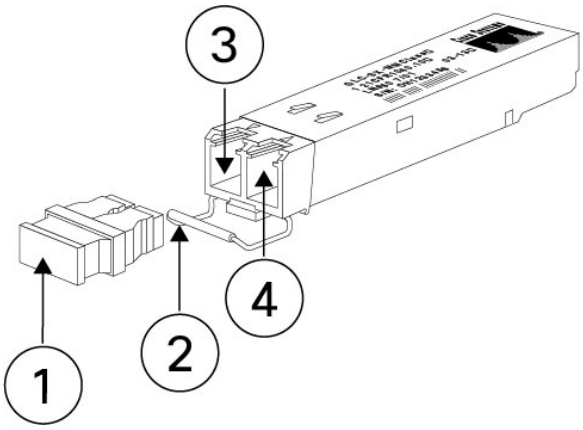
For More Information

- See Front Panel LEDs, on page 11 for the location and description of the SSD LEDs on the front panel.
- See Remove and Replace the SSD for the procedure for removing and replacing the SSD.
- See the configuration guide for your software for the procedures for removing and adding an SSD from the RAID1 configuration.

Supported SFP/SFP+/QSFP+ Transceivers

The SFP/SFP+/QSFP+ transceiver is a bidirectional device with a transmitter and receiver in the same physical package. It is a hot-swappable optical or electrical (copper) interface that plugs into the SFP/SFP+/QSFP+ ports on the fixed ports and the network module ports, and provides Ethernet connectivity.

Figure 15: SFP Transceiver



1	Dust plug	**2**	Bail clasp
3	Receive optical bore	**4**	Transmit optical bore

Safety Warnings

Take note of the following warnings:

Warning **Statement 1055—**Class 1/1M Laser

Invisible laser radiation is present. Do not expose to users of telescopic optics. This applies to Class 1/1M laser products.

Warning **Statement 1056—**Unterminated Fiber Cable

Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view directly with optical instruments. Viewing the laser output with certain optical instruments, for example, eye loupes, magnifiers, and microscopes, within a distance of 100 mm, may pose an eye hazard.

Warning **Statement 1057—**Hazardous Radiation Exposure

Use of controls, adjustments, or performance of procedures other than those specified may result in hazardous radiation exposure.

Warning Use appropriate ESD procedures when inserting the transceiver. Avoid touching the contacts at the rear, and keep the contacts and ports free of dust and dirt. Keep unused transceivers in the ESD packing that they were shipped in.

Caution Although non-Cisco SFPs are allowed, we do not recommend using them because they have not been tested and validated by Cisco. Cisco TAC may refuse support for any interoperability problems that result from using an untested third-party SFP transceiver.

The following table lists the supported transceivers for the fixed ports on all 3100 models, and the FPR3K-XNM-8X10G and FPR3K-XNM-8X25G network modules.

Table 4: Supported 1-Gb SFP Transceivers

Optics Type	PID	Comments
1G, 1000Base-T	GLC-TE	1 Gb-copper SFP
1G multimode	GLC-SX-MMD	850 nm
1G single mode	GLC-LH-SMD	1310 nm
1G SM extended r.	GLC-EX-SMD	40 km
1G SM	GLC-ZX-SMD	80 km

The following table lists the supported transceivers for the fixed ports on all 3100 models and the FPR3K-XNM-8X10G and FPR3K-XNM-8X25G network modules.

Table 5: Supported 10-Gb SFP Transceivers

Optics Type	PID	Comments
10G-SR	SFP-10G-SR	—
10G-SR	SFP-10G-SR-S	Ethernet only
10G-LR	SFP-10G-LR	—
10G-LR	SFP-10G-LR-S	Ethernet only
10G-ER	SFP-10G-ER	—
10G-ER	SFP-10G-ER-S	—

Optics Type	PID	Comments
10G-ZR	SFP-10G-ZR	—
10G-T-X	SFP-10G-T-X	—
10G-ZR	SFP-10G-ZR-S	—
10G DAC copper	SFP-H10GB-CUxM	Length 1, 1.5, 2, 2.5, 3, 4, 5 m **Note** You must set the link partner transmit strength to 400mV or greater.
10G DAC CU active	SFP-H10GB-ACUxM	Length 7, 10 m
10G AOC	SFP-10G-AOCxM	Length 1, 2, 3, 5, 7, 10 m

The following table lists the supported transceivers for the fixed ports on the Secure Firewall 3130 and 3140, and the FPR3K-XNM-8X25G network module.

Table 6: Supported 25-Gb SFP Transceivers

Optics Type	PID	Comments
25G-SR	SFP-25G-SR-S	—
25G-CSR	SFP-10/25G-CSR-S	Dual rate, longer reach
25G-LR	SFP-10/25G-LR-S	Dual rate
25G DAC copper	SFP-H25G-CUxM	Length 1, 1.5, 2, 2.5, 3, 4, 5 m
25G AOC	SFP-25G-AOCxM	Length 1, 2, 3, 4, 5, 7, 10 m

The following table lists the supported transceivers for the FPR-X-NM-4X40G and FPR-X-NM-2X100G network module.

Table 7: Supported 40-Gb SFP Transceivers for FPR-X-NM-4X40G and FPR-X-NM-2X100G

Optics Type	PID	Comments
40G-SR4	QSFP-40G-SR4	—
40G-SR4-S	QSFP-40G-SR4-S	Ethernet only
40G-CSR4	QSFP-40G-CSR4	300 m with OM3
40G-SR-BD	QSFP-40G-SR-BD	LC connector
40G-LR4-S	QSFP-40G-LR4-S	Ethernet only
40G-LR4	QSFP-40G-LR4	Ethernet and OTU3
40G-LR4L	WSP-Q40GLR4L	LR4 Lite, up to 2 km

Optics Type	PID	Comments
40G-CU	Cisco QSFP-H40G-CUxM	QSFP to QSFP copper direct-attach cables (passive); length 1, 3, 5 m
40G-CU-breakout	QSFP-4SFP10G-CUxM	QSFP to 4xSFP copper direct-attach cables; length 1, 2, 3, 4, 5 m
40G-CU-A	Cisco QSFP-40G-ACUxM	QSFP to QSFP copper direct-attach cables (active); length 7, 10 m
40G-CU-A-breakout	Cisco QSFP-4X10G-ACUxM	QSFP to QSFP copper direct-attach cables (active); length 7, 10 m
40G-AOC	QSFP-H40G-AOCxM	QSFP to QSFP active optical cables; length 1, 2, 3, 5, 7, 10, 15, 30 m
40G-AOC-breakout	QSFP-4X10G-AOCxM	QSFP to 4xSFP active optical cables; length 1, 2, 3, 5, 7, 10 m

The following table lists the supported transceivers for the FPR-X-NM-2X100G network module.

Table 8: Supported 100-Gb QSFP Transceivers for FPR3K-X-NM-2X100G

Optics Type	PID	Comments
100G-SR4	QSFP-100G-SR4-S	100GBASE SR4 QSFP, MPO, 100 m over OM4 MMF
100G-LR4	QSFP-100G-LR4-S	100GBASE LR4 QSFP, LC, 10 km over SMF
40/100G	QSFP-40/100G-SRBD	100 m OM4, LC connector
100G-LR	QSFP-100G-LR-S	Single Mode, 10K m, LC
100G-AOC	QSFP-100G-AOCxM	Multimode up to 30 m (direct attach); length 1, 2, 3, 5, 7, 10,15, 20, 25, 30 m
100G-CR4	QSFP-100G-CUxM	100G copper up to 5 m (direct attach); length 1, 2, 3, 5 m
100G-CR4 breakout	QSFP-4SFP25G-CUxM	100G copper breakout; length 1, 2, 3, 5 m)
100G-FR	QSFP-100G-FR-S	100GBASE FR QSFP transceiver, 2 km over SMF, LC connector
100G-SM-SR	QSFP-100G-SM-SR	Single mode, 2m to 500 m, LC
100G-SR1.2	QSFP-100G-SR1.2	Multimode, SR BiDi, 100 m with OM4, LC

Optics Type	PID	Comments
100G-DR	QSFP-100G-DR-S	100GBASE DR QSFP transceiver, 500 m over SMF, LC connector

Hardware Specifications

The following table contains hardware specifications for the Secure Firewall 3100.

Specification	3105	3110	3120	3130	3140
Chassis dimensions (H x W x D)	1.75 x 17 x 20 inches (4.4 x 43.3 x 50.8 cm)				
Network module dimensions (H x W x D)	1.5 x 3.7 x 10.5 inches (4.39 x 9.4 x 26.67 cm)				
Chassis component weights	Network Module: 1.6 lb (.73 kg) SSD: 0.25 lb (.11 kg) Power supply module: 2 lb (.91 kg) Fan module: 0.5 lb (.23)				
Chassis weight	23 lb (10.5 kg) 1 power supply module, 1 network module, 2 dual fan modules, 1 SSD			25 lb (11.4 kg) 2 power supply modules, 1 network module, 2 dual fan modules, 1 SSD	
System power	100/240 VAC 6 A (at 100 VAC), 50 to 60 Hz				
Temperature	Operating: 32 to 104°F (-0 to 40°C) Nonoperating: -4 to 149°F (-20 to 65°C) maximum altitude is 40,000 ft				
Humidity	Operating: 5 to 85% noncondensing Nonoperating: 5 to 90% noncondensing				
Altitude	Operating: 10,000 ft maximum Nonoperating: 40,000 ft maximum				
Sound pressure	65 dBA @ 77°F (25°C) typical 74 dBA maximum				
Sound power	72 dB (typical) 80 dB (maximum)				

Product ID Numbers

The following table lists the product IDs (PIDs) associated with the Secure Firewall 3100. All of the PIDs in the table are field-replaceable. If you need to get a return material authorization (RMA) for any component, see Cisco Returns Portal for more information.

Note See the **show inventory** command in the Cisco Firepower Threat Defense Command Reference or the Cisco ASA Series Command Reference to display a list of the PIDs for your Secure Firewall 3100.

Table 9: Secure Firewall 3100 PIDs

PID	Description
Chassis	
FPR3105-ASA-K9	Cisco Secure Firewall 3105 ASA chassis 1 RU
FPR3110-ASA-K9	Cisco Secure Firewall 3110 ASA chassis 1 RU
FPR3120-ASA-K9	Cisco Secure Firewall 3120 ASA chassis 1 RU
FPR3130-ASA-K9	Cisco Secure Firewall 3130 ASA chassis 1 RU
FPR3140-ASA-K9	Cisco Secure Firewall 3140 ASA chassis 1 RU
FPR3105-NGFW-K9	Cisco Secure Firewall 3105 next generation firewall chassis 1 RU
FPR3110-NGFW-K9	Cisco Secure Firewall 3110 next generation firewall chassis 1 RU
FPR3120-NGFW-K9	Cisco Secure Firewall 3120 next generation firewall chassis 1 RU
FPR3130-NGFW-K9	Cisco Secure Firewall 3130 next generation firewall chassis 1 RU
FPR3140-NGFW-K9	Cisco Secure Firewall 3140 next generation firewall chassis 1 RU
Accessories	
FPR3K-ACY-KIT	Accessory kit that ships with the chassis
FPR3K-ACY-KIT=	Accessory kit (spare)
FPR3K-PWR-AC-400	400-W AC power supply
FPR3K-PWR-AC-400=	400-W AC power supply (spare)
PWR-CC1-400WDC	400-W DC power supply

PID	Description
PWR-CC1-400WDC=	400-W DC power supply (spare)
FPR3K-PSU-BLANK	Power supply blank slot cover
FPR3K-PSU-BLANK=	Power supply blank slot cover (spare)
FPR3K-SSD900	900 GB SSD
FPR3K-SSD900=	900 GB SSD (spare)
FPR3K-SSD-BLANK	SSD blank slot carrier
FPR3K-SSD-BLANK=	SSD blank slot carrier (spare)
FPR3K-FAN	Dual fan module
FPR3K-FAN=	Dual fan module (spare)
FPR3K-SLIDE-RAILS	Slide rail kit
FPR3K-SLIDE-RAILS=	Slide rail kit (spare)
FPR3K-CBL-MGMT	Cable management brackets
FPR3K-CBL-MGMT=	Cable management brackets (spare)
FPR3K-BRKT	Rack-mount brackets
FPR3K-BRKT=	Rack-mount brackets (spare)
Network Modules	
FPR3K-XNM-6X1SXF	6-port 1-Gb SFP hardware bypass network module, SX multimode
FPR3K-XNM-6X1SXF=	6-port 1-Gb SFP hardware bypass network module, SX multimode (spare)
FPR3K-XNM-6X10SRF	6-port 10-Gb SFP hardware bypass network module, SR multimode
FPR3K-XNM-6X10SRF=	6-port 10-Gb SFP hardware bypass network module, SR multimode (spare)
FPR3K-XNM-6X10LRF	6-port 10-Gb SFP hardware bypass network module, LR single mode
FPR3K-XNM-6X10LRF=	6-port 10-Gb SFP hardware bypass network module, LR single mode (spare))
FPR3K-XNM-6X25SRF	6-port 25-Gb SFP hardware bypass network module, SR multimode

PID	Description
FPR3K-XNM-6X25SRF=	6-port 25-Gb SFP hardware bypass network module, SR multimode (spare)
FPR3K-XNM-6X25LRF	6-port 25-Gb SFP hardware bypass network module, LR single mode
FPR3K-XNM-6X25LRF=	6-port 25-Gb SFP hardware bypass network module, LR single mode (spare)
FPR3K-XNM-8X1GF	8-port 10/100/1000Base-10 hardware bypass network module
FPR3K-XNM-8X1GF=	8-port 10/100/1000Base-10 hardware bypass network module (spare)
FPR3K-XNM-8X10G	8-port 1/10-Gb SFP+ network module
FPR3K-XNM-8X10G=	8-port 1/10-Gb SFP+ network module (spare)
FPR3K-XNM-8X25G	8-port 1/10/25-Gb QSFP network module
FPR3K-XNM-8X25G=	8-port 1/10/25-Gb QSFP network module (spare)
FPR3K-XNM-4X40G	4-port 40-Gb QSFP+ network module
FPR3K-XNM-4X40G=	4-port 40-Gb QSFP+ network module (spare)
FPR3K-X-NM-2X100G	2-port 200-Gb QSFP/QSFP28 network module
FPR3K-X-NM-2X100G=	2-port 200-Gb QSFP/QSFP28 network module (spare)
FPR3K-NM-BLANK	Network module blank slot cover
FPR3K-NM-BLANK=	Network module blank slot cover (spare)

Power Cord Specifications

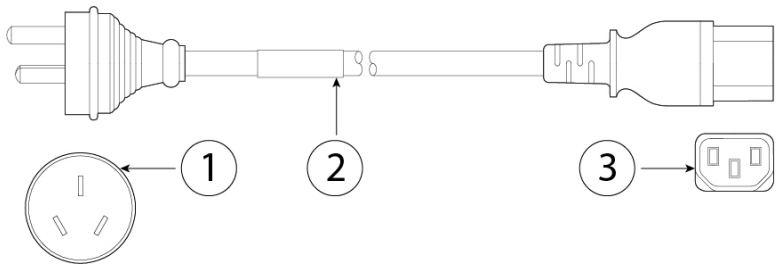
Each power supply has a separate power cord. Standard power cords or jumper power cords are available for connection to the secure firewall. The jumper power cords for use in racks are available as an optional alternative to the standard power cords.

If you do not order the optional power cord with the system, you are responsible for selecting the appropriate power cord for the product. Using a incompatible power cord with this product may result in electrical safety hazard. Orders delivered to Argentina, Brazil, and Japan must have the appropriate power cord ordered with the system.

Note Only the approved power cords or jumper power cords provided with the Secure 3100 are supported.

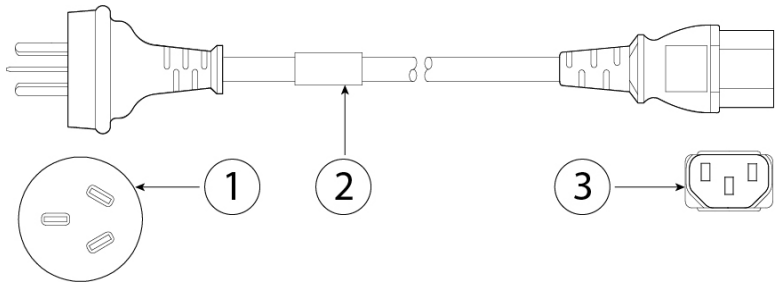
The following power cords are supported.

Figure 16: Argentina (CAB-ACR)



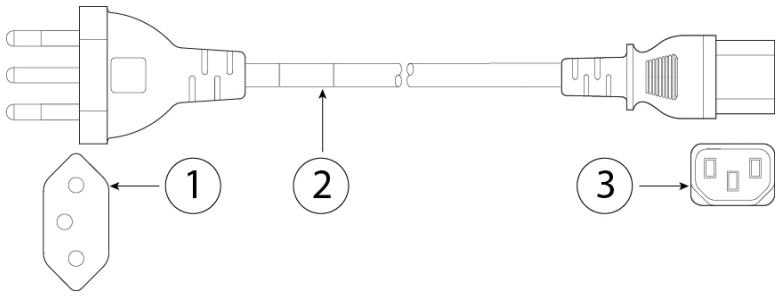
1	Plug: EL 219/IRAM 2073	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

Figure 17: Australia (CAB-ACA)



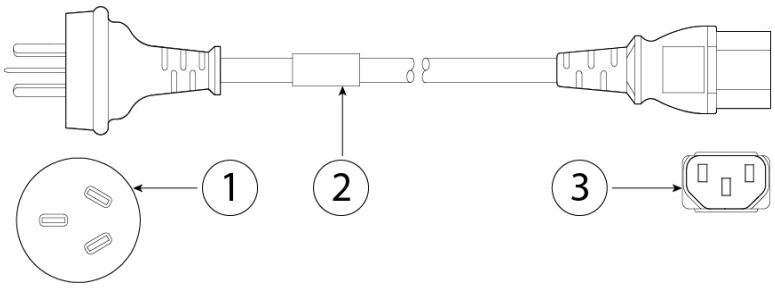
1	Plug: A.S. 3112	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

Figure 18: Brazil (CAB-C13-ACB)



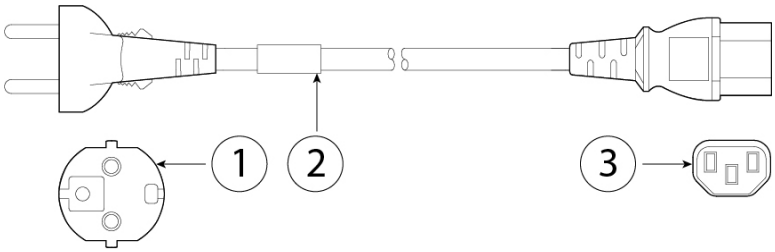
1	Plug: NBR 14136	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.1 m

Figure 19: China (CAB-ACC)



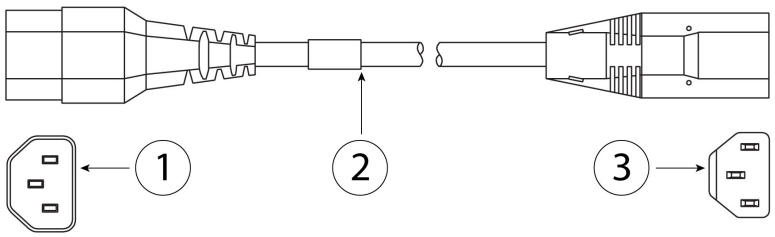
1	Plug: GB2099.1-2008	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

Figure 20: Europe (CAB-ACE)



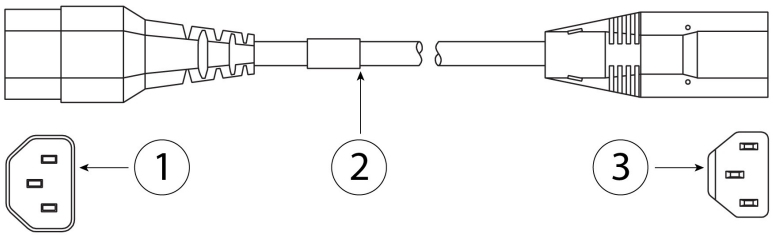
1	Plug: CEE 7 VII	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 1.5 m

Figure 21: India Jumper (CAB-C13-C14-3M-IN)



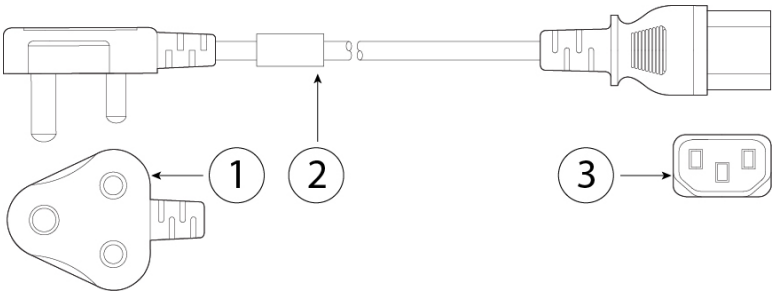
1	IEC 60320/C14G	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 3 m

Figure 22: India Jumper (CAB-C13-C14-IN)



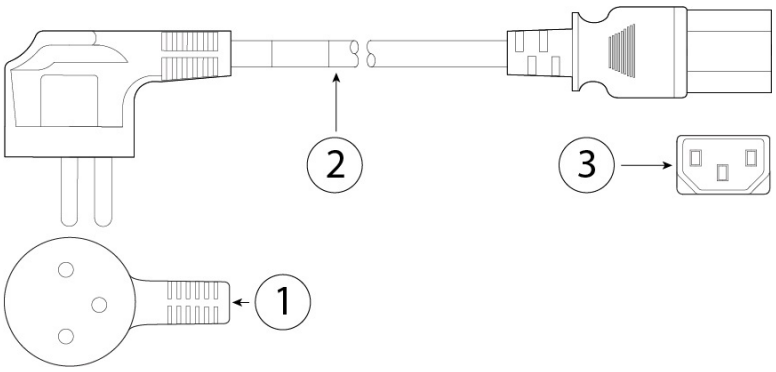
1	IEC 60320/C14G	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 1.4 m

Figure 23: India (PWR-CORD-IND-D)



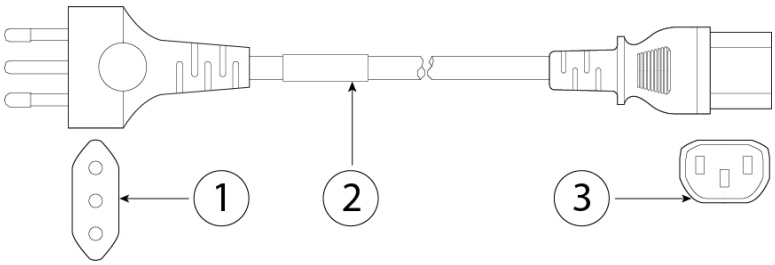
1	Plug: IS 6538-1971	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 1.8 m

Figure 24: Israel (CAB-250V-10A-IS)



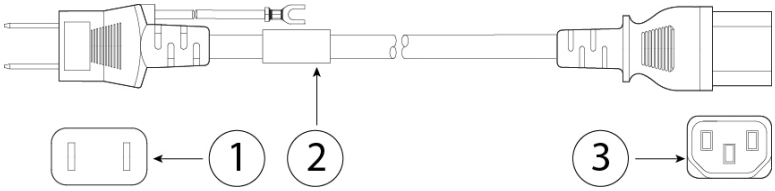
1	Plug: SI-32	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

Figure 25: Italy (CAB-ACI)



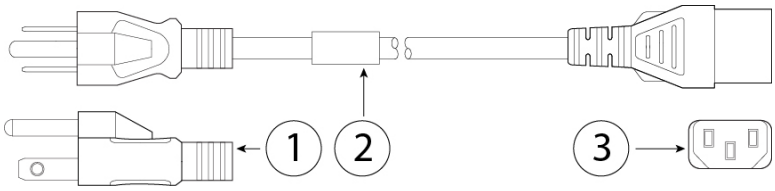
1	Plug: CEI 23-16	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

Figure 26: Japan (CAB-JPN)



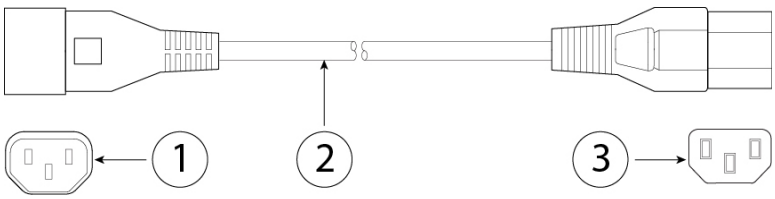
1	Plug: JIS C8303	**2**	Cord set rating: 12 A, 125 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

Figure 27: Japan (CAB-JPN-3PIN)



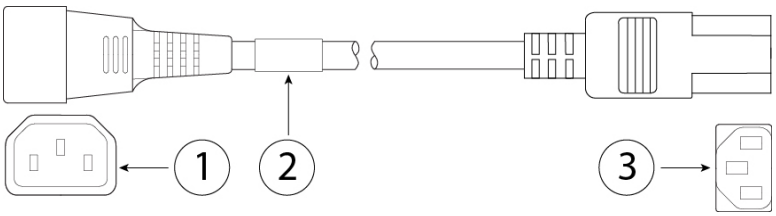
1	Plug: JIS C8303/JIS C8306	**2**	Cord set rating: 12 A, 125 V
3	Connector: IEC 60320/C13		Cord length: 2.3 m

Figure 28: Japan (CAB-C13-C14-2M-JP) PSE Mark



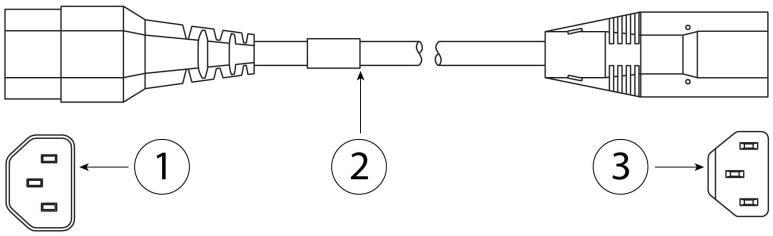
1	IEC 60320-2-2/E	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2 m

Figure 29: Jumper (CAB-C13-C14-2M)



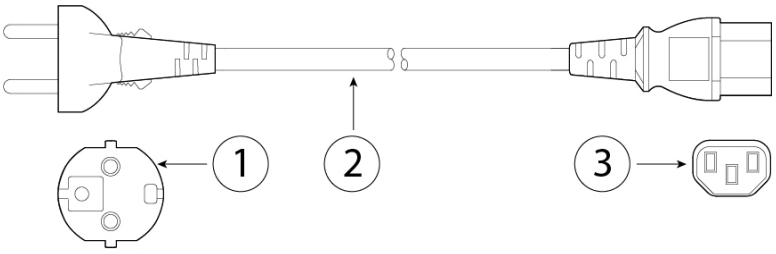
1	IEC 60320/C14G	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

Figure 30: Cabinet Jumper (CAB-C13-CBN)



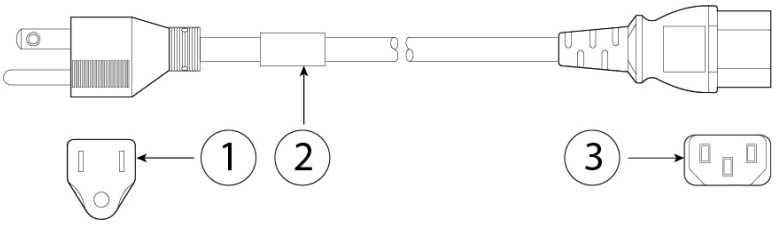
1	IEC 60320-2-2/E	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 0.7 m

Figure 31: Korea (CAB-AC-C13-KOR)



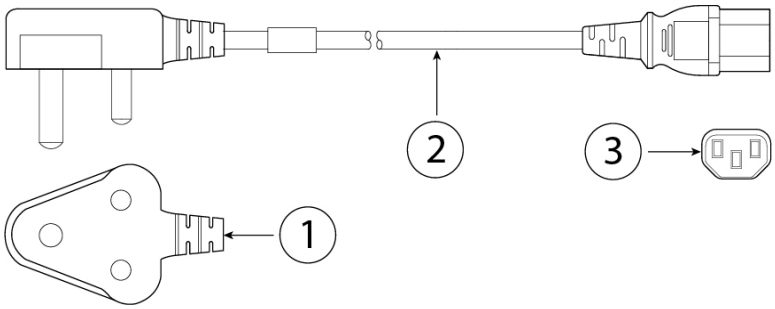
1	Plug: KSC 8305	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 1.8 m

Figure 32: North America (CAB-AC)



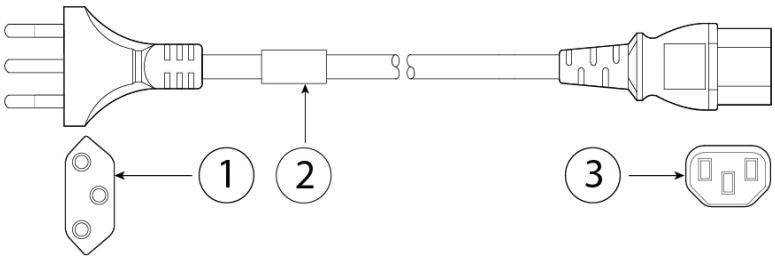
1	Plug: NEMA 5-15P	**2**	Cord set rating: 10 A, 125 V
3	Connector: IEC 60320/C13		Cord length: 2.1 m

Figure 33: South Africa (CAB-ACSA)



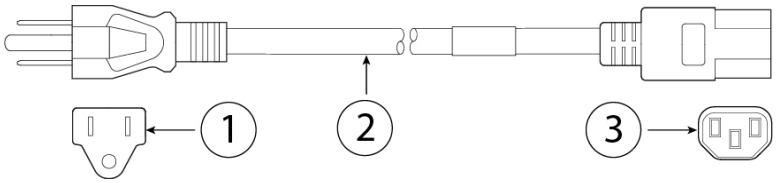
1	Plug: SABS 164/1	**2**	Cord set rating: 16 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 1.8 m

Figure 34: Switzerland (CAB-ACS)



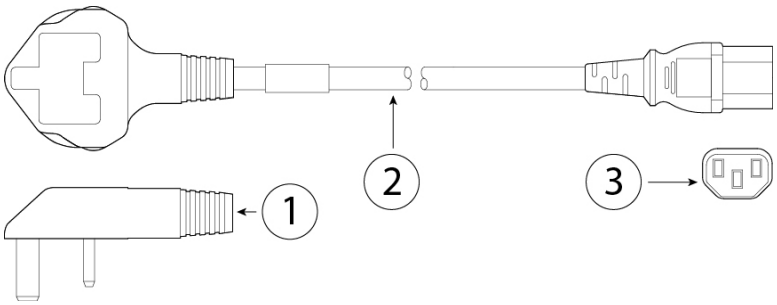
1	Plug: SEV 1011	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

Figure 35: Taiwan (CAB-ACTW)



1	Plug: CNS10917	**2**	Cord set rating: 10 A, 125 V
3	Connector: IEC 60320/C13		Cord length: 2.29 m

Figure 36: United Kingdom (CAB-ACU)



1	Plug: BS1363A/SS145	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m